ISBN 978-9928-210-09-8
ISSN 2413-1334

Konferenca e III-të Shkencore Ndërkombëtare

VËLLIMI I DYTË

# Policimi dhe SIGURIA

## Krimi kompjuterik, kërcënimi kibernetik dhe siguria kombëtare

NËNTOR
2018

PROCEEDINGS
Botim i Akademisë së Sigurisë, Tiranë 2018


**POLICIMI DHE SIGURIA**
AKADEMIA E SIGURISË

KONFERENCA E III-TË NDËRKOMBËTARE

# Krimi kompjuterik, kërcënimi kibernetik dhe siguria kombëtare

PROCEEDINGS

*Vëllimi II*

AKADEMIA E SIGURISË

Në bashkëpunim me :

AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Me mbështetjen e:

OSCE Organizata për Siguri dhe Bashkëpunim në Evropë Prezenca në Shqipëri

Botuar nga Akademia e Sigurisë, Tiranë 2018

**CIP Katalogimi në botim BK Tiranë**

**Akademia e Sigurisë**
Krimi kompjuterik, kërcënimi kibernetik dhe siguria kombëtare : konferenca III-të ndërkombëtare : Tiranë, 2018 : proceedings / Akademia e Sigurisë ; red. Albert Hitoaliaj. – Tiranë : Akademia e Sigurisë, 2018
Vol. 1 ; ...f. ; 16.5cmx24cm.

**ISBN ISBN 978-9928-210-09-8**

1.Policia 2.Siguria kombëtare 3.Kriminologjia 4.Konferenca

351.74 (062)
343 (062)

"POLICIMI DHE SIGURIA"
ISSN 2413-1334
*Viti i III-të i botimit*

NR 13
NËNTOR
2018

# BORDI EDITORIAL



**Redaktor shkencor**
Dr. Albert HITOALIAJ

**Përkthyes**
Dr. Irvin FANIKO

**Punimet grafike**
Andi OSMANI

**Realizimi teknik**
*Qendra e Kërkimeve Shkencore, Akademia e Sigurisë*

AKADEMIA E SIGURISË
**ISBN 978-9928-210-09-8**
**ISSN 2413 - 1334**

KONFERENCA E III-të SHKENCORE NDËRKOMBËTARE
*"Krimi kompjuterik, kërcënimi kibernetik dhe siguria kombëtare"*

## Komiteti shkencor/ Scientific Committee

### Kryetar i Bordit/Chair

**Prof. Dr. Ismet ELEZI**
Kriminolog

### Anëtarët/Members

**Prof. Dr. Xhovani ARCUDI**
*Profesor, Universiteti i Romës "Tor Vergata", Itali*
**Prof. Dr. Vasilika HYSI**
*Kriminologe, ligjvënëse*
**Prof. Dr. Ilirjan MANDRO**
*Dekan i Fakultetit të Sigurisë dhe Hetimit, Akademia e Sigurisë*
**Prof. Dr. Irakli KOÇOLLARI**
*Rektor i Kolegjit të Lartë Universitar "Akademia Profesionale e Biznesit"*
**Prof. Dr. Laura TAFARO**
*Profesor, Universiteti i Barit, Itali*
**Prof. Dr. Kseanela SOTIROFSKI**
*Rektore e Universitetit "Aleksandër Moisiu", Durrës*
**Prof. Dr. Emiljano GIARDINA**
*Profesor, Universiteti i Romës "Tor Vergata", Itali*
**Prof. Dr. Ethem RUKA**
*Rektor i Kolegjit të Lartë Universitar "Luarasi"*
**Gen. (ret.) Volker HELBAUER**
*Kryetar i Këshillit të Kolegjit Universitar ISPE-Kosovë*
**Prof. Asc. Idriz HAXHIAJ**
*Zëvendësshef i Misionit të Shqipërisë në NATO, Bruksel*
**Prof. Asc. Ferdinand ELEZI**
*Prokuroria e Apelit, Durrës - Anëtar*
**Dr. Vilma TOMÇO**
*Drejtoreshë e Përgjithshme e Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike*
**Dr. Bilbil MEMAJ**
*Drejtori/Rektori i Akademisë së Sigurisë*
**Dr. Xhavit SHALA**
*Drejtor i Qendrës së Kërkimeve Shkencore, Akademia e Sigurisë*
**Dr. Sandër LLESHI**
*Këshilltar për Sigurinë, Këshilli i Ministrave*
**Dr. Frank HARRIS**
*MSc, D. Crim. J., University of Portsmouth*
**Z. Ismail SMAKIQI**
*Drejtor i Përgjithshëm i Akademisë së Kosovës për Siguri Publike*
**Dr. Albert HITOALIAJ**
*Redaktor shkencor/Lektor, Akademia e Sigurisë, Tiranë*

AKADEMIA E SIGURISË
**ISBN 978-9928-210-09-8**
**ISSN 2413 - 1334**

KONFERENCA E III-të SHKENCORE NDËRKOMBËTARE
*"Krimi kompjuterik, kërcënimi kibernetik dhe siguria kombëtare"*

## Komiteti organizator/Organizational Committee

### Kryetari/Chair

**Dr. Bilbil MEMAJ,** Drejtori/Rektori i Akademisë së Sigurisë.

### Zëvendëskryetari

**Dr. Xhavit SHALA,** Drejtori i Qendrës së Kërkimeve Shkencore, Akademia e Sigurisë

### Anëtarët/Members

**Prof. Asc. Dr. Sokol SADUSHI,** Drejtor i Shkollës së Magjistraturës
**Z. Brian THIESSEN,** OSCE, Law Enforcement Development Officer Security Cooperation Department
**Prof. Asc. Dr. Elton NOTI,** Zëvendësrektor, Universiteti "Aleksandër Moisiu" Durrës
**Znj. Anna MARINELI,** Team Leader Project "Countering Serious Crime in the Western Balkans", Ministria e Brendshme
**MSc. Arjan MUÇAJ,** Prokuror në Prokurorinë e Përgjithshme, Tiranë
**Prof. Dr. Laura TAFARO,** Profesor, Universiteti i Barit, Itali
**MSc. Edlira BEJKO,** Drejtore drejtorie në Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike
**Magjistër Dr. (Proc.) Armando GURAKUQI,** Prokuror në Prokurorinë pranë Gjykatës së Shkallës së Parë, Tiranë
**Prof. Dr. Emiljano GIARDINA**, Profesor, Universiteti i Romës "Tor Vergata", Itali
**Dr. Bajram IBRAJ,** Ushtrues detyre, Drejtor/Rektor i Kolegjit ISPE
**Prof. Asc. Dr. Gaqo TANKU,** Lektor, Universiteti "Aleksandër Moisiu", Durrës
**Dr. Artur BEU**, Oficer Kontakti i Policisë së Shtetit, Itali
**Z. Giovanni PASQUA**, Ekspert afatgjatë për burimet njerëzore pranë Projektit Pameca V.
**MSc. Dashamir ÇALI,** Shef i sektorit të hetimit të krimeve kompjuterike, departamenti i policisë kriminale në Policinë e Shtetit
**MSc. Bilbil DERVISHI,** Qendra e Kërkimeve Shkencore, Akademia e Sigurisë, Tiranë

### Koordinatorët / Coordination

**MSc. Anisa AGASTRA**, Koordinatore e Përgjithshme, Qendra e Kërkimeve Shkencore, Akademia e Sigurisë
**Dr. Irvin FANIKO**, Koordinator, Qendra e Kërkimeve Shkencore, Akademia e Sigurisë
**MSc. Qetësor GURRA**, Koordinator, Fakulteti i Sigurisë dhe Hetimit, Akademia e Sigurisë

### Redaktor Shkencor

**Dr. Albert HITOALIAJ**, Qendra e Kërkimeve Shkencore, Akademia e Sigurisë.

### Punimet grafike

**MSc. Andi OSMANI**, Qendra e Kërkimeve Shkencore, Akademia e Sigurisë.

*Realizimi teknik:* Qendra e Kërkimeve Shkencore, Akademia e Sigurisë

**AKADEMIA E SIGURISË**

KONFERENCA E III-të SHKENCORE NDËRKOMBËTARE, nëntor 2018, Tiranë

KRIMI KOMPJUTERIK, KËRCËNIMI KIBERNETIK DHE SIGURIA KOMBËTARE

*Në bashkëpunim me:*
Organizatën e Traktatit të Atlantikut të Veriut (NATO),
Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK),
Universitetin Aleksandër Moisiu Durrës (UAMD).

*Me mbështetjen e:*
Organizatës për Siguri dhe Bashkëpunim në Evropë, Prezenca Shqipëri (OSCE),
Misionit PAMECA V,
IPA /2017 Countering Serious Crime in the Western Balkans.

## Përmbajtja

### SESIONI II/SECOND SECTION
Hetime profesionale të krimeve kibernetike



### SESIONI III/THIRD SECTION
Aspekte ligjore, ekonomike e psikosociale
të krimeve kibernetike


AKADEMIA E SIGURISË
1971

**KONFERENCA E III-të SHKENCORE NDËRKOMBËTARE**
**Krimi kompjuterik, kërcënimi kibernetik dhe siguria kombëtare**
*Nëntor 2018, Tiranë*

## Fokusi i konferencës

Vrulli i zhvillimit të komunikimit masiv në hapësirën kibernetike (virtuale), sidomos pas vitit 2000, orienton drejt një problemi të ri që po kërcënon vrullshëm sigurinë kombëtare: lufta kibernetike dhe krimet kompjuterike. Këto krime, si aktivitete kriminale të zhvilluara në rrjeta, kërcënojnë informacionin, shkëmbimin e informacionit, hapësirën kibernetike dhe shoqërinë e sotme njerëzore. Kjo nxit drejt një lufte të re globale virtuale që kërkon rishikim të politikave e masave mbrojtëse. Në ditët e sotme kjo formë e krimit po përhapet vrullshëm në nivel individual, institucional, organizativ, kombëtar e ndërkombëtar. Zhvillimi i madh i teknologjisë dhe internetit ka mundësuar që pjesa më e madhe e aktiviteteve ekonomike, shkencore, sociale, ligjore, hetuese, policore, politike, etj., të mundësohen e të realizohen nëpërmjet kompjuterit dhe komunikimit virtual.

Nga aspekti hetimor, kjo veprimtari kriminale paraqet vështirësi për t'u gjurmuar, hetuar, ndjekur e zbuluar sepse nuk kufizohet nga kufijtë kombëtarë gjeografikë. Gjithashtu këto krime mund të përgatiten nga kudo dhe kundrejt çdo përdoruesi të kompjuterit, kërkojnë resurse të vogla materiale e humane, kryhen në kohë relativisht të shkurtër, me ose pa praninë e autorit në vendin e kryerjes së veprës penale, si dhe aftësimi për përdorim të kompjuterit nuk është i shtrenjtë dhe është i aksesueshëm nëpërmjet rrjetave e programeve kudo në botë. Autorët e këtyre veprave penale gjenden fizikisht në vende të ndryshme, nga ato ku vijnë pasojat e veprimeve të tyre, ndërkohë që legjislacionet vendase përgjithësisht kufizohen brenda territorit vendas. Nga aspekti strategjik, mbrojtja nga kërcënimet e reja të kufijve virtualë dhe rrjeteve e

sistemeve nga mashtrimet kompjuterike, është çështje e rëndësishme e sigurisë kombëtare. Sipas "Strategjisë për mbrojtjen kibernetike 2018-2020", trendi aktual tregon se incidentet e kësaj natyre do të vazhdojnë të rriten.

Ndërmarrja e projekteve, studimeve e kërkimeve në fushën e krimeve e luftës kibernetike përfshin aplikimet shkencore, punimet, trajtimet, studimet dhe analizat e thelluara lidhur me procedurat, metodat e teknikat hetimore brenda e jashtë vendit; vlerësimin e faktorit të rrezikut dhe ndikimit në shoqëri; digjitalizimin e komunikimit dhe format e reja të mbrojtjes, si dhe me programet, kurikulat e modulet ekzistuese për këtë formë krimi, në kuadër të ndërtimit të strategjive të nevojshme për zhvillimin e vazhdueshëm të kapaciteteve njerëzore e materiale, për përmirësimin e metodave hetimore dhe për bashkëpunime të fushave e nivele të ndryshme në nivel kombëtar e ndërkombëtar.

Në këtë konferencë do të diskutohet rreth masave strategjike, organizative dhe teknike të sigurisë kibernetike në sistemet e komunikimit dhe të informacionit, lidhur me rrezikun e krimeve kompjuterike dhe kërcënimeve kibernetike. Kjo konferencë shërben në kuadrin shkencor, për të ndihmuar institucionet, programet, agjencitë, ekspertët për të nxitur debate konstruktive akademike e për të dhënë sugjerime për masa e politika për mbrojtjen nga kërcënimet në rritje në sigurinë publike në hapësirën kibernetike dhe në aspektin hetimor sa më efektiv, me qëllim nxitjen e bashkëpunimeve në nivel ndërkombëtar e kombëtar, dhënien e ekspertizave e praktikave që ofrojnë risi dhe rekomandimet përkatëse për politikat në vazhdim të Policisë së Shtetit e më gjerë.

### Objekti i konferencës

Objekti kryesor i kësaj konference, është paraqitja e analizave e prognozave, nga aspekti i hetimit të krimeve kompjuterike dhe kërcënimeve kibernetike të sigurisë kombëtare e ndërkombëtare. Këto do të konkretizohen me punime të mirëfillta shkencore për të nxitur debate dhe për të trajtuar në nivel të gjerë, kombëtar e ndërkombëtar, rëndësinë dhe nevojën e zgjerimit të dijeve dhe aplikimit të tyre përballë sfidës së hetimit, kërcënimeve të reja të kufijve virtualë dhe parandalimit të krimeve kibernetike në Shqipëri, si dhe hartimin e politikave, masave, kurrikulave e trajnimeve për këtë çështje.

### Qëllimi i konferencës

Trajtim në mënyrë shkencore rreth *aspektit proceduralo-hetimor* të krimeve kompjuterike; *aspektit analitik strategjik* të kërcënimeve të krimeve kibernetike dhe terrorizmit kibernetik në sigurinë kombëtare dhe *aspektit akademik,* për paraqitjen e praktikave ekzistuese dhe rekomandime të mëtejshme të kurrikulave, programeve e trajnimeve për fushën e krimeve kibernetike te punonjësit e policisë e më gjerë.

### Synimi i konferencës

Kjo konferencë synon të bashkojë njëzëri akademikët, shkencëtarët, profesionistët dhe ekspertët e fushave të shkencave kompjuterike, prokurorë, gjyqtarë, oficerë të policisë gjyqësore, e të tjerë për të ndarë eksperiencat, praktikat, punimet shkencore dhe gjetjet për të gjitha aspektet gjithëpërfshirëse të fushës së krimeve kibernetike.

### Tipi konferencës

Konferenca është shkencore ndërkombëtare, në një auditor me staf akademik të

Akademisë së Sigurisë, studiues dhe ekspertë vendas dhe të huaj të çështjeve të sigurisë, drejtues dhe specialistë të strukturave të Policisë së Shtetit, agjencive të tjera ligjzbatuese, përfaqësues të misioneve të huaja policore që asistojnë Policinë e Shtetit, përfaqësues të institucioneve akademike partnere në vend dhe të akademive, kolegjeve, universiteteve policore partnere të huaja.

### Struktura e konferencës

Konferenca organizohet në tre sesione:

***Sesioni I***

Aspektet ligjore, procedurale e hetimore të krimeve kompjuterike, me nënçështje si:

- trajtimi i krimit kompjuterik sipas legjislacionit shqiptar;
- hapat dhe procedurat hetimore për krimet kibernetike;
- parimet, veçoritë dhe trajtimi i provave kompjuterike;
- hulumtime mbi kërkimet, evidentimet, këqyrjet dhe sekuestrimin e provave në fushën e rrjeteve dhe hapësirës kibernetike;
- analiza të thelluara për provat elektronike: mënyrat e paketimit, transportimit e magazinimit;
- paraqitja e formave të mbledhjes dhe ruajtjes së informacionit elektronik;
- problematikat e hetimit të sistemeve dhe të dhënave kompjuterike: praktika vendase e të huaja;
- procedurat hetimore dhe masat e veprimit nga oficerë të policisë gjyqësore për krimet kompjuterike: risi dhe rekomandime;
- veprat penale nëpërmjet krimeve kibernetike;
- roli i policisë në përpjekjet në luftën kibernetike: paraqitja e nevojave për bashkëpunim;
- institucionet e drejtësisë në Shqipëri përballë krimeve kibernetike: problematika, praktika e sugjerime;
- risitë e policisë shqiptare në parandalimin, zbulimin e goditjen e krimeve kompjuterike.

***Sesioni II***

Analiza strategjike dhe masat organizative të sigurisë kibernetike. Terrorizmi kibernetikë, rreziqet dhe kërcënimet, me nënçështje si:

- analiza strategjike të hapësirës kibernetike dhe kërcënimeve me natyrë kriminale e terroriste pas vitit 2000;
- koncepti i ri i kufijve virtual dhe kërcënimet e sigurisë publike e kombëtare;
- kriza globale e të dhënave personale: kontrolli, kërcënimet dhe mbrojtja e tyre;
- koncepti i inteligjencës artificiale dhe luftës kibernetike;
- raportimi dhe vlerësimi i impaktit të krimit kibernetik; si mund ta inkurajojmë për ta raportuar më shpesh atë?
- paraqitje kronologjike të formave të kërcënimeve të terrorizmit kibernetik;
- bashkëpunimi ndërkombëtar për parandalimin e sulmeve kibernetike;
- kërcënimet kibernetike: impakti dhe shpërndarja e tyre në institucionet shtetërore në Shqipëri;
- bashkëpunimet mes ligjit dhe qeverisjes për të tejkaluar me sukses krimet dhe kriminelët kibernetikë;
- siguria dhe terrorizmi kibernetik;
- paraqitja e profileve të autorëve tipik të krimeve kibernetike;

- praktika dhe rekomandime për mbrojtjen e sigurisë kibernetike brenda dhe jashtë vendit;

- lufta e informacionit *online,* një problem i ri i mbrojtjes së sigurisë kombëtare;

- trajtimi i rritjes së mjeteve miqësore "hacking"; hetime dhe masat për parandalim;

- përpjekjet në nivel kombëtar e ndërkombëtar për parandalimin e krimeve kibernetike;

- menaxhimi i rrezikut të kompjuterizimit të informacionit dhe terrorizmit kibernetik;

- digjitalizimi dhe globalizimi i rrjeteve; kërcënimet e krimet kibernetike në botë, Europë, Ballkan e në Shqipëri;

- format e reja të mbrojtjes nga kërcënimet e jashtme e të brendshme të rrjetave kompjuterike: risi dhe praktika;

- analizë të formave të reja të kërcënimeve nga mashtrimet kompjuterike dhe krimet kibernetike në Shqipëri;

- kërcënimet e sulmeve kibernetike ndaj sigurisë kombëtare të Shqipërisë;

- lufta në hapësirën kibernetike të Ballkanit: pozicioni i Shqipëri dhe niveli i rrezikut;

- sabotimet kompjuterike në vendet fqinje, në Shqipëri e në Europë;

- manipulimet në hapësirën kibernetike dhe rrjetet kompjuterike me anë të terrorizmit kibernetik;

- tekno-terrorizmi dhe veçoritë e tij;

- hakerat, sulmet dhe shfrytëzimi i sistemit kompjuterik;

- shpjegime psikosociale të profileve të terrorizmit kibernetik: simptoma, shkaqe e pasoja.

***Sesioni III***

Zhvillimi i një platforme për edukim dhe trajnime, për mbrojtjen ndaj krimeve kompjuterike e sulmeve kibernetike, me nënçështje si:

- trajtimi i kurrikulave, programeve mësimore e trajnuese në fushën e krimeve kompjuterike e kërcënimeve kibernetike;

- evidentim të kurrikulave ekzistuese për punonjësit e policisë për trajtimin e krimeve kibernetike: praktika të policisë shqiptare si dhe të policive të vendeve të rajonit dhe jo vetëm;

- rekomandime për kurrikula, programe, trajnime e *workshop*-ëve në akademinë e sigurisë për çështje të kërcënimeve të sigurisë publike e kombëtare nga krimet kompjuterike e kibernetike;

- bashkëpunime në nivele akademike, brenda e jashtë vendit, për nxitjen dhe shpërndarjen të punonjësit e policisë dhe jo vetëm, të njohurive, risive apo praktikave të identifikimit, menaxhimit, hetimit, zbulimit e parandalimit të krimeve kompjuterike.

**Pjesëmarrja në konferencë**

Pjesëmarrja ishte e hapur: për staf akademik, studentë të Akademisë së Sigurisë, ekspertë e studiues nga radhët e strukturave të Policisë së Shtetit e agjencive të tjera të zbatimit të ligjit, akademikë të institucioneve të tjera të arsimit të lartë publik e privat në vend, studiues e ekspertë të çështjeve të hetimit dhe të sigurisë në vend dhe vende partnere, përfaqësues nga organizma ndërkombëtare partnere të Policisë së Shtetit etj.


AKADEMIA E SIGURISË
AS
1971

*~ Sesioni II ~*

# Hetime profesionale të krimeve kibernetike

# Siguria kibernetike në Forcat e Armatosura

■**Dr. Zihni GOXHAJ**
*Akademia e Forcave të Armatosura*
*zihni.goxhaj@aaf.mil.al*

**Abstrakt**

*Ky është një punim, në të cilin trajtohet qëllimi i përdorimit, i shfrytëzimit të tyre dhe se si funksionojnë e se si shërbejnë sistemet dhe mjetet kompjuterike, në interes të Forcave të Armatosura. Siguria kibernetike është një element i rëndësishëm i sigurisë i sistemeve të ndërlidhjes dhe informacionit (SNI) duke mundësuar shpërndarjen dhe menaxhimin e shërbimeve të SNI-ve në përgjigje të veprimeve të dëmshme të përjetuar nëpërmjet hapësirës kibernetike. Siguria e informacionit është një çështje shumë e rëndësishme për SNI pasi sistemet dhe rrjetet menaxhojnë informacionet kritike të një organizate dhe informacioni duhet të jetë i besueshëm, i sigurt dhe proceset të jenë në vendin e duhur për të zbuluar dhe luftuar aktivitetin e padëshirueshëm. Është me shumë interes edhe realizimi nga strukturat ushtarake të masave për sigurinë e për mbrojtjen e komunikimit, informacionit dhe sistemeve të tjera elektronike i cili është i depozituar, përpunuar, ose transmetuar në këto sisteme në lidhje me konfidencialitetin, integritetin, disponueshmërinë, vërtetimin dhe mos mohimin e tij. Pse është e vështirë dhe e domosdoshme siguria, mbrojtja kibernetike,"... Sepse, ky armik (sulm kibernetik), nuk na sulmon me kamionë eksplozivësh, as me valixhe të gazit Sarin, as me dinamit të varur në trupat e fanatikëve. Ky armik na sulmon me një dhe zero, në një vend ku jemi më të pambrojtur: pika në të cilën bota fizike dhe virtuale konvergojnë."*[1]

**Fjalëkyçe:**

**Fjalëkyçe: sistemet e ndërlidhjes dhe të informacionit, mbrojtja kibernetike, siguria e informacionit, siguria kibernetike.**

"Nëse një këshilltar për sigurinë kompjuterike deklaron se ju, organizata juaj dhe vendi juaj janë të sigurt pas *firewalls*, pas një sistemi të vënë në vend nga njerëz që nuk kanë luftuar kurrë betejat kibernetike, pas shtigjeve të auditimit, fjalëkalime dhe enkriptim, atëherë një gabim i madh dhe i rrezikshëm ose fantazi po kryhet mbi ju. Zgjidhja e vetme është vendosja e shpejtë e një counter-CyberTerrorist - dikush që e di se çfarë jeni kundër sot, dikush që jeton në botën e njerëzve që janë dhe do të sulmojnë - dikush që mund të trajnojë njerëzit që duhet të luftojnë betejat."[2]

## 1. Hyrje

Sulmet kibernetike janë rrezik potencial për sigurinë në përgjithësi dhe Forcat e Armatosura në veçanti. Sulmet kibernetike mund të shkaktojnë dëme të mëdha dhe pritet të bëhen më të sofistikuara e më të organizuara, me synim cenimin e sigurisë dhe stabilitetit kombëtar dhe rajonal. Eksperti i sigurisë Dorothy Denning e përkufizon kiberterrorizmin si: "…operacione piraterie kompjuterike të motivuar politikisht me qëllim që të shkaktojë dëme të rënda si humbja e jetës apo dëme të rënda ekonomike"[3]. Ndërsa Agjencia Federale e Menaxhimit të Emergjencave(FEMA), si: "Sulme të paligjshme dhe kërcënime për sulm ndaj kompjuterëve, rrjeteve dhe informacionit të ruajtur aty, kur bëhen për të trembur apo detyruar qeverinë ose popullin e saj të veprojë në mbështetje të objektivave të caktuar politikë apo social"[4]. Forcat e Armatosura

[1] Instituti për siguri dhe informim, Stanford, CA94309-9877, SHBA.
[2] Po aty.

për realizimin e misionit dhe të detyrave të tyre duhet të mbajnë një hapësire kibernetike të besueshme e të sigurt dhe t'i kushtojnë vëmendje të veçantë, zbatimit të rregullave të rrepta për sigurinë e informacionit të klasifikuar, në të gjitha sistemet dhe format e shkëmbimit të tij. Për pasjen e një hapësire të besueshme, kërkohet një mbrojtje kibernetike e cila me mjetet dhe zbatimin e masave mbrojtëse t'i kundërpërgjigjet sulmeve kibernetike dhe zbutjen e efekteve të tyre, duke parandaluar dhe rivendosur sigurinë e komunikimit, informacionit ose sistemin tjetër elektronik, ose të informacionin që ruhet, përpunohet ose transformohet në këto sisteme.

Mbrojtja kibernetike kërkon zhvillim të qëndrueshëm dhe sistematik të aftësive, teknologjisë së komunikimit dhe informacionit dhe të masave të sigurisë të cilat bëjnë të mundur të mbrohemi kundër kërcënimeve kibernetike. Kjo shprehet qartë dhe në Strategjinë e Sigurisë Kombëtare 2014-2020 "Për vendosjen dhe respektimin e standardeve më të larta në drejtim të ruajtjes dhe mbrojtjes së informacionit në të gjitha trajtat e ekzistencës së tij, duke përqendruar përpjekje të veçanta për mbrojtjen nga sulmet kibernetike".

## 2. Informacioni, komunikimi dhe siguria kibernetike

Informacioni duhet mbrojtur në lartësinë e vlerave e rëndësinë e tij nga individët, organizmat, nga krimet qe synojnë manipulim, fshirje, modifikim, survejim, spiunazh në informacion që qarkullojnë në rrjetet e komunikimit. Këto veprime cenojnë, prekin interesat e individit, organizmave dhe vetë shtetit. Pra, siguria e informacionit është e lidhur direkt me sovranitetin e një shteti, me sistemet, pasuritë kulturore të kombit, me një fjalë: mbrojtja e vlerave. Sistemet e ndërlidhjes dhe të informacionit (SNI) në Forcat e Armatosura ndërtohen, zhvillohen dhe modernizohen në bazë politikave kombëtare, të NATO-s, BE-së, OKB-së dhe agjencive ndërkombëtare të teknologjisë së informacionit, ku vendi ynë bën pjesë. Organizimi dhe funksionimi i tyre mbështetet në gjendjen aktuale të tyre në FA, në planet afatmesme dhe afatgjata të zhvillimit dhe modernizimit të FA, objektivat e kapaciteteve (OK), rishikimin e strategjisë së mbrojtjes, strategjinë ushtarake, politikat e mbrojtjes, si dhe në kërkesat për integrim dhe ndërveprim të sistemeve tona me sistemet e SNI-ve të NATO-s.

Sistemi i ndërlidhjes është bashkimi i pajisjeve, metodave dhe procedurave dhe, nëse është e nevojshme, personeli, i organizuar për të realizuar funksionet e transferimit të informacionit[5].

Informacioni është dije në lidhje me qëllimin (p.sh., faktet, ngjarjet, gjërat, proceset ose idetë dhe konceptet) që, brenda një konteksti të caktuar, kanë një kuptim të veçantë. Informacioni mund të përdoret për qëllim të zbulimit, ndërgjegjësimit të situatës ose çdo lloj të dhënash (p.sh., operative dhe logjistike) të cilat duhet të shkëmbehen gjatë një operacioni ushtarak.

Rrjetëzimi[6] i të gjitha elementeve të FA krijon aftësi për ndarjen dhe bashkëpunimin e pakrahasueshëm të informacionit, njësitë/organizatat e tjera që përshtaten me to dhe një bashkim më të madh të përpjekjeve nëpërmjet sinkronizimit dhe integrimit të

[3] Dorothy Denning, *Siguria e rrjeteve*, 2007, f. 35.
[4] Agjencia Federale e Menaxhimit të Emergjencave (FEMA), 2011.
[5] AJP-6, *Doktrina e përbashkët e Aleancës për sistemet e ndërlidhjes dhe informacionit*, Botimi A, version 1, shkurt 2017.
[6] FMI 6-02.45 *Signal Support to Theater Operations*, 2007, Headquarters Department of The Army.

elementëve të forcës në nivelet më të ulëta.

Siguria e informacionit është ruajtja dhe mbrojtja e sistemeve të informacionit dhe informacionit duke siguruar disponueshmërinë, integritetin dhe konfidencialitetin e tyre. Siguria kibernetike[7] përcaktohet si mjet për të arritur dhe ekzekutuar masa mbrojtëse për të luftuar sulmet kibernetike dhe për të zbutur efektet e tyre, duke ruajtur dhe rivendosur sigurinë e komunikimit, informacionit dhe sistemeve të tjera elektronike. NATO ka pranuar që mbrojtja kibernetike të përfshihet në sigurimin e sistemeve të ndërlidhjes dhe të informacionit (SNI). Duke pranuar këtë, NATO ka miratuar një qasje gjithëpërfshirëse për sigurinë e SNI-ve (duke përfshirë mbrojtjen kibernetike), integruar përpjekjet përkatëse ndërmjet reagimit të incidenteve, masave parandaluese të sigurisë të SNI dhe ndërgjegjësimit të përdoruesve për të mbrojtur rrjetet statike dhe të dislokuara të NATO-s. Në këtë mënyrë sigurohet vazhdimësia e punës ose garantimi i misionit për operacionet. Kjo përfshin integrimin e elementëve të mbrojtjes kibernetike në operacionet dhe misionet e Aleancës.

Siguria[8] e sistemeve të ndërlidhjes dhe të informacionit është një element i sigurisë të informacionit e cila përbëhet nga zbatimi i masave të sigurisë për mbrojtjen e komunikimit, informacionit dhe sistemeve të tjera elektronike dhe informacionin që ruhet, përpunohet ose transmetohet në këto sisteme në lidhje me disponueshmërinë, integritetin, vërtetësinë, konfidencialitetin dhe mos hedhjen poshtë të tij. Ajo përfshin masa mbrojtëse për të luftuar sulmet kibernetike dhe për të zbutur efektet e tyre, masat parandaluese të sigurisë së dhe ndërgjegjësimin e përdoruesit si mbrojtje kibernetike.

## 3. Informacioni kompjuterik dhe siguria e tij

Departamenti amerikan i Mbrojtjes, përdor pajisje dhe programe nga produktet e tregut edhe në sistemet luftarake së të gjitha shërbimeve si p.sh. në sistemet e integruara të luftës për avionët transportues bërthamor. Prej vitit 2007, raportohen infiltrime virusesh në sistemet kompjuterike *top secret* në "Komandën e Mbrojtjes Raketore dhe Hapësinore Ushtarake". Sulmi i kiberspiunazhit nuk u dallua prej disa muajsh dhe u emërtua "shiu Titanik". Sulmet ishin:

- kundër Agjencisë të Sistemit të Informacionit të Mbrojtjes (US, Defense Information Sistems Agency, DISA);

- kundër bazës amerikane, US Redstone Arsenal (shënim, Z.G. : zemra e programimit të raketave dhe anijeve hapësinore, nga ku më pas lindi NASA);

- instalimeve hapësinore dhe strukturave të mbrojtjes si dhe kundër sistemeve kompjuterike të logjistikës ushtarake.

Shkëmbimi i besueshëm, pa ndërhyrje dhe përpunimi i informacionit është thelbësor për vendimmarrësit politikë dhe ushtarakë. Sistemet e ndërlidhjes dhe të informacionit përbëhen nga shërbimet e përpunimit të informacionit. Këto shërbime sigurojnë mbështetjen e nevojshme për të arritur komandim-kontrollin (C2). Ato ndahen më tej në shërbime bazë dhe shërbime funksionale. Shërbimet bazë ofrojnë shërbime të përbashkëta për të gjithë përdoruesit. Shërbimet funksionale ofrojnë mbështetje për zonat funksionale dhe të veçanta të stafit. Shërbimet e përpunimit të informacionit përbëhen nga depozita të dhënash dhe programe kompjuterikë të përputhur për të

[7] Po aty.

[8] Instituti për siguri dhe informim, Stanford, CA94309-9877, SHBA.

përmbushur nevojat e funksioneve specifike të përdoruesve. Të dy shërbimet bazë dhe funksionale mbështeten në shkëmbimin e informacionit, sigurimin e informacionit dhe shërbimet mbështetjes të afateve të përdorimit të CIS-it.

- *Shërbimet e shkëmbimit të informacionit.* Këto shërbime ofrojnë shërbimet të rrjetit kryesor të komunikimit dhe shërbimet e transportit të komunikimit me valë (pa tel) që nevojiten për të aksesuar dhe shpërndarë informacion në mbështetje të vendimmarrjes politike dhe ushtarake. Shërbimet e shkëmbimit të informacionit mbështesin shkëmbimin e sasive të mëdha të informacionit në formate të ndryshme (p.sh., zë, tekst, imazh, video dhe të dhëna) midis vendndodhjeve të shpërndara gjeografikisht në një mënyrë të besueshme, në kohë dhe të sigurt.

- *Shërbimet elektronike të sigurisë së informacionit.* Shërbimet elektronike të sigurisë së informacionit janë të domosdoshme për të siguruar masat e sigurisë së informacionit, si pjesë e një strukture të balancuar të masave të sigurisë. Për të mbështetur objektivat e sigurisë kërkohet një strukturë e përputhshme e masave për sigurimin e informacionit për të gjitha sistemet që përpunojnë si informacionin e klasifikuar, edhe atë të paklasifikuar, të FA.

- *Menaxhimi i informacionit.* Menaxhimi i informacionit (IM) është një disiplinë që drejton dhe mbështet trajtimin e informacionit gjatë gjithë ciklit të jetës së tij duke siguruar që ai të bëhet informacion i duhur në formën e duhur dhe të cilësisë së mjaftueshme për të përmbushur kërkesat e organizatës. Plani IM drejton shkëmbimin e informacionit në mbështetje të zinxhirit të komandimit duke përshkruar në mënyrë specifike se sa informacion të përshtatshëm duhet të menaxhohet si nga brenda ashtu edhe nga jashtë organizatës. Për të siguruar C2 efektiv, kërkohet një shkallë e lartë operacionale e shkëmbimit të informacionit - si vertikalisht ashtu edhe horizontalisht - midis entiteteve apo komandave të ndryshme. Plani i IM-it cakton përgjegjësitë e IM-së për stafin e veçantë, përshkruan kërkesat e informacionit dhe siguron udhëzime në lidhje me kërkesat e qarkullimit të informacionit dhe nevojat për mbrojtjen e tij.

- *Siguria e informacionit.* Informacioni është burim jetik për Forcat e Armatosura. Si i tillë, ai duhet të menaxhohet duke organizuar dhe kontrolluar informacionin gjatë gjithë ciklit të jetës së tij pavarësisht nga forma e medies që e përpunon dhe dërgon dhe format në të cilin mbahet informacioni.

Siguria e informacionit është ruajtja dhe mbrojtja e informacionit dhe sistemeve të informacionit duke siguruar disponueshmërinë, integritetin dhe konfidencialitetin e tyre. Sigurimi i informacionit kërkon proceset e menaxhimit për të siguruar që sistemet dhe rrjetet e përdorur për të menaxhuar informacionet kritike nga një organizatë janë të besueshme dhe të sigurta, dhe proceset janë në vendin e duhur për të zbuluar dhe luftuar aktivitetin e padëshirueshëm. Sigurimi i informacionit përfshin elementë të sigurisë fizike (p.sh. siguria e personelit dhe dokumenteve) dhe siguria e informacionit. Siguria e komunikimeve dhe siguria kompjuterike janë elemente përbërëse së të gjitha operacioneve ushtarake të SNI-ve dhe duhet të konsiderohen të tilla gjatë planifikimit dhe ekzekutimit. Aktivitetet e mbrojtjes kibernetike janë një element i rëndësishëm i sigurisë i SNI-ve duke mundësuar shpërndarjen dhe menaxhimin e shërbimeve të SNI-ve në përgjigje të veprimeve të dëmshme të përjetuar nëpërmjet hapësirës kibernetike. Informacioni duhet të mbrohet në nivelin e duhur, duke siguruar që ai të jetë i vlefshëm në dispozicion të përdoruesve të autorizuar dhe duke parandaluar marrjen e informimit të vlefshëm nga personat e paautorizuar. Shkalla e sigurisë e ofruar duhet të jetë në përputhje me kërkesat e përdoruesve të SNI-ve, cenueshmërinë e mjeteve të ndërlidhjes

që transmetojnë, që janë në përgjimin dhe shfrytëzim, si dhe besueshmërinë në dhënien e pajisjeve dhe programe kompjuterike.

Tre shtyllat e sigurisë së informacionit janë:

*1. Disponueshmëria.* Informacioni është i arritshëm dhe i përdorshëm sipas kërkesës nga

një individ ose subjekt i autorizuar.

*2. Konfidencialiteti.* Informacioni nuk vihet në dispozicion ose nuk zbulohet për persona, entitete apo procese të paautorizuara.

*3. Integriteti.* Informacioni (përfshirë të dhënat) nuk është ndryshuar ose shkatërruar në mënyrë të paautorizuar.

Kombinimi i këtyre tri shtyllave siguron dy nënproduktet e sigurisë, të cilat janë: autentifikimi dhe mosrefuzimi.

Siguria e informacionit përfaqësohet si i përbërë nga pesë elementë të sigurisë: siguria e personelit, siguria fizike, siguria e informacionit, siguria e SNI-ve (përfshin mbrojtjen kibernetike) dhe siguria industriale. Mbrojtja kibernetike, përcaktohet si mjet për të arritur dhe ekzekutuar masat mbrojtëse, për të luftuar sulmet kibernetike dhe për të zbutur efektet e tyre, duke ruajtur dhe rivendosur sigurinë e komunikimit, informacionit dhe sistemeve të tjera elektronike.

## 4. Siguria kibernetike në Forcat e Armatosura

"Siguria kibernetike"[9] është tërësia e mjeteve ligjore, organizative, teknike dhe edukative, me qëllim mbrojtjen e hapësirës kibernetike. Me zhvillimet e shpejta të teknologjisë së informacionit dhe komunikimit, me shtrirjen e përdorimit të saj pothuajse në të gjitha fushat e veprimtarisë së shoqërisë, bëhet evidente kërkesa për shërbime të sigurta dhe të besueshme. Rritja e përdorimit të TIK dhe internetit po ndryshon shoqërinë duke krijuar mënyra të reja të lidhjes, komunikimit, bashkëpunimit dhe të zhvillimit ekonomik nëpërmjet aksesit në hapësirën kibernetike. Kjo ka bërë, që shoqëria jonë, të varet gjithnjë e më shumë në përdorimin e këtyre teknologjive. Shqipëria renditet ndër vendet ku zhvillimi i telekomunikacionit, qasja në internet dhe informatizimi i shoqërisë përparon shumë shpejt. Rritja e përdorimit të komunikimit përbën një vlerë të shtuar në zhvillimin ekonomik dhe shoqëror të vendit, por, në të njëjtën kohë, ajo e ekspozon atë ndaj rreziqeve të natyrës kibernetike me aktorë shtetërorë dhe joshtetërorë.

Sulmet kibernetike kanë potencial për të dëmtuar rëndë shkëmbimin e informacionit në institucionet publike, të telekomunikacionit dhe sistemin financiar e bankar, duke shkaktuar edhe ndërprerje të shërbimeve jetike. Aksesi në hapësirën kibernetike së bashku me elementët pozitivë të tij rrit rrezikun potencial nga dëmtimi apo keqpërdorimi i të dhënave dhe sistemeve kompjuterike. Si pasojë e rreziqeve kibernetike në rritje, sigurimi i integritetit së të dhënave dhe konfidencialitetit, si dhe hyrja e sigurt në hapësirën kibernetike, janë kthyer në një nga sfidat më të mëdha me të cilat përballet shoqëria në ditët e sotme, duke e kthyer atë në një çështje të sigurisë kombëtare.

Në këtë situatë, me qëllim mbajtjen e një hapësire kibernetike të besueshme e të sigurt për Forcat e Armatosura për realizimin e misionit dhe të detyrave të tyre, është përgatitur "Strategjia për mbrojtjen kibernetike, 2018-2020"[10].

[9] Ligj nr. 2/2017 "Për sigurinë kibernetike në Republikën e Shqipërisë".
[10] *Strategjia e MM për mbrojtjen kibernetike*, 2018-2020.

- *Sfidat e sigurisë informacionit.* Sfidat e sigurisë informacionit përfshijnë të gjitha nivelet e strukturave FA-së, duke filluar nga pajisjet individuale, që përdoren në mjediset zyrtare të punës, deri në sigurimin e sistemeve themelore, të cilat janë kritike për mbarëvajtjen e punës. Disa nga sfidat që karakterizojnë këtë situatë dhe orientimi i tyre për të ardhmen përfshijnë:

- *Kërcënimet në hapësirën kibernetike.* Hapësira kibernetike[11], tek një fushë globale brenda mjedisit të informacionit, është një nga fushat e tjera të ndërvarura nga njëra tjetra; të ajrit, tokës, detit dhe hapësirës. Hapësira kibernetike përfshin internetin, rrjetet, sistemet, përdoruesit fundor të lidhur, të dhënat dhe përdoruesit në mjedisin e informacionit. Ky mjedis i ndërlidhur është i rëndësishëm për qeverisjen, sigurinë e përgjithshme, ushtarake dhe kombëtare. Aktivitetet në hapësirën kibernetike mund të mundësojnë lirinë e veprimit për aktivitetet në fushat fizike Për shembull, serverët e rrjetit mund të qëndrojnë në një kompleks të dhënash, me bazë në tokë ose në det, në bordin e anijeve luftarake dhe transmetimet në rrjetet me valë, realizohen përmes ajrit dhe hapësirës, dhe madje edhe nga nënuji.

Aktivitetet në fushat fizike, mund të krijojnë ndikime në hapësirën kibernetike dhe përmes saj, duke ndikuar në spektrin elektromagnetik (EMS) ose në infrastrukturën fizike. Marrëdhënia midis hapësirës dhe hapësirës kibernetike është unike, në atë se, pothuajse të gjitha operacionet hapësinore, varen nga hapësira kibernetike dhe një pjesë kritike e hapësirës kibernetike, mund të sigurohet vetëm nëpërmjet operacioneve hapësinore. Hapësira kibernetike, të cilën çdo njeri mund ta përdorë pa kufij kohorë dhe gjeografikë, jep në mënyrë asimetrike avantazhe për sulmuesit keqdashës, jo atyre që mbrohen. Si rezultat i metodave të sofistikuara, zhvillimit të mjeteve teknologjike të sulmeve kibernetike ose sponsorizimi i këtyre sulmeve nga shtetet janë kërcënime serioze, gjithnjë e në rritje ndaj sigurisë kombëtare. Për të parandaluar përkeqësimin e mëtejshëm të këtyre kërcënimeve, krijimi "Hapësirës kibernetike të lirë dhe të ndershme" duhet të jetë paralel me krijimin e "Hapësirës kibernetike të sigurt".

- *Interneti dhe pajisjet e lëvizshme/mobile.* Zhvillimi i internetit dhe i sistemeve të reja kompjuterike, sistemet industriale të kontrollit, telefonat mobile, pajisjet magazinuese të lëvizshme (*memory stick*) dhe tabletat, na bëjnë më shumë efiçent, por edhe më shumë të pambrojtur në mjedisin ku ushtrojmë detyrat funksionale.

- *Rrjetet sociale dhe portalet.* Një sfidë e veçantë për shoqëritë e hapura është përdorimi i komunikimit digjital, për të ndikuar në mendimin e publikut, për shembull nëpërmjet përpjekjeve të fshehura për të ndikuar në diskutimet mbi mediet sociale dhe duke manipuluar informacionet në portalet e lajmeve. Kjo qasje tashmë ka fituar një rëndësi të veçantë si një element i luftës hibride.

- *Komunikimi dhe transmetimi i informacionit.* Rrjeti i FA-së nuk është i mbyllur në një mjedis të kufizuar. Komunikimet elektronike me struktura të tjera të administratës publike, brenda dhe jashtë vendit, përbëjnë një sfidë më vete për shkak të kushteve, rrezikut të dyanshëm, ligjeve e rregullave të ndryshme, të cilat e bëjnë shumë të vështirë kontrollin mbi to. Sipas vendimeve të Samitit të Varshavës (qershor 2016), i cili rikonfirmoi mandatin mbrojtës të NATO-s, u njoh hapësira kibernetike si një "domain" operacional, në të cilin NATO-ja duhet të mbrojë veten me efektivitet ashtu siç vepron në ajër, tokë dhe det. Dokumenti i NATO-s "Cyber Defence Pledge", përfshin miratimin e vendeve të Aleancës që të zgjerojnë mbrojtjen kibernetike për rrjetet dhe

[11] Joint Publication 3-12 (R), *Cyberspace Operations*, 5 February 2013.

infrastrukturat kombëtare, të cilat konsiderohen si një çështje me prioritet në çdo vend aleat, dhe në respekt të përgjegjësive të tyre, të përmirësojnë qëndrueshmërinë dhe aftësinë për t'u përgjigjur shpejt dhe me efektivitet ndaj sulmeve kibernetike. Çdo vend Aleat është dhe do të jetë përgjegjës, për të mbrojtur rrjetet e tij kombëtare, të cilat janë të nevojshme të jenë të përshtatshme me ato të NATO-s dhe të njëri-tjetrit, si dhe të zgjerohet shkëmbimi i informacionit për mbështetje të përbashkët me qëllim parandalimin, zvogëlimin dhe rigjenerimin nga sulmet kibernetike.

*Strategjia e sigurisë kombëtare*, 2014-2020, reflekton këtë pikëshikim: "Për vendosjen dhe respektimin e standardeve më të larta, në drejtim të ruajtjes dhe mbrojtjes së informacionit, në të gjitha trajtat e ekzistencës së tij, duke përqendruar përpjekje të veçanta për mbrojtjen nga sulmet kibernetike".

Në takimin e Kryetarëve të Shteteve të NATO-s[12], në Varshavë, më korrik 2018, u konsiderua që "Sulmet kibernetike paraqesin një sfidë të qartë për sigurinë e Aleancës dhe mund të jenë po aq të dëmshme për shoqëritë moderne, sa një sulm konvencional. Në Varshavë u rikonfirmua njohja e hapësirës kibernetike si fushë e operacioneve, në të cilat NATO-ja duhet ta mbrojë veten në mënyrë efektive, ashtu siç ndodh në ajër, në tokë dhe në det. Kjo do të përmirësonte aftësinë e NATO-s për të mbrojtur dhe kryer operacione në këto fusha, dhe për të ruajtur lirinë tonë të veprimit dhe vendimit, në të gjitha rrethanat". Vendet u angazhuan për të rritur sigurinë kibernetike të rrjeteve dhe infrastrukturave kombëtare, si çështje prioritare.

Për këtë, është përgatitur dhe miratuar "Strategjia për mbrojtjen kibernetike". Janë përmirësuar politikat e mbrojtjes kibernetike, procedurat dhe doktrinat për lidhje logjike me dokumentin "Rritja e politikës së NATO-s mbi mbrojtjen kibernetike, bazuar në takimin e Varshavës" që përfshin: integrimin e mbrojtjes kibernetike në operacionet dhe proceset e planifikimit operacional; njohjen dhe zbatimin e ligjit ndërkombëtar mbi hapësirën kibernetike; vendosjen e masave të fuqishme duke bashkëndarë midis palëve të interesuara, të vlerësimeve të rrezikut, kërcënimit të mbrojtjes kibernetike ushtarake dhe të tjera kombëtare, me ato ndërkombëtare (përfshirë NATO-n), për të siguruar plotësim të ndërsjellë.

Të bëhet e mundur mbështetja e konfidencialitetit, integritetit dhe vërtetimit së të dhënave të informacionit në linjë me kërkesat e tij të sigurisë së misionit duke siguruar ndërveprueshmërinë dhe renditjen/bashkimin të kriptos kombëtare me transformimin e kriptos së NATO-s duke përfshirë pajisjet e kriptos dhe mekanizmat të lidhura me çelësat elektronikë, algoritmet e zhdërvjellëta dhe shërbimin e menaxhimit e kontrollit. Në lidhje me edukimin, trajnimit dhe aftësimit për mbrojtjen kibernetike, është bërë e mundur realizimi i një programi të edukimit dhe trajnimit të mbrojtjes kibernetike për përdorim brenda Forcave të Armatosura i cili përfshin personel teknik, operator dhe detyra më të larta teknike në këtë fushë dhe zbatohen programet e ngritura për të qenë të informuar mbi mbrojtjen kibernetike për të gjitha kategoritë e personelit.

## 5. Përfundime

1. Ndërtimi i një strategjie koherente, na ndihmon të zgjidhim hallkat e dobëta që rrezikojnë sistemin dhe gjithë sigurinë. Strategjia gjithëpërfshirëse, është e nevojshme në këtë rast. Pa këtë strategji nuk mund të zbatohen zgjidhje efikase.

[12] https://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber.

2. Në kuadër të NATO-s, FA po zhvillon një infrastrukturë rrjeti të aftë që të mbështesin një ambient koalicioni të federuar në mision. Infrastruktura të jetë e aftë që të sigurojë shërbimet e informacionit të kërkuar, të jetë e shkallëzuar dhe fleksibël që të bëjë të mundur zhvendosjen, mbijetesën dhe rizhvendosjen e forcave të dërguara dhe të mbështesë funksionet e komandim kontrollit (C2) të vendit tonë dhe forcave pjesëmarrëse të Aleancës në një operacion të NATO-s.

3. Sfidat e sigurisë për sistemet e ndërlidhjes dhe informacionit (SNI) përfshijnë të gjitha nivelet e strukturave të FA-së, duke filluar nga pajisjet individuale, që përdoren në mjediset zyrtare të punës, deri në sigurimin e sistemeve themelore, të cilat janë kritike për mbarëvajtjen e punës.

4. Hapësira kibernetike dhe interneti, janë një infrastrukturë e hapur e komunikimit global që mund të arrihet nga kushdo për të ndarë, shkëmbyer ose për të shkarkuar informacione në internet. Kjo infrastrukturë mbështet asetet e rëndësishme komerciale për kryerjen e transaksioneve elektronike (*e-commerce*) globalisht, si dhe transaksionet jotregtare.

5. Edukimi, trajnimi dhe aftësimit i personelit për përdorimin e shfrytëzimin e mjeteve kompjuterike si dhe në të njëjtën kohë trajnimi dhe aftësimi i tyre për Mbrojtjen Kibernetike, ka bërë të mundur realizimin e programeve të edukimit dhe trajnimit të personelit si brenda vendit, gjithashtu dhe në kuadër të ndihmës dhe bashkëpunimit me vendet aleate të NATO-s. Kjo pasi shumë dobësi në sistemet e informacionit janë për shkak të mungesës së ndërgjegjësimit mbi sigurinë kibernetike për pjesën e përdoruesve të kompjuterëve, administratorëve të sistemit, zyrtarëve të prokurimit, personelit të auditimit të sistemeve, të sigurisë të informacionit. Këto dobësi mund të paraqesin risk serioz kundrejt sistemeve, megjithëse ata mund të mos jenë pjesë e vetë infrastrukturës TIK. Mungesa e personelit të trajnuar vështirëson më tej detyrën për të zvogëluar dobësitë.

6. "Ndërtimi i një ekipi kundër kiberterrorizmit, duhet të jetë në kohë reale dhe dinamike, meqë armët do të ndryshojnë vazhdimisht, ... nëse kiberterroristi humbet sot, ai nuk vdes - ai mëson atë që nuk ka punuar dhe do ta përdorë atë informacion nesër kundër jush"[13].

## Bibliografi


1. Ligj nr. 2/2017 *Për Sigurinë Kibernetike në Republikën e Shqipërisë*.
2. *Strategjia e Sigurisë Kombëtare*, Tiranë, korrik 2014.
3. *Strategjia Ushtarake e RSH*, miratuar me ligjin nr. 72/2015.
4. *Strategjia e MM për Mbrojtjen Kibernetike* 2018-2020
5. VKM nr. 922, datë 19.12.2007, "Për sigurimin e informacionit te klasifikuar "Sekret shtetëror" që prodhohet, ruhet, përpunohet apo transmetohet ne sistemet e komunikimit (INFOSEC)", i ndryshuar.
6. Dokumenti i C-M (2007) 0118 *NATO Information Management Policy*.
7. Joint Publication 3-12 (R), *Cyberspace Operations,* 5 February 2013.
8. Joint Publication (6-0), *Joint Communications System,* 10 June 2015.
9. *NATO Federated Mission Networking Implementation Plan*, Secretary General, North Atlantic Treaty Organization, MCM-0106-2014 (REV1; 26 November 2014).
10. Military Decision on MC 0571/1, *NATO Military Concept for Cyber Defence,* 16 September 2015.
11. *Cyber Infrastructure Protection*, Volume III, Strategic Studies Institute and The U.S. Army War College Press, June 2017
12. *Strategic Cyberspace Operations Guide,* United States Army War College, 1 July 2017.


AKADEMIA E SIGURISË
1973

# Pornografia *online* me fëmijët: shkaqet, hetimi dhe parandalimi

**MSc. Luljeta Ismajlukaj**[1]
*Drejtoria e Përgjithshme e Policisë së Shtetit*
*luljeta.ismajlukaj@asp.gov.al*

**Abstrakt**

*Interneti ka hapur një botë të re - një botë me mundësi të pafundme në dukje. Është një botë emocionuese, ku çdokush që mund të përdorë internetin mund të ketë fjalën e tij, të gjejë informacion më lehtë se kurrë më parë dhe të ndajë me botën edhe mendimet apo preferencat e tij më private. Ne çdo ditë përballemi me mundësitë e errëta që u ofron interneti atyre që konsumojnë pornografinë online me fëmijë. Për të gjithë është i njohur fakti që shfrytëzimi seksual ka ekzistuar shumë kohë para revolucionit të informacionit dhe se të gjithë njerëzit kryesisht meshkujt, ishin dhe janë të aftë për të abuzuar në forma të ndryshme me fëmijë të moshave të ndryshme. Diferenca sot është se disponueshmëria dhe qasja në pornografinë me fëmijët është shumë më e lehtë. Në epokën e internetit abuzuesit mund të gjejnë viktimat e tyre fare lehtë nëpërmjet rrjeteve sociale.*

*Ne shohim dhe dëgjojmë për kaq shumë raste se kush janë shkelësit dhe viktimat dhe se si ato janë të lidhura përmes internetit dhe teknologjive të tjera. Pornografia e fëmijëve në internet është një krim tipik global, që sjell me vete problemet gjithnjë e më të njohura të krimeve policore të përkufizuara ndryshe në shtete të ndryshme dhe me juridiksione të shumëfishta, për shkak të decentralizimit të internetit, aftësisë për të transmetuar imazhe menjëherë nëpër botë dhe disponueshmërisë së smartfonëve dhe pajisjeve të tjera mobile për fëmijët dhe ata që do t'i shfrytëzonin ato. Prodhimi dhe shpërndarja e imazheve pornografike të fëmijëve rezultojnë të jenë nga abuzimi seksual i kontaktit nga të rriturit me marrëdhënie të afërta familjare ose sociale me fëmijët. Por kjo nuk ngelet në një fushë juridiksioni vendore, sepse shpërndarja ndërkombëtare dhe konsumi i imazheve nëpërmjet internetit konvertojnë këto krime lokale në ato globale. Prandaj konstatohet se ky krim global po merr përmasa gjigante çdo ditë e më tepër. Gjithë aktorët e interesuar në luftën për parandalimin dhe hetimin e këtyre krimeve e paraqesin si një kërcënim moral, ndaj të cilit duhet reaguar për ta neutralizuar dhe për të evidentuar dhe vënë përgjegjësit e këtyre krimeve para drejtësisë. Abuzimi i fëmijëve online është një problem i gjithë komunitetit. Kjo kërkon koordinimin e përpjekjeve nga ana e bizneseve dhe zbatimit të ligjit në nivel lokal dhe ndërkombëtar. Interneti tashmë është pjesë shumëdimensionale e jetës së çdo individi duke luajtur kështu një rol të patjetërsueshëm në psikologjinë e njerëzve e duke ndikuar në këtë mënyrë, që edhe problematika e varësisë nga ai të njohë shifra tepër të larta. Sigurisht, të lindur nën frymën e një bote ku çdo gjë është një klikim larg, fëmijët janë grupshënjestra më e ndjeshme ndaj këtij fenomeni. Kështu që është detyrë e gjithsecilit të përpiqet për të krijuar një mjedis sa më të sigurt për ta.*

**Fjalëkyçe:**
**pornografi, internet, vetmi, turp, vetëvlerësim, fëmijë, abuzim.**

## 1. Hyrje

Zhvillimi teknologjik me hapa galopantë, që ka përfshirë gjithë botën, ka sjellë krahas të mirave në shumë aspekte të jetës së përditshme edhe rreziqe të jashtëzakonshme me të cilat përballemi në ditët e sotme. Një nga rreziqet më sensitive që prek ndjeshëm shoqërinë e sotme, është përdorimi i internetit nga fëmijët. Sot të gjithë jemi të vetëdijshëm që fëmijët janë shumë të lidhur me internetin dhe pajisjet elektronike. Vet fëmijët për faktin që truri i tyre është në fazën e thithjes së informacionit dhe të resë në përgjithësi e shohin internetin si diçka argëtuese dhe interesante, me të cilën mund të kalojnë shumë kohë. Duke qenë të vetëm në përdorimin e internetit, që do të thotë se jo gjithmonë janë nën vëzhgimin e prindërve, mësuesve apo kujdestarëve të tyre, ata shpesh bien pre e keqbërësve në internet. Dhe rastet më të rrezikshme janë ato të pornografisë *online*. Në këtë temë studimore modestish do prezantohet një panoramë se kush janë shkaqet e këtyre rasteve, si mund të hetohen raste të tilla dhe kryesorja si mund të parandalohen raste të tilla.

Tregtia ilegale me materiale të papërshtatshme seksuale, sot është një nga më të përhapurat, e ndoshta më rekreative e shfrytëzuesve të rrjeteve kompjuterike. Pornografia *online* është një dukuri tejet e popullarizuar dhe fitimprurëse. Ajo është një biznes tejet i madh, veçanërisht në sektorin e shërbimeve BBS (*Buletin Board System*), organizatorët e të cilës tërheqin klientët që të anëtarësohen në koleksionet e materialeve pornografike. Ekziston një numër prej mijëra BBS, shërbimet e të cilave paguhen me kartela kredituese. Pesë BBS më të mëdha, realizojnë qarkullim prej më shumë se 1

[1] Autore e botimit: Luljeta Ismajlukaj, Arben Zela, *Manual për punonjësit e Policisë, për mbrojtjen e fëmijëve nga abuzimi dhe shfrytëzimi nëpërmjet internetit*, Tiranë: CRCA Shqipëri, 2016.

milionë dollarë.

Kjo ndoshta nuk do të ishte edhe aq e tmerrshme në krahasim me ekzistencën dhe përhapjen e pornografisë së fëmijëve në internet, me tendenca të rritjes permanente, e cila shkakton brengosje të madhe për shoqërinë. Kjo për arsye se një numër i madh i fëmijëve, kanë qasje në shërbimet *online*, të cilat kanë ndikim të madh në jetën e tyre. Rritja e shpejtë e fëmijëve të mbyllur në ambientet interaktive, u mundësojnë atyre të shfrytëzojnë çka të dëshirojnë dhe nga dëshirojnë, kjo paraqet një vërejtje për prindërit, mësimdhënësit dhe faktorët relevantë shoqërorë, vërejtje që nuk duhet anashkaluar për asnjë moment.

## 2. Shkaqet

*Interneti* është sistem global i rrjetave të ndërlidhura kompjuterike të cilat bëjnë shkëmbimin elektronik të të dhënave (tekst, muzikë video, fotografi, etj) nëpërmjet përdorimit të kabllove të bakrit, fibrave optike, lidhjeve pa tela dhe teknologjive të tjera. Këto informacione mund të lexohen, shikohen apo shkarkohen nga përdoruesit e tjerë. Pra interneti mundëson praktikisht komunikimin nga një pajisje kompjuterike në tjetrën.

Disa nga shërbimet që interneti ofron aktualisht janë:

- Kërkimi në internet (*WebBrowsing*) – Ofron mundësi shfletimi në faqe të ndryshme nëpërmjet aplikacioneve kompjuterike të tilla si *Google Chrome*, *Safari*, *Internet Explorer*, *Mozilla Firefox* etj.;
- Posta elektronike (e-mail) - mundëson dërgimin e mesazheve të tipit tekst, foto, muzikë, video nga një person te një tjetër;
- Bisedat *Online* (Chat *Online*) – përdoren për të komunikuar në mënyrë të menjëhershme me personat që janë në linjë *online*;
- rrjetet sociale (p.sh. *Facebook, Twitter, Instagram, Snapchat* );
- lojërat *online*.

Fotografitë e pornografisë së fëmijëve si edhe fotografitë tjera, shumë lehtë mund të konvertohen në formë të lexueshme kompjuterike, si me anë të skenimit apo në formë digjitale. Në këtë formë, ato shumë lehtë transferohen nëpërmjet rrjetit kompjuterik dhe shpërndahen në lokacione të ndryshme në mbarë botën. Të gjithë ata që kryejnë veprën penale të pornografisë *online* me fëmijët mund të incizojnë porno film në çdo vend të botës dhe pastaj nëpërmjet internetit mund t'i dërgojë ato në adresën e tij të email.

Problemi i pornografisë kompjuterike si dukuri shoqërore negative, me pasoja të mëdha brengosëse për shoqërinë në përgjithësi dhe gjithnjë me tendencë të rritjes permanente, u krijon mundësi subjekteve të ndryshme, autorëve dhe organizatorëve të kësaj dukurie, që të realizojnë fitime të mëdha materiale nga njëra anë, ndërsa dëme të mëdha morale nga ana tjetër, duke shfrytëzuar të arriturat nga fusha kompjuterike dhe sistemet e internetit.

Ndërkohë individë të caktuar të moshave dhe gjinive të ndryshme me probleme psikologjike janë në kërkim të presë së tyre, pre e cila nëpërmjet internetit sot gjendet më lehtë se kurrë. Fëmijë të moshave të ndryshme duke qenë pjesën më të madhe të kohës në internet eksplorojnë nëpër shumë site të cilat përmbajnë pamje pornografike ose mund të çojnë në chat rooms ku kushdo mund të shkëmbejë biseda. Fëmijët në ditët e sotme janë shumë të dhënë pas internetit dhe shpesh ndihen të vetmuar, të frustuar

apo të papranuar në shoqërinë e fëmijëve të tjerë, duke u bërë kështu viktima të veprimeve të paligjshme të "gjuetarëve të internetit". Fillimisht fëmijët joshen me shoqëri dhe mbështetje për të ndarë gjërat që ata kanë për zemër dhe pastaj vjen një moment kur përdoren për t'ju bërë keq atyre nga "gjuetarët e internetit". Sot fëmijët e mbarë botës janë çdo ditë e më shumë të bombarduar nga lajme, video, këngë apo filma ku përmbajnë imazhe "soft-porno". Këto i ç'destabilizojnë për sa i përket seksit, duke i bërë të kërkojnë çdo ditë e më shumë imazhe akoma më të forta, duke arritur deri te "hard-porno", përpara se në jetën reale të kenë pasur përvojën e parë seksuale. Ekspertët psikoseksologë kanë shtrirë alarmin e përdorimit dhe ndikimit të pornografisë në një moshë shumë të re. Imazhet brutale të pornos (që në fakt prodhohen për të rriturit) ndikojnë në zhvillimin e parakohshëm seksual të fëmijës, jo vetëm që ai ekspozohet paraprakisht nga stimuj hiperseksualë, por ndonjëherë pëson traumë vizive.

## 3. Hetimi

Për të kuptuar qartë se si mund të hetohet një vepër penale e klasifikuar si pornografi *online* me fëmijët, fillimisht po japim disa përkufizime të rëndësishme që lidhen drejtëpërdrejtë me hetimin e rasteve të tilla.

*Krimi kompjuterik*, është i ndarë në dy kategori :

a) në një kuptim të ngushtë, me krim kompjuterik do të kuptohet çdo sjellje e kryer nëpërmjet veprimeve elektronike të cilat drejtohen ndaj sigurisë së sistemeve kompjuterike dhe të dhënave të përpunuara prej tyre ;

b) në një kuptim më të gjerë, me krim kompjuterik do të kuptohet çdo sjellje e paligjshme e kryer nga mënyra apo nëpërmjet një kompjuteri apo sistem kompjuterik, përfshirë krime të tilla si *përpunimi i paligjshëm, ofrimi apo shpërndarja e informacionit nga një kompjuter apo rrjet, për të abuzuar dhe tërhequr vëmendjen* me forma të tilla si ato për përkrahje të grupeve p.sh terroriste, neonaziste, *pornografia dhe pedofilia*. Këtu do të përfshihen edhe llojet e krimeve të mashtrimeve, duke shkelur sigurinë e rrjeteve si, bixhozi i paligjshëm, skemat piramidale, mashtrimi me karta krediti dhe lloje të tjera të aktiviteteve të paligjshme. Në cybercrime, komponenti "cyber", zakonisht i referohet për të kualifikuar shkeljet e reja të mundësuara nga teknologjia e informacionit apo ndërveprimit të hapësirës kompjuterike, në shumë aktivitete tradicionale.

"*Siguria online*": do të nënkuptojë çdo masë të ndërmarrë nga institucionet dhe organizatat nënshkruese të kësaj marrëveshjeje, që ka si qëllim të forcojë mbrojtjen e fëmijëve gjatë lundrimit të tyre në internet dhe që mund të paraqesë rrezik ose mundësi që fëmija të bëhet viktimë e shfrytëzimit dhe abuzimit *online*.

*"Cyberbullying"* është kur një fëmijë apo adoleshent është kërcënuar, keqtrajtuar, poshtëruar, tallur, ofenduar ose është vënë në shënjestër në mënyrë të qëllimshme nga një fëmijë ose adoleshent tjetër duke shfrytëzuar përdorimin e internetit, teknologjitë interaktive dhe dixhitale ose telefonat celularë. Cyberbullying zakonisht nuk është një komunikim i vetëm, ai mund të ndodh në vazhdimësi.

*"Sexting"* është transmetimi apo shpërndarja e fotografive digjitale të trupit të zhveshur të dikujt ose nxitja në një akt seksual, sidomos nëpërmjet pajisjeve elektronike.

"*Grooming*" janë veprimet e ndërmarra me qëllim krijimin e një lidhje emocionale me një fëmijë, për të ulur rezistencën e fëmijës në përgatitje për aktivitet seksual me fëmijë, ose shfrytëzimi i fëmijëve për t'i joshur në biznese të paligjshme të tilla si prostitucionin e fëmijëve apo prodhimin e pornografisë së fëmijëve. Edhe pse praktika

gjyqësore në të gjithë botën ka një histori në vetvete heterogjene të shkelësve, abuzimi seksual në përgjithësi, fëmijëve u ndodh në duart e dikujt personalisht të afërt dhe të njohur edhe për atë fëmijë. Kështu, abuzimi paraprihet zakonisht nga "grooming".

*"Lojrat online"* janë një teknologji e përhapur në më tepër se një zhanër, një mekanizëm për lidhjen e lojtarëve nëpërmjet internetit. Lojrat *online* kanë aftësitë për të lidhur në lojëra shumë përdores interneti. Lojrat *online* kanë një avantazh se një përqindje e madhe e tyre nuk kërkojnë pagesë. Gjithashtu vlen të përmendet disponueshmëria e gjerë, shumëllojshmëri e lojërave për të gjitha llojet e lojës dhe për të gjitha moshat e lojtarëve.

*"Pedofilia online"* është në mënyrë të pashmangshme një thjeshtëzim i një realiteti që përfshin disa lloje të ndryshme të individëve: njerëz që shohin pornografinë e fëmijëve (*Voyeurs internet*); njerëzit që bëjnë dhe shpërndarjen e pornografisë së fëmijëve; abuzuesit seksual të fëmijëve të cilët e përdorin internetin për të arritur qëllimet e tyre (grabitqarët *online*); dhe pedofilët.

Të gjitha format e mësipërme kanë marrë zhvillim tejet të madh në vitet e fundit dhe kryesisht më të prekurit e këtyre formave janë fëmijët. Mbrojtja dhe respektimi i të drejtave të fëmijës, të konceptuara dhe sanksionuara si të drejta themelore të njeriut, qëndrojnë në esencë të legjislacionit tonë kushtetues dhe atij penal. Në kuptimin institucional, Policia e Shtetit përbën një nga institucionet kryesore të Shtetit Shqiptar, garantues, veç të tjerash edhe të së drejtave të fëmijëve dhe mbrojtjes së tyre. Si e tillë Polica e Shtetit ka një strukturë të specializuar për ndjekjen e krimeve kompjuterike në përgjithësi dhe për abuzimin/shfrytëzimin *online* të fëmijëve. Kjo strukturë është krijuar në vitin 2009 dhe ndjek veprat penale të klasifikuara si krime kibernetike. Ndër veprat penale që janë pjesë e punës së hetimit të krimit kompjuterik është edhe "Pornografia".

Rastet e abuzimit të fëmijëve *online* kanë karakteristika unike që i bëjnë ato të ndryshme nga llojet e tjera të rasteve. Për një numër arsyesh të listuara më poshtë, fëmijët bëjnë viktimat e "përsosura", dhe krimet që përfshijnë abuzimin *online* me fëmijë, abuzimin seksual në veçanti, janë ndër më të vështirat për t'u hetuar nga punonjësit e zbatimit të ligjit:

1. Fëmijët zakonisht nuk janë në gjendje për të mbrojtur veten e tyre, për shkak të nivelit të tyre të zhvillimit fizik dhe mendor; shpesh ata nuk kanë dëshirë të flasin për abuzimin. Ato mund të vonojnë në dhënien e informacioneve shpjeguese ose tregojnë vetëm një pjesë të tregimit.

2. Ka raste të shpeshta kur ekziston një lidhje emocionale midis fëmijës dhe abuzuesit me të; fëmijët mund të duan që të ndalojë abuzimi, por nuk duan që shkelësi të dënohet.

3. Krimet e abuzimit zakonisht nuk janë incidente të izoluara; përkundrazi, ato zhvillohen gjatë një periudhe kohore, shpesh me rritjen e ashpërsisë.

4. Në shumicën e rasteve të abuzimit seksual, nuk ka dëshmi përfundimtare mjekësore se abuzimi seksual ka ndodhur. Për më tepër, kjo ndodh në një vend privat pa dëshmitarë të ngjarjes.

5. Intervistat e fëmijëve kërkojnë trajtim të veçantë; çështje ligjore që rregullojnë dëshminë e fëmijëve janë të komplikuara dhe gjithnjë e në ndryshim, dhe fëmijët, viktima ose dëshmitarë qofshin, shpesh shihen si më pak të besueshëm apo kompetent se i akuzuari.

6. Rastet e abuzimit me fëmijë shpesh përfshijnë hetimet penale, dhe ndonjëherë hetimet administrative; gjithashtu duhet të kemi parasysh që nëpërmjet internetit mundësitë e abuzimit me fëmijë shpesh kalon linjat juridiksionale.

7. Sistemi i drejtësisë penale nuk është projektuar për të trajtuar nevojat e veçanta të fëmijëve.

Zyrtarët që merren me rastet e abuzimit me fëmijë duhet të jenë objektive dhe proaktiv në hetimet e tyre. Pyetjet të tilla në lidhje me kush, çfarë, ku, kur, si, dhe pse duhet të kenë përgjigje. Është e rëndësishme të kujtojmë se abuzimi me fëmijët është një krim dhe zbatimi i ligjit ka për detyrë ligjore dhe përgjegjësi të përgjigjet në përputhje me rrethanat.

Neni 117 i Kodit Penal të Republikës së Shqipërisë, parashikonte se:

"Prodhimi, shpërndarja, reklamimi, importimi, shitja e botimi i materialeve pornografike në ambientet e të miturve, përbëjnë kundërvajtje penale dhe dënohen me gjobë ose me burgim gjer në dy vjet.

*Përdorimi i të miturit për prodhimin e materialeve pornografike, si dhe shpërndarja ose publikimi i tyre në internet apo në forma të tjera, dënohet me burgim nga një deri në pesë vjet dhe megjobë nga një milion deri në pesë milionë lekë".*

Me ndryshimet e fundit të Kodit Penal, pikërisht me ligjin 144/2014, ashtu sikurse kërkohej dhe nga Konventa e Lanzarotit kjo dispozitë ka ndryshuar si më poshtë; "Neni 117" ndryshohet si do e shohim në vijim.

## 4. Pornografia

*Prodhimi, shpërndarja, reklamimi, importimi, shitja e botimi i materialeve pornografike në mjediset ku ka fëmijë, me çdo mjet ose formë, përbëjnë kundërvajtje penale dhe dënohen me burgim deri në dy vjet.*

*Prodhimi, importimi, ofrimi, vënia në dispozicion, shpërndarja, transmetimi, përdorimi ose posedimi i pornografisë së fëmijëve, si dhe krijimi i aksesit në mënyrë të vetëdijshme në të, me çdo mjet ose formë, dënohet me burgim nga tre deri në dhjetë vjet.*

Rekrutimi, përdorimi, shtrëngimi, ose bindja e një fëmije, për të marrë pjesë në shfaqje pornografike, ose marrja pjesë në shfaqje pornografike që përfshijnë fëmijët, dënohet me burgim nga pesë deri në dhjetë vjet".

Korniza ligjore ndërkombëtare, e pranuar dhe tashmë pjesë e sistemit tonë ligjor lidhur me fëmijët dhe mbrojtjen e tyre konsiston kryesisht në:

1. Konventa e OKB-së për të drejtat e fëmijëve.
2. Konventa e Këshillit të Europës të Budapestit për Krimin Kibernetik, ratifikuar me ligjin nr. 8888 viti 2002 "Për ratifikimin e konventës për krimin kibernetik".
3. Konventa e Këshillit të Europës të Lanzarotit "Për mbrojtjen e fëmijëve nga shfrytëzimi seksual dhe abuzimi seksual", ratifikuar me ligjin nr. 10071, datë 9.2.2009, të botuar në Fletoren Zyrtare nr. 21, datë 6 mars 2009, faqe 1353.

Në të njëjtën mënyrë, vlerësohet edhe rëndësia e dokumenteve të tjerë juridike ndërkombëtare që trajtojnë jo në mënyrë të posaçme të drejtat e fëmijëve. Për sa i përket kuadrit ligjor kombëtar që konturon punën dhe veprimtarinë e policisë së shtetit, duhet të theksojmë majën e piramidës ligjore në këtë kuadër, Kushtetutën, e cila në nenet 18, 21, 54/1, 54/2, 54/3, 320, 5, 13, 24, 22, 46 dhe 55 të saj ligjëron dhe i garanton çdo fëmije të drejta dhe liri themelore si, e drejta e jetës, e emrit, pasurore, për të mos u diskriminuar etj, si të drejtën e mbrojtjes nga shteti. Në të njëjtën linjë trajtohen edhe të drejtat dhe lehtësitë që parashikohen në Kodin Penal dhe në Kodin e Procedurës Penale.

Kur kemi të bëjmë me veprën penale të pornografisë *online*, me rëndësi paraqitet

identifikimi i viktimave nga ofruesit e shërbimeve. Kjo ka për qëllim verifikimin e viktimizimit dhe referimin për ndihmë në bazë të vlerësimit të përputhjes së nevojave të viktimës me shërbimet që ekzistojnë e mund të ofrohen. Në shumë raste është e pamundur të zotërohet informacioni paraprak për një person me të cilin do të kryhet një intervistë identifikuese. Pavarësisht nga kjo, personat apo strukturat që bëjnë identifikimin duhet të kenë së paku një informacion të përditësuar lidhur me prirjet e abuzimit *online* në vend, situatën aktuale të këtyre prirjeve, mënyrat e abuzimit *online* me të mitur nëpërmjet internetit.

Rastet e abuzimit/shfrytëzimit *online* të fëmijëve zakonisht përfshijnë akte në seri të dhunës shumëplanëshe, ku fëmijët e abuzuar përjetojnë dëmtime të ndërgjegjes, paaftësi për të menduar dhe vepruar, kanë ritëm të ulët të proceseve mendore dhe janë tejet të traumatizuar. Si rezultat i ndikimit të traumës, viktimat shfaqin pasiguri dhe dyshim ndaj ndihmës që iu ofrohet dhe reagojnë me zemërim ndaj atyre që mundohen t'i ndihmojnë. Në disa raste ata janë të ndërgjegjshëm se kanë kryer veprime të paligjshme dhe për këtë arsye kanë frikë të përballen me punonjësit e policisë. Në këto kushte procesi i intervistimit të tyre nuk është i lehtë dhe duhet realizuar me shumë profesionalizëm.

Veprimet e Policisë në këto raste duhet të përqendrohen tek:

- verifikimi i informacionit,
- kërkimi, gjetja e fëmijës dhe identifikimi,
- zhvillimi i intervistës dhe marrja e denoncimit nga viktima ose familjarë,
- marrje e deklarimeve nga persona që kanë dijeni për ngjarjen,
- bashkëpunimi ndërkombëtar, pasi vepra penale mund të jetë kryer jashtë kufijve juridiksionalë të Shqipërisë,
- gjetja e autorëve të dyshuar dhe shoqërimi i tyre në Polici,
- marrja në pyetje dhe fiksimi i shpjegimeve,
- verifikimi i thënieve e alibive dhe marrjen e deklarimeve nga shtetas të tjerë,
- marrje e dokumenteve si certifikatë e gjendjes civile, raporte mjekësore etj.,
- sigurimi i provave te ndryshme nëpërmjet akteve procedurale, përcaktimi i saktë i ISP (*internet service provide*) adresës unike të pajisjes së internetit nga e cila është kryer vepra penale, ekzaminimi kompjuterik i pajisjeve me të cilat është kryer vepra penale.

Hetimi i veprave penale të pornografisë *online* është tejet kompleks dhe në shumicën e rasteve përfshin edhe njësitë ligjzbatuese të shteteve të tjera. Por e rëndësishme është se punonjësit e policisë e konsiderojnë këtë lloj vepre shumë serioze pasi ajo prek shtresën e fëmijëve. Gjithsecili që është i përfshirë në luftën ndaj një kriminaliteti të tillë përfshin të gjitha aftësitë profesionale, personale dhe ligjore, për të vënë para përgjegjësisë autorët e këtyre veprave penale.

## 5. Parandalimi

Format e reja të abuzimit *online*, pedofilia *online*, grooming, *cyberbulling*, *sexting*, komunikimi *online* me përmbajtje seksuale, po shndërrohen në një fenomen të rrezikshëm, jo vetëm për të rinjtë, por edhe për të miturit. Ky fenomen si në gjithë botën, edhe në Shqipëri, paraqet një problematikë që shqetëson të gjithë aktorët e interesuar të shoqërisë shqiptare. Qeveria shqiptare duke njohur avantazhet dhe fuqinë transformuese dhe zhvilluese te internetit për shoqërinë shqiptare, penetrimin e shpejtë

të internetit edhe në zonat më të largëta, ka pasur dhe vazhdon të ketë nën fokus kryesor të punës rregullimin e politikave adekuate në këtë kudër.

Megjithatë avancimi i shpejtë i teknologjisë nënkupton edhe sfida, rritja e përdorimit të internetit nga fëmijët dhe të rinjtë si një mjet socializimi, edukimi dhe argëtimi sjell nevojën për rritje të sigurisë dhe përdorimin e përgjegjshëm të teknologjive *online*. Qeveria shqiptare është e angazhuar të transformojë internetin në një vend më të mirë dhe të sigurt për fëmijët dhe të rinjtë shqiptarë.

Rregullimi ligjor është aspekti i parë ku qeveria shqiptare ka fokusuar punën, përmendim këtu: ratifikimin e Konventës së Krimit Kibernetik, protokolleve shtesë të tij dhe reflektimin e këtyre angazhimeve të ndërmarra në legjislacionin e brendshëm konkretisht amendimet e Kodit të Procedurës Penale dhe Kodit Penal; Ratifikimin e Konventës për Mbrojtjen e të Drejtave të Fëmijëve; parashikimet e draft-strategjisë agjenda digjitale lidhur me masat mbrojtëse për internetin për fëmijët në shkolla, etj.

Ndërgjegjësimi dhe edukimi i mbarë shoqërisë shqiptare me një kulturë të re digjitale është thelbësore në arritjen e një niveli të mbarëpranuar shoqëror për përdorim të sigurtë të internetit. Kësisoj do të realizohet minimizimi i rreziqeve të shumta që teknologjia e komunikimit dhe informacionit mbartin.

Në këtë kuadër duhet të vazhdohet me ndërgjegjësimin e prindërve për rolin e tyre të pazëvendësueshëm dhe kujdesin prindëror në mjedisin *online*, rritja e vëmendjes të shkollës, industrisë, organizmave të tjerë jo qeveritarë etj.

Në këtë kuadër dhe në zbatim të VKM Nr. 182, datë 13.03.2013 "Plani i veprimit për fëmijë 2012- 2015", AKSHI ka punuar për inkurajimin dhe koordinimin e procesit të hartimit dhe miratimit të Kodit të Sjelljes: "Për përdorim të sigurt dhe të përgjegjshëm të rrjeteve të komunikimeve elektronike" nga operatorët që ofrojnë rrjete apo shërbime të komunikimeve elektronike në Shqipëri, ISP-të si dhe nga Shoqata AITA. Kodi i sjelljes si një praktikë vetërregullimi u nënshkrua nga kompanitë më të mëdha të komunikimeve elektronike në Shqipëri dhe shoqata e kompanive IT, AITA. Me nënshkrimin e këtij kodi kompanitë janë angazhuar për ofrimin e instrumenteve teknike të filtrimit si dhe për ofrimin e kështillimit prindëror, për mbrojtjen e fëmijëve dhe të rinjve nga përmbajtjet e paligjshme, të dëmshme në komunikimet elektronike.

Gjithashtu në vitin 2014, Agjencia Kombëtare për Shoqërinë e Informacionit (AKSHI) në koordinim me dhe institucione të tjera si, Ministria e Inovacionit dhe Administratës Publike (MIAP), Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT), Autoriteti i Komunikimeve Elektronike dhe Postare (AKEP), Komisioneri për Mbrojtjen e të Dhënave Personale (KMDP) dhe ISP-të zhvilluan takim për një internet më të mirë përmes një interneti më të sigurt. Gjatë këtij takimi u nënshkruan dy memorandume mirëkuptimi për bashkëpunim midis ALCIRT dhe AKEP dhe midis ALCIRT dhe KMDP.

Vlen të theksohet që edhe UNICEF në Shqipëri, ka një rol të rëndësishëm në koordinimin e të gjithë aktorëve për marrjen e nismave për krijimin e një mjedisi të sigurtë në internet për fëmijët dhe për parandalimin e ndodhjes së veprave të tilla.

## 6. Përfundime

Asnjë strukturë e vetme nuk ka trajnimin e plotë, fuqi punëtore, burime të mjaftueshme dhe mandat ligjor për të ndërhyrë në mënyrë efektive në rastet e abuzimit të fëmijëve, pra nuk mund të jetë përgjegjësi e vetme e një hallke për t'u marrë me

fëmijët e abuzuar. Kur një fëmijë është abuzuar *online*, grupi ideal për t'u marrë me rastin do ishte i përbërë nga: terapistët psikologë që këshillojnë fëmijët; shërbimet sociale që punojnë me fëmijën dhe familjen; policia që do arrestojë shkelësin; prokurorët që do ndjekin penalisht rastin, etj. Një ndërhyrje efektive do të ishte përmes formimit të një ekipi për mbrojtjen e fëmijëve, që do përfshinte profesionistë nga policia, drejtësia penale, puna sociale, arsimi, institucione shtetërore dhe partnerë që punojnë dhe kujdesen për sigurinë *online* të fëmijëve. Anëtarët e këtij ekipi duhet të kuptojnë dhe të vlerësojnë rolet e ndryshme, përgjegjësitë, pikat e forta, dobësitë e tyre, për të bashkëpunuar dhe koordinuar përpjekjet e tyre për t'ju ofruar fëmijëve një internet të sigurt. Aftësitë e secilës hallkë janë parë si të ndryshme, por janë po aq të rëndësishme. Roli i zbatimit të ligjit në rastet e abuzimit të fëmijëve është që të hetojë për të përcaktuar nëse një shkelje e ligjit penal ka ndodhur, identifikimin dhe kapjen shkelësit, dhe të bëje padinë përkatëse penale.

Në shtete të ndryshme janë ngritur *Qendra Kombëtare për të Luftuar Pornografinë online* me fëmijë. Roli i tyre është të kryejnë dhe koordinojnë të gjitha hetimet dhe veprimtaritë parandaluese në lidhje me abuzimin e fëmijëve *online*. Këto lloj qendrash përditësojnë rregullisht *listën e zezë* të faqeve të pornografisë me fëmijë, duke ofruar gjithashtu:

- monitorim 24 orë,
- pritje dhe njoftim,
- vënia në listën e zezë dhe filtrimi,
- marrëdhëniet me inst. financiare,
- analizimi i pamjeve,
- koordinimi i hetimeve,
- bashkëpunimi ndërkombëtar.

*Parandalimi dhe reagimi* konkret dhe i shpejtë ndaj veprave penale të abuzimit *online* do të mbështetej në tre shtylla kryesore:

- qasje sinergjike = partneriteti publik-privat = siguri e përbashkët,
- ndarja dhe qarkullimi i të dhënave dhe informacionit,
- përfshirja e agjencive të specializuara të zbatimit të ligjit.

*Sidomos*, krijimi i një *task force publike-private* dhe, ndarja e qarkullimi i të dhënave dhe informacionit, me qëllim parandalimin dhe luftën kundër krimit dhe garantimin e politikave të duhura të sigurisë.

Së fundmi, në përballjen me sfidat e reja të krimit kompjuterik, strukturat e hetimit të krimit kompjuterik duhet të veprojnë në bashkëpunim dhe koordinim të vazhdueshëm me të gjithë aktorët e shoqërisë që mund të ndihmojnë në krijimin e një mjedisi të sigurt për fëmijët që janë e ardhmja e kombit.

## Bibliografia


1. Veton Vula, Mensut Ademi, *Krimi Kompjuterik.*
2. Luljeta Ismajlukaj, Arben Zela, *Manual për punonjësit e Policisë, për mbrojtjen e fëmijëve nga abuzimi dhe shfrytëzimi nëpërmjet internetit,* Tiranë: CRCA Shqipëri, 2016.

# Kërcënimet kibernetike, ndikimi dhe shpërndarja e tyre, në institucionet shtetërore, në Shqipëri

**Dr. (proc.) Kozeta LIGEJA**
*Universiteti i Tiranës*
*k.oz.i2006@hotmail.com*

**Abstrakt**

*Shqipëria renditet ndër vendet ku zhvillimi i telekomunikacionit, qasja në internet dhe informatizimi i shoqërisë përparon shumë shpejt. Rritja e përdorimit të komunikimit përbën një vlerë të shtuar në zhvillimin ekonomik dhe shoqëror të vendit, por, në të njëjtën kohë, ajo e ekspozon atë ndaj rreziqeve të natyrës kibernetike me aktorë shtetërorë dhe jo shtetërorë. Sulmet kibernetike kanë potencial për të dëmtuar rëndë shkëmbimin e informacionit në institucionet publike, të telekomunikacionit dhe sistemin financiar e bankar, duke shkaktuar edhe ndërprerje të shërbimeve jetike. Qëllimi i këtij punimi është të vërtetojë nëpërmjet provave, kryesisht të analizës teorike, por edhe asaj praktike se Shqipëria si shoqëri përjeton problematika nga sulmet kibernetike. Punimi do të mbështetet mbi disa metoda studimore. Do të përdoret kryesisht metoda induktive, duke kaluar nga fakte të veçanta në përfundime të përgjithshme, por edhe ajo deduktive duke kaluar nga konkluzione të përgjithshme për të nxjerrë përfundime për pasojat e ardhura dhe problemet e veçanta. Nëpërmjet analizës së rasteve të veçanta në Shqipëri, të cilat kanë adresuar çështje specifike me rëndësi për zhvillimin e punimit.*

**Fjalëkyçe:**
**kërcënime kibernetike, institucione shtetërore, sulme kibernetike, ndikim kibernetike.**

## 1. Hyrje

Deri më sot njerëzimi ka njohur sistemin më të madh të krijuar prej tij, internetin, që realizohet përmes lidhjeve të ndryshme komunikuese, apo shumë përdorues të tij që përdorin tableta, *laptop*, telefona të markave të specializuara. Aktualisht, vihet re që ky sistem është kthyer në trend. Duke iu referuar statistikave botërore, kryesisht viteve 2000-2014, ka një rritje të përdorimit të internetit me 741%. Ndërsa, sipas shkencëtarëve të shkencave elektronike, rreth vitit 2020 do jenë afërsisht 26 miliardë pajisje në internet. Por, krahas rritjes me galop të përdorimit të internetit, dalin në pah problematikat lidhur me sigurinë dhe privatësinë e tij, të cilat sjellin shqetësime kryesore.

Ne jetojmë në një botë të globalizuar, si rrjedhojë edhe zhvillimi i internetit përbën një nga shtyllat kryesore të ekonomisë shtetërore, duke sjellë inovacion dhe konkurrencë ndërmjet politikave shtetërore në mbarë botën. Interneti me gamën e madhe të aktiviteteve të tij, po fiton shumë terren në progresin e zhvillimit. Është krijuar kaq shumë liri në internet, sa që është krijuar mundësia për abuzime dhe aktivitete keqdashëse. Në këtë drejtim janë institucionet qeveritare, ato që luajnë një rol kryesor rreth këtyre aktiviteteve. Pra janë këto qeveri, që më politikat dhe udhëzimet e tyre përcaktojnë jo vetëm hapësirën e qytetarit në internet, por edhe sigurinë e hapësirës kibernetike. Tashmë administrimi, sigurimi i shërbimeve publike, mbështeten në integritetin e hapësirës kibernetike, te infrastruktura dhe të dhënat që e mbështesin atë.

## 2. Terminologjia[1]

*Siguria në hapësirën kibernetike:* një sërë projektesh organizative, ligjore, teknike,

[1] Strategjia Kombëtare për mbrojtjen Kibernetike 2018-2020, Ministria e Mbrojtjes.

fizike dhe arsimore që synojnë sigurimin e funksionimit të pandërprerë të sigurisë kibernetike.

*Abuzimi:* përdoret nga siguria e sistemeve TIK, e cila menaxhon incidentet e sigurisë kompjuterike, si dhe shqyrton ankesat të cilat vijnë për abuzimet në rrjetet kompjuterike.

*Ekipi i reagimit emergjent*, "Computer Emergency Response Team" (CERT): ekip i krijuar për t'iu përgjigjur ndërhyrjeve në rrjet, të cilat synojnë të shkelin sigurinë kompjuterike.

*Sulm kibernetik:* do të quajmë një sulm të qëllimshëm në sistemet kompjuterike, si dhe ndërmarrjeve të cilat kanë akses në internet.

*Krimi kibernetik:* krimi kibernetik është përcaktuar si një krim në të cilin një kompjuter është objekt i krimit (*hacking, phishing, spamming*) ose përdoret si një mjet për të kryer një vepër penale. Kriminelët kibernetikë mund të përdorin teknologjinë kompjuterike për të pasur akses në të dhënat personale ose përdorin internetin për qëllime shfrytëzuese ose keqdashëse.

*Hapësira kibernetike:* i referohet botës kompjuterike virtuale, dhe më konkretisht, është një rrjet i madh kompjuterësh i përbërë nga shumë rrjete kompjuterike në mbarë botën, që përdorin protokollin TCP/IP, për të ndihmuar në komunikimin dhe aktivitetet e shkëmbimit së të dhënave.

*Terrorizmi kibernetik:* përdorimi i internetit për të kryer veprime të dhunshme, që rezultojnë ose kërcënojnë humbje të jetës, ose dëmtime të rënda trupore, me qëllim që të arrihen përfitime politike përmes frikësimit. Gjithashtu, konsiderohet një akt terrorizmi në internet ku aktivitetet terroriste, duke përfshirë akte të ndërprerjes së qëllimshme dhe të përhapur të rrjeteve kompjuterike, veçanërisht të kompjuterëve personalë të bashkangjitur në internet me anë të mjeteve të tilla, si viruset kompjuterike, viruset kompjuterike apo skripte të tjera të përdorura me qëllim të keq.

*Incident kompjuterik:* është një ngjarje e sigurisë kibernetike, gjatë së cilës shkaktohet cenimi i sigurisë së shërbimeve ose sistemeve të informacionit e të rrjeteve të komunikimit që sjell një efekt real negativ. Infrastrukturë e rëndësishme e informacionit: Është tërësia e rrjeteve dhe sistemeve të informacionit të zotëruara nga një autoritet publik, i cili nuk është pjesë e infrastrukturës kritike të informacionit, por që mund të rrezikojë apo të kufizojë, punën e administratës publike, në rastin e cenimit të sigurisë së informacionit.

*Infrastrukturë kritike e informacionit:* është tërësia e rrjeteve dhe sistemeve të informacionit, cenimi apo shkatërrimi i të cilave do të kishte ndikim serioz në shëndetin, sigurinë dhe/ose mirëqenien ekonomike të qytetarëve, dhe/ose funksionimin efektiv të ekonomisë në Republikën e Shqipërisë.

*Rrezik i sigurisë kibernetike:* është një rrethanë ose një ngjarje e identifikueshme në mënyrë të arsyeshme, e cila mund të shkaktojë cenimin e sigurisë së shërbimeve ose sistemeve të informacionit dhe të rrjeteve të komunikimit.

*Spiunazh kibernetik*: konsiderohet sulmi kibernetik që ka si objekt të tij cenimin e konfidencialitetit të një sistemi TIK.

*Sabotazh kibernetik:* konsiderohet sulmi kibernetik që ka si objekt të tij cenimin e integritetit dhe disponueshmërisë së një sistemi TIK[2].

[2] Po aty.

[3] http://www.gsh.al/2018/07/09/krimi-kibernetik

## 3. Vështrim rreth krimit kibernetik në Shqipëri

Krimi kibernetik[3] është çdo veprim kriminal që përfshin një kompjuter, një pajisje të rrjetëzuar ose një rrjet. Ndërsa shumica e viruseve kibernetike janë kryer në mënyrë që të gjenerojnë fitim për kriminelët, disa krime kibernetike janë kryer kundër kompjuterëve ose pajisjeve direkt për të dëmtuar ose çaktivizuar ato, ndërsa të tjerët përdorin kompjuterë ose rrjete për të përhapur informacion të paligjshëm, imazhe apo materiale të tjera

Fenomeni i krimit kibernetik është bërë gjithnjë e më shqetësues. Këto sulme kibernetike kanë për qëllim që duke u future në sistemet kompjuterike qëndrojnë sa më shumë të jetë mundur pa u vënë re. Qëllimi është që të marrin të dhënat personale si p.sh., informacione sekrete, kartat e identitetit, materiale poseduese si një fotografi me qëllim kryerjen e transaksioneve të paligjshme, gjasat janë që të mos dyshohet aspak rreth të qenit personi të cilit i janë marrë të dhënat personale. Në këtë mënyrë, një viktimë ka pasoja të ndryshme, si, monetare, apo mund të ketë probleme me procedimin penal. Në këtë mënyrë lind pyetja: a ka Shqipëria kapacitetet e duhura për ta luftuar krimin kibernetik? Vendi ynë nuk ka shumë burime njerëzore dhe teknologji të avancuar për të luftuar krimin kibernetik, me qëllim sigurimin e mbrojtjes së qytetarëve. Mbrojtja ndaj krimit kibernetik kërkon një impenjim më të lartë nga të gjitha organizmat shtetërorë njëkohësisht edhe privatë duke i dhënë dhe rëndësi edhe qytetarëve si përdorues që kanë qasje në internet. Në këtë kuadër më preokupim madhor tregojnë kompanitë e mëdha private që respektojnë ligjin për mbrojtjen e të dhënave të tyre dhe të dhënave të klientëve. Duhet theksuar se Shqipëria po ecën pozitivisht në mbrojtjen nga krimi kibernetik. Kjo vihet re nga ndërgjegjësimi që kanë bërë strukturat shtetërore si Prokuroria e Përgjithshme. Kjo instancë ka ngritur në vitet 2014 strukturat e duhura të posaçme në 8 prokuroritë e vendit njëkohësisht edhe Prokuroria e Krimeve të Rënda që do të ndjekin këto lloj krimesh.

Konventa e Budapestit është bosht orientues trajtimin e krimit kompjuterik, që zhvillohet nga prokuroria shqiptare. Veprat penale përfshijnë jo vetëm veprimet me kompjuterë, por edhe krimet që lidhen me ndërhyrjen në të dhëna personale kryesisht në rrjetet sociale si edhe në rrjetet e gjëra teknologjike.

Meqenëse krimi kibernetik përbën rrezikshmëri të lartë për shoqërinë, është konsideruar një krim i mirëfilltë dhe i nënshtrohet ligjit shqiptar. Kryesisht mund të përmendim disa vepra penale që kanë objekt krimin kibernetik; ato janë[4]:

"Strategjia ndërsektoriale për shoqërinë e informacionit, 2008-2013" (SNSHI) e miratuar me VKM nr. 59 dt. 21.1.2009 përveçse përbën dokumentin strategjik që përcaktonte drejtimet kryesore dhe objektivat e zhvillimit në fushën e shoqërisë së informacionit për periudhën 2008-2013 ishte edhe dokumenti i vetëm ku përmendej shkurtimisht siguria kibernetike si një nga fushat që duhej konsideruar me prioritet për shkak të vizionit të qeverisë shqiptare për të rritur e zhvilluar e qeverisjen përmes ofrimit të e-shërbimeve[5].

Në zbatim të "Strategjisë ndërsektoriale për shoqërinë e informacionit, 2008-2013"

[2] Po aty.
[3] http://www.gsh.al/2018/07/09/krimi-kibernetik
[4] http://www.gazetadita.al/hetimi-kibernetik-dhe-ne-shqiperi-ja-veprat-penale-qe-perbejne-krim/
[5] Dokumenti i Politikave për Sigurinë Kibernetike 2015 - 2017

(SNSHI), Agjencia Kombëtare e Shoqërisë së Informacionit, ka ofruar:

1) vërtetim dhe identifikim të sigurt, për 25 institucione, 2500 përdorues;

2) internet të sigurt, për 65 institucione;

3) instalim automatik dhe qendror të aplikimeve; 2000 kompjuterë të ministrive që janë në *domain*;

4) menaxhim qendror i mbrojtjes antivirus, 7 institucione, 1000 kompjuterë;

5) *E-signature* përmes "Infrastrukturës qeveritare të çelësit publik" (PKI), – 2 institucione; 6) përdorimi i teknologjisë së informacionit dhe komunikimit është rritur ndjeshëm në vitet e fundit.

Nga të dhënat zyrtare të Policisë së Shtetit mbi krimin kibernetik, të rregulluar sipas Kodit Penal të Republikës së Shqipërisë, rezultojnë se në periudhën janar-dhjetor 2014 janë evidentuar 180 vepra penale, janë zbuluar 76, me 86 autorë, nga të cilët 74 janë në gjendje të lirë, 10 të arrestuar dhe 2 në kërkim. Për periudhën janar-dhjetor 2013, janë evidentuar 108 vepra penale nga të cilat janë zbuluar 63 prej tyre, me 69 autorë, nga të cilët 58 janë në gjendje të lirë, 9 arrestuar dhe 2 në kërkim[6].

Të ndara sipas veprave penale ato paraqiten si më poshtë:

- neni 119/a, "Shpërndarja e materialeve raciste ose ksenofobike nëpërmjet sistemit; kompjuterik", evidentuar 1 rast, pa autor;

- neni 143/b, "Mashtrimi kompjuterik", evidentuar 49 raste, me 14 autorë në gjendje të lirë, 8 arrestuar;

- neni 186/a, "Falsifikim kompjuterik", evidentuar 28 raste, me 20 autor, nga të cilët 4 arrestuar dhe 16 në gjendje të lirë;

- neni 192/b, "Hyrja e paautorizuar kompjuterike", evidentuar 14 raste, me 7 autorë në gjendje të lirë;

- neni 293/a, "Përgjimi i paligjshëm i të dhënave kompjuterike", evidentuar 1 rast me 2 autorë, në gjendje të lirë;

- neni 293/b, "Ndërhyrja në të dhënat kompjuterike", evidentuar 33 raste me 16 autorë, nga të cilët 2 të arrestuar dhe 14 në gjendje të lirë;

- neni 293/c, "Ndërhyrja në sistemet kompjuterike", evidentuar 4 raste, me 3 autorë në gjendje të lirë;

- neni 121 "Ndërhyrje të padrejta në jetën private", 4 raste, pa autor;

- neni 117, paragrafi i tretë, "Pornografia", evidentuar 38 raste me 14 autorë në gjendje të lirë;

- neni 121/a "Përndjekja", evidentuar 4 vepër penale, zbuluar 3, me 2 autorë të proceduar në gjendje të lirë, 1 i arrestuar;

- neni 137/a "Vjedhja e rrjetit të komunikimeve elektronike", evidentuar 1 vepër penale, zbuluar 1, me 1 autor në gjendje të lirë;

- neni 149/a "Shkelja e të drejtave të pronësisë industriale", evidentuar 1 vepër penale, zbuluar 1, me 1 autor i cili është proceduar në gjendje të lirë. Shpifja e parashikuar nga neni 120 i Kodit Penal, evidentuar 1 rast me 1 autor në gjendje të lirë.

## 4. Kuadri ligjor dhe institucional në Shqipëri

Zhvillimi i shpejtë i TIK kushtëzohet dhe nga përshtatja e legjislacionit përkatës të nevojshëm. Në përgjithësi Shqipëria është në pajtueshmëri me detyrimet që rrjedhin

[6] Po aty.

nga MSA-ja në këtë fushë. Ka disa ligje që rregullojnë ndjekjen penale të krimeve kompjuterike në Republikën e Shqipërisë si:

Ligji nr. 8888 i datës 25.4.2002 "Për ratifikimin e konventës për krimin kibernetik" është reflektuar në Kodin Penal si dhe ligji nr. 9262 i datës 29.7.2004 "Për ratifikimin e protokollit shtesë të konventës për krimin kibernetik, për penalizimin e akteve me natyrë raciste dhe ksenofobe të kryera nëpërmjet sistemeve kompjuterike" sërish është reflektuar në Kodin Penal përkatësisht në ligjin nr. 9859, datë 21.1.2008 "Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995", "Kodi Penal i RSh" dhe ligji nr. 10023, datë 27.11.2008, për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995 "Kodi Penal i Republikës së Shqipërisë; dhe ligji nr. 10054, datë 29.12.2008, "Për disa shtesa dhe ndryshime në ligjin nr. 7905, datë 21.3.1995"[7].

### *4.1 Kuadri ligjor i strukturave qeveritare që merren me sigurinë dhe krimin kibernetik në Shqipëri* [8]

*Agjencia Kombëtare për Sigurinë Kompjuterike* (ALCIRT), është autoriteti qendror për identifikimin, parashikimin dhe marrjen e masave për mbrojtjen ndaj kërcënimeve/ sulmeve kompjuterike, në përputhje me legjislacionin në fuqi.

*Drejtoria e Sigurimit të Informacionit të Klasifikuar* (DSIK), është autoriteti që kontrollon, garanton sigurinë e sistemeve të klasifikuara të komunikimit dhe informacionit dhe bën akreditimin e tyre nëpërmjet lëshimit të *Certifikatës së Sigurisë* për këto të fundit.

*Autoriteti Kombëtar për Certifikimin Elektronik* (AKCE), është autoriteti që ka përgjegjësinë e mbikëqyrjes së zbatimit të ligjit "Për nënshkrimin elektronik" dhe të akteve nënligjore, të nxjerra në zbatim të tij. AKCE bën akreditimin e ofruesve të shërbimit të certifikimit elektronik.

*Agjencia Kombëtare e Shoqërisë së Informacionit* (AKSHI), është përgjegjëse për administrimin e infrastrukturës qeveritare të *Çelësit Publik* (PKI) dhe siguron, pajtueshmërinë me nenin 19 të ligjit nr. 9880, datë 25.2.2008 "Për nënshkrimin elektronik". Në shërbimet që ofron në *Qendrën e të Dhënave Qeveritare*, për administratën publike, garanton vërtetësinë dhe identifikimin e sigurt, internet të sigurt dhe DNS të sigurt.

*Policia e Shtetit*, është organi përgjegjës për parandalimin, zbulimin dhe hetimin e veprave penale, ndër të cilat përfshihen dhe veprat penale në fushën e TIK, që ndiqen nga sektori i kundër krimit kompjuterik.

*Prokuroria e Përgjithshme*, përmes sektorit të krimeve kibernetike ushtron ndjekjen penale për vepra penale në fushën e kibernetikës. Kjo strukturë kontrollon aktivitetin e njësive të posaçme për ndjekjen e krimeve kibernetike, që janë ngritur në prokuroritë e rretheve gjyqësore.

*Shërbimi Informativ i Shtetit* (SHISH), përmes seksionit të kundër krimit kibernetik, ka për detyrë kërkimin, zbulimin dhe analizimin e krimeve kibernetike që cenojnë sigurinë kombëtare.

*Ministria e Mbrojtjes*, ka rol në ruajtjen e sigurisë kibernetike përmes drejtorisë së automatizimit dhe inovacionit, por edhe institucioneve të përmendura më poshtë në varësi të ministrit të Mbrojtjes (DSH dhe AISM).

[7] Për ndryshime të mëtejshme ne Kodin Penal, referoju Ligjit nr. 144/2013 "Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995 "Kodi Penal i Republikës së Shqipërisë", të ndryshuar.

[8] Dokumenti i Politikave për Sigurinë Kibernetike 2015 – 2017.

*Shtabi i Përgjithshëm i Forcave të Armatosura të Republikës së Shqipërisë*, drejtoria e ndërlidhjes, përgjigjet për zhvillimin e sistemeve të ndërlidhjes dhe të informacionit (SNI) në Forcat e Armatosura të Republikës së Shqipërisë, duke u mbështetur në standardet kombëtare, të NATO-s dhe ato ndërkombëtare.

*Drejtoria e Shifrës* (DSH), është autoriteti kombëtar për sigurimin e komunikimeve dhe autoritet kombëtar i shpërndarjes.

*Agjencia e Inteligjencës së Mbrojtjes dhe Sigurisë* (AISM), përmes sektorit të mbrojtjes kibernetike dhe *infosec* ka si detyrë parashikimin, identifikimin dhe analizimin e kërcënimeve kibernetike që cenojnë sistemet TIK të FASH.

*Banka e Shqipërisë* (BSH), ka autoritetin e organit që ka të drejtën ekskluzive të japë[9] miratimin për fillimin e aktivitetit bankar nëpërmjet dhënies së licencës, si dhe të mbikëqyrë aktivitetin e çdo subjekti, i cili ka marrë licencë për ushtrimin e veprimtarisë bankare në Republikën e Shqipërisë. Në fushën e sigurisë së sistemeve të tij TIK, subjekti përcakton objektiva, strategji dhe kërkesa të sigurisë si dhe miraton procedura për administrimin, për operimin, për ruajtjen e sistemeve, për mbrojtjen e të dhënave si edhe për nxjerrjen jashtë përdorimit te tyre.

*Autoriteti i Komunikimeve Elektronike dhe Postare* (AKEP), mbikëqyr, kontrollon dhe monitoron, veprimtaritë e sipërmarrësve të rrjeteve të komunikimeve elektronike dhe të shërbimeve të komunikimeve të elektronike. AKEP-i, mbikëqyr zbatimin e masave të nevojshme, të ndërmarra nga sipërmarrësit, mbi sigurinë dhe integritetin e shërbimeve dhe rrjeteve të komunikimeve elektronike publike, në lidhje me mbrojtjen e të dhënave personale.

*Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale* (IDP), është autoriteti përgjegjës, i pavarur, që mbikëqyr dhe monitoron, në përputhje me ligjin, mbrojtjen e të dhënave personale elektronike gjatë ruajtjes, përpunimit dhe transmetimit të tyre, duke respektuar e garantuar të drejtat dhe liritë themelore të njeriut.

### *4.2 Institucione të tjera mbështetëse në arritjen e objektivave të Dokumentit*

*Shkolla Shqiptare e Administratës Publike* (ASPA), është organi që ka si detyrë formimin, trajnimin profesional të nëpunësve të administratës të cilat fokusohen në ngritjen e kapaciteteve menaxhuese të qëndrueshme; rritjen e përgjegjshmërisë së punonjësve të administratës; krijimin e një trupe funksionarësh publikë profesionistë, të paanshëm dhe eficentë në kryerjen e funksioneve të tyre. Ky institucion do të ofrojë ndihmë për organizimin e trajnimeve për profesionistët IT të administratës publike.

*Instituti i Zhvillimit të Arsimit* (IZHA), është institucioni që ka si detyrë hartimin e kurrikulës së TIK-ut për arsimin parauniversitar (k-12), e cila përmban tematika shumë të rëndësishme, të fushës së sigurisë kibernetike, përmbajtja e të cilave konsiston në përdorimin e sigurt të internetit nga nxënësit dhe mësuesit. Në bazë të VKM nr. 303, datë 31.3.2011 "Për krijimin e njësive të teknologjisë së informacionit e të komunikimit në ministritë e linjës dhe institucionet e varësisë" çdo institucion ka drejtori TI, e cila është përgjegjëse për sigurinë në sistemet e TIK dhe në këtë kuadër ka edhe përgjegjësi për sigurinë kibernetike.

## 5. Përfundime dhe rekomandime

Globalisht fenomeni i sulmeve kibernetike ka pasoja të rënda për të dhënat personale,

institucionet dhe me gjerë. Shqipëria nuk i ka kapacitete e duhura, si burimet dhe teknologjinë, për të marrë masat e duhura në mënyrë maksimale rreth këtij fenomeni mbarëkombëtar. Ajo që rekomandohet, është:

1) Qeveria të ndërmarrë iniciativa dhe të hartojë programe për edukimin dhe ndërgjegjësimin e përdoruesve të TIK. Këto programe do përfshijnë të gjithë nivelet e administratës publike si: specialistët IT, administratorët e sistemeve dhe TIK, etj. Ky proces do të garantojë përdorimin, ngritjen dhe ofrimin e shërbimeve digjitale të administratës në mënyrë të sigurt dhe të besueshme.

2) Shpërndarja dhe publikimi i informacionit mbi rreziqet e hapësirës kibernetike, nxjerrja e udhëzimeve dhe këshillave për një siguri minimale do jetë një proces i vazhdueshëm nëpërmjet të cilit do synohet të rritet ndërgjegjësimi dhe siguria e përdoruesve të thjeshtë. Përveç publikimit të tyre në faqet zyrtare të internetit të institucioneve të specializuara do bashkëpunohet në mënyrë të ngushtë me medien për të siguruar një informim sa më të gjerë dhe të shpejtë të publikut.

3) Rekomandohet që në sistemin arsimor, në nivelet e arsimit parauniversitar dhe atij universitar, të realizohen fushata vlerësuese për futjen e programeve edukative dhe fushatave të informimit rreth informatikës.

## Bibliografia


1. Chang, Lennon Y.C., & Grabosky, P. (2014) "Cybercrime and establishing a secure cyber World", in M. Gill (ed) Handbook of Security (pp. 321–339). NY: Palgrave.
2. Dokumenti i Politikave për Sigurinë Kibernetike 2015 - 2017
3. *Mohanta, Abhijit (6 December 2014). "Latest Sony Pictures Breach : A Deadly Cyber Extortion". Retrieved20 September 2015.*
4. Steve Morgan (January 17, 2016). "Cyber Crime Costs Projected To Reach $2 Trillion by 2019". *Forbes*. Retrieved September 22, 2016.
5. Warren G. Kruse, Jay G. Heiser (2002). *Computer forensics: incident response essentials*. Addison-Wesley.

# Pastrimi i parave në krimin kibernetik

■**Dr. Oreta SALIAJ**
*Kolegji ISPE, Prishtinë*
*saliajoreta@gmail.com*

■**MSc. Vehbi MORINA**
*Kolegji ISPE, Prishtinë*

**Abstrakt**

*Shumë nga hakerët kanë në plan të parë pasionin ose përfitimin, varësisht nga lloji i hakerit dhe natyra e tij e punës. Kur hakeri ka si qëllim përfitimin, atëherë në radhë të parë, ka për të gjetur rrugë më të lehta për të kryer transaksione komplekse, për pasojë, pastrimin e parave të fituara nga veprimtaria e tij kriminale, i ndihmuar edhe nga krimi kibernetik. Duke ditur se Shqipërinë, shpeshherë e gjejmë në raporte ndërkombëtare për krimin e organizuar dhe pastrimin e parave të pista, mendojmë se trajtimi i kësaj teme do të ishte një indice për shtetin, për të qenë më vigjilent në transaksionet në internet e për të minimizuar sa më shumë nivelin e pastrimit të parave, meqenëse pastrimi parave në nivel global, kalon disa miliarda euro ndër vite. Pra, duke ditur se në Shqipëri ekzistojnë grupe të ndryshme kriminale, ato grupe fare lehtë mund të bashkëpunojnë me hakerët, për realizimin e një morie transaksionesh ndërkombëtare komplekse. A ka mundësi të hetimit Shqipëria në raport me kriptovalutat e me teknologjinë block-chain të hetimit të pastrimit të parave? Ky punim do të analizojë e këqyrë disa forma të pastrimit të parave në internet, ndihmuar nga krimi kibenerik, si rrezik për ekonominë e vendit, pastrimin e parave, evazion fiskal etj.*

**Fjalëkyçe:**
**kriminalitet, interneti, pastrim parash, kriptovaluta, transaksione.**

## 1. Hyrje

Sot jetojmë në një shekull ku përveç parasë fizike, në treg gjejmë jo rrallëherë edhe vlera të ndryshme të parasë virtuale apo kriptovaluta të emëruara si *token* apo *koinsa*. Kush do t'i kishte menduar këto forma valute në vitet '90 apo në vitet 2000? Duke u nisur nga fakti që Kosova, por edhe Shqipëria, janë dy vende që shpeshherë i gjejmë në raportet e ndryshme ndërkombëtare për nivelin e lartë të kriminalitetit si dhe për përfshirjen e tyre në rrjetin e trafikimit me emigrant, droga, armë, mallra etj. Veç këtyre formash të kriminalitetit, sot pothuajse e gjithë bota është e kërcënuar nga kriminaliteti kibernetik falë zhvillimit të hovshëm të teknologjisë si dhe ndikimit të madh të teknologjisë në zhvillimin ekonomik si dhe avancimet profesionale të njerëzimit.

Kur kemi të bëjmë me kalimin e mallrave, ilegalisht në kufijtë e shtetit tonë, themi se personi po kryen vepër penale "kontrabandë me mallra apo narkotik", varësisht nga produkti qe i dyshuari kontrabandon. Por, lind pyetja: sa ueb-sajte vendore ndërkombëtare e kombëtare operojnë mbi hapësirat e shtetit tonë? Sa informata, sa materiale, sa dosje, sa ueb-sajte pornografike, sa ueb-sajte të lojërave të fatit, kazino, basteve *online,* operojnë në shtetin tonë? Lind pyetja: si tatohen ato? Sa përfiton shteti nga ato? Sa humb shteti nga ato? Sa qytetarë bien viktima nga e shteti ynë, e në fund fare, kush e bën rimbursimin dhe zhdëmtimin e tyre, qoftë moral, apo edhe financiar?

Por, nuk ka vetëm kaq. Kriminaliteti kibernetik, nga natyra e vet punës së tij, është kompleks dhe hetimi i këtij lloj kriminaliteti është tepër kompleks e kërkon kohë. Bazuar në praktikat e shkuara të këtij lloj hetim krimi dhe zbulimit të tij, shpeshherë kërkohet edhe ndihma juridike nga shtet tjetër ose nga disa shtete. A mendoni se sa transaksione mund të realizojnë një haker brenda disa bankave dhe disa shteteve? Ju mund të thoni se kjo është e lehtë, sepse kriminaliteti ekonomik ndjek lëvizjen e parasë,

por këto hetime mund t'ua vështirësojë shteti ku është kryer vepra, pasi nuk ju jep informacione; në disa shtete ajo mundet të mos cilësohet fare si vepër penale, sepse e dimë që ka shtete të dobëta, që njihen për parajsa fiskale.

Duke ditur rëndësinë e këtij krimi dhe zhvillimin e hovshëm të krimit kibernetik, do të trajtojmë në vazhdim, vetëm çështjen e pastrimit të parave ndihmuar nga hakerët dhe realizuar vetëm me anë të internetit, duke realizuar transaksione komplekse, për t'i hetuar organet e hetuesisë të cilitdo shteti në botë. Në këtë punim do të aplikohet metodologjia kibernetike e hulumtimit, bazuar në të dhënat dhe hulumtimet kombëtare dhe ndërkombëtare. Ndërsa për literaturë, do të përdorim libra e punime shkencore, hulumtime nga organet e rendit si dhe studiues të ndryshëm të kësaj fushe.

## 2. Pastrimi parave koncepti i përgjithshëm

Fillimisht do t'i hedhim një vështrim të përgjithshëm konceptit të pastrimit të parave, bazuar në literaturë nga autorë të ndryshëm si në legjislacionin shqiptar dhe atë të Kosovës. Grupet kriminale, në veçanti ato të krimit të organizuar, gjatë veprimtarisë së tyre kriminale, si rezultat kanë përfitime që vijnë nga burime ilegale. Kur themi se kemi të bëjmë me burime ilegale financiare, është e natyrshme që ato grupe të gjejnë rrugë e forma nga më të avancuarat për t'i shndërruar ato para në legale. Prandaj, mbi bazën e kësaj ideje, pastrimi parave është i domosdoshëm. Kur kemi në fokus hakerët dhe realizimet e tyre financiare në rrugët kibernetike, duhet thënë se ata, si plan të dytë të veprimit kanë gjetjen e hapësirave juridike dhe liritë e lëvizjes së parasë për t'ju shmangur kontrolleve të sigurisë së shtetit.

Pra, pastrimi i parave është procesi i fshehjes së burimeve ilegale së hyrjeve, i realizuar nëpërmjet veprave penale, me qëllim të futjes së këtyre të ardhurave në rrjedhat e biznesit legal financiar[1]. Me termin "pastrimi i parave" nënkuptohet posedimi, fitimi, këmbimi, bartja ose shfrytëzimi i pasurisë, e cila është krijuar me veprime kriminale ose me pjesëmarrje personale në këso veprimesh, me qëllim të fshehjes së pasurisë me prejardhje të kundërligjshme, ose me ofrimin e ndihmës ndaj ndonjë personi që është përzier në veprimtari të tilla, me qëllim të evitimit të pasojave ligjore të parashikuara me dispozitat e Kodit Penal[2].

Terminologjia e saktë juridike e përcaktimit të pastrimit të parave, është "fshehja ose maskimi i natyrës së vërtetë, burimit, vendndodhjes, disponimit, lëvizjes, të drejtave reale në lidhje me pronësinë, duke qenë në dijeni se prona të tilla rrjedhin nga një vepër penale"[3]. Ndërsa përfaqësuesi i Departamentit të Drejtësisë së Shteteve të Bashkuara të Amerikës, Paul Byron, shprehet se: "Pastrimi i parave ka të bëjë me përfitimin e pasurisë nga aktivitetet ilegale dhe përpjekjet që këto përfitime të vendosen në sistemet bankare, në atë mënyrë që të fshihet origjina e parave apo edhe të vazhdohet aktiviteti kriminal, duke përdorur sistemin financiar"[4].

### *2.1 Fazat e pastrimit të parasë*

Pastrimi i parave të fituara me vepra penale ose me veprimtari kriminale, qoftë

[1] Mersida Suçeska, *Bazat e kriminaliteti ekonomik*: (Prishtinë, 2006), 155.
[2] Po aty, f.155.
[3] Naim Mëçalla, *Pastrimi i parave*: (Tiranë, 2011),12.
[4] Albana Isufi, Prishtinë. Seminari "Pastrimi i parave përbën kërcënim global" datë 21.9.2004.
I disponueshëm në internet http://www.evropaelire.org/content/Article/1020095.html.Marrë shtator 2018.

edhe nga hakerët apo nga krimi kibernetik në përgjithësi, - edhe ky lloj pastrimi kalon në faza të ndryshme që ndjekin njëra-tjetrën. Procesi i pastrimit të parave ndjek tri faza:

a. deponimi ose vendosja;

b. shtresëzimi ose transformimi;

c. integrimi.

Në vazhdim do të shtjellojmë këto tri faza, në aspektin e përgjithshëm e më pas do të shtjellojmë këto faza, se si bëhet realizimi i tyre në krimin kibernetik.

*a) Deponimi ose vendosja:* me depozitim kuptojmë një procedurë kur individi apo në këtë rast hakeri, ose organizata kriminale, një grup hakerësh, që parat e gatshme të cilat i kanë realizuar nga veprat penale, përpiqen që t'i fusin në sistemin financiar ose t'i transferojnë në vende të ndryshme. Prandaj, kjo mënyrë e pastrimit të parave, mund të zbulohet më së lehti.

*b) Shtresëzimi ose transformimi:* gjatë kësaj faze të shtresëzimit, kriminelët e pastrimit të parave përpiqen që të fshehin gjurmët e tyre, nëpërmjet shtresave të shumta të transaksioneve, kompanive të biznesit, dyqaneve pa aktivitet dhe mekanizmave të tjetër të fshehjes. Shtresëzimi mund të përfshijë edhe vende të tjera, në të cilët rregullat e bankave për ruajtjen e sekretit e bëjnë më të vështirë ndjekjen e parave. Faza e shtresëzimit ka si synim të ngatërrojë hetuesit duke krijuar një linjë dokumentimi të produkteve të paligjshme, që i lëviz fondet përmes një sërë llogarish bankare dhe/ose transaksionesh. Shtresëzimi mund të përfshijë edhe transaksione false, si transferimin elektronik të parave nga një llogari në një tjetër, duke e maskuar si veprim biznesi

*c) Integrimi* **:** pas procesit të transformimit, në qoftë se zhvillohet mirë, pason procesi i integrimit të sërishëm të mjeteve në sistemin ekonomik, si mjete legale. Integrimi paraqet fazën e fundit të ciklit të pastrimit së parave. Paratë kthehen përsëri në qarkullim publik, duke u deponuar ose në llogari afariste, ose në llogari të kursimit, apo në ndonjë fond investues, kështu që është vështirë që në këtë fazë të bëhet dallimi midis fondeve të lejueshme dhe fondeve të palejueshme[5]; p.sh., në një rast kur pastruesi i parave ka futur para të paligjshme në një biznes që ka në pronësi, fondet i kthehen po atij në formën e rrogës së tij apo rrogës së anëtarëve të familjes, ose, si "hua" nga biznesi. Madje, ai mund edhe të paguajë taksa për ato para. Pastruesi mund të zgjedhë t'i investojë fondet në pasuri të paluajtshme, pasuri luksi ose biznese tjera. Integrimi ofron një shpjegim legjitim për burimin e fondeve pas shtresëzimit.

## 3. Pastrimi i parave në krimin kibernetik

Hakerët një ndër sfidat e para për pastrimin e parave e kanë gjetjen e hapësirave në ueb-sajte të ndryshme që ofrojnë shërbime, pa qenë të verifikuar apo identifikuar, sidomos nga forma KYC (*Know your Customer*, "njihni klientin tuaj") e sigurisë. Për këtë shkak, ata zgjedhin një kriptovalut tjetër: atë virtualen apo kriptovaluta që në të shumtën e rasteve ju ofrojnë transaksione pa kurrfarë identifikimi dhe krejtësisht në kushte anonimiteti. Padyshim që hakerëve, kjo formë e transaksioneve ju shkon shumë për shtat. Fillimisht do të flasim për etapën e parë, atë të vendosjes, dhe do të shohim disa shembuj dhe forma se nga rrjedhin dhe cilat janë burimet e fitimit nga krimi kibernetik. Nëse do të flasim për krimin e organizuar të një rrjeti trafikimi drogash, apo prostitucioni, ose shitje armësh, do të duhet të ndjekim lëvizjen e shitësve të drogave apo prostitucionit,

[5] Mersida Suçeska, vep. cit, f. 163-165.

ose të armëve; por, te krimi kibernetik kemi diçka krejt tjetër të formave të burimeve të fitimit të hakerve.

## 4. Burimi i të ardhurave në krimin kibernetik

Krimi kibernetik, mund të themi se ka një numër të konsiderueshëm burimesh së të ardhurave, për përfitime materiale. Ne do të mundohemi të shtjellojmë vetëm disa prej tyre, që mendoj se mund të jetë ose mund të preket shteti shqiptar.

### *41. "Scam online" ( mashtrimet* online*)*

Mashtrimet kompjuterike janë forma më e vjetër e keqpërdorimit të teknologjisë kompjuterike. Duke marr në konsideratë numrin dhe vendin që kanë në strukturën e këtij fenomeni kriminal, ato janë forma më të rrezikshme shoqërore të kriminaliteti kompjuterik[6]. Ne do të gabojmë rëndë nëse mendoj se interneti është një vend i sigurt dhe i mbrojtur sado që teknologjia dhe siguria ka avancuar shekullin e fundit. Gjithsesi, nuk duhet harruar se mund të bëhemi një objektiv i lehtë për hakerët që duan të vjedhin të dhënat tona më të vlefshme personale. Taktika dhe zhvillimi i aplikacioneve të ndryshme, e ka bërë edhe më të lehtë qasjen në të dhënat tona personale dhe tepër të ndjeshme. Sipas një raporti nga Komisioni Federal i Tregtisë (FTC), të rinjtë janë veçanërisht më të prekshëm ndaj mashtrimeve *online* sesa të moshuarit, - aq tronditës sa mund të duket. Hulumtimi konstaton se "40 për qind e të rriturve të moshës 20-29 vjeç, të cilët kanë raportuar mashtrim, kanë përfunduar duke humbur para në një rast mashtrimi"[7]. Ndërsa ne mund të biem lehtësish viktima të mashtrimeve *online,* sidomos në tri raste si p.sh.:

a) dyqane *online* në internet;

b) në kontrollin e postës tuaj elektronike;

c) në kontrollin e medieve tuaja sociale.

Ajo që duhet të kemi në fokus, gjithsesi, tek këta mashtrues, është se këta objektiv nuk kanë vrasjet, por synimi i tyre i vetëm është paraja jonë. Ne do t'ju sjellim listën e mashtrimeve *online* që janë më të shpeshta në mënyrë që të qëndroni larg tyre: mashtrimet elektronike (*phishing*); "nigerin scam"; mashtrimet me kartolina urimi; mashtrime me kartë krediti; mashtrime me lotari; softueri i rremë antivirus; mashtrimi i *facebook*-ut (marrje e të dhënave); mashtrime të bërit shpejtë para (mashtrime ekonomike); mashtrime në udhëtime; mashtrime me *bitcoin;* mashtrime me lajme të rreme; mashtrimet e ofertave të punës, etj.[8]

Ndërsa, si në Kosovë, edhe në Shqipëri, kanë qen më të theksuara vetëm disa lloje të këtyre mashtrime, që për motiv kanë pasur përfitimin financiar duke i viktimizuar shtresa të ndryshme të qytetarëve, pa dallim gjinie apo grupmoshe.

### *4.2 "Spaming - email spam"*

Ky synon që përdoruesve individualë t'ju dërgojë me mesazhe *email* informacione të ndryshme që janë të dobishme për *spamer*-in. Listat *email spam* janë të krijuara shpesh nga: skanimi i individëve të ndryshëm, ose i kompanive të ndryshme; nga vjedhja

[6] Vesel Latifi, *Kriminalistika zbulimi dhe të provuarit e krimit* , Prishtinë, 2011, f. 462-465.
[7] Marrë nga https://heimdalsecurity.com/blog/top-online-scams/, qasur në shtator 2018.
[8] Po aty.

e listave të postimeve në internet; nga kërkime në *ueb* për adresat. *Spam email-et* zakonisht u kushtojnë shumë përdoruesve dhe kompanive, sepse kapaciteti i tyre është i lartë. ISP-ve dhe shërbimeve *online* u kushton shumë transmetimi i *spam*-ve, dhe këto shpenzime transmetohen drejtpërdrejt te abonentët[9].

Nuk duhet harruar se kjo është një formë shumë dobiprurëse për hakerët, meqë ata, nga këto të dhëna fitojnë në disa lloje formash, si p.sh.: shesin listat e *email*-ve për *spam,* me para virtuale: dikur me LR tani me *Bitcoin*, *Etherum* etj. Të dhënat e fituara nga viktimizimi me *spam email*-e, i shesin po ashtu me para virtuale. Bazuar në disa të dhëna për vitin 2011 shihet se janë regjistruar mbi shtatë trilion *email*-e të dërguar, të kësaj natyre. Një shembull i *email spam* i ndodhur në Kosovë gjatë viti 2014/2015, ose ndryshe i njohur si "*mashtruesi nigerian"* ("Nigerian scam").

Mashtruesi në shembullin e më poshtëm i paraqitet viktimës nga Kosova se gjoja është avokat, dhe se posedon një klient me mbiemrin Berisha, që sipas këtij të ashtuquajturi avokat, klienti i tij kishte vdekur në një aksident ajror dhe kishte lënë një xhirollogari me 2.9 milionë dollarë dhe kërkon nga viktima që të bëhet trashëgimtar i tij, pasi i përputhet mbiemri.

*Spam*-i i paraqitet viktimës si avokat dhe i bën një përshkrim të shkurtër të vendit se ku jeton. I tregon gjoja se ka grua dhe tre fëmijë dhe se së bashku jetojnë në Lome-Togo. Ai i thotë se ka një klient të familjes Berisha dhe posedon një trashëgimi prej 2.9 milionë dollarë në një bankë të Togos. Nga ky *email* shohim se *spam*-i e josh viktimën për një shumë prej 2.9 milion dollarësh. Teknika që përdor *spam*-i në këtë rast, shihet se ai përdor mbiemrin e viktimave për t'i i edituar dhe për tua dërguar viktimave. Si shembull mund të shohim se ky *spam* mundë të ketë me mijëra *email,* por që për bazë merr vetëm mbiemrin e viktimave, në bazë të mbiemrit ai shkruan *email* e më pas, ua dërgon të njëjtin tekst me mbiemër të ndryshuar.

Sa për ilustrim po sjellim vetëm një nga 35 *email*-et e komunikimit të këtij kosovari të rënë viktimë.

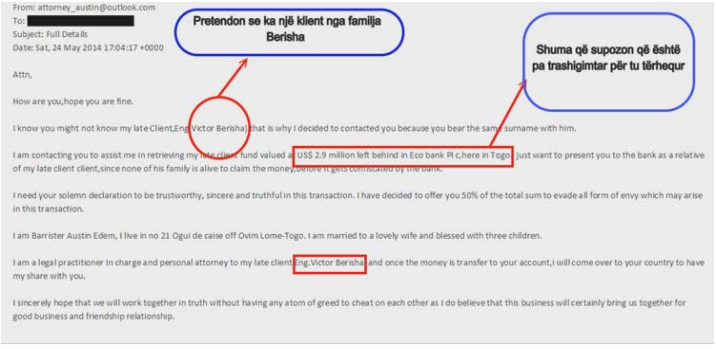


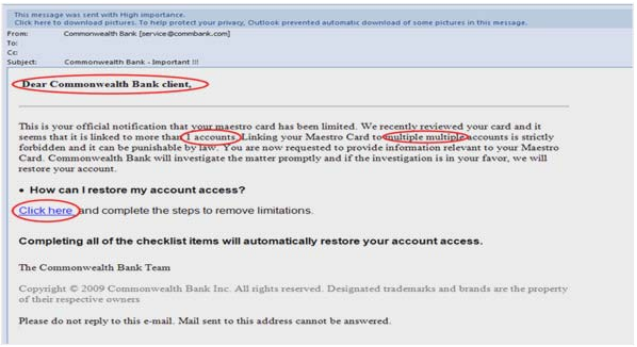

**Fig. 1. *Email*-i i viktimës nga Kosova, A. Berisha.**

### *4.3 "Phishing"*

Postë elektronike që ngjan sikur është nga ndonjë burim që njihet mirë (për shembull bankë ose dhënës i shërbimeve të internetit) me të cilën kërkohet të vërtetohen të dhënat personale. Është përpjekje për të marrë informacione të tilla te përdoruesit, si fjalëkalime, dhe detajet e kartave të kreditit (dhe nganjëherë, në mënyrë indirekte). Kjo

[9] Marrë nga: http://spam.abuse.net/overview/whatisspam.shtml, qasur në shtator 2018.

formë pretendohet të jetë popullarizuar në faqe sociale, faqet e ankandeve, bankave, përpunuesit *online* të pagesave ose administratorët, zakonisht faqe që kanë për synim përfitimin e të dhënave.


This message was sent with High importance.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.
From: Commonwealth Bank [service@commbank.com]
To:
Cc:
Subject: Commonwealth Bank - Important !!!

Dear Commonwealth Bank client,

This is your official notification that your maestro card has been limited. We recently reviewed your card and it seems that it is linked to more than 1 accounts. Linking your Maestro Card to multiple multiple accounts is strictly forbidden and it can be punishable by law. You are now requested to provide information relevant to your Maestro Card. Commonwealth Bank will investigate the matter promptly and if the investigation is in your favor, we will restore your account.

- How can I restore my account access?

Click here and complete the steps to remove limitations.

Completing all of the checklist items will automatically restore your account access.

The Commonwealth Bank Team

Copyright © 2009 Commonwealth Bank Inc. All rights reserved. Designated trademarks and brands are the property of their respective owners

Please do not reply to this e-mail. Mail sent to this address cannot be answered.

**Fig. 2 *Email* model për "phishing"**[10]

Si shembull mund të marrim një hulumtim të bërë në Australi, i cili kishte identifikuar një "phishing". Pra, këta hapin faqe identike duke i ndryshuar në pika ose presje një shkronjë më pak ose më shumë nga ueb-faqja origjinale. Nëse ju do të klikoni në "Click here", atëherë me automatizim do të futeni me një faqe të "bankës" mashtruese që do t'ju kërkojë të dhënat tuaja[11].

Kjo faqe mashtruese pretendon t'ju heqë limitin e kartës suaj, e në fakt të gjitha të dhënat që ju do të shënoni aty, do t'i dërgohen në server të dërguesit të këtij *email*-i[12].


http://www.fmslnj.com/netbanking/
www.commonwealth.com.au/index.php
Click to follow link
access?
Click here and complete the steps to remove limitations.

**Fig. 3. Huazuar nga:**
**http://www.aahb.com.au/sites/aahb.com.au/files/uploads/phishing-example-2.gif**

Kjo është një formë që hakerët e përdorin në të shumtën e rasteve kur kanë për synim vjedhjen e të dhënave personale, e në veçanti, të dhënat e kartave të kreditit. Hakerët me përfitimin e këtyre të dhënave, i përdorin për blerje *online* përmes mashtrimit si dhe duke i hedhur ato të dhëna në treg për shitje. E gjithë këto të dhëna shiten nga 1.5$ deri në 50$ në varësi të gjenerimit së të dhënave nga viktima. Nuk duhet harruar se edhe këto shitje i realizojnë gjithnjë me para virtuale apo digjitale. Dikur përdornin LR dhe PM ndërsa sot përdorin për shitje, *bitcoin*, *ethertum* etj.

### *4.4 "Skimming"*

Janë aparate që shfrytëzohen për mbledhjen e paautorizuar së të dhënave nga kartat për pagesë, edhe atë së të dhënave që gjenden në shiritin magnetik të kartës për pagesë dhe të dhënave të PIN-it të kartës. Ka dy lloje të *skimer*-ësh: à) fiks, që montohen

[10] Marrë nga :http://www.aahb.com.au/sites/aahb.com.au, qasur në shtator 2018.
[11] Marrë nga: http://www.aahb.com.au/dont-get-scammed-identifying-phishing-emails, qasur në korrik, 2018.
[12] Po aty.

në ÀÒÌ (bankomate) dhe, b) të lëvizshëm, që lexojnë vetëm shënimin që gjendet në shiritin magnetik. *Skimer*-ët përmbajnë në vetvete disa komponentë:

- lexues së të dhënave nga shiriti magnetik;
- video-kamerë për video-incizim nga video-mbikëqyrja në pjesën e aparatit ku shfrytëzohet karta për pagesë, e që gjendet në pjesën ku futet kodi PIN për përdorimin e kartës për pagesë[13].

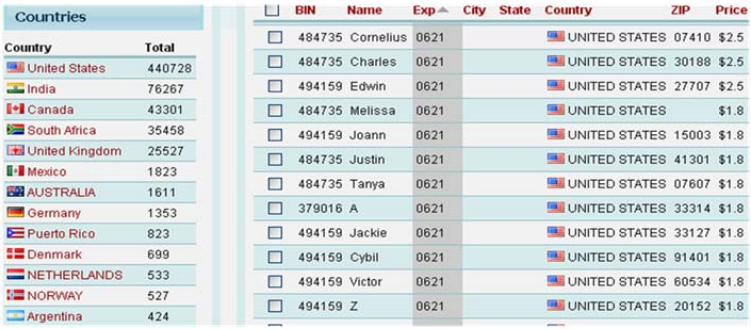
*Skimming* është bërë një industri miliardë dollarësh. Një oficer i lartë i Interpolit deklaroi se kartat e klonuara janë përdorur për të tërhequr mbi 1 miliard $ amerikanë në të gjithë globin, gjatë dekadës së fundit, - sipas *indiatimes.com*.

Në vende të tilla, si Malajzia, klonohen rreth 5000 në ditë. Një raport lajmesh referuar një videoje në *YouTube* për informimin e shikuesve, tregon se mund të fitohet në javë deri në 75.000 $ nga *skimming* [14].

Duke ditur fitimet e larta që kanë, hakerët këtë formë të fitimit së të dhënave të kartave bankare, si dhe shitjen e tyre në formë virtuale dhe si të klonuara, e bëjnë në pjesën më të madhe të rasteve përmes shitjes me para virtuale, me përjashtim të atyre rasteve kur ata e përdorin klonimin e kartës atëherë kur ata tërheqin direkt nga bankomatet e ndryshëm, sasi të caktuara parash.

### *4.5 Shitblerja e të dhënave të kartave të kreditit*

Zgjerimi i vazhdueshëm i pagesave *online* është duke rritur mashtrimet me karta krediti. Popullariteti në rritje i pagesave të lëvizshme ofron mundësi të reja për vjedhjen e të dhënave dhe për mashtrimin. Grupet kriminale investojnë në metodat e inxhinierisë teknike dhe sociale për të kompromentuar këto lloj pagesash. Mashtrimet në pagesat me anën e kartave paraqesin rrezik të ulët e ndërkohë i sjellin fitime të larta aktivitetit kriminal, i cili gjeneron të ardhura vjetore prej rreth 1.5 miliardë eurosh. Mashtrime të tilla kanë një ndikim negativ mbi sigurinë dhe komoditetin e pagesave jo-*cash* në Europë, dhe kanë shkaktuar humbje të konsiderueshme për ekonominë e BE-së.



Countries

| Country | Total |
|---|---|
| United States | 440728 |
| India | 76267 |
| Canada | 43301 |
| South Africa | 35458 |
| United Kingdom | 25527 |
| Mexico | 1823 |
| AUSTRALIA | 1611 |
| Germany | 1353 |
| Puerto Rico | 823 |
| Denmark | 699 |
| NETHERLANDS | 533 |
| NORWAY | 527 |
| Argentina | 424 |

| BIN | Name | Exp | City | State | Country | ZIP | Price |
|---|---|---|---|---|---|---|---|
| 484735 | Cornelius | 0621 | | | UNITED STATES | 07410 | $2.5 |
| 484735 | Charles | 0621 | | | UNITED STATES | 30188 | $2.5 |
| 494159 | Edwin | 0621 | | | UNITED STATES | 27707 | $2.5 |
| 484735 | Melissa | 0621 | | | UNITED STATES | | $1.8 |
| 494159 | Joann | 0621 | | | UNITED STATES | 15003 | $1.8 |
| 484735 | Justin | 0621 | | | UNITED STATES | 41301 | $1.8 |
| 484735 | Tanya | 0621 | | | UNITED STATES | 07607 | $1.8 |
| 379016 | A | 0621 | | | UNITED STATES | 33314 | $1.8 |
| 494159 | Jackie | 0621 | | | UNITED STATES | 33127 | $1.8 |
| 494159 | Cybil | 0621 | | | UNITED STATES | 91401 | $1.8 |
| 494159 | Victor | 0621 | | | UNITED STATES | 60534 | $1.8 |
| 494159 | Z | 0621 | | | UNITED STATES | 20152 | $1.8 |

**Fig.5 *Shop online* i kartave të kreditit, të kryera me LR në vlerën "dollar".**

Shumë individë janë prekur drejtpërdrejt dhe kanë pësuar humbje të konsiderueshme financiare për shkak të të tilla mashtrimeve. Në vitin 2011, rreth 60% e humbjeve të pagesave me karta, janë shkaktuar nga karta joaktuale dhe fitimet kanë arritur deri në 900 milionë euro[15].

[13] Marko Zvërlevski. *Doracak për krimin kompjuterik*, (Shkup; 2014), 37.
[14] Marrë:http://www.businessinsider.com/hackers-tech-credit-card-skimming-2011-10qasur në tetor 2018.
[15] Raporti i Europolit, Socta 2013.

## 5. Pastrimi i parave në internet

Një ndër pika më të ndjeshme dhe me komplekse është padyshim fshehja e burimit së të ardhurave të hakerëve, duke realizuar një mori transfertash, nga më komplekset. Bazuar te të dhënat dhe informacionet e dhëna nga hakerët e besuar dhe ata bashkëpunuesit, nga Kosova, po vëmë në dukje disa nga metodat e tyre për pastrimin e parave. Ata fillimisht përdornin vetëm dy lloje parash: *LR liberty Reserve* dhe *UebMoney*, si dy lloje të parave virtuale që sipas tyre ofronin një siguri të lartë të transfertave si dhe, e mira e gjithë këtyre ishte ngaqë këto dy ueb-faqe interneti nuk kërkoni kurrfarë identifikimi me dokument zyrtar. Ata hapnin zakonisht llogari fiktive, me emra të rremë, kryesisht me nofka. LR, ofronte dy lloje pagesash: LR në dollar, dhe LR në euro. Gjithashtu, edhe *Uebmoney* ofronte po këto lloje llogarish, në euro dhe dollar etj.

Fillimisht, hakerët përdornin paranë virtuale, dhe pothuajse të gjitha shitblerjet i bëjnë me para virtuale sepse ueb-faqet që ofrojnë para virtuale mundësojnë ruajtjen e privatësisë së lartë ose mundësojnë hapjen e adresave në kushte anonimiteti dhe pa kërkuar të verifikohen ato me dokumente identiteti.

Por, për transferimin e pagesave *online* kompania kishte vendos një nivel të sigurisë shumë të lartë. Ata për verifikimin e transferimeve kishin vendosur fjalëkalime dhe kode të sigurisë së veçantë, për sigurinë e pajisjeve. Vetëm në momentin e hapjes do t'ju japin edhe një kod sigurie, të cilin ju sugjerojnë që të mos e humbisni dhe ta mbani shumë sekret, sepse asnjë transfertë nuk mund të realizohet pa e ditur atë kod sigurie, edhe pse do të keni akses në atë llogari. Sipas "figurës 1", të paraqitur më lart në artikull, jepet: hyrja për shitblerje *online* të LR-së, te "2" shihet gjendja e xhirollogarisë në tri vlera monetare: USD, Euro dhe Gold; ndërsa në opsionin "3" shihet vendosja e kodit të sigurisë shtesë. E gjithë kjo, bëhet për shitblerje e produkteve, softuerëve, të dhënave ose ndonjë marrëveshjeje të tregut të zi.

Të gjitha përfitimet, hakerët i vendosnin në LR dhe puna e tyre do të ishte e padobishme për ta, sikur ato të mbeteshin vetëm aty dhe të mos përdoreshin edhe në jetën reale si kartëmonedha të zakonta. Për të ardhur deri aty, padyshim që hakerëve u është dashur të mendojnë për rrugë të sigurta të transferimit dhe konvertimit të tyre, nga para virtuale në ato fizike. Ata janë detyruar që të realizojnë transaksione komplekse, duke përdorur rrugë të shpejta shtete të ndryshme, duke krijuar kompani fiktive dhe duke ndërtuar ueb-faqe sa për të bërë pastrimin e parave dhe injektimin e tyre në treg, si të rregullta.

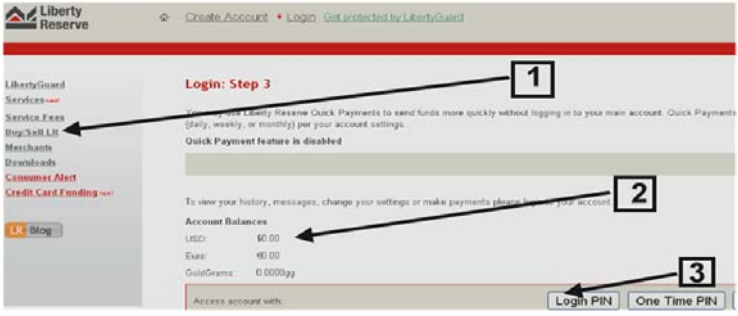



**Fig. 6 *LR LibertyReserve* hapja e një llogarie**[16]

[16] Marrë: http://www.onlinepaysystems.info/system/19/Liberty%20Reserve, qasur në shtator 2018.

Një ndër format më të shpeshta është konvertimi i tyre *online* me anë të ueb-faqeve *online* që ofrojnë shërbime të tilla *online*.


Fig. 7. Konvertimi nga LR në Euro ose Dollar

Këtu, futen hakerët, që paratë e fituara në mënyrë të paligjshme i konvertojnë në para reale, ose i transferojnë diku tjetër, në këmbim të ndonjë produkti. Zakonisht në raste të tilla, agjencitë që merren me këto konvertime do i dërgojnë në adresën e kërkuar nga personi. Kështu që ai do t'i marri ato nga një shtet tjetër; në të shumtën e rasteve nga gjini e kundërta p.sh.: dërgesa bëhet nga një agjente e këmbimores, femër, për ta bërë edhe më kompleks konvertimin.

Të gjithë këtë që u tha më lart e vërteton fakti se ndaj kësaj kompanie është zhvilluar një hetim i thellë nga FBI-ja, me një bashkëpunim ndërkombëtar. Kjo ueb-faqe kishte funksionuar nga viti 2005 deri në vitin 2013. Ndërsa, në vitin 2013, kjo ueb-faqe mbyllet përfundimisht. Në lidhje me këtë faqe ishe arrestuar themeluesi i saj, Arthur Budovsky në moshën 42 vjeçare, i cili ishte arrestuar në Spanjë dhe pas një periudhe kohe, ishte ekstraduar në SHBA ku u dënua me 20 vjet burg[17].

### *5.1 Kush ishte "Liberty Reserve"?*

Sipas FBI-së, *Liberty Reserve* kishte përpunuar më shumë se 8 miliardë dollarë transaksione dhe kishte më shumë se 5.5 milion llogari përdoruesish në mbarë botën. Për llogaritë me bazë në SHBA, z. Budovsky, kishte pranuar se kjo ueb-faqe kishte arritur pastrimin e të paktën 250 milion dollarësh nga të ardhura kriminale. Një formë tjetër e pastrimit të parave nga hakerët, është edhe përdorimi lojërave të fatit *online*, si kazino *online*, poker, rulet, *slote* etj. Vlen të theksohet sidomos konvertimi dhe bashkëpunimi i madh në lojën e pokerit duke përdorur disa llogari të rreme sa për të bërë transferimin e tyre, për ta bërë këtë pune edhe më komplekse.

Firma e softuerit të sigurisë *McAfee*, paralajmëroi për rritjen e shpejtë të faqeve të paligjshme "të palicencuara" të lojërave të fatit në internet, të cilat tani janë kaq të shumta saqë janë të vështira të kapen nga autoritetet e policisë dhe nga ku rrjedha e parasë është anonime dhe e lehtë për t'u maskuar. Faqet e palicencuara u lehtësojnë kriminelëve kibernetikë pastrimin e parave të pista, pasi identitetet dhe vendndodhjet

[17] Marrë nga: https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years , qasur në shtator 2018.

e lojtarëve janë të maskuara. Kur përdoren të lidhura me mjetet e pastrimit të parave, ato gjithashtu mund t'u lejojnë klientëve që të konvertojnë në mënyrë anonime monedhat virtuale. *McAfee* paralajmëroi se *Bitcoin,* monedha e njohur digjitale, mund të ofrojë anonimitet të mëtejshëm ndaj hajdutëve në internet[18].

## 6. Përfundimi

Jemi qasur qëllimisht në argument e fakt, vetëm në drejtim të LR-së, meqë ajo dikur ishte në modë dhe pothuajse ishte libër për paratë virtuale. Dhe natyrisht, kjo ishte thuajse fillimi i primahakërve për shitblerje *online* në internet. Por, tani nuk duhet harruar se jemi në vitin 2018 dhe kemi në modë *Bitcoin,* Etherum, Reeple, *Litecoin*, etj. Nëse i marrim në përgjithësi, numri i tyre i kalon mbi 2000 kriptovaluta duke përfshirë edhe ato *coins* dhe *token*. Lind pyetja: Sa e lehtë është që të hetohet një lëvizje e kriptovalutave ku ato mund të këmbehen me një numër kaq të lartë të tyre? As Shqipëria, as Kosova, nuk e ka shumë larg shtetin e Maltës që po ndërton politika për të investuar për të qenë një qendër e kriptovalutave *block chain*, dhe padyshim që kjo do t'i rrisë vlerat e kriptovalutave dhe interesimin për të marrë me këto lloj valutash.

Një element tjetër interesant tek hakerët, është se tanimë ata nuk kanë nevojë të mendojnë fare për falsifikimin e parasë euro, dollar, lek etj., sepse ata tani po ndërtojnë miniera të ndryshe në shtëpitë e tyre, duke prodhuar *bitcoin*, *etherum,* pa pasur nevojë të falsifikojnë paranë sepse tani kanë një mundësi të artë për të prodhuar para digjitale. Megjithatë, edhe prodhimi i tyre ka një kosto: nga energjia elektrike. E natyrisht, kjo i shton orekset te hakerët, për gjetjen e rrugëve më të mira për vjedhjen e energjisë elektrike, me qëllim uljen e kostos. Ndërsa për sa i përket raportit të taksave të Shqipërisë po edhe të Kosovës, pritet që shtetet të nxjerrin sa më parë ligje për tatimin e këtyre prodhimeve, si dhe, për avancime në teknologjinë e detektimit të tyre. Pra, shteti shqiptar patjetër që duhet të pajiset me detektor për detektimin e këtyre minierave.

Një tjetër kërcënim, është ai që paraqet bashkëpunimi i hakerëve dhe grupeve kriminale të trafikimit të drogës, apo të ndonjë forme tjetër kriminale, pasi kjo teknologji do t'ju mundësojë lehtësisht pastrimin e parave dhe realizimin e transaksioneve tepër komplekse për të u hetuar.

Mendoni këtë fakt: që për të kaluar kufirin me 1.000.000$ do t'ju nevojitet një çantë mjaft e madhe dhe do t'ju zinin shumë vend në makinën tuaj. Këtyre grupeve kriminale u vështirësohet shumë puna, meqë kërkojnë që atë ta fshehin mirë, të kamuflohen mirë gjatë transportit e sidomos kur bëhet fjalë për kalim kufiri pa i deklaruar fare. Ndërsa një haker i mençur do të instalojë një aplikacion *blockchain* në *smartphone-in* e tij, dhe aty do të kalojë lehtësisht çdo kufi me mbi 1.000.000$ të konvertuara në *bitcoin* apo *etherum*. Mendoj se shteti shqiptar, por edhe shtete të tjera, lidhur me këta persona të dyshuar ose me të kaluar kriminale, duhet t'i lejojë kontrollet e *smatphone*-ve të tyre gjatë kalimit të kufijve ose në ndonjë kontroll policor, nëse kanë të instaluar aplikacione të kësaj natyre.

Një tjetër formë e rreziqeve të kësaj natyre, në lidhje me pastrimin e parave, mund të vijë nga numri i madh i ueb-faqeve *online* që ofrojnë lojëra fati, kazino, poker, *slote* etj. Sepse tani, veçse janë shfaqur disa ueb-sajte të kësaj natyre që pranojnë deponime

[18] Marrë nga: https://www.cnbc.com/2014/04/25/online-gambling-the-new-home-for-money-launderers.html, qasur në shtator 2018.

me anë të kriptovalutave. Mendoj se një synim tjetër për pastrim parash do të kishte edhe në fushën pornografike, duke rritur numrin e ueb-faqeve për komunikim *online videochat,* me mundësi pagese me anë të kriptovalutave. Duke parë specifikat e veçanta të kriptovalutave, shteti shqiptar duhet të nxjerrë ligje të veçanta me natyrën e punës së kriptovalutave, sidomos në luftimin e pastrimit të parave me anë të kriptovalutave. Sepse nxjerra e këtyre ligjeve miratimi i tyre thuajse të gjitha shtetet ju merr shume kohë për përpilim dhe miratim ndërsa kjo teknologji avancon me shpejtësi shumë më të lartë në krahasim me shpejtësinë e miratimeve të ligjeve.

## Bibliografi


1. Macella Naim, *Pastrimi i parave*, Tiranë, 2011.
2. Suçeska Mersida, *Bazat e kriminaliteti ekonomik*, Prishtinë, 2006.
3. Vesel Latifi, *Kriminalistika zbulimi dhe të provuarit e krimit* , Prishtinë, 2011.
4. Zvërlevski Marko. *Doracak për krimin kompjuterik*, Shkup, 2014.
5. Raporti i Europolit, Socta 2013.

**Faqe interneti:**

1. https://heimdalsecurity.com/blog/top-online-scams/,
2. http://spam.abuse.net/overview/whatisspam.shtml
3. http://www.aahb.com.au/sites/aahb.com.au,
4. http://www.businessinsider.com/hackers-tech-credit-card-skimming-2011-10
5. http://www.aahb.com.au/dont-get-scammed-identifying-phishing-emails
6. http://www.onlinepaysystems.info/system/19/Liberty%20Reserve,
7. https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years
8. Isufi Albana, Prishtinë. Seminari "Pastrimi i parave përbën kërcënim global" datë 21.09.2004. marrë në http://www.evropaelire.org/content/Article/1020095.html.

# Hyrja ndërkufitare në sistemet kompjuterike dhe parimi i sovranitetit shtetëror

■ **Magjistrat Ylli PJETËRNIKAJ**
*Prokuroria pranë Gjykatës së Shkallës së Parë, Shkodër*
*ylli_1987@live.com*

■ **Enisa SHAHINI**
**(Magjistrat kandidat)**
*Shkolla e Magjistraturës*

**Abstrakt**

*Aftësia për të hyrë në të dhëna kompjuterike, të cilat gjenden në juridiksione të tjera, në mënyrë të shpejtë, është një aspekt i rëndësishëm i hetimeve penale moderne. Megjithatë, fakti që organet proceduese kanë kapacitetin për të kryer kërkime të tilla, nuk e bën të lejuar atë. Kjo, do të konsiderohet zakonisht si një shkelje e sovranitetit territorial, për ndërhyrjet, nga vendi ku kryhen hetimet, në një vend të huaj, pa autorizimin e këtij të fundit. Parimi i të drejtës ndërkombëtare, parashikon se asnjë shtet nuk mund të zbatojë juridiksionin e vet, në territorin e një shteti tjetër sovran. Rrjedhimisht, një shtet nuk mund të zbatojë ligjet e tij, të kryejë hetime apo të arrestojë një person, në territorin e një shteti tjetër, pa autoritet të qartë ligjor, që e lejon ta bëjë këtë. Çështja e ndërhyrjes ndërkufitare në provat elektronike, është njohur që nga viti 1980, edhe pse në atë kohë çështja nuk dukej "shumë impresionuese, dhe në fazat embrionale". Megjithatë, ndryshimet në teknologji, treguan se çështja u bë shpejt urgjente dhe u debatua, ndër të tjera, nga Komiteti Evropian për problemet kriminale, G8-a dhe Këshilli i Europës. Hartuesit, konstatuan në fund, se nuk ishte ende e mundur për të përgatitur një regjim të plotë, ligjërisht të detyrueshëm në këtë fushë. Problematikat e vërejtura lidhen me çështjen e urdhërimit të gjykatave të Republikës së Shqipërisë, ndaj subjekteve që nuk ndodhen në territorin e vendit tonë, për të vënë në dispozicion të dhëna kompjuterike. Gjithashtu, karakteri ndërkombëtar i krimit kompjuterik, ngre problematikën lidhur me kriteret e përmendura nga konventa, për të përcaktuar se cili shtet-palë ka juridiksion, në rastet kur veprimi kryhet nga një shtetas i huaj jashtë territorit dhe pasoja vjen në territorin e një shteti tjetër.*

**Fjalëkyçe:**
**krimit kompjuterik, sovranitet territorial, sisteme kompjuterike, ndërhyrja ndërkufitare, krimi transnacional.**

## 1. Hyrje

Rreziku që rrjetet kompjuterike dhe informacioni kompjuterik të përdoren për kryerjen e veprave penale, ndërsa faktet e lidhura me to mund të memorizohen, të ruhen dhe të transferohen nëpërmjet këtyre mjeteve, është permanent dhe i dukshëm[1]. Fenomenet moderne të digjitalizimit, konvergjencës dhe globalizimit të vazhdueshëm të rrjeteve kompjuterike[2] dhe të dhënave kompjuterike[3], kanë krijuar një terren të përshtatshëm për kryerjen e krimeve kompjuterike, duke formatuar karakterin transnacional të tij dhe e shndërruar një nga format tipike të veprimit të krimit të organizuar.

Këto karakteristika të krimit kompjuterik e kanë bërë atë objekt analizë nga organizata të ndryshme ndërkombëtare, ndër to edhe Organizata e Kombeve të Bashkuara. Asambleja e Përgjithshme e Kombeve të Bashkuara ka miratuar disa rezoluta. Rezolutat 55/63 të 4 dhjetorit 2000[4] dhe 56/121 të 19 dhjetorit 2001[5] mbi "Luftën kundër keqpërdorimit të teknologjive të informacionit", janë më të rëndësishmet. Rezoluta 55/63 parashikon detyrimin e shteteve për të siguruar që ligjet dhe praktikat e tyre të eliminojnë strehët e sigurta për ata që keqpërdorin teknologjitë e informacionit. Megjithatë instrumenti më i rëndësishëm europian është Konventa mbi Krimin

[1] Shih preambulën e Konventës "Për krimin në fushën e kibernitikës".
[2] "Sistem kompjuterik" do të thotë çdolloj pajisje apo grup i ndërlidhur ose pajisje të lidhura, një ose më shumë prej të cilave, vazhduese të një programi kryejnë procesime automatike së të dhënave.
[3] "Të dhëna kompjuterike" do të thotë çfarëdolloj përfaqësimi të fakteve, informacioni apo konceptesh në një formë të përshtatshme për procesim në një sistem kompjuterik, që përfshijnë një program të përshtatshëm për punën e një sistemi kompjuterik për të kryer një funksion.
[4] Shih https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf akses 13 shtator 2018.
[5] Shih https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf akses 13 shtator 2018.

Kibernetik,[6] e Këshillit të Europës (Konventa e Budapestit), e cila u hap për nënshkrim në Konferencën e Budapestit, më 23 nëntor 2001 dhe hyri në fuqi me 1 korrik 2004[7]. Konventa e Budapestit është nënshkruar dhe ratifikuar edhe nga shtete që nuk janë anëtare të Këshillit të Europës, ku mund të përmënimin Australinë, Shtetet e Bashkuara të Amerikës dhe Japoninë. Kjo ishte një arritje historike në luftën kundër krimit kibernetik[8].

Aftësia për të aksesuar në të dhënat kompjuterike, të cilat gjenden në juridiksione të tjera, në mënyrë të shpejtë, është një aspekt i rëndësishëm i hetimeve penale moderne. Megjithatë, fakti që organet proceduese kanë kapacitetin për të kryer kërkime të tilla nuk e bëjnë të lejuar atë. Kjo zakonisht do të konsiderohet si një shkelje e sovranitetit territorial për ato nga një vend që kryejnë hetimet në një vend të huaj pa autorizimin e atij vendi.

Praktika gjyqësore ka pasur raste në të cilat gjykatat urdhërojnë subjektet, që nuk ndodhen në territorin e vendit tonë, të vënë në dispozicion të dhënat kompjuterike. A është i justifikueshëm juridikisht një gjë e tillë?

Gjithashtu karakteri ndërkombëtar i krimit kompjuterik ka bërë që jurisprudence të mbajë qëndrime të ndryshme lidhur me kriteret e përmendura nga konventa për të përcaktuar se cili shtet palë ka juridiksion, në rastet kur veprimi kryhet nga një shtetas i huaj jashtë territorit dhe pasoja vjen në territorin e një shteti tjetër.

## 2. Karakteri ndërkombëtar i krimit kompjuterik

Krimet kompjuterike paraqesin karakter transnacional[9], që nënkupton operim dhe ushtrim aktiviteti kriminal në dy ose më shumë shtete. Organizatat transnacionale kërkojnë të mobilizojë burimet e tyre dhe të hartojnë strategjitë e duhura për të penetruar në mënyrë efiçente në territoret, në të cilat ato ushtrojnë aktivitetin[10].

Krimit transnacional nënkupton, duke u trajtuar atë si një aktivitet kriminal, i cili konsiderohet vepër penale nga të paktën dy shtete, në territorin e të cilave vepron.[11] Disa studiues arrijnë në përfundimin se krimi transnacional është më shumë një problem politik, sesa problem ligjor. Ky fenomen influencohet nga zhvillimet botërore dhe merr avantazhe nga të gjitha format e progresit, veçanërisht nga zhvillimi i transportit, telekomunikacionit dhe zhvillimet e tjera teknologjike[12].

Krimi transnacional nuk është vetëm një koncept ligjor. Ai mbetet një koncept në fushën e kriminologjisë, i cili përshkruan një fenomen social[13]. Gjithashtu ai është një koncept sociologjik, sepse lidhet me kuptimin e grupeve ose rrjeteve kriminale që operojnë brenda një mjedisi ndërkombëtar i përbërë nga shtete dhe politika të ndryshme[14]. Disa autorë theksojnë natyrën e organizimit të krimit transnacional, ndërsa



[6] Konventa për Krimin Kibernetik. (ETS 185 Convention on Cybercrime, 23.XI.2001).
[7] Shih http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 akses 13 shtator 2018.
[8] S. Schjolberg,"*The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva*", 2008, f. 4.
[9] Shih Making the ëorld safer from drugs, crime and terrorism - The European Union (EU) and the United Nations Office on Drugs and Crime (UNODC), 2015, fq.13.
[10] Shih David Felsen, Akis Kalaitzidis " A historical overview of transnational crime", f. 5.
[11] Shih Bossard A., Transnational Crime and Criminal Laë, University of Chicago, Office of international Criminal Justice, 1990, f. 5.
[12] Shih Bossard A., Transnational Crime and Criminal Laë, University of Chicago, office of international Criminal Justice, 1990, f. 146.
[13] Shih Mueller, G.O, Transnational Crime Definitions and Concepts, 2001, f. 13.
[14] Shih Serrano,M., Transnational organized crime and International Security: Business as usually, 2002, fq.16.

të tjerë vënë theksin tek natyra ndërkufitare e tij[15].

Në konventën e OKB-së kundër krimit të organizuar janë përcaktuar disa kritere, mbi bazën e të cilave përcaktohet natyra transnacionale e një krimi. Një vepër penale ka një natyrë ndërkombëtare në qoftë se kryhet në më shumë se një shtet, ose kryhet në një shtet, por pjesa thelbësore e përgatitjes, planit, drejtimit ose kontrollit është ndërtuar në një shtet tjetër, ose kryhet ne një shtet, por në të është përfshirë një grup kriminal i organizuar, i cili angazhohet në aktivitete kriminale në më shumë se një shtet, ose kryhet në një shtet, por pasojat thelbësore i ka në një shtet tjetër[16].

Pavarësisht mendimeve të ndryshme që ekzistojnë, lidhur me përkufizimin e konceptit të krimit transnacional, si krimi i organizuar ose jo, ajo çfarë është e qartë është fakti që ky fenomen përfshin një rrjet të gjerë të aktivitetit kriminal.

Nëse dimensioni transnacional që ka fituar sot krimi kompjuterik, karakterizon çdo veprimtari hetimore që, edhe kur zhvillohet ende në nivel lokal, priret të marrë tipare përtej territoriale, bashkëpunimi ndërkombëtar përfaqëson një parakusht për çdo veprimtari të përbashkët lufte[17].

Për këtë arsye, vetëm nëpërmjet veprimtarive hetimore që përfshijnë të gjitha vendet e prekura nga krimi kompjuterik apo pasojat e tij dhe, analizës së informacioneve që mund të merren përmes kanaleve të bashkëpunimit, sot është e mundur të realizohen operacione të cilat janë në gjendje të ndikojnë në mënyrë domethënëse mbi këtë fenomen, duke zbuluar edhe flukset e parave që rrjedhin prej tyre.

Sistemet kompjuterike kanë shërbyer, gjithashtu, si një ndër mjetet efikase për kryerjen e krimeve, të cilat në vetvete nuk klasifikohen si kibernetike. Kështu, përmendim revolucionin që sollën komunikimet mobile, të cilat kanë ofruar mundësi të reja ndaj rrezikut të zbulimit të krimit. Në vend që të angazhohen në kontakt personal me bashkëpunëtorët apo viktimat, tani ata përdorin komunikimet elektronike[18].

Autorët e krimeve mund të përdorin për të mbrojtur komunikimet e tyre softuerë të koduar. Ky është shndërruar në një problem për autoritetet ligjzbatuese duke marrë parasysh popullaritetin në rritje të softuerëve vendas të instaluara në telefonat celularë[19]. *Europol* ka vënë në dukje fenomenin e grupeve kriminale që punësojnë hakerët specialistë dhe pritet që aktivitete të tilla të rriten dukshëm[20].

Një problematikë serioze për shtetet përbëjnë dhe faqet e internetit anonime. "Darknet" është një prej tyre, është rrjet i koduar, në të cilin përdoruesit mund të shkëmbejnë në mënyrë anonime mallrat dhe shërbime të ndaluara. Përdoruesit marrin drogat e postuara pas pagimit të çmimit, i cili është në *bitcoin*. Anonimiteti i këtij rrjeti zvogëlon rrezikun e zbulimit si për tregtarët dhe për përdoruesit[21]. Përdorimi i këtyre sistemeve ose të dhënave kompjuterike, për të kryer vepra penale, i shndërron ato në burime ose mjete provuese për këtë të fundit, të cilat mund të gjenden në shtete, të ndryshme, nga ai në territorin e të cilit është kryer krimi.

[15] Shih Sheptycki, J., Against transnational organized crime, University of Toronto Press, 2003, f. 142.
[16] Shih nenin 3 të Konventës kundër krimit te organizuar ndërkombëtar, e ratifikuar me ligjin nr. 8920, datë 11.7.2002.
[17] Shih Itali-Shqipëri: Instrumente ligjorë dhe teknika të luftës kundër krimit të organizuar transnacional përballje përvojash nën kujdesin e Corrado Lembo, Koordinator shkencor i Kursit të trajnimit për gjyqtarë, prokurorë dhe oficerë të policisë gjyqësore (Tiranë, 5-16 mars 2007; Romë, 15-19 tetor 2007; Tiranë, 12-16 nëntor 2007), f. 100.
[18] Shih Agnés Cadet-Tairou and others, "Substances psychoactives, usagers et marchés: les tendances récentes (2015-2016)", Tendances, vol. 8, No. 115 (December 2016).
[19] Europol, IOACTA 2016: Internet Organized Crime Threat Assessment, The Hague, 2016.
[20] Shih "Police warning after drug traffickers' cyber-attack", 16 October 2013, BBC News. Available at http://www.bbc.com/ news/world-europe-24539417. Aksesuar më 14.04.2018.
[21] Cadet-Taïrou and others, "Substances psychoactives, usagers et marchés: les tendances récentes".

Kriteret e caktimit të juridiksionit të parashikuara nga konventa "Për krimin në fushën e kibërnitikës", në raste të caktuara të krimit transnacional, mund të mos jenë të mjaftueshme për të përcaktuar se cili shtet pale ka juridiksion[22]. I tillë është rasti i veprave penale të kryera nëpërmjet sistemeve kompjuterike që ndodhen në territorin e një vendi, ndërsa pasojat e krimit vijnë në territorin e një vendi tjetër. Në këtë rast në bazë të kritereve të zakonshme të juridiksionit, më shumë se një shtet palë do të ketë juridiksion.

Për të shmangur përpjekjet e shumëfishta, shqetësimet e panevojshme për dëshmitarët, apo "konkurrencës" mes organeve të zbatimit të ligjit të shteteve, ose për të lehtësuar efikasitetin procedimit penal, shtetet pale duhet të konsultohen në mënyrë që të përcaktojnë shtetin pale të përshtatshëm për të realizuar ndjekjen penale. Në disa raste, mund të jetë më efektive për shtetet e interesuara për të zgjedhur një shtet që të procedojë për ndjekjen, si dhe në disa të tjera, mund të jetë më efektive që një shtet të ndjekë penalisht disa pjesëmarrës, ndërsa një ose disa shtete të tjera të ndjekin të tjerët. Duhet të theksohet se detyrimi për t'u konsultuar nuk është absolut, por duhet të ndodhë "kur është e përshtatshme." Kështu, në qoftë se një nga palët konsideron se konsultimi nuk është i nevojshëm (p.sh, ka konfirmim se pala tjetër nuk ka vullnet të ndërmarrë veprime hetimore), ose mund të dëmtojë hetimet apo procedimin penal të saj, ajo mund të shtyjë ose të refuzojë konsultimin.

Në rastet kur shtetet nuk përcaktojnë vullnetarisht juridiksionin, pyetja që lind është: Cili shtet palë ka juridiksion, në rastet kur një shtetas që ndodhet në territorin e një shteti pale nëpërmjet përdorimit të sistemit kompjuterik sjell pasojat e veprës penale në territorin e një shteti tjetër? Pra në rastet kur veprimi kryhet nga një shtetas i huaj jashtë territorit dhe pasoja vjen në territorin e një shteti tjetër?

Në nenin 22 të konventës përcaktohen një sërë kriteresh, në bazë të cilave shtetet anëtare duhet të përcaktojnë kompetencën tokësore lidhur me veprat penale të renditura në nenet 2-11 të Konventës së Budapestit[23]. Megjithatë këto kritere nuk përcaktojnë juridiksionin e shteteve pale lidhur me rastet e mësipërme.

Prandaj është e nevojshme referimi në konventën e OKB-së kundër krimit të organizuar, në të cilën janë përcaktuar disa kritere, mbi bazën e të cilave përcaktohet natyra transnacionale e një krimi[24]. Një vepër penale ka një natyrë ndërkombëtare në qoftë se kryhet në më shumë se një shtet, ose kryhet në një shtet, por pjesa thelbësore e

[22] Shih nenin 22 të Konventës "Për krimin në fushën e kibernetikës", ratifikuar me ligjin nr 8888 datë 25.04.2002.
[23] Shih nenin 22 të Konventës "Për krimin në fushën e kibernetikës", ratifikuar nga ana e vendit tone me ligjin nr 8888 datë 25.04.2002 "Për ratifikimin e "Konventës në fushën e kibernetikës, të cilin theksohet se:
"Juridiksioni 1. Secila Palë merr masa të tilla legjislative ose të tjera, që janë të nevojshme për të caktuar juridiksionin për çdo vepër penale të kryer në pajtim me nenet 2 –11 të kësaj Konvente, kur një vepër e tillë kryhet: a) në territorin e tij; ose b) në bordin e një anijeje që mban flamurin e asaj Pale; ose c) në bordin e një avioni të regjistruar sipas ligjit të kësaj Pale; ose d) nga njeri prej shtetasve të saj, nëse vepra penale është e dënueshme sipas ligjit penal ku ajo është kryer ose nëse vepra është kryer jashtë juridiksionit territorial të çdo Shteti. 2. Secili Shtet mund të rezervojë të drejtën për të mos zbatuar ose për të zbatuar vetëm në raste të caktuara ose kushte të caktuara rregullat juridiksionale të parashikuara në paragrafët (1)b – (1)d të këtij neni ose të ndonjë pjese të tyre. 3. Secila Palë merr masa të tilla që janë të nevojshme për të caktuar juridiksionin mbi të gjitha veprat penale të përmendura në nenin 24, paragrafi (1) i kësaj Konvente, në rastet kur kryerësi i prezumuar i veprës penale është prezent në territorin e saj dhe ajo nuk e ekstradon atë tek një Palë tjetër, kryesisht mbi bazën e shtetësisë së tij/saj pas kërkesës së bërë për ekstradim. 4. Kjo Konventë nuk përjashton asnjë juridiksion penal të ushtruar në pajtim me ligjin vendas. 5. Nëse më shumë se një Palë pretendon juridiksionin mbi një vepër që prezumohet e kryer në pajtim me këtë Konventë, Palët e interesuara, kur është e përshtatshme, bëjnë një konsultë për të përcaktuar juridiksionin më të përshtatshëm për të bërë ndjekjen penale.
[24] Shih nenin 3 të Konventës kundër krimit te organizuar ndërkombëtar, e ratifikuar me ligjin nr. 8920, datë 11.7.2002.

përgatitjes, planit, drejtimit ose kontrollit është ndërtuar në një shtet tjetër, ose kryhet ne një shtet, por në të është përfshirë një grup kriminal i organizuar, i cili angazhohet ne aktivitete kriminale në më shumë se një shtet, ose kryhet në një shtet, por pasojat thelbësore i ka në një shtet tjetër. Karakteri transnacional i krimit kompjuterik derivon juridiksionin e një shteti për të ushtruar ndjekjen penale për këtë krim.

Një shtet do të ketë juridiksion territorial, edhe në qoftë se krimi është kryer jashtë territorit të tij, për sa kohë që një element konstituiv i figurës së veprës penale është kryer në atë Shtet. Në doktrinën juridike ky është quajtur juridiksioni territorial subjektiv. Juridiksioni territorial subjektiv, është variabël nga provueshmëria se elementi i krimit dhe krimi në vetvete janë krejtësisht të pandashëm. E thënë ndryshe nëse do të mungonte elementi përbërës, krimi nuk do të kishte ndodhur.

Këtë qëndrim ka mbajtur edhe Gjykata Ndërkombëtare e Drejtësisë(GJND)[25], në çështjen "Lotus" (France vs Turkey) (*Judgment*) të vitit 1927, nr. 10, në të cilën thekson se: "Turqia dhe Franca të dyja kishin juridiksion në lidhje me incidentin: d.m.th kanë juridiksion konkurrues...

Vepra ka prodhuar efektet e saj në anije turke dhe si pasojë në një vend të asimiluar me territorin turk, në të cilin zbatimi i ligjit penal turk nuk mund të kundërshtohet, madje edhe në lidhje me vepra penale të kryera atje nga të huajt. Pra, nëse një akt i kryer në det të hapur prodhon efektet e tij në një anije që mban flamur të një shteti të huaj ose në territor të huaj, të njëjtat parime duhet të zbatohen si në qoftë se territoret e dy shteteve të ndryshme janë të prekura, dhe konkluzioni duhet pra të jetë se nuk ka rregulla të ligjit ndërkombëtar që ndalojnë shtetin e anijes në të cilën efektet e veprës penale kanë ardhur, për ta konsideruar rastin si vepër penale të kryer në territorin e tij dhe për të ushtruar ndjekjen penale, në përputhje me rrethanat……..

Vepra penale për të cilën *Lieutenant Demons* është ndjekur penalisht ishte një akt - i neglizhencës apo pakujdesisë - që ka origjinën e vet në bordin e Lotus, ndërsa efektet e aktit janë ndier në bordin e Boz-Kourt. Këto dy elemente janë, ligjërisht, në tërësi të pandashme, aq shumë sa ndarja e tyre e bën veprën penale joekzistente ... Është e natyrshme që secili shtet duhet të jetë në gjendje për të ushtruar juridiksion dhe për ta bërë këtë në lidhje me këtë incident si një e tërë. Prandaj është një rast i juridiksionit konkurrues".

Të njëjtin qëndrim ka mbajtur edhe Gjykata e Lartë e Shteteve të Bashkuara të Amerikës. Kështu në rastin[26] Shtete e Bashkuara kundër Ivanov, ajo theksoi se:"rastet e mëparshme përbënin precedent për aplikimin e juridiksionit ekstraterritorial, për sa kohë që "efekte e dëshiruara dhe të dëmshme" kanë ndodhur brenda juridiksionit".

Gjykata duke iu referuar precedentit Shtetet e Bashkuara kundër Muench[27], theksoi se: "Qëllimi për të shkaktuar efekte brenda Shteteve të Bashkuara, e bën të arsyeshme zbatimin për personat jashtë territorit të Shteteve të Bashkuara të një statuti që nuk është shprehimisht ekstraterritorial në fushëveprim". Gjykata, gjithashtu, duke iu referuar precedentit Shtetet e Bashkuara kundër Steinberg, argumentoi se: "...Ka qenë prej kohësh e zakonshme dhe e pranuar përgjegjësia penale e një personi, i cili mund të akuzohet në vendin ku rezultojnë pasojat, edhe pse ai është jashtë juridiksionit në momentin kur ai fillon trenin e ngjarjeve, fryt i të cilave është pasoja e ardhur. "

Gjykata argumentoi se efektet e dëmshme të sulmeve të Ivanov në të vërtetë kanë

[25] Vendimin e Gjykatës Ndërkombëtare të Drejtësisë (GJND)², Çështja "Lotus" (France vs Turkey) (Judgment) të vitit 1927, Nr 10, 18–19.

[26] Shih vendimin Shtetet e Bashkuara kundër Ivanov, 175 F Supp 2d 367 (D Conn, 2001)

ndodhur në Shtetet e Bashkuara, duke deklaruar se: "..Fakti që kompjuterët janë aksesuar me anë të një procesi kompleks të iniciuar dhe kontrolluar nga një vend i largët nuk e ndryshon faktin se aksesimi i kompjuterëve, pra, pjesë e efektit të dëmshëm të ndaluar me statut, ka ndodhur në vendin ku kompjuterët janë të vendosura fizikisht, d.m.th. në vendndodhjen e OIB, pra në Vernon, Connecticut. Në një argument të dytë, gjykata deklaroi se pavarësisht logjikës së mëparshme, "në secilën prej statuteve për të cilat i pandehuri është akuzuar për një vepër materiale, ka prova të qarta se statuti kishte për qëllim për tu aplikuar ekstraterritorialisht."

Më lart theksuam se krimi kibernetik është shndërruar një nga format tipike të veprimit të krimit të organizuar. Përdorimi i internetit nga krimi organizuar në nivel ndërkombëtar shihet si një veprimtari që po njeh një rritje të konsiderueshme[28]. Përdorimi i internetit në Shqipëri, në pesë vitet e fundit, është trefishuar nga 20% në vitin 2009, në 60.1% në vitin 2014[29]. Mbi 80% e sulmeve kompjuterike në botë rezulton të kryhen nga grupe të organizuara kriminale, në tregje informale të krijuara mbi një cikël krijimi *malware*-esh, infektim kompjuterësh, vjelje *botnet*, vjelje e informacionit personal dhe të dhënave financiare etj. Kompania softuerike Norton, shkon edhe më tej, duke raportuar se në vitin 2011 rreth 90% e sulmeve vinin nga krimi i organizuar[30].

Krahas krimeve si mashtrim me kartat e kreditit, shpërndarjes së materialeve pornografike me fëmijë apo piratimi audovizual, interneti thjeshton trafikimin dhe shpërndarjen e drogës, rekrutimin e viktimave të trafikimit, shpërndarjen e mallrave false dhe shumë veprimtari të tjera kriminale, si trafiku i drogës dhe i qenieve njerëzore[31].

Edhe në Shqipëri, përdorimi në rritje i internetit ka shtuar rrezikun e formave të organizuara kriminale, nëpërmjet përdorimit të teknologjisë. Krimi në fushën kibernetike ka njohur një rritje progresive. Krimi kibernetik në formë të organizuar është një ndër krimet që, ndoshta në dukje jo shumë i përhapur, priret drejt sofistikimit, element ky që e ka vështirësuar goditjen e tij në Shqipëri.

## 3. Sovraniteti territorial dhe hyrja ndërkufitare në sistemet kompjuterike

Aftësia për të aksesuar në të dhëna kompjuterike, të cilat gjenden në juridiksione të tjera, në mënyrë të shpejtë, është një aspekt i rëndësishëm i hetimeve penale moderne. Megjithatë, fakti që organet proceduese kanë kapacitetin për të kryer kërkime të tilla nuk e bëjnë të lejuar atë. Kjo zakonisht do të konsiderohet si një shkelje e sovranitetit territorial për ato nga një vend që kryejnë hetimet në një vend të huaj pa autorizimin e atij vendi. Parim i të drejtës ndërkombëtare parashikon se asnjë shtet nuk mund të zbatojë juridiksionin e vet në territorin e një shteti tjetër Sovran[32]. Rrjedhimisht, një

[27] Shih vendimin Shtetet e Bashkuara të Amerikës, v. Stephen MUENCH, Defendant-Appellant. 97-2304. No. Decided: September 10, 1998.

[28] Transnational Organized Crime: A Growing Threat to National and International Security, retrieved from http:/ /m.whitehouse.gov/administration/ eop/nsc/transnational-crime/threat

[29] Shiko Internet World Stats, Albania, aksesuar më 13/11/2014, http://www.internetworldstats.com/ euro/ al.htm

[30] Shih Fabian Zhilla Besfort Lamallari "Vlerësimi Riskut të Krimit të Organizuar në Shqipëri" Fondacioni Shoqëria e Hapur për Shqipërinë, Tiranë 2015, f. 95.

[31] Trafficking in Human Beings: Internet recruitment. 2007 Council of Europe

[32] Shih SS Lotus (France v Turkey) (Judgment) [1927] PCIJ (ser A) No 10, 18–19. Shih, eg, Royal Canadian Mounted Police, Protocol on Foreign Criminal Investigators in Canada (15 February 2007) <http://www.rcmp-grc.gc.ca/ interpol/fcip-pcece-eng.htm>.

shtet nuk mund të zbatojë ligjet e tij, të kryejë hetime apo arrestojë një person në territorin e një shteti tjetër, pa autoritet të qartë ligjore që e lejon të bëjë këtë[33].

Mbrojtja e sovranitetit është një parim detyrues për shtetet palë, i parashikuar në mënyrë eksplicite nga konventa e OKB-së kundër krimit të organizuar[34]. Sipas këtij parimi shtetet palë do të zbatojnë detyrimet e tyre që rrjedhin nga kjo konventë në pajtim me parimet e barazisë së sovranitetit dhe integritetit territorial të shteteve dhe të mosndërhyrjes në punët e brendshme të shteteve të tjera. Asgjë në këtë konventë, nuk i jep të drejtën një shteti palë që të ushtrojë juridiksionin e tij në territorin e një shteti tjetër, dhe të kryejë funksione, që janë e drejtë ekskluzive e autoriteteve të shtetit tjetër sipas ligjit të tij të brendshëm.

Shqetësimet lidhur me të drejtat procedurale të autorëve, të privatësisë dhe mbrojtjes të dhënat personale, baza ligjore për qasje në të dhënat e ruajtura në juridiksione të huaja, si dhe sovraniteti kombëtar pengojnë ndërhyrjen ndërkufitare të paautorizuar. Nga anë tjetër procedurat e ndihmës së ndërsjellë juridike, shpesh herë janë joefikase, të pazbatueshme, si dhe bashkëpunimi nga ofruesit është në rënie. Ka një trend midis ofruesve të mos bashkëpunojnë me organet ligjzbatuese edhe kur lejohet nga ligji për ta bërë. Për këto arsye, shumica e këtyre organeve mendojnë se duhet zgjeruar mundësitë për akses ndërkufitar në të dhëna për qëllime të drejtësisë penale, por me masat mbrojtëse të nevojshme.

Raportet mbi mbikëqyrjen masive dhe aktivitetet e tjera të institucioneve të sigurisë kombëtare kanë shkaktuar mosbesim tek institucionet e sigurisë kombëtare, ndryshme nga ato të autoriteteve të drejtësisë penale.

Çështja e aksesit ndërkufitar në provat elektronike është njohur që nga viti 1980, edhe pse në atë kohë çështja nuk duket "shumë impresionuese dhe në fazat embrionale"[35]. Megjithatë, ndryshimet në teknologji treguan se çështja shpejt u bë urgjente dhe u debatua, ndër të tjera, nga Komiteti Evropian për problemet kriminale, G8 dhe Këshilli i Evropës[36]. Gjatë diskutimit u bë një analizë e detajuar e rasteve, në të cilat mund të jetë e pranueshme për shtetet që të veprojnë në mënyrë të njëanshme dhe ato në të cilat nuk mund të bënin diçka të tillë.

Hartuesit në fund konstatuan se nuk ishte ende e mundur për të përgatitur një regjim të plotë, ligjërisht të detyrueshëm në këtë fushë. Pjesërisht, kjo ishte për shkak të mungesës së përvojës konkrete me të tilla situata deri tani; dhe, pjesërisht, kjo ishte për shkak të një kuptim se zgjidhja e duhur shpesh vjen nga rrethanat e sakta të rastit individual, duke e bërë të vështirë për të formuluar rregulla të përgjithshme.

Ata vendosën që vetëm të parashikonin në nenin 32 të konventës dy situata në të cilat të gjithë ranë dakord se veprimi i njëanshëm është i lejueshëm. Ata ranë dakord për të mos rregulluar situata të tjera deri në atë kohë, derisa përvoja e mëtejshme të mblidhet dhe diskutime të mëtejshme të mbahen për të. Në këtë drejtim, neni 39/3 i konventës, parashikon që situata të tjera as nuk janë të autorizuar as nuk janë të përjashtuara[37].

[33] Teresa Scassa, Robert J Currie, 'New First Principles? Assessing the Internet's Challenges to Jurisdiction' (2011) 42 Georgetoën Journal of International Laë 1017, 1029.

[34] Shih nenin 4 të Konventës kundër krimit te organizuar nderkombetar, e ratifikuar me ligjin nr. 8920, datë 11.7.2002.

[35] Shih Jonathan Clough "A world of difference: The Budapest convention on cybercrime and the challenges of harmonisation". Monash University laë revieë Vol 40 no 3, pg 22.

[36] Shih Transborder Access and Jurisdiction Discussion Paper, above n 15, 6 [14]. Strasbourg, 3 December 2014 (Provisional) T-CY (2014)16 Cybercrime Convention Committee (T-CY).

[37] Shih nenin 39/3 të Konvetës "Për krimin në fushën e kibërnitikës", ratifikuar me ligjin nr 8888 datë 25.04.2002.

Ne nenin 32 të konventës është parashikuar se: "Hyrja ndërkufitare në të dhënat e regjistruara në kompjuter me leje ose kur janë të hapura për publikun pa marrë autorizimin nga pala tjetër, një palë mund: a) të hyjë në të dhënat e regjistruara në kompjuter të hapura për publikun (burim i hapur), pavarësisht se ku ndodhen gjeografikisht të dhënat; ose b) të hyjë ose të marrë, nëpërmjet një sistemi kompjuterik në territorin e tij, të dhënat e regjistruara në kompjuter tek një palë tjetër, nëse pala merr lejen e ligjshme dhe të vullnetshme të personit që ka kompetencën ligjore t'i njoftojë të dhënat palës nëpërmjet sistemit kompjuterik".

Siç konstatohet në dispozitën e mësipërme janë parashikuar dy situata të kërkimit ndërkufitar të trajtuara nga Konventa. E para thotë se një palë mundet, pa autorizimin e palës tjetër "të aksesojë të dhënat kompjuterike publike (burim i hapur) , pavarësisht se ku e dhëna është e vendosur gjeografikisht"[38]. Kjo thjesht pranon se organet proceduese mund të shfrytëzojnë të dhënat në të njëjtën mënyrë si çdo anëtar i publikut, pavarësisht se ku prova është e vendosur. *Rasti i* dytë dhe më i diskutueshëm lejon një palë të "aksesojë ose të marrë, nëpërmjet një sistemi kompjuterik në territorin e saj, të dhënat kompjuterike të vendosura në një palë tjetër, nëse pala merr pëlqimin vullnetar dhe të ligjshëm të personit që ka autoritet ligjor për të zbuluar të dhënat për palën nëpërmjet atij sistemi kompjuterik".

Disa vende, veçanërisht Rusia, kanë kundërshtuar këtë dispozitë mbi bazën se kjo mund të dëmtojë sovranitetin dhe sigurinë e vendeve anëtare dhe të drejtat e qytetarëve të tyre"[39]. Qëndrimi rus ndaj kësaj dispozite, pa dyshim, nuk u ndihmua nga fakti se agjentët e Byrosë Federale të Hetimit, ishin njohur se kanë zhvilluar një kërkim ndërkufitar të mbuluar të kompjuterëve rusë, në rrjedhën e hetimit të tyre kundër dy shtetasve rusë: Alexey Ivanov dhe Vasily Gorshkov[40].

Është e rëndësishme të theksohet se neni 32 nuk thotë asgjë për situatën që u ngrit në këtë rast, as për ndonjë kërkim ndërkufitar të fshehtë. Kërkimet ndërkufitare të pambuluara nga Konventa nuk janë" as të autorizuara, as të përjashtuara"[41] dhe çështja specifike që u ngrit nga rasti Ivanov/Gorshkov mbetet e pazgjidhur dhe kontraversiale.[42] Prandaj, kundërshtimet ndaj nenit 32 (b) mbi bazën se autorizon kërkimet e tilla të fshehta janë të gabuara. Kjo nuk do të thotë se neni 32 (b) nuk është kontraversial.

Në shumë raste, hetuesit nuk mund të sigurojnë që ata janë në gjendje për të gjurmuar një komunikim për burimin e tij duke ndjekur gjurmët përmes të dhënave të transmetimeve të mëparshme, pasi të dhënat kryesore të trafikut mund të jenë fshirë automatikisht nga një ofrues shërbimi në zinxhirin e transmetimit para se ato të mund të ruhen. Prandaj është e rëndësishme për hetuesit në çdo pale që të kenë aftësinë për të marrë të dhëna të trafikut në kohë reale në lidhje me komunikimet që kalojnë nëpërmjet një sistemi kompjuterik në palët e tjera[43].



[38] Shih nenin 32/a të. Konvetës "Për krimin në fushën e kibërnitikës", ratifikuar me ligjin nr 8888 datë 25.04.2002

[39] Shih "Putin Defies Convention on Cybercrime", CNews (online), 27 March 2008. See also Cybercrime Convention Committee (T-CY), 'Report on the 2nd Multilateral Consultation of the Parties d Strasbourg, 13 and 14 June 2007' (Information Document No CM/Inf(2007)38, Council of Europe, 20 July 2007) [6]

[40] Shih generally United States v Gorshkov (WD Wash, No CR00-550C, 23 May 2001); United States v Ivanov, 175 F Supp 2d 367 (D Conn, 2001)

[41] Shih Convention Explanatory Report, above n 25, [293]. Convention art 39(3) provides that '[n]othing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party

[42] For a more detailed discussion see Susan W Brenner and Joseph J Schwerha IV, 'Transnational Evidence Gathering and Local Prosecution of International Cybercrime' (2002) 20 John Marshall Journal of Computer and Information Law 347.

[43] Shih nenin 33 të Konventës "Për krimin në fushën e kibernitikës", ratifikuar me ligjin nr. 8888 datë 25.04.2002.

Në jurisprudencën e Republikës së Shqipërisë ka një qasje, sipas së cilës të dhënat kompjuterike, të cilat ndodhen në një shtet tjetër, të merren mbi bazën e vendimit të gjykatës, i iniciuar me kërkesë të organit të prokurorisë, i përcjellë nëpërmjet pikës së kontaktit subjektit që i zotëron këto të dhëna. Kështu Gjykata e Shkallës së Parë, Tiranë, në vendimin nr. 438 datë 19.2.2016[44] ka arsyetuar se: "Gjykata vlerëson ta pranojë kërkesën e organit të prokurorisë për të urdhëruar shoqërinë "Facebook" me adresë 1601 Willow Road, Menlo Park CA 94025, Kaliforni, Shtetet e Bashkuara të Amerikës", për t'i dorëzuar organeve te policisë gjyqësore, të Drejtorisë së Përgjithshme të Policisë së Shtetit të Republikës së Shqipërisë, të dhënat e regjistrimit si emër, mbiemër, datëlindje, adresa, adresa e postës elektronike, nr. telefoni, etj., duke saktësuar dhe ndryshimet e bëra, për përdoruesit e profileve; https//www.facebook.com/469494676572993/?fref=ts, adresat elektronike te rrjetit "Facebook" dhe të dhënat e regjistrimit, adresat të cilat administrohen nga dy profilet e mësipërme, IP-të nga të cilat janë aksesuar linket e mësipërme dhe adresat e tjera te rrjetit "Facebook" në administrim te tyre, për periudhën nga dt. 1.1.2015 e në vijim".

Pyetjet që ngrihen janë: A mundet që gjykatat e Republikës së Shqipërisë të urdhërojnë subjektet, që nuk ndodhen në territorin e vendit tonë, të vënë në dispozicion të dhënat kompjuterike? Një rast i tillë a gjen mbulim ligjor në nenin 32 të konventës?

Lidhur me pyetjen e parë, duke iu referuar trajtimit të bërë më sipër për ndihmën e ndërsjellë, përgjigja është absolute negative, sepse cenohet parimi i të drejtës ndërkombëtare, sipas të cilit asnjë shtet nuk mund të zbatojë juridiksionin e vet në territorin e një shteti tjetër.

Ndërsa lidhur me pyetjen e dytë theksojmë se neni 32 i konventës, e kushtëzon hyrjen ndërkufitare në të dhënat e regjistruara në kompjuter, me leje, ose kur janë të hapura për publikun, pa marrë autorizimin nga pala tjetër, me ekzistencën e kushteve jo komulativ si:

a) të dhënat kompjuterike të regjistruara në kompjuter të jenë hapura për publikun (burim i hapur), pavarësisht se ku ndodhen gjeografikisht të dhënat;

b) ose nëse pala merr lejen e ligjshme dhe të vullnetshme të personit që ka kompetencën ligjore t'i njoftojë të dhënat palës nëpërmjet sistemit kompjuterik.

Në rastin objekt studimi të dhënat e kërkuara nga gjykata, si të dhënat e regjistrimit si emër, mbiemër, datëlindje, adresa, adresa e postes elektronike, nr. telefoni, etj., nuk janë të hapura për publikun. Ato janë të dhëna personale, të cilat nuk janë të aksesueshme nga publiku.

Ndërsa lidhur me kushtin e dytë mendojmë se Republika e Shqipërisë duhet të marrë leje të ligjshme dhe të vullnetshme nga subjekti *Facebook*, si person, i cili është i autorizuar në mënyrë të ligjshme për të zbuluar të dhënat.

Është për t'u theksuar fakti se subjekti *Facebook*, në të gjitha rastet e sipërtreguara i është përgjigjur pozitivisht kërkesës së vendit tonë, pavarësisht procedurës të ndjekur nga organet e drejtësisë.

Duke vërejtur interpretimet e "keqkuptuara" nga shtete të ndryshme, në seancën plenarë të 8-të të mbajtur në dhjetor të vitit 2012, Komiteti i Konventës së Kibernetikës (T-CY) vendosi që të përgatitej një udhëzues, i cili të kishte si qëllim lehtësimin e përdorimit dhe zbatimit efektiv të konventës së Budapestit. Ky komitet në seancën e

[44] I njëjti qëndrim është mbajtur edhe në vendimet nr 439 datë 19.2.2016; nr 500 akti datë 18.3.2016; nr 526 datë 10.3.2016; nr 532 datë 12.3.2016: nr 1005 datë 20.07.2016 të Gjykatës së Shkallës së Parë Tiranë.

12-të plenare të mbajtur me datë 3.12.2014 miratoi raportin *"Qasja ndërkufitare në të dhënat kompjuterike dhe juridiksionin: Opsionet për veprim të mëtejshëm nga T-CY"*, i përgatitur nga nëngrupi Ad-hoc[45].

Në këtë raport arsyetohet se neni 32/b i konventës përben një rast përjashtimor nga parimi i territorialitetit dhe ndërhyrjeve të njëanshme ndërkufitare pa pasur nevojë për ndihmë të ndërsjellë, por e aplikuar në rrethana të kufizuara. Shtetet palë janë inkurajuar që të përdorin në mënyrë efektive të gjitha format e bashkëpunimit ndërkombëtar të parashikuara nga Konventa e Budapestit, duke përfshirë ndihmën reciproke. Në përgjithësi, praktikat, procedurat, kushtet dhe masat mbrojtëse ndryshojnë në mënyrë të konsiderueshme nga njëri shtet në tjetrin.

Në këtë raport sugjerohet që komiteti të marrë në konsideratë hartimin e një projekt-udhëzimi në lidhje me adoptimin e qasjes ndaj ndërhyrjes ndërkufitare. Madje propozohet që të hartohet një protokoll shtesë i konventës kundër krimin kibernetik mbi kufijtë e ndërhyrjes ndërkufitare, i cili do të ishte i nevojshëm.

Në lidhje me rastin e ndërhyrjes ndërkufitare në burimin e hapur të disponueshëm publikisht së të dhënave kompjuterike, në këtë raport nuk janë ngritur çështje specifike dhe nuk ka udhëzime të mëtejshme nga komiteti[46]. Është e qartë që organet hetimore mund të kenë ndërhyrje ndërkufitare në çdo të dhënë që publiku mund të hyjë dhe për këtë qëllim të regjistrohen për shërbimet që janë në dispozicion të publikut. Nëse një pjesë e një ueb-faqe, shërbimi është e mbyllur për publikun, atëherë nuk jemi në kushtet e burimit të hapur[47].

Në raport janë dhënë përcaktime të detajuara lidhur me termat që determinojnë rastin e dytë të parashikuar nga konventa të ndërhyrjes ndërkufitare[48], duke iu referuar shembullit tipik të një *email*-i të një personi, i cili mund të ruhet në një vend tjetër nga ai i ofruesit të shërbimit, ose, ai mund të ruajë me dashje, të dhëna në një vend tjetër. Këta persona mund t'u zbulojnë vullnetarisht të dhënat kompjuterike organeve të hetimit, ose t'i lejojë ata të kenë ndërhyrjes ndërkufitare.

Lidhur me termat "kufi" dhe "vendndodhje" raporti thekson se ndërhyrja ndërkufitare nënkupton qasjen në mënyrë të njëanshme së të dhënave kompjuterike të ruajtura në një shtet palë tjetër, pa kërkuar ndihmë të ndërsjellë juridike[49]. Këta terma i referohen të dhënave të ruajtura kompjuterike të vendosura në një palë tjetër. Kjo nënkupton se ndërhyrja mund të përdoret nëse është e ditur se ku ndodhen të dhënat, duke përjashtuar situatat kur të dhënat nuk janë të ruajtura në një shtet palë tjetër, ose kur është e paqartë se ku ndodhen ato të ruajtura. Një shtet palë nuk mund të përdorë ndërhyrjen ndërkufitare për të bërë zbulimin e të dhënave që ruhen në vend[50].

Në kuptimin të termit "aksesi pa autorizimin e një pale tjetër", sipas raportit, nuk

[45] Shih Transborder Access and Jurisdiction Discussion Paper, above n 15, 6 [14]. Strasbourg, 3 December 2014 (Provisional) T-CY (2014)16 Cybercrime Convention Committee (T-CY)
[46] Shih nenin 32/a të Konventës "Për krimin në fushën e kibernetikës", ratifikuar me ligjin nr 8888 datë 25.04.2002
[47] Shih Transborder Access and Jurisdiction Discussion Paper, above n 15, 6 [14]. Strasbourg, 3 December 2014 (Provisional) T-CY (2014)16 Cybercrime Convention Committee (T-CY)
[48] Shih nenin 32/b të Konventës "Për krimin në fushën e kibernetikës", ratifikuar me ligjin nr. 8888, datë 25.4.2002.
[49] Paragraph 293 Explanatory Report to the Budapest Convention.
[50] Shih Transborder Access and Jurisdiction Discussion Paper, above n 15, 6 [14]. Strasbourg, 3 December 2014 (Provisional) T-CY (2014)16 Cybercrime Convention Committee (T-CY)
[51] Shih Transborder Access and Jurisdiction Discussion Paper, above n 15, 6 [14]. Strasbourg, 3 December 2014 (Provisional) T-CY (2014)16 Cybercrime Convention Committee (T-CY).
[52] Shih Transborder Access and Jurisdiction Discussion Paper, above n 15, 6 [14]. Strasbourg, 3 December 2014 (Provisional) T-CY (2014)16 Cybercrime Convention Committee (T-CY).

kërkohet ndihma e ndërsjellë juridike, si dhe konventa nuk kërkon njoftimin e palës tjetër, por as nuk përjashton atë. Palët mund të njoftojnë palën tjetër nëse e gjykojnë të përshtatshme.

Për nocionin e "pëlqimit", në raport u argumentua se pëlqimi duhet të jetë i ligjshëm dhe vullnetar, që do të thotë se sigurimi i ndërhyrjes ose pajtimi për të zbuluar të dhënat nuk mund të detyrohet ose të mashtrohet[51]. Në shumicën e shteteve palë, bashkëpunimi në një hetim penal do të kërkonte pëlqim të qartë.

Në të gjitha rastet autoritetet e zbatimit të ligjit duhet të zbatojnë të njëjtat standarde procedurale ligjore, që parashikohen në vendin e tyre. Nëse ndërhyrja apo zbulimi nuk do të lejohej brenda vendit, do të ishte e palejueshme ndërhyrja në një vend tjetër.

Person i cili është "i autorizuar në mënyrë të ligjshme" për të zbuluar të dhënat, mund të ndryshojë në varësi të rrethanave, natyrës së personit dhe ligjit të aplikueshëm në fjalë. Për shembull, *email-i* i një personi mund të ruhet në një vend tjetër nga ofruesi i shërbimit, ose, një person mund që me qëllim të ruajë të dhënat në një vend tjetër. Këta persona mund të rifitojnë të dhënat dhe, ata kanë autoritetin e ligjshëm, që të mund të zbulojnë vullnetarisht të dhënat për zyrtarët e zbatimit të ligjit apo të lejojnë që zyrtarë të tillë të hynë te të dhënat[52].

Vendndodhja e personit që jep pëlqimin për të siguruar ndërhyrje ndërkufitare ose zbuluar të dhëna kompjuterike është në territorin e palës kërkuese. Megjithatë, situata të ndryshme janë të mundshme. Është e mundshme që personi fizik apo juridik të ndodhet në territorin e autoritetit kërkues të zbatimit të ligjit kur ai pranon të zbulojë ose sigurojë qasje. Personi, gjithashtu, mund të gjendet fizikisht në një vend të tretë kur pajtohet që të bashkëpunojë ose të ofrojnë qasje.

## 4. Konkluzione

- Dimensioni transnacional që ka fituar sot krimi kompjuterik, karakterizon çdo veprimtari hetimore që, edhe kur zhvillohet ende në nivel lokal, priret të marrë tipare përtejterritoriale, bashkëpunimi ndërkombëtar përfaqëson një parakusht për çdo veprimtari të përbashkët lufte.

- Një vepër penale ka një natyrë ndërkombëtare në qoftë se kryhet në më shumë se një shtet, ose kryhet në një shtet, por pjesa thelbësore e përgatitjes, planit, drejtimit ose kontrollit është ndërtuar në një shtet tjetër, ose kryhet ne një shtet, por në të është përfshirë një grup kriminal i organizuar, i cili angazhohet ne aktivitete kriminale në më shumë se një shtet, ose kryhet në një shtet, por pasojat thelbësore i ka në një shtet tjetër. Karakteri transnacional i krimit kompjuterik e zhvendos juridiksionin e një shteti për të ushtruar ndjekjen penale për këtë krim.

- Ndërhyrja ndërkufitare nënkupton qasjen në mënyrë të njëanshme së të dhënave kompjuterike të ruajtura në një shtet palë tjetër pa kërkuar ndihmë të ndërsjellë juridike. Këta terma i referohen të dhënave të ruajtura kompjuterike të vendosura në një Palë tjetër. Kërkimet ndërkufitare të pambuluara nga Konventa nuk janë "as të autorizuara, as të përjashtuara".

- Komiteti duhet të marrë në konsideratë, hartimin e një projektudhëzimi në lidhje me adoptimin e qasjes ndaj ndërhyrjes ndërkufitare, madje kërkohet që të hartohet një protokoll shtesë i konventës kundër krimit kibernetik, mbi kufijtë e ndërhyrjes ndërkufitare, i cili do të ishte i nevojshëm.

# Bibliografi


1. S.Schjolberg,"*The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva"*, 2008.
2. Making the ëorld safer from drugs, crime and terrorism - The European Union (EU) and the United Nations Office on Drugs and Crime (UNODC), 2015.
3. David Felsen, Akis Kalaitzidis " A historical overvieë of transnational crime".
4. Bossard A., Transnational Crime and Criminal Laë, University of Chicago, Office of international Criminal Justice, 1990.
5. Mueller, G.O, Transnational Crime Definitions and Concepts, 2001.
6. Serrano,M., Transnational organized crime and International Security: Business as usually, 2002.
7. Sheptycki, J., Against transnational organized crime, University of Toronto Press, 2003.
8. Itali-Shqipëri: Instrumente ligjorë dhe teknika të luftës kundër krimit të organizuar transnacional përballje përvojash nën kujdesin e Corrado Lembo, Koordinator shkencor i Kursit të trajnimit për gjyqtarë, prokurorë dhe oficerë të policisë gjyqësore (Tiranë, 5-16 mars 2007; Romë, 15-19 tetor 2007; Tiranë, 12-16 nëntor 2007).
9. Agnés Cadet-Taïrou and others, "Substances psychoactives, usagers et marchés: les tendances récentes (2015-2016)", Tendances, vol. 8, No. 115 (December 2016).
10. Europol, IOACTA 2016: Internet Organized Crime Threat Assessment , The Hague, 2016.
11. "Police ëarning after drug traffickers' cyber-attack", 16 October 2013, BBC News. Available at http:// www.bbc.com/ neës/world-europe-24539417. Aksesuar më 14.04.2018.
12. Cadet-Taïrou and others, "Substances psychoactives, usagers et marchés: les tendances récentes".
13. Transnational Organized Crime: A Growing Threat to National and International Security, retrieved from http://m.ëhitehouse.gov/administration/ eop/nsc/transnational-crime/threat.
14. Internet Ëorld Stats, Albania, aksesuar më 13/11/2014,http://www.internetëorldstats.com/euro/al.htm
15. Fabian Zhilla Besfort Lamallari "Vlerësimi Riskut të Krimit të Organizuar në Shqipëri" Fondacioni Shoqëria e Hapur për Shqipërinë, Tiranë 2015
16. Trafficking in Human Beings: Internet recruitment. 2007 Council of Europe
17. Royal Canadian Mounted Police, Protocol on Foreign Criminal Investigators in Canada (15 February 2007) <http://www.rcmp-grc.gc.ca/interpol/fcip-pcece-eng.htm>.
18. Teresa Scassa, Robert J Currie, 'New First Principles? Assessing the Internet's Challenges to Jurisdiction' (2011) 42 Georgetoën Journal of International Laë 1017, 1029.
19. Jonathan Clough "A world of difference: The Budapest convention on cybercrime and the challenges of harmonisation". Monash University laë revieë Vol 40 no 3,
20. Transborder Access and Jurisdiction Discussion Paper, above n 15, 6 [14]. Strasbourg, 3 December 2014 (Provisional) T-CY (2014)16 Cybercrime Convention Committee (T-CY).
21. Putin Defies Convention on Cybercrime', CNews (online), 27 March 2008 . See also Cybercrime Convention Committee (T-CY).
22. 'Report on the 2nd Multilateral Consultation of the Parties d Strasbourg, 13 and 14 June 2007' (Information Document No CM/Inf(2007)38, Council of Europe, 20 July 2007) [6].
23. Generally United States v Gorshkov (WD Wash, No CR00-550C, 23 May 2001); United States v Ivanov, 175 F Supp 2d 367 (D Conn, 2001).
24. Convention Explanatory Report, above n 25, [293]. Convention art 39(3) provides that '[n]othing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.
25. Susan W Brenner and Joseph J Schwerha IV, 'Transnational Evidence Gathering and Local Prosecution of International Cybercrime' (2002) 20 John Marshall Journal of Computer and Information Law 347.
26. Transborder Access and Jurisdiction Discussion Paper, above n 15, 6 [14]. Strasbourg, 3 December 2014 (Provisional) T-CY (2014)16 Cybercrime Convention Committee (T-CY).
27. Konventa "Për krimin në fushën e kibernetikës", ratifikuar me ligjin nr 8888 datë 25.4.2002.
28. Konventa kundër krimit te organizuar ndërkombëtar, e ratifikuar me ligjin nr. 8920, datë 11.7.2002.
29. Vendimet nr 439 datë 19.2.2016, nr 500, akti datë 18.3.2016; nr 526 datë 10.03.2016; nr 532 datë 12.3.2016, nr 1005, datë 20.07.2016 të Gjykatës së Shkallës së Parë Tiranë.
30. Vendimi i Gjykatës Ndërkombëtare të Drejtësisë (GJND), çështja "Lotus" (France vs Turkey) (Judgment) të vitit 1927, Nr 10, 18–19.
31. Vendimi Shtetet e Bashkuara kundër Ivanov, 175 F Supp 2d 367 (D Conn, 2001)
32. Vendimi Shtetet e Bashkuara të Amerikës, v. Stephen MUENCH, Defendant-Appellant. 97-2304. No. Decided: September 10, 1998.

**Adresa interneti:**

1. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf akses 13 shtator 2018.
2. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf akses 13 shtator 2018.
3. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 akses 13 shtator 2018.

# Kiberdevianca dhe roli i oficerëve të mbrojtjes së të dhënave (DPO), në parandalim: domosdoshmëri e kualifikimit të strukturave ligjzbatuese


■**Dr. (proc.) Silva IBRAHIMI**
*Universiteti i Tiranës*
*silva.ibrahimi@yahoo.it*

■**Dr. Eglantina DERVISHI**
*Universiteti i Tiranës*

■**Dr. Cav. Ervin IBRAHIMI**
*Përfaqësuesi i Këshillit të Sigurisë, Itali*

■**Dr. Eleonora LUCIANI**
*Total Service s.a.s.,Itali*



**Abstrakt**

*Parandalimi, është padyshim një nga pikat kryesore të kujdesit shëndetësor dhe social! Masmedia, teknologjia dhe sistemi i teknologjisë së informacionit, janë mjetet me ndikimin më shumëdimensional në zhvillimin konjitiv dhe psikologjik të jetës shoqërore të një personi. Qëllimi i këtij artikulli është të eksplorojë disa nga sjelljet devijante kibernetike, dhe rolin e strukturave të rendit, sigurisë dhe mbrojtjes kibernetike, si oficerët e mbrojtjes së të dhënave (DPO), që ekzistojnë në procesin e parandalimit të digjitalizimit të internetit. Ky artikull hulumton aspektet bazë të subkulturës devijante kibernetike dhe rolin e oficerëve të DPO-së, në investigimin dhe parandalimin e veprimeve ekstreme kriminale. Zbatimi i strategjive të mbrojtjes dhe sigurisë së konsumatorit nga lundrimi i rrezikshëm dhe sjellja e rrezikshme janë më të rëndësishme për krijimin e prototipit psikoinformatik për personat me tendencë të lartë të kriminalitetit aktiv, duke i fokusuar ata më tepër drejt zhvillimit të personalitetit antisocial.*



**Fjalëkyçe:**
**sjellje kiberdeviante, teknologjia e digjitalizuar, DPO, siguria kombëtare, parandalim.**

## 1. Hyrje

Zhvillimet teknike dhe teknologjike, kanë bërë që jeta njerëzore të ndryshojë shumë, gjatë dekadave të fundit. Brenda zhvillimit dhe përsosjes së teknologjisë në përgjithësi, dhe asaj informative në veçanti, qëndron *"hapësira kibernetike*", si një pjesë e rëndësishme e ndërveprimit. Interneti mund të ketë një ndikim të fuqishëm në zhvillimin e sistemeve të vlerave dhe formësimin e sjelljes.

Rritja e jashtëzakonshme në përdorimin e teknologjisë kompjuterike dhe informacionit, TIK, ka sjellë një gamë shumë të gjerë të mundësive të eksplorimit dhe cenueshmërisë ndaj rrezikut të ekspozimit në popullatën e të miturve. Duke pasur parasysh karakterin e saj global dhe aksesin e lehtë përmes pajisjeve të lidhura në rrjet, interneti ka ndryshuar padyshim socio-evolucionin e njerëzimit. Ndikimet e TIK-ut në inteligjencën fluide dhe të kristalizuar të njeriut, janë dy argumente të rëndësishme në mbështetje të kësaj premise. Alienizimi përmes teknologjisë ka ofruar mundësi të reja kriminaliteti, që mund të përdorin të njëjtat avantazhe, të ofruara nga këto teknologji, për të përmbushur objektivat e tyre. Numri gjithnjë në rritje i përdoruesve të internetit, i ofron shoqërisë perspektivën për të përshpejtuar komunikimet në jetën e përditshme, - edhe nxitjen e marrëdhënieve, reduktimin e transaksioneve dhe shpenzimeve, bërjen e biznesit, rritjen e aksesit ndaj informacionit dhe krijimin e një *identiteti global*.

Nga njëra anë, me zhvillimin e mundësive të reja për rritje ekonomike dhe sociale, shpërndarja e teknologjisë ka ndryshuar imazhin aktual të konceptit të krimit dhe paraqet sfida të reja për komunitetin, për mikro dhe makro-politikëbërësit si dhe për oficerët ligjzbatues. Hapësira kibernetike është vazhdimisht një burim i aktiviteteve të ndryshme ilegale, që përfshijnë jo vetëm llojet e reja të krimit të shfaqur, të tilla si *hakerimi* ose ndjekja përmes programeve të kriptimit ose *spywares*, por gjithashtu

paraqet një shqetësim specifik në shtimin e të drejtës për mbrojtjen e të dhënave personale dhe sigurinë kombëtare, në një rrafsh më të gjerë.

Nga ana tjetër, devijanca agresive kibernetike ka çuar gjithashtu në një fluks të shtuar të migrimit të krimit tradicional siç janë ekspozimi keqdashës, trafikimi, pornografia dhe abuzimi i të miturve, mashtrimet, vjedhjet etj. Nga mënyra sesi ndërtojmë një profil të hetimit, burimet e informacionit, hartimin e planeve, fazat dhe ndihmën që vjen përmes profilizimit, ne mund të ndërtojmë të dhëna mbi profilin psikologjik të autorit dhe grupit të synuar si dhe me sjelljen stimuluese dhe gjendjen psikologjike të një individi në kryerjen e veprës penale[1].

Pa dyshim, lufta kundër krimit kibernetik kërkon forcimin, qoftë në nivel ligjor, por edhe në nivelin penal, procedural dhe të instrumenteve që lejojnë hetimin dhe ndjekjen penale të personave që abuzojnë me TIK-un për kryerjen e veprave penale. Dimensioni i tanishëm global i krimit kibernetik, dhe natyra ndërkufitare e rrjeteve të informacionit përmes TIK-ut, gjithashtu sjellin nevojën për harmonizimin e qasjeve legjislative dhe veprimeve të koordinuara, në parandalimin dhe hetimin e krimit kibernetik, në nivel kombëtar, rajonal dhe ndër-rajonal[2].

Megjithëse rrjetet e TIK-ut kryesisht janë pronësi private, qasja gjithëpërfshirëse e krimit kibernetik përfshin gjithashtu zhvillimin e mjeteve për bashkëpunim efektiv, me sektorët e informatikës industriale që nxisin zbatimin e metodave bashkërregullatore dhe vetërregulluese.

Çdo aktor në këtë mjedis shumëplanësh, të interesuar në luftimin dhe parandalimin e krimit në hapësirën kibernetike, përballet me një gamë të gjerë sfidash që mund të lidhen me problemet e përgjithshme të natyrës globale të kibernetikës, ose karakterit unik të lidhur me ndryshimin e natyrës së detyrave, përgjegjësive dhe funksioneve të palëve të përdorura, për të vepruar në botën reale apo në hapësirën kibernetike-virtuale. Policia, si një entitet përgjegjës dhe rregullator për ruajtjen dhe mbrojtjen e rendit publik, zbulimin, monitorimin dhe parandalimin e krimit, është një nga protagonistët e kësaj skene që ballafaqohet me një gamë të gjerë sfidash[3] lidhur me migrimin e krimit tradicional në mjedisin e TIK-ut, dhe shfaqjen e formave të reja të aktivitetit kriminal, me fokus në grupin e të miturve[4].

## 2. Roli i oficerit të mbrojtjes së të dhënave dhe strukturave ligjzbatuese, në diagnostikimin dhe parandalimin e krimit kibernetik

Qasjet ekzistuese të luftës ndaj krimit në botën reale, shpesh nuk janë funksionale në hapësirën kibernetike, dhe mund të mos jenë të zbatueshme, në rastet e keqpërdorimit të TIK-ut për qëllime kriminale. Prandaj, është e rëndësishme të propozojmë dhe të zhvillojmë, një qasje gjithëpërfshirëse, për një hierarki mikro dhe makrostrukturore, që të trajtojmë aspekte të ndryshme të krimit kibernetik përgjatë sfidave të reja për organet e zbatimit të ligjit dhe ato hetimore. Për çështje të tilla të rëndësishme, strukturat e Zyrës së Oficerit të Mbrojtjes së të Dhënave në Bashkimin Evropian, drejtohen kryesisht nga

[1] Agastra et al.,2017, Profilet psikologjike, domosdoshmëri për hetimin, f. 173 .
[2] Gercke, 2006, 2009.
[3] Wall, D. S. (2007) Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace, Police Practice and Research, 8:2, 1.
[4] Quille, 2009; Kozlovski, 2005; Wall, 2007.

Direktiva e BE për Mbrojtjen e të Dhënave 95/46 / EC2 (Direktiva për Mbrojtjen e të Dhënave), e cila rregullon mbledhjen dhe përpunimin e të dhënave personale në të gjithë sektorët ekonomikë. Direktiva e Mbrojtjes së të Dhënave është zbatuar në të gjitha 28 shtetet anëtare të BE-së, përmes ratifikimit të ligjeve kombëtare dhe ndërkombëtare të mbrojtjes së të dhënave. Reforma ligjore e BE-së për mbrojtjen e të dhënave, ka qenë temë e diskutimit intensiv në botimin e propozimit të Komisionit Evropian në janar të vitit 2012, mbi një rregullore të BE-së për mbrojtjen e të dhënave, e cila do të zëvendësonte Direktivën për Mbrojtjen e të Dhënave dhe do të ndërfuste detyrime të reja për mbrojtjen e të dhënave për përdoruesit e të dhënave dhe të drejta të reja për individët, veçanërisht në sigurinë dhe mbrojtjen e popullatave ndaj krimit kibernetik. Propozimi i Komisionit Evropian u miratua në maj të vitit 2016 si *Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave të BE-së* (Rregullorja) e cila hyri në fuqi në të gjitha shtetet anëtare, nga 25 maji i vitit 2018.

Të dhënat personale *sensitive* lidhen me racën ose etninë e subjektit së të dhënave, jetën politike, anëtarësimet dhe veprimtaritë socio-ekonomike, besimin fetar, shëndetin ose jetën seksuale që mund të përpunohen në rrethana specifike dhe të përcaktuara. Për një hapësirë më të sigurt kibernetike, seksioni i Komunikimeve Elektronike të BE-së propozoi Direktivën 2002/58 / EC (*Direktiva ePrivacy*) për përdorimin elektronik dhe keqpërdorimin e të Dhënave. Kjo direktivë *ePrivacy* vendos kërkesa specifike për ofruesit e shërbimeve të komunikimit elektronik, për të siguruar masat e përshtatshme dhe për të njoftuar shkelje të caktuara të sigurisë, në lidhje me të dhënat personale.

Kjo direktivë *ePrivacy,* ka vendosur kërkesa për dhënësit e shërbimeve të komunikimit elektronik, për të siguruar masa të përshtatshme sigurie dhe për të njoftuar shkelje të caktuara të sigurisë, në lidhje me të dhënat personale. Direktiva e *ePrivacy* u ndryshua në 2009 për të kërkuar që operatorët e internetit të marrin pëlqimin e informuar të përdoruesve përmes "cookie" të internetit ose teknologjive të ngjashme të përdorura për ruajtjen e informacionit. Më 10 janar 2017, Komisioni Europian miratoi një draft tjetër të Rregullores së propozuar për Privatësinë dhe Komunikimet Elektronike për të zëvendësuar Direktivën ekzistuese të *ePrivacy*, e cila është modeluar zyrtarisht më 28 maj 2018.

Më shumë përpjekje nga strukturat e policisë, është e nevojshme, kur u referohemi të drejtave të përdoruesve elektronikë dhe të miturve duke përdorur një hapësirë të sigurt dhe të mbrojtur të kibernetikës. Autorët kanë propozuar që disa qasje të merren parasysh në zhvillimin e strategjive për të luftuar krimin në botën virtuale[5]:

- *Sasia dhe numri i përdoruesve në rrjet.* Përhapja e përdorimit të internetit në jetën e përditshme të njerëzve dhe si një mënyrë për të bërë biznes, është duke u rritur në mënyrë dramatike në numrin e përdoruesve, gjatë viteve të fundit. Kështu, në vitin 2005 numri i përdoruesve të internetit, në vendet në zhvillim, për herë të parë, ka tejkaluar numrin e përdoruesve ndaj vendeve të industrializuara[6].

Në vendin tonë, të dhënat tregojnë se në 2016-2017 nga 175 raste të krimit kibernetik, 143 kanë përfshirjen e personave të dëmtuar ose 81.7% të rasteve, nga të cilat 51% janë femra; 11.8% e rasteve, i përkasin adoleshentëve 14-18 vjeçar[7].

Në perspektivën globale, krimi kibernetik është një formë e krimit që prek të dy

[5] Kenneth A Bamberger and Deirdre K Mulligan, 'Privacy on the Books and on the Ground' (18 November 2011), Stanford Law Review, Volume 63, January 2011; UC Berkeley Public Law Research Paper.
[6] Raporti i Imigracionit dhe Zhvillimit Special, Shoqëria e Informacionit, 2005.
[7] Agastra et al,.2017,f. 164.

gjinitë në të njëjtën kohë, por ekspozimi afatgjatë i moshave në zhvillim, tashmë ka ndryshuar fokusin ndaj kësaj grup-shënjestre. Rritja e numrit të përdoruesve, në lidhje me globalizimin e rrjetit të komunikimit është një sfidë e re për policinë dhe strukturat mbrojtëse të hapësirës kibernetike për të paktën dy arsye: së pari, një nga dobësitë që paraqet një mundësi për krimin, është mungesa trajnimit specifik të strukturave të Policisë së Shtetit mbi politikat e ruajtjes së sigurisë individuale në internet, sipas rregullatorëve të BE-së dhe aplikimi i formave të inxhinierisë sociale e teknikave të ruajtjes së *privacy*[8]. Së dyti, vjedhjet e identitetit, *spam*-met dhe veprimtaritë e *phishing* mund të kryhen automatikisht[9], pa investuar para dhe burime; andaj, është shumë e vështirë të automatizohet procesi i hetimit[10].

- *Disponibiliteti i mjeteve dhe burimeve të informacionit.* Interneti është projektuar si një rrjet i hapur për informacion dhe individët me devijancë ekstreme, mund të kenë burime informacioni ose mjete, për të kryer krime kibernetike. Mundësia e përdorimit të motorëve të kërkimit dhe robotëve për qëllime të paligjshme[11] dhe udhëzimet se si të kryhen vepra penale, kanë lehtësuar zhvillimin e krimit, si në botën reale, ashtu edhe në hapësirën kibernetike.

- *Vështirësitë në gjurmimin e shkelësve të ligjit.* Mundësitë e ndryshme për të fshehur identitetin në rrjetet e TIK dhe mjetet, mënyrat dhe qasjet e ndryshme për të hyrë në lidhjet anonime, *surfing* dhe rrjetet sociale në të vërtetë komplikojnë punën e agjencive të zbatimit të ligjit për të ndjekur dhe monitoruar shkelësit[12] . Mundësitë për përdorimin e serverëve *proxy*, *anonymizers, wireless* të sigurisë dhe përdorimin e shërbimeve të komunikimit *anonim* janë shfrytëzuar gjerësisht nga krimi kibernetik. Kur aktiviteti kriminal përfshin shtete të ndryshme është shumë e vështirë të hetohen akte të tilla që përfshijnë aspektin ndërkombëtar dhe atë të fshehtë të identitetit.

- *Mungesa e mekanizmave të kontrollit.* Që nga zbulimi i tij i parë, në vitet 1960, interneti nuk u krijua për t'u udhëhequr në mënyrë vertikale. Struktura horizontale dhe modeli i rrjetit të decentralizuar pengon kontrollin mbi aktivitetin në internet dhe e vështirëson hetimin e krimeve të kryera në hapësirën kibernetike. Qasjet bashkërregullatore dhe vetërregulluese dhe bashkëpunimi me operatorët e infrastrukturës si dhe me shpërndarësit e shërbimit të internetit janë të nevojshme kur kemi të bëjmë me keqpërdorim të TIK-ut[13].

- Mungesa e kufijve në hapësirën kibernetike dhe ndërkombëtarizimi i krimit kibernetik.

Penologjia dhe hetimet penale konsiderohen si çështje të sovranitetit kombëtar në të drejtën dhe sigurinë ndërkombëtare, ndërsa protokollet e aplikuara për transferimin e të dhënave në internet bazohen në transferimin optimal së të dhënave, andaj proceset e transferimit së të dhënave kalojnë në më shumë se një vend[14].

Pasi hapësira kibernetike është e pakufi, kriminelët dhe viktimat mund të gjenden në vende të ndryshme ose edhe në kontinente të ndryshme, çka do të kërkonte një sërë formash bashkëpunimi nga të gjitha vendet e përfshira në investigime ndërkombëtare. Teksa procedurat formale për bashkëpunim kërkojnë kohën e tyre, procesi i hetimit

[8] Rash et al., 2009
9 Berg, 2007, Ealy, 2003
[10] Gercke, 2009
[11] Long, Skoudis & van Eijkelenborg, 2005, Dornfest, Bausch & Calishain, 2006
[12] Lovet, 2009
[13] Sofaer & Goodman, 2001, f. 7.
[14] Putnam & Elliott, 2001; Sofaer & Goodman, 2001; Roth, 2005, f. 35.

shpesh mund të ballafaqohet me pengesa[15]; të dhënat dhe gjurmët janë *sensitive* dhe mund të zhduken pak pas kryerjes së krimit. Shtetet, të cilat nuk kanë kornizë bashkëpunimi për çështjet e krimit në internet, mund të bëhen një strehë e sigurt për shkelësit e ligjit që duan të pengojnë procesin e hetimit. Për më tepër, interneti mund të motivojë një individ devijant që të jetë fizikisht i pranishëm në një shtet ndërsa kryen një krim në një shtet tjetër.

Roli që policia dhe agjencitë ligjzbatuese duhet të luajnë në luftën kundër krimit kibernetik me fokus te të miturit, është i rrezikuar nga të gjitha problematikat e sipërpërmendura. Jo vetëm hetimi i krimit kibernetik është i komplikuar, por edhe policimi i hetimeve në krimin kibernetik mund të pengohet. Është shumë e vështirë për agjencitë policore të fillojnë hetime, kryesisht, për shkak të dukshmërisë së ulët të këtij krimi dhe mungesës së raportimit nga viktimat[16]. Fenomeni i mosdeklarimit të krimit kibernetik, si dhe shumë dukuri të tjera të aspektit social, mund të ndodhin për arsye të ndryshme, si: mungesa e vullnetit të subjekteve tregtare dhe kompanive financiare që të raportojnë në polici një llogari të caktuar ose të kërcënime nga sjellje kibernetike dëmtuese, neglizhenca e individëve të përfshirë në *kiberbullizëm* në injorimin e këtyre çështjeve, mohimi dhe mosdija se *krimi kibernetik* është i vërtetë dhe mund të ketë përfshirë individin dhe mungesa e besimit në strukturat e policisë e mbibesimi në burimet e vetë individit për zgjidhjen e këtyre konflitkeve[17].

Për shkak të nivelit të ulët të raportimit, mungesës së resurseve dhe raportimit në agjencitë e zbatimit të ligjit, këto struktura nuk janë në gjendje të hetojnë dhe të kërkojnë më shumë se një pjesë "të vogël" të asaj që ndodh në hapësirën kibernetike[18].

Që nga përdorimi i teknologjive të internetit dhe TIK, studiuesit kanë mundësi të krijojnë të dhënat me ndikim të ulët tek një viktimë specifike pasi një nga sfidat më të rëndësishme për policinë, është hapja e procedurave hetimore. Dallimet në veprat penale dhe shkeljet ligjore, dallimet kulturore mbi seriozitetin e krimit, mospërputhjet e mëdha në lidhje me çfarë duhet të konsiderohet vepër e paligjshme, i vënë strukturat e policisë ndër njësitë më të prekura nga këto sfida bashkëkohore të evolucionit. Gjetja e një ekuilibri të drejtë midis pushtetit hetues dhe të drejtave të njeriut, zbatimi i masave parandaluese dhe ruajtja e natyrës së qasjes së hapur në internet mbeten një problem serioz i strukturave të policimit në hapësirën kibernetike.

Mungesa e mekanizmave të kontrollit, të zhvillimit fillestar të arkitekturës së internetit dhe të rrjetit kërkojnë zhvillimin e mjeteve policore në hapësirën kibernetike, mekanizmat për monitorimin e rrjeteve të TIK, parandalimin dhe zbulimin e aktiviteteve ilegale në internet dhe hapësirën në rrjet. Po kështu , ideja fillestare e përdorimit të internetit si një hapësirë për mbajtjen e diskutimeve të hapura, shkëmbimin dhe bashkëndarjen e mendimeve dhe pikëpamjeve, si dhe rrjedhja e lirë e informacionit, nuk duhet të pengohet, e në këtë formë shtohet edhe sfida për ruajtjen e hapjes së rrjetit dhe procesit të tij së bashku me zhvillimet shoqërore.

Sipas *Byrosë Qendrore të Interpolit* (NCB) në një inspektim të prillit 2016, u vërejt se 83% e zyrave ndërkombëtare kishin njësi të dedikuara për krimin kibernetik, por nuk kishin kapacitet për të kryer një incidencë të profilit të lartë[19] (Interpol, 2016).

[15] Gercke, 2006; Sofaer & Goodmann, 2001, f. 142.
[16] Lovet, 2009, f. 69.
[17] CSI & FBI, 2004, Wall, 2007.
[18] Vogel, 2007
[19] Interpol, 2016,f. 11-19

Andaj, një hap tjetër i domosdoshëm dhe i rëndësishëm është zhvillimi i mekanizmave efektivë të përdorimit të burimeve njerëzore dhe kapaciteteve për forcimin e mekanizmave të bashkëpunimit kombëtar dhe ndërkombëtar.

Për të rritur efektivitetin e reagimit ndaj krimit kibernetik me fokus në të miturit, studimet e Agjencive të Larta të Inteligjencës dhe Parandalimit të Krimit kanë sugjeruar:

- krijimi i një ekipi pune *Task Force* brenda strukturave të ligjzbatuese dhe antikrimit me përparësi në krimet kibernetike;

- rritja e kapaciteteve trajnuese për punonjësit e policisë për strukturat psikopatologjike sociale të moshave të miturave, grup-shënjestra me incidencën më të lartë për viktimologji kibernetike;

- rritja e qasjes dhe bashkëpunimit të punonjësit të policisë me komunitetin për të cilin ai përgjigjet,me institucionet arsimore, qendrat e shërbimit të internetit dhe operatorët e sektorit privat;

- zhvillimi i kapaciteteve të burimeve njerëzore të trajnuar dhe certifikuar, për aspektet e krijimit të databazës, hartës së zonave dhe komuniteteve me rrezikshmëri më të lartë dhe laboratorit kibernetik për kujdes dhe ekzaminim prioritar;

- forcimi i akteve ligjore,civile dhe penale për abuzuesit dhe ata të identifikuar si me potencial të lartë të deviancës kibernetike;

- koordinimi i strukturave në nivel lokal dhe qendror, për parandalimin e krimit kibernetik me target të miturit;

- bashkëndarja e përgjegjësisë dhe bashkëpunimi mes policisë,komunitetit dhe sektorëve të shërbimit shtetëror dhe privat duket të jenë mënyra me e efektshme e trajtimit të krimit kibernetik në nivele lokale e kombëtare[20]. Siç është parashtruar edhe në një sërë studimesh dhe publikimesh, një bashkëpunim i tillë së bashku me bashkërregullimin dhe vetërregullimi mund të japë edhe rezultate më të mira sesa thjesht zbatimi i ligjit penal[21].

## 3. Konkluzione

Lufta kundër krimit kibernetik kërkon një qasje gjithëpërfshirëse që përfshin zhvillimin, zbatimin dhe rishikimin e masave teknike, ligjore, strukturore dhe sociale, me ndërtimin e strukturave të specifikuara organizative për të adresuar këtë problematikë në shkallë kombëtare si *Byro Qendrore e Hetimit në Krimin Kibernetik dhe Mbrojtjen e të Dhënave Personale*, nenet 7, 8 dhe 18 të *Direktivës për Mbrojtjen e të Dhënave*.

Trajtimi i krimit kibernetik kërkon koordinim efektiv kombëtar dhe ndërkombëtar në lidhje me çështjet e krimit në internet që duhet të sendërtohen në koordinim me politikat lokale dhe kombëtare[22]. Qasja e shumë pjesëmarrësve, përfshirë komunitetin, institucionet e arsimit, agjencitë e mbrojtjes dhe të zbatimit të ligjit, strukturat e mbrojtjes sociale etj., të zbatuara në nivel kombëtar duhet të jenë koherente me zhvillimet rajonale dhe ndërkombëtare, ku harmonizimi i mjeteve për trajtimin e krimit kibernetik, ka treguar rezultate pozitive dhe efikase. Përpjekjet makrosociale për të vendosur politika dhe masa shtrënguese ligjore, domosdoshmërish duhet të bazohen në respektimin e

[20] Komisioni dhe Parlamenti Evropian, Këshilli i Sigurisë dhe Komiteti i Rajoneve, 2007
[21] Sieber, 2000, fq.319-399; Sieber, 2010
[22] Raporti i WGIG, 2005
[23] Deklarata e Parimeve e të Drejtave të Njeriut,Neni 11 2003

Deklaratës së Lirisë dhe të Drejtave të Njeriut[23], si dhe në ekspertizën teknike dhe ekonomike, në gatishmërinë e shoqërisë civile dhe lehtësinë e ndërveprimit me organizatat dhe strukturat mbështetëse që zhvillojnë standarde të përbashkëta të bashkëveprimit. Pavarësisht nga sfidat me të cilat ballafaqohen, strukturat e policisë dhe të mbrojtjes së të miturve në shtetet e Bashkimit Evropian dhe veçanërisht ndërmjet vendeve fqinjë me njëri-tjetrin, si një nga strukturat kyçe në krimin kibernetik, mund të shërbejnë edhe si një model inkurajues qendror për ndërtimin e lidhjeve mes aktorëve të ndryshëm të brendshëm, funksionimin dhe zhvillimin e qasjeve kombëtare dhe ndërkombëtare për të trajtuar problemin e keqpërdorimit të TIK-ut me pasojë dëmtimin dhe jetëkërcënimin.

## Bibliografi


1. Agastra, A., Ibrahimi, S., Ibrahim, E.,(2017), Profilet psikologjike, domosdoshmëri për hetimin.
2. Gercke, M. (2006) The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International.
3. Gercke, M. (2009) Understanding Cybercrime: A Guide for Developing Countries, ITU, Geneva. Gjendur online: www.itu.int/ITU-D/cyb/ cybersecurity/legislation.htm
4. Quille, M. (2009) Keynote Address. Current Threats and Future Challenges posed by cybercrime. Octopus Conference, CoE
5. Kenneth A Bamberger and Deirdre K Mulligan, 'Privacy on the Books and on the Ground' (18 November 2011), Stanford Law Review, Volume 63, January 2011; UC Berkeley Public Law Research Paper No. 1568385.
   Gjendur online: ssrn.com/abstract=1568385
6. Kozlovski, N. (2005) A Paradigm Shift in Online Policing - Designing Accountable Policing, Yale Law School Dissertation.
7. Wall, D.S. (2007) Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace, Police Practice and Research, 8:2, 1, 2007
8. Development Gateway's Special Report, Information Society — Next Steps, 2005
9. Rash, H. et al. (2009) Crime Online. Cybercrime and Illegal Innovation. NESTA. Research Report. July
10. Berg, T. (2007), The Changing Face of Cybercrime - New Internet Threats Create Challenges to Law Enforcement, Michigan Bar Journal 2007.
11. Ealy, K (2003) A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention.
12. Long, J., Skoudis, E. and van Eijkelenborg, A. (2005) Google Hacking for Penetration Testers, Syngress.
13. Lovet, G. (2009) Fighting Cybercrime: Technical, Juridical and ethical Challenges, Virus Bulletin Conference, September 2009.
14. Sieber, U. (2000) Legal Regulation, Law Enforcement and Self-regulation, in: Watermann, J. and Machill, M. (eds.) Protecting Our Children on the Internet, Gütersloh, Bertelsmann Foundation Publishers.
15. Sieber, U. (2010) Internet Crimes - Annex 1 to the Questionnaire for the 18th International Congress of the IACL.
16. Sofaer, A.D. and Goodman, S.E. (2001) Cyber Crime and Security — The Transnational Dimension in: Sofaer, A.D. and Goodman S.E. (ed.) Transnational Dimension of Cyber Crime and Terrorism, Hoover Institution Press.
17. Putnam, T.L. and Elliott, D.D. (2001) International Responses to Cyber Crime, in: Sofaer, A.D. and Goodman S.E. (ed.) Transnational Dimension of Cyber Crime and Terrorism, Hoover Institution Press.
18. Roth, B. (2005) State Sovereignty, International Legality, and Moral Disagreement
19. CSI and FBI (2004) Computer Crime and Security Survey, San Francisco.
20. Vogel, J. (2007) Towards a Global Convention against Cybercrime. World Conference on Penal Law, Guadalajara, Mexico.
21. Interpol (2016) Crimes against children. Factsheet.
22. Communication from the Commission to the European Parliament the Council and the Committee of the Regions (2007) Towards a general policy on the fight against cyber crime.
23. European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

# Mënyrat e adresimit të kërcënimeve kibernetike

■**MSc. Tereza MATRAKU**
*Akademia e Forcave te Armatosura*
*tereza.matraku@aaf.mil.al*

**Abstrakt**

*Kjo tezë paraqet një kontribut në diskutimin mbi luftën kibernetike dhe mënyrat e adresimit të kërcënimeve kibernetike, duke argumentuar se nocioni i kësaj lufte, është keqpërshtatur në krahasim me kuptimin e vërtetë të saj. Një nga problemet bashkëkohore mbi luftën kibernetike është sintetizimi i sulmeve kibernetike të ndryshme. Prandaj, unë kam studiuar dhe analizuar kërcënime si DDoS, deformimin e faqeve të internetit dhe sulmet SCADA. Kam analizuar gjithashtu se si aktorë të ndryshëm, nga kriminelët tek haktivistët, përdorin sulmet kibernetike, për të dëmtuar aktorët shtetërorë dhe joshtetërorë dhe kam përpunuar këtë tezë, në formën e rekomandimeve dhe konkluzioneve mbi kërcënimet kibernetike. Përveç dallimeve teknike, edhe kuadri ligjor është i rëndësishëm. Në qoftë se një sulm kibernetik përbën një akt lufte, shteti viktimë ka të drejtë të hakmerret, duke përdorur forcën e armatosur. Edhe pse shumica e sulmeve nuk bien në këtë kategori, ato janë trajtuar në kontekstin e kuadrit ligjor të kohës. Kam analizuar disa raste, të cituara shpesh si shembuj të luftës kibernetike, duke përfshirë sulmet DDoS në Estoni, incidentet në Gjeorgji dhe sulmet kundër Google. Për secilin rast kam diskutuar nëse kualifikohet si akt i luftës kibernetike apo jo. Si një histori delikate është trajtuar edhe rasti i virusit "Stuxnet worm", që konsiderohet si një akt i luftës kibernetike të kryer nga Izraeli dhe SHBA kundër impianteve bërthamore të pasurimit në Natanz të Iranit. Unë e vlerësoj të pamundur një luftë kibernetike të vërtetë, duke u bazuar në faktin se sulmet kibernetike janë shumë më të vështira se sa supozohet, dhe se të gjitha aktet aktuale, do të çonin drejt një përshkallëzimi në konflikte kinetike. Bazuar në këto vëzhgime, mendoj që lufta kibernetike nuk është një koncept i përshtatshëm për të adresuar kërcënimet e sigurisë. Shumica e sulmeve nuk janë akte të luftës, por bien në nivelin e krimit. Kështu, mënyra më e mirë për t'u marrë me to nuk do të ishte një kundërpërgjigje ushtarake, por një civile. Në këtë tezë janë paraqitur disa rekomandime, për mënyrën si mund të përmirësohet siguria kibernetike. Ndër to, përmendim një diskutim të gjerë publik, forcimin e përpjekjeve ndërkombëtare për të luftuar krimin kibernetik, ndërgjegjësimin në lidhje me sigurinë IT, përqendrimin tek elasticiteti dhe futjen e instruksioneve inteligjente për të mbrojtur infrastrukturën kritike.*

**Fjalëkyçe:**

**kërcënimeve kibernetike, Lufta kibernetike, burimeve të hapura, informimi publik, siguria e IT.**

## 1. Mënyrat e adresimit të kërcënimeve kibernetike

Çfarë mund të bëhet për të adresuar kërcënimet serioze kibernetike që ne po përballemi? Më poshtë paraqes argumentin tim pse, pavarësisht nga të gjitha pretendimet për të kundërtën, lufta kibernetike ndoshta nuk është e pashmangshme dhe pse një qasje e ndryshme është e nevojshme për t'u marrë me kërcënimet kibernetike reale me të cilat ballafaqohemi sot. Bazuar në këtë analizë jepen disa rekomandime për hapat konkretë që duhen ndërmarrë për të adresuar këto kërcënime të cilët mund të jenë hapa të dobishëm për tu ndërmarrë në mënyrë që të përmirësohet situata.

## 2. Nxitja e debatit publik

Ky debat duhet të përfshijë jo vetëm specialistë nga fusha e sigurisë së informacionit dhe nivelit të lartë të politikë-bërësve por edhe qytetarët në përgjithësi. Pikërisht për shkak se kërcënimet kibernetike janë trajtuar shpesh si çështje të sigurisë ushtarake apo kombëtare, thelbi tenton të mbështillet me fshehtësi. Kjo është problematike për një numër arsyesh ku transparenca e politikëbërjes ka qenë vetëm një prej tyre. Ajo është gjithashtu kundër-produktive nga pikëpamja praktike. Që kur pjesa më e madhe e infrastrukturës së internetit ka kaluar në pronësi private, një pjesë e madhe e përmirësuar në sigurinë e saj do të kalojnë në sektorin e biznesit. Bizneset, megjithatë, për t'iu përgjigjur kërkesave të tregut dhe tregu do ti përgjigjet vetëm kërkesave për rritjen e sigurisë nëse njerëzit janë të vetëdijshëm për këtë problem:

Në qoftë se do të vendosim në krye të sigurisë kibernetike agjencitë e inteligjencës, nga natyra e tyre e të vepruarit në mënyrë të fshehtë, ata nuk do të jenë në gjendje të vendosin presionin publik mbi bizneset për të bërë reformat e nevojshme dhe

përmirësimet e produkteve të tyre. Presioni publik nuk vjen nga kjo. Susan Landau ngriti këtë pikë në kohën kur janë komentuar katër faturat Kibernetike (Lieberman-Collins, McCain, CISPA, dhe Lungren) që ishin nën diskutim në Senatin amerikan:

Një pikë për tu mbajtur në mend është se Kibernetika nuk është një problem, por një i problem i shumfishtë. Mbrojtja e sistemeve të kontrollit të rrjetit të energjisë nga ndërhyrjet është rrënjësisht i ndryshëm nga mbrojtja e informacionit të pronarit në sektorin privat kundër spiunazhit elektronik, dhe të drejtat e vendosura me ligj, rregulloret, dhe teknikat, se çfarë duhet të bëjë secili do të ndryshojnë në mënyrë të konsiderueshme[1].

## 3. Luftimi i krimit kibernetik

Krimi kibernetik është prapa shumicës së sulmeve kibernetike sot, dhe ky është një biznes në rritje. Prandaj, krimi kibernetik, jo lufta kibernetike, është çështja më kryesore për të cilën ne duhet të jemi të shqetësuar.

Një aspekt i rëndësishëm i kësaj është që të përmirësojmë bashkëpunimin ndërkombëtar, kur bëhet fjalë për luftimin e krimit kibernetik. Një pjesë e kësaj mund të jetë nxitja për të përhapur ratifikimin dhe realizimin aktual të Konventës së Budapestit mbi krimin kibernetik dhe traktateve të tjera të ngjashme ndërkombëtare. Një tjetër pjesë është përforcimi i zbatimit të ligjeve ndërkombëtare ndërkufitare.

Megjithatë e gjithë kjo do të funksionojë vetëm në qoftë se ka marrëveshje ndërkombëtare për ta bërë këtë. Arsyeja kryesore pse krimi kibernetik është kaq efektiv sot është se ka vende që sigurojë "strehë të sigurt" nga e cila kriminelët kibernetikë mund të veprojnë.

Ne nuk duhet të harrojmë se shumë nga vendet që janë strehë për krimet kibernetike kanë investuar miliarda lekë në monitorimin e komunikimeve të brendshme për të plotësuar një grup tashmë të gjerë të mjeteve të policisë për kontrollin politik. Nocioni se një kriminel i tillë që vepron në një nga këto vende pa njohuri dhe kështu pa miratimin e heshtur të qeverisë do ta ketë të vështirë të futet. Kur një haker e ktheu shikimin e tij nga Talini në Kremlin, do të kalonin vetëm disa orë para se shërbimi i tij të ndërpritej, dera e tij të thyej dhe kompjuteri i tij të konfiskohej.

## 4. Vendosja e masave të ndërtimit të besimit për të shmangur përshkallëzimin

Siç është analizuar nga studimet e mia paraprake, njëri nga rreziqet e përdorimit të sulmeve kibernetike si një mjet i luftës janë përshkallëzimet e mundshme. Normat e pranuara ndërkombëtarisht mbi përdorimin e "armëve" kibernetike mund të bëjnë shumë për të zbutur këtë rrezik.

Duhet ndoshta një kohë shumë e gjatë që të kemi një traktat ndërkombëtar mbi luftën kibernetike dhe një traktat për armëkontrollin që ndalon ose kufizon zhvillimin e "armëve kibernetike" të cilat do të jenë të pazbatueshme dhe madje mund të dëmtojnë sigurinë kibernetike. Por hapat duhet të ndërmerren për të ecur përpara në rrugën e mirëkuptimit dhe bashkëpunimit. Ndërtimi i besimit midis shteteve do ta zvogëlojë

[1] Jack Goldsmith, "Susan Landau on Cybersecurity Bills", Ligji i Luftës, 3 maj 2012. http://www.lawfareblog.com/2012/05/susanlandauoncybersecurity-bills/

rrezikun e konfliktit në hapësirën kibernetike, sidomos rrezikun e përshkallëzimit në një konflikt kinetik. Një fillim i mirë do të ishte krijimi i një lidhje telefonike mes komandave kibernetike, të ngjashme me linjat e krijuara mes komandave bërthamore. Nuk jam duke thënë se kërcënimi kibernetik është i krahasueshëm me kërcënimin bërthamor, por, të pasurit e një linje të një niveli të lartë komunikimi, për të shmangur keqkuptimet dhe mbireagimet, mund të jetë thelbësore kur bëhet fjalë për sulmet kibernetike, sidomos për shkak të vështirësisë së atribuimit.

Shtetet e Bashkuara dhe Rusia janë aktualisht në procesin e krijimit të një linje të tillë telefonike. Marrëveshja synon të përmirësojë komunikimin dhe transparencën në mënyrë që të "zvogëlojë shanset që një incident i keqkuptuar mund të ndikojnë negativisht në marrëdhëniet e tyre"[2].

## 5. Përmirësimi i sigurisë së përgjithshme IT

Kjo mund të tingëllojë qartë, por hapi i vetëm më i rëndësishëm për të parandaluar sulmet kibernetike është të përmirësojmë nivelin e përgjithshëm të sigurisë IT.

Incidentet më të zakonshme Kibernetike mund të parandalohen duke ndjekur më mirë praktikat më të thjeshta, të tilla si instalimi i antiviruseve dhe përditësimi rregullisht i tyre. GCHQ ka vlerësuar se më shumë se 80% e sulmeve të suksesshme aktualisht mund të eliminohen duke ndjekur hapat bazë të "higjienës kibernetike"[3].

Për të qëndruar me shembullin e Britanisë së Madhe: vetëm kohët e fundit është raportuar se hakerët kishin arritur të fitonin qasje në disa nga sistemet e fshehta (top-sekret) të Ministrisë së Mbrojtjes, ku gjeneralmajor Jonathan Shaw, kreu i sigurisë kibernetike i Ushtrisë së Mbretërisë së Bashkuar, nxitoi të komentonte me një sinqeritet të pazakontë: *Unë mendoj se kjo "sa të prekshëm ne jemi" ishte një surprizë për shumë njerëz* [4].

## 6. Paraqitja e instruksioneve inteligjente

Ky është një nga rekomandimet më të diskutueshme nga ato që po paraqes, por unë mendoj se ky është një komponent thelbësor i një strategjie gjithëpërfshirëse të sigurisë kibernetike. Në librin e tij të vitit 2010 "Lufta kibernetike, kërcënimi i radhës ndaj sigurisë kombëtare dhe çfarë duhet bërë rreth tij", Richard Clarke futi konceptin e "trekëndëshit mbrojtës". Kjo treshe përbëhet nga rrjetet ushtarake, ISP të një niveli të lartë dhe rrjeti energjetik[5]. Një pikë e rëndësishme për t'u theksuar këtu, është se dy pjesët e këtij trekëndëshi, niveli i lartë i ISP-ve dhe rrjeti i energjisë, janë të paktën pjesërisht në pronësi private në shumicën e botës Perëndimore.

Politikat e instruksioneve konsiderohen si një temë për të cilën nuk duhet të flitet, që nxisin një sërë burokracish të pa nevojshme të cilat mbysin inovacionin dhe prosperitetin.

[2] Ellen Nakashima, "In U.S.-Russia deal, nuclear communication system may be used for cybersecu-rity", Gazeta "The Washington Post", 26 gusht 2012, http://www.washingtonpost.com/world/nationalsecurity/in-us-russia-dealnuclearcommunicationsystemmaybeusedforcybersecurity/2012/04/26/gIQAT521iT_story.html

[3] UK Cabinet Office, "The UK Cyber Security Strategy", nëntor 2011, http://www.cabinetoffice.gov.uk/sites/default/files/resources/ukcybersecurity-strategy-final.pdf

[4] Nick Hopkins, "Hackers have breached top secret MoD systems, cyber-security chief admits", Revista "The Guardian", 3 maj 2012, http://www.guardian.co.uk/technology/2012/may/03/hackersbreachedseet-mod-systems.

[5] Richard A. Clarke, "Cyber War. The Next Threat to National Security and What to Do About It" (Clarke 2010).

Megjithatë, në rastin e dështimeve të tregut, politikat rregulluese janë të përshtatshme dhe të nevojshme. Një rast i tillë, mund të jetë rasti i infrastrukturave në pronësi të korporatave, që është bërë një aset kritik.

## 7. Fokusimi te elasticiteti

Kjo është më shumë një pikë teknike. Një nga përgjigjet më të mira për shumë sulme kibernetike është elasticiteti[6]. Kjo është sigurisht e vërtetë për të zgjidhur sulmet DDoS, por kjo mund të aplikohet edhe në shumë raste të tjera gjithashtu. Mbrojtja është e rëndësishme, por realisht ne duhet të pranojmë se ajo kurrë nuk do të jetë e mundur për të parandaluar të gjitha sulmet. Elasticiteti nënkupton planifikimin për dështim, të paturit e një sistemi të duhur për të minimizuar dëmet nga një sulm, dhe rikuperimin nga ky sulm në të ardhmen.

## 8. Zbutja e rreziqeve të ndërhyrjeve ("backdoors")

Një kërcënim që neglizhohet shpesh është se harduer-ët dhe softuerët mund të përmbajë gabime të qëllimshëm dhe "Backdoors" të fshehura. Ish-nënsekretari amerikan i Mbrojtjes, William III J. Lynn ishte korrekt në identifikimin e këtij rreziku si një shkak madhor për tu shqetësuar: Rrjetet kompjuterike në vetvete nuk janë dobësitë e vetme që ekzistojnë. Kodi Mashtrues, duke përfshirë edhe të ashtuquajturat bomba logjike, të cilat shkaktojnë keqfunksionime të befta, mund të futet në softuer gjatë kohës së zhvillimit të tyre. Sa i përket harduerë-ve, "kill switches" të komanduar nga distance dhe "backdoors" të fshehura mund të programohen në qarqet kompjuterikë të përdorura nga ushtria duke lejuar aktorë të jashtëm të manipulojnë sistemin nga larg[7].

Për të zbutur këto rreziqe, dy qasje mund të jenë të dobishme. Njëra është që të krijohet një zinxhir i sigurt, i furnizimit të brendshëm për komponentët kritikë dhe e dyta është shmangia e harduerëve dhe softuerëve me pagesë, për t'u zëvendësuar me ato *open-source* (platforma pa lek).

## 9. Sigurimi i zinxhirëve të furnizimit për sistemet kritike

Problemi i të ashtuquajturave "bomba logjika" (për të qëndruar me terminologjinë ushtarake për momentin) është një shqetësim i veçantë për shtetet Perëndimore që kur zinxhirët e furnizimit janë bërë kaq të ndërkombëtarizuar. Shumica e qarqeve kompjuterike të përdorura në sistemet kritike, ka të ngjarë të jenë prodhuar në vendet që me shumë gjasa do të jenë kundërshtarët e mundshëm në një konflikt të ardhshëm.

Pentagoni është duke u përpjekur për të adresuar këtë çështje nëpërmjet programit "Trusted Foundry", i cili vërteton komponentët e prodhuar nga prodhuesit e mikroelektronikës vendase. Programi "Trusted Foundry", është një iniciativë e përbashkët e marrë nga Departamenti Amerikan i Mbrojtjes dhe Agjencia Kombëtare e Sigurisë,

[6] Për një hyrje te përgjithshme të elasticitetit si një veçori thelbësore e një sistemi të sigurt, shiko Bruce Schneier, Beyond Fear (Schneier 2003, f. 119–132).

[7] William J. Lynn III, "Defending a New Domain. The Pentagon's Cyberstrategy" (Lynn III 2010). Artikulli gjendet online ne websiten e DoD te SHBA. http://www.defense.gov/home/features/2010/0410_cybersec/lynnarticle.aspx

që filloi në vitin 2004 me qëllimin për të "siguruar sistemet kombëtare të mbrojtjes si misione-kritike, të kenë akses në udhëheqjen me epërsi të qarqeve të integruara nga burime të sigurta të brendshme"[8].

## 10. Preferenca ndaj burimeve të hapura, në vend të atyre alternative

Sugjerimi im për të ulur rrezikun e "backdoors" dhe gabimeve të qëllimshme është që të përdorim burimet e hapura softuer dhe harduer kudo që të jetë e mundur. Zbulimi i kodeve keqdashëse dhe gjetja e hapësirave "backdoors" në qarqet e kompjuterëve, është teknikisht e pamundur nëse këto janë produkte që i përkasin dikujt, që do të thotë se dizajni i tyre nuk është në dispozicion. Me burime të hapura, ky "plan" për të gjithë komponentët është i hapur për shqyrtim në publik. Kodi burimor, zhvillimi i mjeteve-zinxhir, skemat dhe planet, të gjitha mund të inspektohen dhe të analizohen për të parë nëse ka kurthe të fshehura.

Nëse dikush nga ju do të ngrejë pretendimin se burimet e hapura janë disi më pak të sigurta, sepse ato i japin sulmuesit potencial, avantazhin për të ditur më shumë rreth sistemit që ata kanë për synim, dhe pyetjen: "nëse do të jetë më mirë t'i mbajmë të fshehura punët e brendshme të çdo sistemi teknik?", përgjigjja ime e shkurtër është "jo!". Ideja se duke u përpjekur për të arritur siguri më të mirë, duke i fshehur detajet e zbatuara, është përmendur edhe në komunitetin e sigurisë së informacionit si një siguri nëpërmjet errësirës; është shprehur si një ide përçmuese, pasi ajo thjesht nuk funksionon.

Ky rregull themelor është i njohur si parimi Kerckhoffs dhe u mor si i mirëqenë për herë të parë në vitin 1883 nga kriptografi holandez Auguste Kerckhoffs, në punën e tij bazë, "Kriptografia ushtarake" (*La Cryptographie Militaire*) ku: sistemi nuk duhet mbajtur sekret dhe duhet të bjerë në duart e armikut pa vështirësi[9]. Kerckhoffs ishte duke iu referuar në mënyrë specifike kriptografisë ushtarake, por parimi i tij është bërë një doktrinë themelore dhe esenciale e pakontestueshme për komunitetin e sigurisë së informacionit. Sistemet e hapura janë më të sigurta se ato të mbyllura, pasi ato mund të analizohen dhe të studiohen në thellësi. Kjo do të thotë se ndonjë gabim i fshehur ka të ngjarë të zbulohet dhe të riparohet, ndërsa problemet në sistemet e mbyllura, mbeten të panjohura derisa një sulmues i gjen dhe i shfrytëzon ato[10].

## 11. Le të mos e këmbejmë lirinë me sigurinë

Rekomandimi im përfundimtar është se, duhet të jemi të kujdesshëm ndaj kurthit se nëse ekziston balanca midis sigurisë dhe lirisë. Nuk ekziston. Siguria, dhe kjo përfshin dhe sigurinë kibernetike, nuk duhet të vijë në kurriz të së drejtave civile. Ne, si shoqëri dhe si qytetarë individualë, duhet të sigurohemi se çdo përpjekje për ta bërë hapësirën kibernetike më të sigurt, të mos përfundojë duke kufizuar lirinë tonë së të shprehurit, privatësinë dhe të drejtat e tjera themelore.

[8] Trusted Foundry Program, http://www.trustedfoundryprogram.org/

[9] Ne duam që [në sistem] të mos ekzistojë sekreti, dhe ai nuk mund të jetë i papërshtatshëm që të bien në duart e armikut. "Il faut que [le systeme] n'exige pas le secret, et qu'il puisse sans inconvenient ´ tomber entre les mains de l'ennemi" (Kerckhoffs 1883, fq. 12).

[10] Për më shumë mbi parimet e përgjithshme të sistemeve të sigurisë, shiko e.g. (Schneier 1996).

## 12. Konkluzione

Lufta kibernetike është një koncept i papërshtatshëm për të adresuar kërcënimet e vërteta të sigurisë kibernetike me të cilat po përballemi. Shumica e sulmeve kibernetike që kemi parë, nuk kualifikohen si akte lufte. Përse duhet atëherë, të merremi me to, duke përdorur një strukturë ushtarake? Një kundërpërgjigje ushtarake nuk ka gjasa për të zgjidhur ndonjë nga problemet aktuale. Ajo çfarë është e nevojshme, është një qasje civile. Nuk mund të them se kërcënimi nuk është i vërtetë. Ai është. Ekziston një spektër i gjerë i aktorëve që abuzojnë në internet, për qëllimet e tyre të liga. Grupet kriminale transnacionale, të organizuara, kanë zbuluar se interneti është bërë një mjet i shkëlqyer për aktivitetet e tyre, dhe krimi kibernetik është bërë një biznes në lulëzim. Mashtrimi, grabitja, vjedhjet e identitetit dhe spiunazhi i korporatave janë vetëm disa nga krimet që janë bërë më të lehta për tu kryer në një botë në rrjetën globale. Dhe krimi i organizuar nuk është kërcënimi i vetëm. Veprimet e individëve gjithashtu mund të përbëjnë një rrezik të konsiderueshëm, duke filluar nga përpjekjet për të thyer një sistem kompjuterik si akte të motivuara politikisht të vandalizmit *online* apo protestë publike, "vetëm për argëtim". Disa prej këtyre veprimeve janë të natyrës penale, por jo të gjithë. Gjithashtu nuk mund të përjashtohen as aktet e terrorizmit kibernetik në të ardhmen.

Të gjitha këto kërcënime janë serioze, por tashmë ka një sistem të rregullt që merret me këtë: një strukturë të rregullt të zbatimit të ligjit. Nuk ka asnjë arsye përse aktet kriminale të kryera *online* (në internet) nuk duhet të ndiqen penalisht duke përdorur të njëjtin grup rregullash që do të aplikoheshin ndaj krimeve *offline*. Kuadri ligjor me siguri do të duhet të përshtatet, dhe për të vendosur saktësisht se si duhet të merren masa ndaj këtyre kërcënimeve të reja do të kërkohet një shqyrtim publik i zgjatur dhe i ndërlikuar. Për shembull, a është pjesëmarrja në një sulm DDoS, i konsideruar si një vepër penale ose si një shprehje legjitime e mosbindjes civile, e ngjashme me pjesëmarrjen në një demonstratë?[11]

Megjithatë, diskutime të tilla dhe vendosja përfundimisht e rregullave ligjore të reja për të cilat ne kemi nevojë në mënyrë që të adresojmë një realitet të ndryshëm, është pjesë e funksionimit të shëndoshë të shoqërisë në kohë paqeje. Nuk ka asnjë arsye pse ne duhet të braktisim këtë proces dhe të nxisim rregullat e luftës. Kuadri i zbatimit të ligjit në trajtimin e rasteve si: mashtrim, vjedhje, vandalizëm dhe aktet e dhunës *offline* në përgjithësi, ka qenë i suksesshëm. Ai do të funksionojë në të njëjtën mënyrë edhe në trajtimin e këtyre çështjeve *online*.

Më lejoni të theksoj përsëri se unë nuk jam duke u përpjekur të minimizoj seriozitetin e këtij kërcënimi, ose të këshilloj që aktorët shtetërorë nuk kanë ndonjë interes në përdorimin e sulmeve kibernetike. Ata kanë, por përgjigjja e përshtatshme ndaj këtyre kërcënimeve nuk përqendrohet në mbrojtjen (ushtarake) kibernetike, por në përmirësimin e sigurisë kibernetike civile. Një militarizim i vazhdueshëm i qasjes tonë në trajtimin e kërcënimeve kibernetike do të na adresojë më pak drejt problemit real, dhe do të krijojë një gamë të tërë të problemeve të reja në vend. Siç thekson edhe Bruce Schneier: "Kjo ka të bëjë me atë, se kush është përgjegjës për sigurinë kibernetike, dhe se

[11] TechPresident blog, 13 dhjetor 2010, http://techpresident.com/blog-entry/ten-ways-think-about-ddos-attacksand-legitimate-civil-disobedience

sa kontroll do të ushtrojë qeveria mbi rrjetet civile"[12]. Duke inkuadruar debatin në drejtim të luftës kibernetike, ne jemi duke pranuar para së gjithash idenë se interneti i hapur ka dështuar.

Një nga pasojat e të qenit në një luftë (kibernetike) është se ne duhet të pranojmë një kufizim së të drejtave dhe lirive civile[13]. Kohët e fundit ka një numër iniciativash kryesore që na udhëheqin në këtë drejtim, të tilla si "Mbrojtja e akteve kibernetike dhe shpërndarja e inteligjencës kibernetike" (CISPA), aktualisht nën vëmendjen e SHBA-së[14]. CISPA autorizon shprehimisht monitorimin e komunikimeve private dhe do të lejojë kompanitë që të dorëzojnë informacionin personal për qeverinë, pa ndonjë mbikëqyrje gjyqësore. Ashtu siç paralajmëron edhe studiuesi i sigurisë amerikane, Jacob Appelbaum: "Këto të dhëna nuk janë vetëm duke u mbledhur, por tani ata duhet të ndahen edhe me DHS, me FBI dhe me NSA, para së gjithash për të bërë të ligjshme mbikëqyrjen ushtarake mbi qytetarët amerikanë dhe tërë planetin. [ ... ] Ky është një kërcënim ekzistencial për anonimitetin në internet, për privatësinë dhe për sigurinë e përditshme të njerëzve"[15].

Së fundi, kërcënimi më i madh nga internet, si një platformë e hapur për shkëmbimin e lirë të ideve, bashkëpunimin, dhe shpërndarjen e tyre nuk mund të vijnë nga hakerat e "Ushtrisë Blu" të Kinës[16] apo nga lulëzimi i botës së krimit kibernetik. Ai mund të vijë nga ata që pretendojnë se kanë nevojë për më shumë kontroll mbi internetin, në mënyrë që ta "mbrojnë" atë.

Lufta kibernetike ka qenë dhe është prezent edhe sot në kryetitujt e gazetave kryesore. Në një artikull të fundit të New York Times, paraqitet një pamje e detajuar e një programi të SHBA-së, i një niveli të lartë, i dyshuar për zhvillimin dhe përdorimin e sulmeve kibernetike, të koduar me emrin Lojërat Olimpike (Olympic Games)[17].

"Flame malware kit" të zbuluara në fund të majit të vitit 2012, besohet të jenë "pjesë e operacioneve të vazhdueshme të spiunazhit kibernetik të drejtuara nga shteti dhe të mirëkoordinuara"[18]. Në një demaskim të papritur javën e shkuar, qeveria gjermane zbuloi se ata posedojnë kapacitete kibernetike sulmuese[19].

Duket një situatë e rrezikshme. Unë kam dhënë mendimin tim se pse lufta kibernetike në mënyrë të veçantë për shkak të rrezikut të përshkallëzimit, nuk ka të ngjarë të shndërrohet në një konflikt kinetik. Megjithatë, mund të jem gabuar. Sigurisht që ekziston një numër i madh i shteteve që investojnë fuqishëm në zhvillimin e aftësive ushtarake

---

[12] Bruce Schneier, "Threat of 'Cyberwar' Has Been Hugely Hyped", Schneier on Security, 7 korrik 2010, http://www.schneier.com/blog/archives/2010/12/book_review_cyb.html

[13] Në erozionin e lirive civile gjatë kohës së luftës, shiko e.g. Louis Fisher, "Civil Liberties in Time ofWar", Shërbimi Kërkimor i Kongresit, 7 shkurt 2003, http://www.clas.ufl.edu/users/rconley/conferencepapers/Fisher.pdf

[14] Trevor Timm, "Cybersecurity Bill FAQ: The Disturbing Privacy Dangers in CISPA and How To Stop It", EFF, 15 prill 2012, https://www.eff.org/deeplinks/2012/04/cybersecurity-bill-faq-disturbing-privacy-dangers-cispa-and-how-you-stop-it

[15] Jacob Appelbaum intervistuar tani në Demokraci!, 26 Prill 2012, http://www.democracynow.org/2012/4/26/targeted_hacker_jacob_appelbaum_on_cispa

[16] Njësia e luftës kibernetike e Kinës. Shiko "PLA establishes 'Online Blue Army' to protect network security", e përditshmja "Peo-ple's Daily Online", 26 maj 2011, http://english.peopledaily.com.cn/90001/90776/90786/7392182.html

[17] David E. Sanger, "Obama order sped up wave of cyberattacks against Iran", Gazeta The New York Times, 1 qershor 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obamaorderedwave-of-cyberattacks-against-iran.html

[18] Kim Zetter, "Meet 'Flame,' the massive spy malware infiltrating Iranian computers", telegrafuar, 28 maj 2012, http://www.wired.com/threatlevel/2012/05/flame/

[19] Michael Fischer, Joerg Blank and Christoph Dernbach, "Germany confirms existence of operational cyberwarfare unit", Botime Deutsche Presse-Agentur, 5 qershor 2012, http://www.stripes.com/news/germanyconfirmsexistence-of-operational-cyberwarfare-unit-1.179655

kibernetike. Dhe, sapo një armë të jetë ekzistuese, me të vjen edhe tundimi për ta përdorur atë. Kështu që thirrja ime për paqe kibernetike, është edhe në këtë kuptim; edhe pse unë e kuptoj që mund të jetë shumë vonë.

Mendoj vazhdimisht për filmin e vitit 1983 të titulluar "Lojëra lufte" të cilin e kam pasur edhe si pikë referimi për këtë punim. Në këtë film, një burrë i ri fiton akses në një sistem kompjuterik të një niveli të lartë të ushtrisë të SHBA-ve. Ai mendon se është duke luajtur një lojë, por në të vërtetë ai është duke komanduar një superkompjuter inteligjent sekret, që është duke simuluar Luftën e Tretë Botërore, i cili është gati të lëshojë raketa bërthamore kundër Bashkimit Sovjetik. Kur ai e kupton që është duke shkaktuar një luftë botërore termonukleare, ai dëshiron të ndalojë lojën, por kjo nuk është më e mundur. Katastrofa shmanget kur inteligjenca artificiale pas kompjuterit e kupton në momentin e fundit përpara shndërrimit të botës në një asgjësim nuklear, që ka vetëm një mësim për t'u shmangur nga lufta[20].

Një lojë e çuditshme. Lëvizja e vetme e zgjuar është të mos luash!



[20] "Loje Lufte (1983) – Kuotat e paharrueshme", The Internet Movie Database, http://www.imdb.com/title/tt0086567/quotes

## Bibliografi


1. Jack Goldsmith, "Susan Landau on Cybersecurity Bills", Ligji i Luftës, 3 maj 2012. http://www.lawfareblog.com/2012/05/susanlandauoncybersecurity-bills/
2. Ellen Nakashima, "In U.S.-Russia deal, nuclear communication system may be used for cybersecu-rity", Gazeta "The Washington Post", 26 gusht 2012, http://www.washingtonpost.com/world/nationalsecurity/in-us-russia-dealnuclearcommunicationsystemmaybeusedforcybersecurity/2012/04/26/gIQAT521iT_story.html
3. UK Cabinet Office, "The UK Cyber Security Strategy", nëntor 2011, http://www.cabinetoffice.gov.uk/sites/default/files/resources/ukcybersecurity-strategy-final.pdf
4. Nick Hopkins, "Hackers have breached top secret MoD systems, cyber-security chief admits", Revista "The Guardian", 3 maj 2012, http://www.guardian.co.uk/technology/2012/may/03/hackersbreachedseet-mod-systems
5. Richard A. Clarke, "Cyber War. The Next Threat to National Security and What to Do About It" (Clarke 2010).
6. Për një hyrje te përgjithshme të elasticitetit si një veçori thelbësore e një sistemi të sigurt, shiko Bruce Schneier, Beyond Fear (Schneier 2003, f. 119–132).
7. William J. Lynn III, "Defending a New Domain. The Pentagon's Cyberstrategy" (Lynn III 2010). Artikulli gjendet online ne websiten e DoD te SHBA. http://www.defense.gov/home/features/2010/0410_cybersec/lynnarticle.aspx
8. Trusted Foundry Program, http://www.trustedfoundryprogram.org/
9. TechPresident blog, 13 Dhjetor 2010, http://techpresident.com/blog-entry/ten-ways-think-about-ddos-attacksand-legitimate-civil-disobedience
10. Bruce Schneier, "Threat of 'Cyberwar' Has Been Hugely Hyped", Schneier on Security, 7 korrik 2010, http://www.schneier.com/blog/archives/2010/12/book_review_cyb.html
11. Në erozionin e lirive civile gjatë kohës së luftës, shiko e.g. Louis Fisher, "Civil Liberties in Time ofWar", Shërbimi Kërkimor i Kongresit, 7 shkurt 2003, http://www.clas.ufl.edu/users/rconley/conferencepapers/Fisher.pdf
12. Trevor Timm, "Cybersecurity Bill FAQ: The Disturbing Privacy Dangers in CISPA and How To Stop It", EFF, 15 prill 2012, https://www.eff.org/deeplinks/2012/04/cybersecurity-bill-faq-disturbing-privacy-dangers-cispa-and-how-you-stop-it
13. Jacob Appelbaum intervistuar tani në Demokraci!, 26 Prill 2012, http://www.democracynow.org/2012/4/26/targeted_hacker_jacob_appelbaum_on_cispa
14. Njësia e luftës kibernetike e Kinës. Shiko "PLA establishes 'Online Blue Army' to protect network security", e përditshmja "Peo-ple's Daily Online", 26 maj 2011, http://english.peopledaily.com.cn/90001/90776/90786/7392182.html
15. David E. Sanger, "Obama order sped up wave of cyberattacks against Iran", Gazeta The New York Times, 1 qershor 2012,
16. http://www.nytimes.com/2012/06/01/world/middleeast/obamaorderedwave-of-cyberattacks-against-iran.html
17. Kim Zetter, "Meet 'Flame,' the massive spy malware infiltrating Iranian computers", telegrafuar, 28 maj 2012, http://www.wired.com/threatlevel/2012/05/flame/
18. Michael Fischer, Joerg Blank and Christoph Dernbach, "Germany confirms existence of operational cyberwarfare unit", Botime Deutsche Presse-Agentur, 5 qershor 2012,
19. http://www.stripes.com/news/germanyconfirmsexistence-of-operational-cyberwarfare-unit-1.179655
20. "Loje Lufte (1983) – Kuotat e paharrueshme", The Internet Movie Database, http://www.imdb.com/title/tt0086567/quotes

# Kërcënimet kibernetike: ndikimi i tyre në sigurinë shtetërore të Kosovës

■**Dr. (proc.) Riza SHILLOVA**
*Drejtor i Departamentit të Hetimeve,*
*Policia e Kosovës*
*riza.shillova@kosovopolice.com*

**Abstrakt**

*Kërcënimet konvencionale të luftës shtet kundër shtetit, sot janë zvogëluar në masë të konsiderueshme. Sot ka një trend të përgjithshëm të rritjes së kërcënimeve jokonvencionale, siç janë: armët e shkatërrimit në masë, terrorizmi dhe krimi kibernetik. Në bazë së të dhënave në dispozicion sot në Kosovë, Europë dhe më gjerë, sulmet kibernetike ndodhin në baza ditore dhe po bëhen më të ashpra çdo ditë e më tepër. Referuar të dhënave në dispozicion, në Kosovë pritet që kërcënimi i sulmeve kibernetike të shtohet gjatë viteve në vijim. Kërcënime të tilla, mund të shkaktojnë dëme ekstreme në ekonomi, administratë publike dhe te infrastruktura kritike e Kosovës. Këto Sulme konsiderohet se mund të jetë të inkurajuara, jo vetëm nga aktivitete kriminale, por edhe nga agjenda politike. Në këtë mënyrë, krimet kibernetike paraqesin një rrezik ndaj sigurisë, stabilitetit dhe funksionimit të shtetit. Zhvillimi i infrastrukturës digjitale, e ka ndryshuar shumë jetën tonë të përditshme sociale dhe ekonomike, dhe, ka ndikuar edhe në paraqitjen e veprave të reja penale që ndërlidhen me krime kibernetike. Aktiviteti kryesor i grupeve kriminale në Kosovë është trafikimi i narkotikëve, trafikimi i qenieve njerëzore, prostitucioni, terrorizmi, kontrabanda e migracionit, mallrave e armëve, bixhozi, fajdetë, korrupsioni etj. Hapësira kibernetike, ofron mundësi më të mëdha për aktivitetet kriminale të përmendura më lartë, por duke përfshirë edhe forma tjera të kriminalitetit, që ndikojnë në sigurinë shtetërore, siç janë: sulmet kibernetike, spiunimi kibernetik apo sabotimi kibernetik, inteligjenca kibernetike si dhe terrorizmi kibernetik. Në bazë të analizës së rishikimit strategjik, të sektorit të sigurisë në Republikën e Kosovës, krimi kibernetik, si kërcënim jokonvencional, është identifikuar si një prej rreziqeve, sfidave apo kërcënimeve globale që mund të cenojnë edhe sigurinë e Kosovës. Qeveria e Republikës së Kosovës ka hartuar "Strategjinë e sigurisë kibernetike, 2016-2019" dhe "Planin e veprimit", që është në harmoni me standardet e Agjencisë Evropiane për Sigurinë e Rrjeteve dhe Informacionit (ENISA); dhe, në frymën e integrimeve europiane. Në kuadër të qasjes strategjike, institucionet e Kosovës, kanë përcaktuar se prioritet për sigurinë kibernetike, është koordinimi ndërinstitucional, mbrojtja e infrastrukturës kritike të informatave, zhvillimi i kapaciteteve (ligjore, njerëzore dhe infrastrukturore), ndërtimi i partneriteteve publiko-private, reagimi ndaj incidenteve dhe bashkëpunimi ndërkombëtar.*

**Fjalëkyçe:**
**siguri, nacionale, kibernetike, kërcënim, strategji.**

## 1. Hyrje

Referuar të dhënave në nivel botëror, sot interneti, me hapësirën kibernetike, konsiderohet si njëri ndër sistemet më të mëdha të ndërtuar ndonjëherë në nivel global. Sot, në hapësirën kibernetike, operojnë miliarda përdorues të pajisjeve elektronike, siç janë: kompjuterë të ndryshëm, laptopë, tabletë, telefona të mençur, baza së të dhënave etj. Ekzistojnë miliarda pajisje të ndryshme të cilat janë të lidhura me sisteme teknologjike, përfshirë edhe internetin. Sipas *Statistikave botërore të internetit* (Internet World Stats) në vitin 2017, kemi pasur mbi 4 miliardë përdorues të internetit, apo shprehur në përqindje, 54.4 % të numrit të përgjithshëm të popullatës në nivel botëror. Sipas analistëve të *Gartner inc.,* gjithsej në vitin 2020, pajisjet ekektronike të instaluara në të gjithë botën, do të jenë më shumë se dyfishi i tanishëm. Sipas tyre, në vitin 2017 ishin rreth 8.4 miliardë pajisje të lidhura në internet, ndërsa parashikimi është se në vitin 2020, do jenë rreth 20.4 miliardë, pajisjet e internetit. Gjithashtu, rritja e përdorimit të internetit për periudhën 2000-2014, ka qenë 741%, ndërsa përdorimi i internetit në nivel global është rreth 42%.

Nëse e shikojmë këtë zhvillim teknologjik dhe këtë numër të madh të pajisjeve, nga aspekti i sigurisë, atëherë është lehtë të konstatohet se siguria kibernetike, sot paraqet gjithnjë e më shumë një kërcënim për sigurinë nacionale, por edhe sigurinë globale në përgjithësi. Mjafton një pajisje e tillë nga cilido vend në botë të kryej një veprim në secilën pjesë të botës. I ashtuquajturi "revolucion digjital" ka ndikuar të gjitha poret e shoqërisë moderne në nivel global. Kjo në veçanti, vërehet në përpjekjet të cilat i bëjnë shtetet e ndryshme, organizatat dhe individët për të shfrytëzuar hapësirën kibernetike me qëllim të arritjes më të madhe në zhvillimin ekonomik, mirëqenie shoqërore, arsim,

shkencë, politikë dhe siguri. Zhvillimi i teknologjisë mundëson efikasitet më të madh në këto fusha, sikundër, që mund të jetë edhe kërcënim më i shtuar në aspektin e sigurisë e të privatësisë.

Me një shtrirje të tillë të përdorimit të pajisjeve teknike dhe teknologjike të internetit, si platformë kryesore e punës, siguria kibernetike, në përgjithësi, do të jetë njëra ndër brengat kryesore në nivel botëror, për rajonin e Ballkanit, por edhe për Kosovën. Interneti, duke përfshirë hapësirën e tij kibernetike, paraqet një prej shtytësve më të rëndësishëm të inovacionit, rritjes dhe konkurrencës së ekonomive shtetërore në të gjithë botën. Në një botë të globalizuar dhe të ndërlidhur, hapësira kibernetike dhe siguria e saj, kthehen si objektiva kyç, strategjikë, në fushën e sigurisë në secilin vend. Interneti dhe aktivitetet e tij kibernetike, - si ato ekonomike, shkencore dhe sociale, - po fitojnë përditë e më shumë rëndësi. Kjo liri kibernetike dhe vlerat njerëzore duhen mbrojtur, në të njëjtën mënyrë si në botën jashtë internetit. Infrastruktura digjitale duhet mbrojtur nga incidentet, keqpërdorimi dhe aktivitetet keqdashëse. Organet qeveritare duhet të kenë shumë role, fillimisht, duke përcaktuar politika e udhëzime të qarta e transparente, për të siguruar jo vetëm hapjen dhe përfshirjen e secilit qytetar, por edhe sigurinë e hapësirës kibernetike[1].

PËRDORIMI I INTERNETIT NË NIVEL BOTËROR DHE STATISTIKAT E POPULLSISË, Dhjetor 31, 2017

| Regjionet botërore | Popullata (2018 ) | Popullata % | Shfrytëzuesit e internetit (2017) | Shkalla e përdorimit (% Pop.) | Rritje (2000-2018) | Shfrytëzuesit internet % |
|---|---|---|---|---|---|---|
| Afrika | **1 287 914 329** | 16.9 % | **453 329 534** | 35.2 % | 9.941 % | 10.9 % |
| Azia | **4 207 588 157** | 55.1 % | **2 023 630 194** | 48.1 % | 1.670 % | 48.7 % |
| Europa | **827 650 849** | 10.8 % | **704 833 752** | 85.2 % | 570 % | 17.0 % |
| Amerika Latine / Karaibet | **652 047 996** | 8.5 % | **437 001 277** | 67.0 % | 2.318 % | 10.5 % |
| Lindja e Mesme | **254 438 981** | 3.3 % | **164 037 259** | 64.5 % | 4.893 % | 3.9 % |
| Amerika Veriore | **363 844 662** | 4.8 % | **345 660 847** | 95.0 % | 219 % | 8.3 % |
| Oqeania / Australia | **41 273 454** | 0.6 % | **28 439 277** | 68.9 % | 273 % | 0.7 % |
| Total | **7 634 758 428** | **100.0 %** | **4 156 932 140** | **54.4 %** | **1.052 %** | **100.0 %** |

**Tabela 1. Internet World Stats[2]**

Nga të dhënat e *Internet World Stats* vërehet një shkallë mjaft e gjerë e përdorimit të internetit. Gjithashtu, në bazë të parashikimeve, pritet që të kemi një rritje mjaft të ndjeshme, në të ardhmen, të përdorimit të internetit si dhe përqindje mjaft të lartë të shkallës së përdorimit. Amerika dhe Evropa, si kontinent, paraprijnë, për sa i përket përdorimit dhe shfrytëzuesve të internetit në raport me popullsinë, me kontinentet tjera. Evropa është pasuesja e menjëhershme.

Prioritetet e BE-së në fushën e sigurisë për 5 vitet e ardhshme, janë se BE duhet të mbetet vigjilente ndaj kërcënimeve të tjera në zhvillim, të cilat gjithashtu kërkojnë një përgjigje të koordinuar të BE-së. Agjenda e BE-së i jep përparësi trajtimi, terrorizmit,

[1] Strategjia shtetërore e sigurisë kibernetike dhe plani i veprimit të Kosovës, 2016-2019.
[2] https://www.internetworldstats.com/stats.htm

krimit të organizuar dhe krimit kibernetik, si fusha të ndërlidhura me një dimension të fortë ndërkufitar, ku veprimi i BE-së mund të bëjë një ndryshim real. BE-ja në kuadër të tri prioriteteve të saja, ka përcaktuar edhe krimin kibernetik si prioritet kryesor. Në strategjinë e sigurisë kibernetike të bashkimit evropian (*Hapësirë kibernetike e hapur, e sigurt dhe e mbrojtur*)[3], siguria kibernetike përgjithësisht iu referohet masave mbrojtëse dhe veprimeve që mund të ndërmerren për të mbrojtur domenin kibernetik, edhe në fushën civile edhe në atë ushtarake, nga ato kërcënime që ndërlidhen me to, apo që mund të dëmtojnë rrjetet dhe infrastrukturën komunikuese të ndërvarur, krahas krimit të organizuar dhe terrorizmit. Në kuadër të BE-së, vepron agjencia e quajtur ENISA (*European Union Agency For Network and Information Security*), e cila ka një rol të theksuar në përcaktimin e standardeve, rekomandimeve dhe angazhimeve tjera në fushën e sigurisë kibernetike.

Ky trend i zhvillimit, angazhimit dhe përkushtimit ndaj sigurisë kibernetike është i njëjtë edhe në vendet e Ballkanit përfshirë edhe Kosovën. Meqë Kosova, si shtet është duke zbatuar një agjende të integrimit evropian, është krejt normale se në këtë drejtim duhet të ndjek edhe udhëzimet dhe kriteret që duhet të plotësohen, për vendet aspiruese për integrim në BE, sa i përket edhe sigurisë, dhe në këtë kontekst, sigurisë kibernetike. Në Kosovë mungon njëra nga strategjitë kryesore, që është *strategjia kombëtare e sigurisë* prandaj edhe prioritetet nuk janë të përcaktuara në kuadër të një strategjie gjithëpërfshirëse.

## 2. Rëndësia e sigurisë kibernetike në Kosovë

Në Kosovë, përdorimi i teknologjisë së informimit dhe komunikimit (TIK) ka qenë në zgjerim të shpejtë që prej vitit 1999, ndërsa tanimë TIK-u luan rol të rëndësishëm në të gjitha aspektet e jetës sonë. Përdorimi i internetit në Kosovë është 80.40 %, shkallë kjo shumë e ngjashme me mesataren e Bashkimit Evropian, derisa edhe sjelljet e kosovarëve në internet duket se janë të ngjashme me prirjet globale. Organizatat qeveritare, organizatat që ofrojnë shërbime në sektorët kritikë të infrastrukturës, si: energjia, uji, shëndetësia, transporti, komunikimi dhe financat, i kanë zhvendosur tashmë punët e tyre të përditshme në internet. Këto sisteme përmirësojnë cilësinë dhe shpejtësinë e shërbimeve që ofrohen, duke u ndihmuar kështu organizatave që të punojnë në mënyrë më produktive, duke kontribuar kështu drejt përmirësimit të standardeve të jetesës. Megjithatë, në të njëjtën kohë, ato u ekspozohen edhe rreziqeve të ndryshme në hapësirën e internetit. Këto rreziqe qëndrojnë te cenimi i pashmangshëm në TIK, si dhe mund të shkaktojnë mungesa të shërbimit, apo edhe keqpërdorim të shërbimeve, duke rezultuar kështu me dëmtim (humbje) të mundshme të jetëve të njerëzve, humbje ekonomike në masë të madhe, rrënim të rendit publik dhe kërcënime ndaj sigurisë kombëtare[4].

Nga aspekti i sigurisë kibernetike, është i rëndësishëm përkufizimi i rolit dhe rëndësisë që ka siguria kibernetike në raport me sigurinë kombëtare. Vështrimi i trajtimit të sigurisë kibernetike në Kosovë duhet parë nga tri këndvështrime: a) përshkrim i rreziqeve, kryerësve dhe caqeve të sulmeve kibernetike dhe rritje e vetëdijes për cenimet/dobësitë; b) ofrimi i një pasqyre të sigurisë kibernetike në Kosovë, përfshirë kornizën ligjore dhe

[3] JOIN(2013) 1 final, 7 Feb 2013 - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013JC0001
[4] Strategjia Shtetërore e Sigurisë Kibernetike dhe Plani i Veprimit të Kosovës, 2016-2019

institucionale c) politikat, strategjitë dhe ndërlidhja mes tyre. Me qëllim të adresimit të këtyre çështjeve, Kosova nuk mund të jetë e përjashtuar nga zhvillimet globale. Për këtë arsye, në vitin 2016, në Kosovë është hartuar "Strategjia e sigurisë kibernetike të Kosovës, 2016-2019" e cila përmban qëllimet, objektivat dhe mënyrën e zbatimit të aktiviteteve konkrete. Me këtë dokument, janë bërë përpjekjet që të trajtohen në mënyrë ndërinstitucionale rreziqet dhe kërcënimet që shfaqen në hapësirën kibernetike në vendin tonë.

Republika e Kosovës ka resurse të limituara në aspektin e burimeve njerëzore, teknike dhe teknologjike, për tu përballuar me rreziqe të natyrave të tilla, prandaj është shumë i domosdoshëm krijimi i mekanizmit ndërinstitucional, i cili do të jetë më i efekshëm në shfrytëzimin racional të burime në mes të të gjitha institucioneve shtetërore përshfirë edhe sektorin privat. Në Kosovë, përdorimi i teknologjisë së informimit dhe komunikimit pra ka një rritje të shpejtë. Organizatat që ofrojnë shërbime në sektorët kritikë të infrastrukturës si energjia, uji, shëndetësia, transporti, komunikimi dhe financat kanë zhvendosur tashmë punët e tyre të përditshme në internet. Këto sisteme përmirësojnë cilësinë dhe shpejtësinë e shërbimeve që ofrohen, duke u ndihmuar kështu organizatave që të punojnë në mënyrë më produktive, duke kontribuar kështu drejt përmirësimit të standardeve të jetesës. Megjithatë, në të njëjtën kohë, ato u ekspozohen edhe rreziqeve të ndryshme në hapësirën e internetit. Këto rreziqe qëndrojnë te cenimi i pashmangshëm në TIK, si dhe mund të shkaktojnë mungesa të shërbimit apo edhe keqpërdorim të shërbimeve, duke rezultuar kështu me dëmtim (humbje) të mundshme të jetëve të njerëzve, humbje ekonomike në masë të madhe, rrënim të rendit publik e edhe kërcënime ndaj sigurisë kombëtare[5].

Nëse vështrojmë në aspektin krahasues, Kosova ka një përqindje më të lartë të përdorimit të internetit në krahasim me vendet e rajonit. Kjo normalisht që është një përparësi, në aspekt të potencialit për zhvillim të përgjithshëm ekonomiko–shoqëror, por njëkohësisht paraqet edhe rrezik për fushën e sigurisë kibernetike.

| Krahasimi i numrit të përdoruesve të internetit dhe përqindja e hyrjes në internet të shteteve të rajonit | | |
|---|---|---|
| **Shteti** | **Numri i Përdoruesve** | **Përdorimi** |
| **Kosova** | 1,523,373 | 80.40% |
| **Shqipëria** | 1,932,024 | 65.80% |
| **Maqedonia** | 1,583,315 | 75.90% |
| **Serbia** | 6,325,816 | 72.20% |
| **Mali i Zi** | 439,624 | 69.90% |

**Tabela 2. Internet World Stats [6]**

Nga paraqitja grafike në tabelën 2. shihet shkalla e përdorimit të internetit në Kosovë në krahasim me vendet fqinje. Nga kjo konstatohet se në Kosovë kemi një shkallë më të lartë të përdorimit të internetit e cila tregon edhe rëndësinë e sigurisë kibernetike dhe rreziqet kibernetike. Përdorimi i internetit nga popullsia e Kosovës, është përafërsisht i barabartë me shtetet e Bashkimit Evropian. Krahas zhvillimit ekonomik në vendin tonë kemi paralelisht edhe avancim sa i përket hapësirës kibernetike sepse ajo gjithnjë e

[6] https://www.internetworldstats.com/stats.htm

më shumë po përdoret për të ndikuar në zhvillimin e përgjithshëm. Kosova, me qëllim të përgjigjes adekuate të rreziqeve kibernetike, ka përgatitur *Strategjinë e sigurisë kibernetike, 2016 -2019.*

## 3. Kërcënimet kibernetike

Kërcënimet dhe rreziqet kibernetike, sot paraqesin pothuajse në mbarë globin, krahas terrorizimit, krimit të organizuar dhe armëve të shkatërrimit në masë, njërin ndër rreziqet kryesore. Edhe në Kosovë, është vlerësuar se kërcënimet kibernetike janë njëri ndër kërcënimet e së ardhmes. Kjo vërehet qartë në vlerësimet e kryera deri tani në fushën e sigurisë. Rreziqet, sfidat dhe kërcënimet globale që mund të ndikojnë në sigurinë e Kosovës, rrjedhin nga pabarazia ekonomike, aktivitetet terroriste, krimi ndërshtetëror, armët nukleare dhe armë të tjera të shkatërrimit në masë, përhapja e armëve të vogla, krimi i organizuar përfshirë trafikimin, dhe krimi kibernetik. Në një botë të ndërvarur, Kosova si dhe shumë vende të tjera, në mënyrë të direkt ose indirekt, përballet me rreziqe të ngjashme[7].

Krimi kibernetik konsiderohet si njëri ndër kërcënimet jokonvencionale dhe si njëri ndër kërcënimet më serioze, të kërcënime të sotme në Kosovë. Zhvillimi i sistemeve komunikuese dhe informative ka bërë secilin shtet, pavarësisht nga fuqia dhe zhvillimi, të jetë i cenueshëm ndaj sulmeve kibernetike, të cilat mund të shkaktojnë dëme të mëdha në sistemet kombëtare, rrjetet dhe infrastrukturën e informimit, ekonomi, banka, biznese dhe te trafiku ajror e tokësor. *InfoSecurity Europe* paralajmëron se, qindra e mijëra sulme kibernetike ndodhin në baza ditore, dhe po bëhen më të ashpra çdo ditë e më tepër. Pritet që kërcënimi i sulmeve kibernetike do të shtohet gjatë viteve në vijim. Si i tillë, mund të shkaktojë dëme ekstreme në administratë publike, në ekonomi dhe në infrastrukturë të Kosovës. Krimi kibernetik, konsiderohet të jetë inkurajuar dhe të jetë shkaktuar nga agjendat politike dhe aktivitetet kriminale. Në këtë mënyrë, krimet kibernetike paraqesin një rrezik ndaj sigurisë, stabilitetit dhe funksionimit të shtetit[8].

Kërcënimet kibernetike, janë të shumëllojshme duke filluar nga: krimi kibernetik, sabotimi, spiunimi, terrorizmi etj. Kriminaliteti kibernetik, si kërcënim, nënkupton një sërë veprimtarish kriminale të ndryshme, ku kompjuterët dhe sistemet informative angazhohen si vegël për të kryer veprimin kriminal. Krimi kibernetik përfshin vepra penale të ndryshme, siç janë: sulmet ndaj sistemeve informative, mohimi i shërbimit dhe maluer (*malware*), mashtrimi, falsifikimi dhe thyerja e identitetit, pornografia e fëmijëve, nxitja e urrejtjes etnike, racore etj. Sabotimi, si kërcënim, nënkupton aktivitetet të cilat atakojnë apo kanë për qëllim të çrregullojnë funksionimin normal të sistemeve të komunikimit e të informacionit të një shteti.

Sulmet kibernetike ndaj integritetit dhe disponueshmërisë së sistemeve TI, quhen sabotim kibernetik. Spiunimi është njëra ndër veprimtaritë kundër sigurisë së një vendi, ku hapësira kibernetike përdoret për të ndërhyrë në mënyrë tinëzare, të pavërejtur, në një shtet tjetër, brenda sistemeve të komunikimit e të informacionit, duke vjedhur informacione apo informatat të ndryshme, duke ndryshuar apo fshirë të dhëna të ndryshme. Sulmet kibernetike të cilat zhvillohen ndaj në vendi, ushtrohen apo menaxhohen nga shërbimet e huaja inteligjente dhe në këtë kuptim i njohim si spiunim

[7] Analizë e Rishikimit Strategjik të Sektorit të Sigurisë së Republikës së Kosovës, 2014.
[8] Po aty.

kibernetik. Terrorizmi kibernetik, sot paraqet një ndër kërcënimet jokonvenciale mjaft serioze për sigurinë kombëtare. Terrorizmi kibernetik ka të bëjë me shënjim të nivelit të lartë, që bëhet për qëllime të grupeve ose organizatave terroriste, si dhe terroristëve individual. Informacionet shpesh janë shënjestër e sulmeve, përditë e më komplekse kibernetike. Këto sulme veçanërisht shënjohen nga terroristët dhe hakerët që kërkojnë informata të ndjeshme. Ekstremizmi dhe radikalizmi sot paraqet gjithashtu një sfidë në nivel global sikundër që është një sfidë edhe për Kosovën. Hapësira kibernetike dhe sidomos interneti, përmes platformave të ndryshme sociale, përdoret për të përhapur ideologji ekstreme dhe radikale. Gjithashtu, interneti, sot gjithnjë e më shumë, po përdoret për të rekrutuar anëtarë të rinj në organizata të ndryshme ekstremiste, por edhe terroriste. Mashtrime e falsifikime kibernetike në masë të madhe mund të kryhen në internet, përmes instrumenteve si vjedhja e identitetit, *phishing*, posta e padëshiruar dhe kodimet keqdashëse; pastaj, përmbajtja e paligjshme *online*, duke përfshirë materialet me keqpërdorim seksual të fëmijëve, nxitjen e urrejtjes racore, nxitjen e akteve terroriste dhe idealizimin e dhunës, terrorizmit, racizmit dhe ksenofobisë[9].

Caku i sulmeve kibernetike, sot, padyshim që është ai i infrastrukturave kritike në një vend, ku përfshihen: energjia, financat, teknologjitë e informacionit dhe të komunikimit (TIK), shëndetësia, uji, ushqimi, rendi dhe siguria publike e juridike, administrata civile, transporti, industria kimike dhe bërthamore, sistemi arsimor dhe hulumtimet etj. Kosova akoma nuk e ka të miratuar infrastrukturën e nevojshme ligjore për të mbrojtur infrastrukturën kritike. Prandaj është nevojë e domosdoshme që të miratohet sa më parë ligji për infrastrukturën kritike.

## 4. Infrastruktura ligjore

Në fushën e sigurisë kibernetike, Republika e Kosovës, ka në zbatim një bazë të gjerë ligjore, e cila përfshin, por nuk kufizohet, te:

- Kushtetuta e Republikës së Kosovës;
- ligji nr. 3/L-050 "Për themelimin e Këshillit të Sigurisë së Kosovës";
- ligji nr. 3/L –166 "Për parandalimin dhe luftimin e krimit kibernetik";
- ligji nr. 4/L-145 "Për organet qeveritare të shoqërisë së informacionit";
- ligji nr. 4/L-094 "Për shërbimet e shoqërisë së informacionit";
- ligji nr. 4/L-109 "Për komunikimet elektronike";
- ligji nr. 3/L – 172 "Për mbrojtjen e të dhënave personale";
- ligji nr. 4/L-076 "Për Policinë";
- ligji "Për FSK-në";
- ligji nr. 3/L-142 "Për rendin dhe qetësinë publike";
- ligji nr. 3/L063 "Për Agjencinë Kosovare të Inteligjencës";
- ligji nr. 4/L-149 "Për ekzekutimin e sanksioneve penale";
- ligji nr. 4/L-065 "Për të drejtën e autorit dhe të drejtat e përafërta";
- ligji nr. 3/ L-183 "Për zbatimin e sanksioneve ndërkombëtare";
- ligji nr. 4/L-213 "Për ndihmën juridike ndërkombëtare në çështje penale";
- ligji nr. 4/L-052 "Për marrëveshjet ndërkombëtare";
- ligji nr. 4/L-072 "Për kontrollimin dhe mbikëqyrjen e kufijve shtetërorë";
- ligji nr. 4/L-093 "Për bankat, institucionet mikrofinanciare dhe institucionet

[9] Strategjia Shtetërore e Sigurisë Kibernetike dhe Plani i Veprimit të Kosovës, 2016-2019

financiare jobankare";

- ligji nr. 4/L-064 "Për Agjencinë Forenzike të Kosovës";
- ligji nr. 4/L-198 "Për tregtimin e mallrave strategjikë";
- ligji nr. 4/L –004 "Për shërbimet private të sigurisë";
- ligji nr. 3/L-046 "Për Forcën e Sigurisë së Kosovës";
- Kodi nr. 3/L-109 Doganor dhe i Akcizës, i Kosovës ;
- Kodi nr. 4/L-082 Penal i Republikës së Kosovës;
- Kodi nr. 4/L-123 i Procedurës Penale;
- ligji nr. 3/L-122 "Për shërbim të Jashtëm të Republikës së Kosovës".

Kosova për dallim nga shumë shtete ka në fuqi edhe ligin "Për parandalimin dhe luftimin e krimeve kibernetike", i cili sanksionon një mori veprash penale siç janë:

1. veprat penale kundër konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave të sistemeve kompjuterike;
2. transferuat e paautorizuara;
3. pengimi i funksionimit të sistemeve kompjuterike;
4. prodhimi, posedimi dhe tentativa e paautorizuar.[10]

Në fushën e sigurisë kibernetike, Republika e Kosovës, ka në zbatim, një bazë të gjerë ligjore mjaft moderne dhe të konsoliduar, sidoqoftë edhe në këtë fushë ka nevojë për rishikim të ligjit "Për parandalim dhe luftim të krimit kibernetik", ligj i cili, tani thjesht sa nuk i përshtatet më kohës, ndryshimeve teknike dhe teknologjike. Kosova ka Kodin Penal, i cili përmban veprat penale, megjithatë ka një kolizion me ligjin *Për parandalim dhe luftim të krimit kibernetik*. Nga aspekti ligjor, ajo që është më e rëndësishme, është nxjerrja e ligjit *Për mbrojtjen e infrastrukturës kritike*.

Referuar sanksionimit ligjor dhe krahasimit me aspektin praktik të veprave penale në fushën e krimit kibernetik në Kosovë, veprat më të shpeshta penale që ndërlidhen me sulmet kibernetike aktuale, janë:

- kërcënime dhe shantazhe përmes *email*-it (përfshirë edhe ndaj personaliteteve të rëndësishme publike dhe institucioneve);
- lajm i rrejshëm (përmes *email*-it të falsifikuar);
- publikim i paautorizuar;
- cenim i të drejtave të autorit (në *YouTube*);
- hyrje e paautorizuar në sistem kompjuterik (sulme DDoS, vjedhje e fjalëkalimeve, sulme në ueb-faqe qeveritare, të institucioneve të ndryshme publike, kompani biznesi etj.);
- blerja *online* me karta të vjedhura - vjedhje e identitetit;
- blerja me karta të vjedhura (klonimi i kartave);
- vjedhja e të dhënave të kartave bankare dhe të kreditit si dhe vjedhja e parave nga bankomatët (vendosja e SKIMMING pajisjeve dhe pajisjeve tjera të modifikuara);
- mashtrim përmes falsifikimit të *email*-ëve (modifikim i faturave dhe ndryshim i xhirollogarive bankare);
- mashtrime në internet përmes ofrimit të shërbimeve të ndryshme;
- keqpërdorimi i fëmijëve përmes internetit (pornografia e fëmijëve në internet)[11].

## 5. Strategjia kosovare për sigurinë kibernetike

Duke u nisur nga prirjet e zhvillimit në fushën e kibernetikës, pasur parasysh se

[10] Ligji Nr. 03/L-166 për parandalim dhe luftim të krimit kibernetik, 2010.
[11] Raporti i Vlerësimit të kërcënimeve nga Krimi i Organizuar dhe Krimet e Rënda "SOCTA" 2016.

qytetarët e rëndomtë të Kosovës kanë qenë viktima të sulmeve kibernetike, duke vlerësuar rrezikun dhe nevojën e mbrojtjes dhe sigurisë në fushën e kibernetikës, Kosova në dhjetor të vitit 2015 ka hartuar për herë të parë strategjinë e sigurisë kibernetike dhe planin e veprimit 2016-2019. Kosova, krahasuar me vendet e rajonit, është e para, e cila ka arritur ta hartojë një strategji të tillë. Qeveria e Republikës së Kosovës, në kuadër të përpjekjeve të saj për qasje strategjike në këtë fushë, në kuadër të programit e qeverisë, 2015-2018, ka paraparë hartimin e *Strategjisë shtetërore për sigurinë kibernetike* dhe *Planin e veprimit* 2016-2019, si dhe me vendimin nr. 01/30 të datës 20.5.2015, në kuadër të planifikimit për hartim të dokumenteve strategjike për vitin 2015.

Republika e Kosovës, do të sigurojë një mjedis të sigurt të hapësirës kibernetike, duke minimizuar dhe parandaluar kërcënimet kibernetike në bashkëpunim me partnerët vendorë dhe ndërkombëtarë[12].

Strategjia shtetërore për sigurinë kibernetike, është hartuar me pjesëmarrjen e shumicës së aktorëve kryesorë, të cilët kanë detyra dhe përgjegjësi në këtë fushë. Kjo strategji përmban pesë objektiva kryesore: 1. mbrojtja e infrastrukturës kritike të informacionit; 2. zhvillimi institucional dhe ngritja e kapaciteteve; 3. ndërtimi i partneriteteve publiko-private; 4. reagimi ndaj incidenteve; 5. bashkëpunimi ndërkombëtar.

Në kuadër të analizave të strategjisë, respektivisht metodologjisë së hartimit, është bërë edhe përshkrimi i sfidave, rreziqeve, kërcënimeve ndaj sigurisë, në hapësirën kibernetike në Kosovë, adresimi i krimit kibernetik dhe baraspeshimi i sigurisë dhe i privatësisë.

Cikli jetësor i kësaj strategjie, sikundër edhe e gjithë strategjia, është përpiluar duke marrë për bazë rekomandimet e ENISA-s, për hartimin e strategjive. Në bazë të rekomandimeve kyçe të organeve ndërkombëtare (NATO, ENISA), *Strategjia shtetërore e sigurisë kibernetike* është hartuar brenda një cikli jetësor, i cili përfshinë fazat vijuese: zhvillimi, zbatimi, vlerësimi dhe përshtatja e strategjisë.

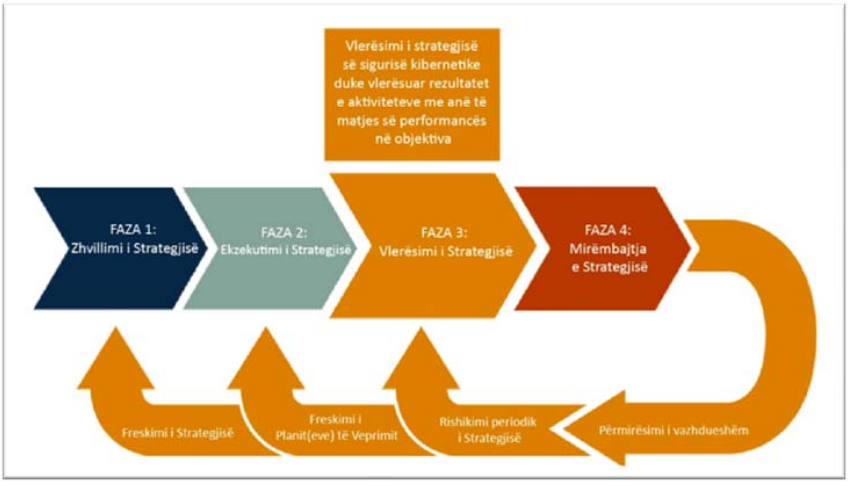



**Figura 3: Cikli jetësor i sigurisë kibernetike (Burimi: ENISA, 2012)**

Qëllimi i strategjisë është krijimi i mekanizmave për mbrojtje, zbulim, reagim dhe

[12] Strategjia Shtetërore e Sigurisë Kibernetike dhe Plani i Veprimit të Kosovës, 2016-2019.

rikuperim, mbrojtja e infrastrukturës kritike të informacionit (CIIP), alarmimi apo paralajmërimin, themelimin e ekipeve reagues ndaj incidenteve të sigurisë kompjuterike (CSIRT), ekipet reaguese ndaj emergjencave kompjuterike (CERT).

Në kuadër të strategjisë është vlerësuar, analizuar korniza ligjore duke u dhënë rekomandimet konkrete si dhe është krijuar mekanizmi institucional për zbatim të objektivave dhe aktiviteteve.

Kjo strategji është në përputhje me aktet ndërkombëtare që rregullojnë fushën e sigurisë kibernetike, strategjinë e sigurisë kibernetike të bashkimit evropian "Hapësirë e hapur, e sigurt dhe e mbrojtur kibernetike (2013)"; Udhëzuesin e ENISA-s për "Strategjitë shtetërore të sigurisë kibernetike" (2012) dhe strategjitë e sigurisë kibernetike të vendeve të tjera të BE-së[13].

Lidhur me ndërtimin e partneritetit publiko-privat, në veçanti, janë përcaktuar procedurat për shkëmbimin e informatave mes: ofruesit e shërbimit të internetit; sektorit bankar; sektorit energjetik; sektorit të ujësjellësit; transportit (ajror dhe tokësor) dhe fushës akademike.

Themelimi, listimi dhe akreditimi i CERT /CSIRT[14] në *Trusted Indroduced* dhe *First*[15] është një hap gjithashtu i rëndësishëm në krijimin e mekanizimit institucional, në fushën e sigurisë kibernetike. Kosova tani veç sa ka themeluar disa CERT/CSIRT dhe ka arritur t'i regjistrojë në këtë listë. E veçanta e kësaj strategjie është themelimi i "Këshillit shtetëror për sigurinë shtetërore", i cili ka për qëllim të ofrojë qasje ndaj masave të sigurisë në "hapësirën kibernetike" përmes bashkëpunimit ndërmjet palëve të ndryshme të përfshira, në kuadër të një reagimi të koordinuar ndaj kërcënimeve të ndryshme.

Këshilli për sigurinë shtetërore, përbëhet nga përfaqësuesit e institucioneve vijuese: Ministria e Brendshme, Policia e Kosovës, Ministria e Forcës së Sigurisë së Kosovës, Agjencia Kosovare e Inteligjencës, Agjencia e Shoqërisë së Informacionit, Këshilli i Sigurisë së Kosovës, Ministria e Drejtësisë, Ministria e Ekonomisë dhe e Financave, Ministria e Arsimit, e Shkencës dhe e Teknologjisë, Ministria e Punëve të Jashtme, Autoriteti Rregullator për Komunikimet Elektronike dhe Postare, Banka Qendrore e Kosovës. Në raste të veçanta, do të përfshihen edhe ministri e agjenci të tjera. Përfaqësuesit e bizneseve do të ftohen si anëtarë të lidhur. Përfaqësues akademikë, do të angazhohen gjithashtu, në nivel teknik. Këshilli shtetëror për sigurinë kibernetike synon të bashkërendojë mjetet parandaluese dhe qasjet ndërdisiplinore të sigurisë kibernetike në sektorin publik dhe atë privat[16].

Me këtë strategji është përcaktuar edhe sfera e hulumtimit dhe zhvillimit si një sferë e rëndësishme. Republika e Kosovës do të vazhdojë të zhvillojë kapacitetet për hulumtim e zhvillim brenda Kosovës, përfshirë edhe pjesëmarrjen në projekte shtetërore e ndërkombëtare si qëllim final përmirësimin e reagimit të Kosovës ndaj kërcënimeve të sigurisë kibernetike. Ndërtimi i partneritetit publiko-privat, zë vend të rëndësishëm në kuadër te strategjisë dhe përcakton procedurat për këmbimin e informatave me: ofruesit e shërbimit të internetit; sektorin bankar; sektorin e energjisë; furnizimit me ujë; transportin (ajror e tokësor) dhe botën akademike.

[13] Strategjia shtetërore e sigurisë kibernetike dhe plani i veprimit të Kosovës, 2016-2019.
[14] CERT nënkupton - Ekipin Reagues për Emergjenca Kompjuterike;
CSIRT nënkupton - Ekipin Reagues për Incidentet e Sigurisë Kompjuterike;
[15] Lista e CERT-ve/CSIRT-ve në Trusted Introducer - https://ww.trusted-introducer.org/directory/country_LICSA.html, lista e anëtarëve të FIRST-it - https://www.first.org/members/teams
[16] Strategjia shtetërore e sigurisë kibernetike dhe plani i veprimit të Kosovës, 2016-2019.

Në kuadër të pjesës së reagimit, është paraparë themelimi i "Qendrës shtetërore për siguri kibernetike" e cila furnizon me informacione drejtpërdrejt *Këshillin shtetëror për siguri kibernetike*, të udhëhequr nga koordinatori përgjegjës për siguri kibernetike.

Kosova do ta formulojë politikën e jashtme kibernetike, në atë mënyrë që interesat dhe idetë shtetërore për sigurinë kibernetike, të koordinohen dhe të ndiqen në organizata ndërkombëtare, si, ENISA, OSBE, Këshilli i Evropës, OECD dhe NATO. Qasja përditë e më shumëpalëshe duhet përafruar me domosdoshmërinë e vlerësimit dhe fuqisë vendimmarrëse sovrane. Në këtë kontekst, duhet vendosur një kod për veprimin shtetëror në hapësirën kibernetike (kodi kibernetik), i cili duhet nënshkruar nga sa më shumë shtete që të jetë e mundur, që ai të përfshijë masa sigurie për ndërtimin e besimit. Kosova do të ofrojë kontributin më të madh në aktivitetet anti-*botnet* në gjithë botën. Kosova aspiron të bëhet anëtare e NATO-s në të ardhmen e afërt. NATO-ja shërben si bazë e sigurisë transatlantike. Kështu, NATO-ja duhet të marrë parasysh sigurinë kibernetike në të gjithë spektrin e përgjegjësive të saj[17].

## 6. Përmbledhje

Shoqëria moderne sot ballafaqohet në njërën anë me të arriturat më të mëdha të zhvillimit tekniknologjik, i cili zhvillim ka mundësuar progres në aspektin e zhvillimit ekonomik dhe shoqërorë në përgjithësi ndërsa në anën tjetër mundëson keqpërdorim të këtyre të arriturave teknologjike, duke krijuar një numër problemesh dhe rreziqesh, si për individët dhe grupet poashtu edhe për shoqërinë në përgjithësi dhe sigurinë nacionale ne veçanti.

Me këtë përdorim të madh të Internetit, si platformë kryesore e punës, shkencës e komunikimit social, siguria dhe privatësia e tij kthehen në brenga kryesore edhe për ne.

Duke iu referuar *"Analizës së rishikimit strategjik të sektorit të sigurisë në Republikën e Kosovës"*[18], krimi kibernetik si krim jokonvencional është identifikuar si një prej rreziqeve, sfidave apo kërcënimeve globale që mund të cenojnë edhe sigurinë e Kosovës.

Kosova nuk është imune ndaj Kriminalitetit kibernetik. Autoritetet dhe qytetarët e rëndomtë të Kosovës tashmë kanë qenë viktima të krimeve dhe sulmeve kibernetike, e sigurisht që edhe do të përballen me sulme të tilla në të ardhmen e afërt.

Sipas të dhënave në dispozicion, shënjestra kryesore e sulmeve kompjuterike në Kosovë deri më sot kanë qenë llogaritë dhe domenet në Internet, të cilat gjithashtu kanë qenë raste të krimeve virtuale. Të dyshuarit që merren me këtë formë krimi në Kosovë janë nga Kosova, por edhe shtetas të huaj, sulme nga jashtë por edhe nga Kosova jashtë saj.

Kosova është në proces të integrimeve euro atlantike, anëtarësimi në organizata si BE, NATO, Intepol, EUROPOL kërkon arritjen e standardeve në fushën e sigurisë kibernetike.

Ne duhet të mbrohemi me efikasitet nga Sulmet kibernetike, spiunimi kibernetik dhe sabotazhi kibernetik. Për të arritur këtë, Kosova duhet së pari të hartojë strategjinë kombëtare të sigurisë dhe pastaj, nga ajo, të zhvillohen strategjitë e tjera sektoriale. Siguria kibernetike është e lidhur ngushtë me sigurinë kombëtare, kjo, për faktin se cak i sulmeve kibernetike, mund të jenë shpesh infrastruktura kritike, si: energjia, teknologjitë

[17] strategjia shtetërore e sigurisë kibernetike dhe plani i veprimit të Kosovës, 2016-2019.

[18] Analiza - http://www.kryeministri-ks.net/repository/docs/Analysis_ of_ Strategic_ Security_ Sector_ Review _ of_ RKS_060314. pdf

e informacionit dhe të komunikimit (TIK), uji, ushqimi, shëndetësia, financat, rendi dhe siguria publike e juridike, administrata civile, transporti, industria, infrastruktura kritike e informacionit (telekomunikacioni, kompjuterët/softuerët, interneti ) etj.; cenimi i të cilave, paraqet edhe cenim të sigurisë kombëtare.

Në fushën e sigurisë kibernetike, Republika e Kosovës ka në zbatim një bazë të gjerë ligjore mjaft moderne dhe të konsoliduar. sidoqoftë, edhe në këtë fushë ka nevojë për rishikim të ligjit "Për parandalim dhe luftim të krimit kibernetik", Kodit Penal dhe Kodit të Procedurës Penale, respektivisht harmonizimit të tyre si dhe miratimit të ligjit "Për infrastrukturën kritike". Institucionet publike të Republikës së Kosovës, kanë përcaktuar politika dhe udhëzime, për të siguruar jo vetëm përfshirjen e secilit qytetar, por edhe sigurinë e hapësirës kibernetike në përgjithësi. Për këtë qëllim, është hartuar strategjia kombëtare për sigurinë kibernetike duke u bazuar në vlerësimet dhe analizat e agjencive të zbatimit të ligjit, institucioneve qeveritare dhe organizatave vendore dhe ndërkombëtare.

Në hartimin e kësaj strategjie, janë marrë parasysh udhëzimet e ENISA-s për hartimin të strategjive (*European Network and Information Security Agency*). Me qëllim të rritjes së efikasitetit dhe efektivitetit sot mbetet angazhim me përkushtim i institucioneve publike dhe sektorit privat në zbatimin e kësaj strategjie dhe plani të veprimit.

## Bibliografi


1. Strategjia Shtetërore e Sigurisë Kibernetike dhe Plani I Veprimit të Kosovës, 2016-2019.
2. Raporti i Vlerësimit të kërcënimeve nga Krimi i Organizuar dhe Krimet e Rënda "SOCTA" 2016.
3. Annual report Telecom security incidents 2017, ENISA, 2018.
4. Exploring the opportunities and limitations of current Threat Intelligence Platforms, ENISA, 2018.
5. Exploring the opportunities and limitations of current Threat Intelligence Platforms ENISA, 2018.
6. Public Private Partnerships (PPP) - Cooperative models, ENISA, 2018.
7. European Cyber Security Month 2017, ENISA, 2018.
8. Cyber Security Culture in organisations, ENISA, 2018.
9. Privacy and data protection in mobile applications, ENISA, 2018.
10. ENISA Threat Landscape Report 2017, ENISA, 2018.
11. The European Cyber Security Challenge: Lessons Learned report, ENISA, 2018.
12. JOIN(2013) 1 final, 7 Feb 2013 - http://eur-lex.europa.eu/legal-content/ EN/TXT/ ?uri=celex: 52013JC0001
13. https://ww.trusted-introducer.org/directory/country_LICSA.html, lista e anëtarëve të FIRST-it - https://www.first.org/members/teams
14. Ligji nr. 03/L-166 "Për parandalim dhe luftim të krimit kibernetik".
15. Ligji nr. 03/L063 "Për Agjencinë Kosovare të Inteligjencës".
16. Ligji nr. 04/L-149 "Për ekzekutimin e sanksioneve penale".
17. Ligji nr. 04/L-065 "Për të drejtën e autorit dhe të drejtat e përafërta".
18. Ligji nr. 03/ L-183 "Për zbatimin e sanksioneve ndërkombëtare".
19. Ligji nr. 04/L-213 "Për ndihmën juridike ndërkombëtare në çështje penale".
20. Ligji nr. 04/L-052 "Për marrëveshjet ndërkombëtare".
21. Ligji nr. 04/L-072 "Për kontrollimin dhe mbikëqyrjen e kufijve shtetërorë".
22. Ligji nr. 04/L-093 "Për bankat, institucionet mikrofinanciare dhe institucionet financiare jobankare".
23. Ligji nr. 04/L-064 "Për Agjencinë Forenzike të Kosovës".
24. Ligji nr. 04/L-198 "Për tregtimin e mallrave strategjikë".
25. Ligji nr. 04/L –004 "Për shërbimet private të sigurisë";
26. Ligji nr. 03/L-046 "Për Forcën e Sigurisë së Kosovës;
27. Kodi nr. 03/L-109 Doganor dhe i Akcizës i Kosovës.
28. Kodi nr. 04/L-082 Penal i Republikës së Kosovës.
29. Kodi nr. 04/L-123 i Procedurës Penale.
30. Ligji nr. 03/L-122 "Për shërbim të Jashtëm të Republikës së Kosovës".
31. Analizë e rishikimit strategjik të sektorit të sigurisë së Republikës së Kosovës, 2014.
32. https://www.internetworldstats.com/stats.htm

# Përdorimi i sistemeve kompjuterike për kryerjen e veprimtarive antiligjore dhe sulmeve kibernetike

**M.P. Sabrina QYPI**
*Policia e Shtetit*
*sabrina.qypi@asp.gov.al*

**Abstrakt**

*Me zhvillimet teknologjike të kohëve moderne, përdorimin e sistemeve kompjuterike, rrjeteve sociale, internetit, aplikacioneve dhe platformave të ndryshme që ofrohen në fushën e teknologjisë së informacionit, janë shfaqur dukshëm mënyra të reja të kryerjes së veprimtarive antiligjore dhe kriminale. Sulmet kibernetike, si një formë e re e ndërhyrjeve nga hakerat në sistemet kompjuterike, rrit në mënyrë eksponenciale rrezikun për të vjedhur të dhëna, informacione, për ti dëmtuar ato, si dhe kryerjen e veprimeve të paligjshme në sistemet bankare e monetare dhe jo vetëm. Mënyrat dhe metodat e ndryshme të këtyre sulmeve janë të vështira për t'u kapur dhe frenuar, pasi kërkohen specialistë të mirë për të ndërtuar një sistem sigurie kibernetik efikas. Fokusi dhe strategjitë e strukturave policore janë të vazhdueshme, në marrjen e masave të përshtatshme për parandalimin, ndërprerjen, zbulimin e veprimtarive kriminale dhe sulmeve kibernetike që zhvillohen. Sulmet kibernetike dhe shfrytëzimi i sistemeve kompjuterike janë shqetësim në mbarë botën, pasi shërbejnë si katalizator të kriminalitetit. Vështirësia qëndron në kohë e madhe, shpeshherë dhe në pamundësinë për të zbuluar, gjetur dhe kapur autorët e këtyre sulmeve. Me digjitalizimin e Shqipërisë , dita ditës po vëmë re boshllëqe në dispozitat ligjore, që nuk i parashikojnë këto forma të reja të kriminalitetit kibernetik. Vlen të përmendet nevoja e domosdoshme e rritjes së kapaciteteve profesional, strukturave të mirë organizuara e të specializuara, bashkëveprimit dhe bashkëpunimit institucional dhe ndërkombëtar si dhe sensibilizimit të popullsisë për rreziqet dhe mënyrat sesi mund të mbrohen nga sulmet kibernetike, për të mos rënë pre e tyre duke sjell minimizimin e pasojave. E ardhmja do mbizotërohet nga këto krime e sulme kibernetike, prandaj përpjekjet e Policisë së Shtetit duhet të orientohen dhe intensifikohen, në këtë drejtim kaq delikat.*

**Fjalëkyçe:**
**sulme kibernetike, sisteme kompjuterike, hakera, teknologji informacioni, siguria kibernetike.**

## 1. Hyrje

Rritja e niveli të sigurisë kibernetike është një domosdoshmëri në ditët e sotme. Numri i përdoruesve të sistemeve kompjuterike dhe platformave digjitale, rrjeteve sociale, celularëve është rritur në mënyrë të konsiderueshëm, vetëm në 2018 numri i përdoruesve të internetit në Shqipëri sipas Autoriteti Shqiptar i Komunikimeve Elektronike dhe Postare (AKEP),është 2.16 milionë përdorues[1]. Në periudhën Tetor-Nëntor 2017 numri i personave që përdornin rrjetin 3G/4G ishte 18.4 % më shumë se tremujori i parë dhe ai i dytë i viti 2017. Interneti i ofruar nga kompanitë ka arritur në 98,000 përdorues, duke u rritur me 23% në vitin 2017, krahasuar me vitin 2016[2]. Ky fluks individësh që përdorin çdo ditë këto teknologji të reja,mund të jenë objektiv potencial i sulmeve kibernetike apo edhe subjekte të veprimtarive antiligjore.

Problemi dhe vështirësia e sulmeve kibernetike, qëndron në faktin që ato mund të fillojnë në shtete të huaja dhe nga persona të ndryshëm duke e bërë të vështirë parandalimin dhe zbulimin e tyre. Interneti, në vetvete është krijuar duke u bazuar në filozofin e një shërbimi të aksesueshëm nga të gjithë pa kufizime dhe pengesa. Për këtë arsye çdokush i ka të gjitha mjete e nevojshme të zhvilloj veprimtari kriminale, pa u shqetësuar për pasojat e tyre. Në Shqipëri nuk ka studime të mirëfillta mbi fenomenin e sulmeve kibernetike, kjo si rrjedhojë e infrastrukturës dhe zhvillimeve teknologjike të ardhura më vonë se shtetet e tjera në botë, por mund të themi me siguri që vitet e fundit situata ka ndryshuar. Një rrezik eminent është mos kontrollimi i adoleshentëve dhe fëmijëve që janë dhe grup-shënjestra më e ndjeshme e shoqërisë. Kompani që ofrojnë

[1] https://www.akep.al/. Parë së fundi, më 10.9.2018.
[2] Po aty.

internet, kompani celulare, biznesi i elektronikës dhe shtrirja e rrjeteve kompjuterike duke përdorur fibra optike, ka sjell një mundësi të shtuar në përdorimin e teknologjisë më të fundit për popullsinë. Rreziku është shumë i madhe, jo vetëm për individët por edhe për pronën, organizatat dhe shoqërinë, në vazhdim do përpiqemi të shpjegojmë sulmet kibernetike sipas disa kategorizimeve, do cekim në vija të përgjithshme problematikat që lidhen më këto sulme, metodat që përdoren për të marrë të dhëna. Do shohim qasjen dhe pozicionin e Policisë së Shtetit në veprimtarin për të parandaluar dhe zbuluar këto sulme kibernetike joligjore.

## 2. Terminologjia në lidhje me sulmet kibernetike referuar legjislacionit shqiptar

Fillimisht duhet kuptuar çfarë quajmë sulm kibernetik edhe pse terminologjia është e re dhe e paplotë, pasi kemi të bëjmë me një fenomen të ri të shfaqur në Shqipëri mbas viteve 2000. Për të sqaruar konceptet lidhur me sistemet kompjuterike, sulmet kibernetike dhe krimet kibernetike, do të shohim përcaktimet e bëra në ligjin nr. 8888, datë 25.4.2002 "Për ratifikimin e 'Konventës për krimin në fushën e kibernetikës'" ku është përcaktuar lidhur me sistem kompjuterik :"*çdolloj pajisje apo grup i ndërlidhur ose pajisje të lidhura, një ose më shumë prej të cilave, vazhduese të një programi kryejnë procesime automatike të të dhënave"*[3]. Ndërsa me krimi kibernetik: *"konsiderohet ndërhyrje e paautorizuar drejt dhe/ose përmes përdorimit të TIK(Teknologjisë së Informacionit dhe Komunikimit), penaliteti për të cilin rregullohet në Kodin Penal të Republikës së Shqipërisë"*[4] Sipas 'Strategjisë për mbrojtjen kibernetike 2018-2020' të Ministrisë së Mbrojtjes, sulm kibernetik: "*do të quajmë një sulm të qëllimshëm në sistemet kompjuterike, si dhe ndërmarrjeve të cilat kanë akses në internet"* dhe krimi kibernetik :*"një krim në të cilin një kompjuter është objekt i krimit (hacking, phishing, spamming) ose përdoret si një mjet për të kryer një vepër penale"*[5].

Në Kodin Penal[6] parashikohen disa nene në lidhje me krimin kibernetik dhe sulmet kibernetike:

a) neni 74/a i Kodit Penal "Shpërndarja kompjuterike e materialeve progjenocidit ose krimeve kundër njerëzimit";

b) neni 84/a i Kodit Penal "Kanosja me motive racizmi dhe ksenofobie nëpërmjet sistemit kompjuterik;

c) neni 119/a i Kodit Penal "Shpërndarja e materialeve raciste ose ksenofobike nëpërmjet sistemit kompjuterik";

d) neni 119/b i Kodit Penal "Fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik";

e) neni 143/b i Kodit Penal "Mashtrimi kompjuterik";

f) neni 186/a i Kodit Penal "Falsifikimi kompjuterik";

g) neni 192/b i Kodit Penal "Hyrja e paautorizuar kompjuterike";

h) neni 293/a i Kodit Penal "Përgjimi i paligjshëm i të dhënave kompjuterike";

[3] Qendra e Publikimeve Zyrtare. Ligj nr. 8888, datë 25.4.2002: "Për ratifikimin e Konventës për krimin në fushën e kibernetikës". *Fletorja Zyrtare e Republikës së Shqipërisë*, nr. 18, maj 2002.
[4] Po aty.
[5] Ministria e Mbrojtjes, RSH. *Strategjia për Mbrojtjen Kibernetike, 2018-2020* .
Versioni elektronik: http://www.mod.gov.al/images/PDF/2017/Strategjia_Mbrojtjen_Kibernetike_2018_2020.
[6] Kodi Penal i Republikës së Shqipërisë.

i) neni 293/b i Kodit Penal "Ndërhyrja në të dhënat kompjuterike";
j) neni 293/c i Kodit Penal "Ndërhyrja në sistemet kompjuterike";
k) neni 293/ç i Kodit Penal "Keqpërdorimi i pajisjeve";
si dhe, për veprat penale që kryhen nëpërmjet sistemeve kompjuterike:
a) neni 108, paragrafi i katërt i Kodit Penal "Vepra të turpshme";
b) neni 117 i Kodit Penal "Pornografia";
c) neni 147 i Kodit Penal "Mashtrimi me veprat e artit e të kulturës";
d) neni 148 i Kodit Penal "Botimi i veprës së tjetrit me emrin e vet";
e) neni 149 i Kodit Penal "Riprodhimi pa të drejtë i veprës së tjetrit";
f) neni 149/a i Kodit Penal "Shkelja e të drejtave të pronësisë industriale";
g) neni 149/b i Kodit Penal "Shkelja e të drejtave të topografisë së qarkut të gjysmëpërçuesit".

Po të shohim nenet e parashikuara në Kodin Penal të Republikës së Shqipërisë në lidhje me veprimtarin antiligjore, që kryhen duke përdorur sistemet kompjuterike vëmë re një mungesë në dispozitat ligjore. Ky vakum ligjor ekziston si rezultat i risive dhe teknologjisë së informacionit dhe fenomeneve të reja të lidhura me këto zhvillime që jo gjithmonë ecin paralelisht me përditësimin e legjislacionit.

## 3. Kategorizim i sulmeve kibernetike

Kemi disa lloj ndarjesh dhe kategorizimesh, në këtë artikull do shqyrtojmë disa prej tyre. Si fillim do përqendrohemi në ndarjen e bërë në bazë të sulmeve ndaj individit, pronës, organizatave dhe shoqërisë. Ndarje tjetër është ajo sipas Brenner[7], i cili i ndanë sulme ndaj kompjuterit/sistemeve kompjuterike, sulme që përdorë kompjuterin si mjetë, sulme në kompjuter/makinë. Sulmi ndaj kompjuterit konsiston në hakimin dhe instalimin e viruseve, sulmet që përdorin kompjuterin si mjetë janë mashtrimet *online*, pornografia me fëmijët, ndërsa sulmet në kompjuter/makinë janë manipulimi, ndërhyrja në të dhënat dhe informacionet për të kryer aktivitet kriminal.

Ndaja me e kuptueshme është ajo e sulmeve kibernetike të ndarë në katër grupe të mëdha:
- sulme ndaj individit,
- sulme ndaj pronës,
- sulme ndaj organizatave ,
- sulme ndaj shoqërisë.

### *3.1 Sulmet ndaj individit*

a) *E-mailspoofing*

Kjo është një metodë e cila përdorë *header*-in e *email*-it dhe e modifikon atë në mënyrë të tillë, që *email* të duket sikur vjen nga një burim i caktuar por në fakt është dërguar nga një person tjetër.

b) *Spamming*

Janë ato *email*-e, që dërgohen në përdorues të ndryshëm dhe përmbajnë në brendësi të tyre viruse të cilat po të klikohen instalohen në platformat kompjuterike në të cilin po përdoret *email*-i. Gjithashtu këto *spam*-e kanë *link*-e me qëllim mbledhjen e informacioneve të përdoruesve të ndryshëm.

c) Shpifjet dhe bullizmi kibernetik

Në këtë rast shpifja bëhet me anë të sistemeve kompjuterike dhe/ose internet apo celularëve, duke publikuar materiale të pavërteta e ofendimeve për dikë në faqe interneti, në rrjete sociale ose dërgon *email* mbi persona që kanë rënë pre e shpifjeve dhe bullizmit kibernetik. Ky fenomen është rritur me hapa galoponte sidomos tek të rinjtë dhe adoleshentët, që përdorin dhe publikojnë në masë informacione të hollësishme të jetës së tyre të përditshme. Kjo mund të sjell ankth, depresion dhe me keq akoma në vetëvrasjen e tyre. Bullizmi kibernetik shfaqet në disa forma si:

1. dërgimi i mesazheve apo kërcënimeve duke përdorur celularët apo *email*-et,
2. përhapja e thashethemeve *online*,
3. postimi i mesazheve në faqe *web*-i ose në rrjete sociale,
4. vjedhja e profileve personale për të marrë informacione private dhe dërgimi i mesazheve dëmtuese personave të tjerë,
5. të hequrit si një person tjetër *online* për të dëmtuar persona të tjerë,
6. marrja e fotografive të një personi dhe shpërndarja e tyre në internet,
7. *seksting* ose shpërndarja e mesazheve apo fotografive provokuese të një personi.

Së fundmi, Ministria e Arsimit dhe Këshillit të Evropës, ka zhvilluar një anketim në 144 shkolla të vendit. Në përfundim të analizimit të këtyre anketimeve , në Shqipëri bullizmi shfaqet më shumë në shkollat urbane sesa ato rurale dhe viktima të bullizmit janë vajzat në numër më të madhe sesa djemtë, këta të fundit janë gjithmonë agresorët[8]. Evidentohet bullizmi virtual ose kibernetik, pra tallja në rrjete sociale, si një metodë e re e përdorur nga të rinjtë. Sipas "Qendrës së Kërkimit mbi Bullizmin Kibernetik" në Shtetet e Bashkuara të Amerikës rreth 36.7 % e femrave raportojnë që kanë qenë viktima të bullizmit kibernetike në një periudhë të jetës së tyre, krahasuar me 30.5 % të djemve[9].

*d) Ngacmimet dhe përndjekja kibernetike.*

Ngacmimi dhe përndjekja janë veprimet që kontrollojnë çdo aktivitet, një individ kryen në rrjetet sociale apo në internet. Në legjislacionet e huaja përndjekja dhe ngacmimet kibernetik janë të përcaktuar në mënyrë të qartë si krime ndaj personit, ndërsa në legjislacionin Shqiptar vihet re një mungesë e në mirë përcaktimin e dispozitave të tilla. Në librin"Për pak e ikur" [*Almost Gone*] e autores Mackenzie Baldwin[10], tregohet historia personale e saj sesi ra pre e një njohje të realizuar *online* në rrjetet sociale. Gjatë një viti ajo ndërroi besimin e saj fetar dhe ishte gati të shkonte në Kosovë, pasi djali me të cilin ajo fliste, ishte nga Kosova. Në libër shpjegohet sesi Mackenize përjetoj një histori sa romantike në pamje të parë, aq dhe të tmerrshme nga dikush i panjohur që kishte arritur ta manipulonte në atë mënyrë, sa ajo kishte ndryshuar fenë dhe donte të largohej nga SHBA-ja për të jetuar në Kosovë. Mackenize ishte vetëm 17 vjeç kur kjo histori ndodhi.

### *3.2 Sulmet ndaj pronës*

*a) Vjedhja e identitetit/të dhënave*

[7] Brenner, Susan. *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara, California: ABC-CLIO, 2010.
[8] Dragoti, Edmond, Emanuela Ismaili. *Raport studimor: Studim kombëtar mbi bullizmin dhe ekstremizmin e dhunshëm në sistemin arsimor shqiptar*. Tiranë: Këshilli i Evropës, 2017.
[9] U. S. Department of Health and Human Services. "Bullying Prevention". *Federal government website*. Washington, D. C.: https://www.stopbullying.gov/. Parë së fundi, më 10.9.2018.
[10] Baldwin, John, Mackenzie Baldwin. *Almost Gone: Twenty-Five Days and One Chance to Save Our Daughter*. New York: Simon and Schuster, 2017.

Sistemet kompjuterike përdoren për të marrë të dhëna apo informacione nga më të larmishmet, si dokumente, foto, numra llogarie bankare, karta krediti duke i ndryshua, shtuar apo modifikuar ato.

*b) Krime ndaj pronës intelektuale dhe të drejtës së autorit*

Në këtë grup përfshihen kopjimi jo i ligjshëm i programeve, sistemeve operative, aplikacioneve, shpërndarja e tyre, shkelja e të drejtave të autorit, vjedhja e bar kodeve, miratimi i mallrave dhe i shërbimeve etj. Kjo formë e sulmit kibernetik shkakton dëme të mëdha financiare e ekonomike, duke shkatërruar mijëra kompani dhe individ të cilët bien pre e tyre.

*c) Vjedhje te kohës se internetit*

Shpesh gjenden programe apo aplikacione të cilat janë ndërtuar për të ndërhyrë në linjat e shërbimit të internetit duke marrë internet falas nga persona që e kanë paguar këtë shërbim. Në shumicën e rasteve ndërhyhet në *wirless* duke gjetur në mënyrë automatike *password*-in nga programet e ideuar për të kapur dhe zbërthyer këto pajisje dhe sinjale. Shumicën e kohës personat që paguajnë për këtë shërbim nuk e dinë, që dikush tjetër i paautorizuar është duke shfrytëzuar internetin e tij.

### *3.3 Sulmet ndaj organizatës*

*a) Aksesi i paautorizuar në kompjuter*

Aksesi i paautorizuar në kompjuter apo në rrjet pa dijenitë personit bëhet në dy mënyra:

1. *Ndryshimi/fshirja e të dhënave*. Në kohët moderne kompjuteri, laptopi, tabletët dhe celularët janë bërë pajisje në të cilat ruhet gjithçka, dokument, video, fotografi, të dhëna konfidenciale, materialet e punës, me pak fjalë e gjithë jeta e individit dhe jo vetëm por të dhëna e informacionet e kompanive më të mëdha, bankave, institucioneve administrative, ushtrisë, policisë e shumë organizatave të ndryshme. Për një moment imagjinoni sikur këto të dhëna, detaje, informacione të shkonin në duart e gabuara, sesa e madhe do të ishte pasoja që këto të dhëna të keqpërdorura mund të sillnin. Do ishte e paimagjinueshme impakti që do kishin. Në eksperiencat e deritanishme një nga aktivitetet më të mëdha në lidhje më të dhënat janë ndryshimi, fshirja apo ekspozimi i tyre. Këto sulme janë të shpeshta dhe shumë të vështira për tu zbuluar.

2. *Spiunazhi kompjuterik*. Spiunazhi kompjuterik lidhet më marrjen dhe zbulimin e të dhënave , informacioneve. Këto informacione merren për qëllime të ndryshme, të cilat mund të jenë për përfitime ekonomike, zbulime të dhënash të rëndësishme, marrje informacionesh sekrete etj. Hyrja në sistemet kompjuterike bëhet në mënyre të paautorizuar dhe të panjohur nga përdoruesit. Hakeri, që kryen spiunazh kompjuterik përpiqet të mos lërë gjurmë se në këto sisteme është bërë ndonjë ndërhyrje e tille. Ky lloj sulmi kryhet dhe nga agjencitë e spiunazhit të shteteve të ndryshme, për këtë arsye dhe mbrojtja e të dhënave sekrete kërkon ekspert të mirë të fushës së krimit kibernetik dhe sulmeve kibernetike.

*b) Mohimi i shërbimit*

Mohimi i shërbimit quhet sulm Dos (*Denial of Service*), ky lloj sulmi shfrytëzon dobësitë e sistemeve operative ose Protokollet Internet si TCP/IP. Me shënjimin dhe

sulmimin e tyre bëhet ndërprerja e shërbimeve që ofrohen; ka raste kur sulmohen disa shërbime në të njëjtën kohë duke paralizuar sistemin. Në mënyrë me të qartë këto sulme nuk lejojnë ofrimin e shërbimeve ose i ndërpresin këto shërbime përdoruesve që i përdorin.

Disa metoda sulmesh që mohojnë shërbimin (Dos) janë:

- sulmet me ping,
- "SYN Flooding",
- "Tear Drop",
- "Smurf",
- "TARGA3",
- "Semirandom".

c) Kontaminimi i kompjuterit/infektimi me virus

Çfarë është një virus? Një virus është një program i ideuar e i programuar për të depërtuar dhe infektuar programet e tjera që ndodhen në kompjuter. Viruset prekin *file*-et ose pjesën e *boot*-it të kompjuterit. Kjo bënë ngadalësimin e sistemeve kompjuterike apo mos funksionimin e tyre.

d) *EmailBombing*

Kjo metodë e sulmeve kibernetike konsiston në dërgimin e një sasie të madhe e-mail-ve personave, organizatave, kompanive apo institucioneve duke bërë kreshimin e tyre pra mos funksionimin si shërbim.

e) Sulmi *Salami*

Këto lloj sulmesh janë shumë të përhapura në sistemin bankar , pasi merren shuma të papërfillshme nga llogaritë e klientëve por duke u grumbulluar këto shuma arrin shifra të mëdha në fund të ditës. Janë sulme të vështira për tu kuptuar si dhe dëmet nuk rikuperohen shumë lehtë.

f) Bombat logjike

Bombat logjike ndodhin atëherë kur kryhet një veprim i caktuar në sistemet kompjuterike , në momentin e ndodhjes kjo bombë logjike aktivizohet dhe bën krash kompjuterit , duke dëmtuar sistemin operativ ose duke lëshuar një virus.

g) *Trojan horse*

Janë programe false, të cilat duken sikur janë programe të autorizuara por në fakt janë programe të dëmshme që infektojnë sistemin operativ duke mos lejuar përdoruesin apo serverin për të kryer funksionin e tij.

### *3.4 Sulme ndaj shoqërisë*

a) Falsifikimi

Objektiv i falsifikimit qëndron në ndryshimin e informacionit ose të dhënave në sistemet kompjuterike. Kompjuteri ose celulari mund të përdoren për të kryer aktivitet kriminal të falsifikimit. Kohët e fundit me zhvillimin e printer 3 D apo fotokopjeve e skaner të teknologjisë së fundit, është lehtësuar falsifikimi i dokumenteve. Duke sjell prodhimin e tyre me një cilësi të lartë dhe aq të vërteta saqë është e pamundur dallimi

midis dokumentit të falsifikuar nga ai origjinal, pa ndihmën e ekspertit.

b) Terrorizmi kibernetik

Kjo është një çështje shumë sensitive, në këto momente të shoqërisë botërore përdorimi i sistemeve kompjuterike dhe internetit janë instrumentet më të përdorur për të kryer terrorizëm kibernetik. Terrorizmi është një aktivitet kriminal i cili ka si qëllim përhapjen e panikut, frikës në popullatë, mund të jetë i motivuar nga ide politike, etnik ose nga kazuse të ndryshme. Elementi kryesor i terrorizmit kibernetik është mediumi që përdoret në këtë rast mund të jenë rrjetet sociale, *blog*-et e ndryshme, videot, interneti etj. Këto forma komunikimi përdoren nga persona për të propaganduar, rekrutuar, persona e individ nga e gjithë bota. Sulme terroriste mund të jenë edhe ato sulme që dëmtojnë serverët qendrorë të institucioneve qeveritare, apo institucioneve bankare e financiare. Impakti i këtyre ngjarjeve mund të jetë shumë i madhe duke menduar që digjitalizimi dhe ofrimi i shërbimeve si telefonike apo edhe ekonomike në botë është bërë mënyra e vetëm e komunikimit.

c) *Web Jacking*

Web Jacking është kontrolli që fitohet nga ndërhyrja e hakerat mbi faqet e internetit duke shfrytëzuar dobësitë e tyre. Këto faqe përdoren për të dhënë mesazhe me përmbajtje politike, terroriste apo për përfitime ekonomike, ndryshojnë informacionin dhe të dhënat, me qëllim dezinformomini e publikut. Shembuj të sulmeve të *webjacking* ka pafund, shumë faqe zyrtare të qeverive të shteteve të ndryshme kanë rënë viktimë e tyre.

d)Pedofilia dhe pornografia

Një nga problemet më shqetësuese me internetin dhe me sistemet kompjuterike është aksesi për tu përdorur nga të gjithë për gjithçka. Kufizimet janë të pakta për materialet që hidhen apo shfaqen në site të ndryshme. Fëmijët dhe adoleshentët janë kategoria më e preku nga këto fenomene. Kontrolli dhe monitorimi i tyre është shumë i vështirë pasi shumicën e kohës prindërit nuk kanë dijeni rreth aktivitetit që fëmijët e tyre kryejnë. Mos menaxhimi i tyre por edhe dhënia e celularëve dhe pajisjeve me teknologjinë që në moshat e vogla e bënë të vështirë parandalimin e këtyre krimeve. Problemet psikologjike por edhe mashtrimet që mund të ndodhin në rrjetet sociale duhet të rrisin ndërgjegjen e prindërve por më kryesorja të fëmijëve. Sensibilizimi i tyre për të mos rënë pre apo viktimë e pedofilisë apo materialeve pornografike. Fushat si mos lejimi i celularëve nëpër shkolla, instalimi i programeve mbrojtëse në sistemet e ndryshme teknologjike, vendosja e *proxy* për disa faqe interneti për të ndaluar aksesimin në to, të gjitha këto metoda do të ulnin ndjeshëm numrin e viktimave të prekur nga këto veprimtari antiligjore.

## 4. Policia shqiptare përballë sulmeve kibernetike dhe veprimtarive antiligjore

Policia Shqiptare, gjatë viteve të fundit është përballur me një rritje të vazhdueshme të veprave penale që përfshihen në krimet kibernetike. Në disa raste legjislacioni nuk ja ka lehtësuar punën policisë, pasi fenomenet e reja të sulmeve kibernetike por edhe keqpërdorimi i sistemeve kompjuterike nuk ka qenë plotësisht i parashikuar në dispozitat

ligjore. Siguria personale, ajo e organizatave dhe siguria e institucioneve shtetërore është përgjegjësi e Policisë së Shtetit, e për këtë arsye zbulimi e parandalimi i sulmeve kibernetike duhet të jetë në fokusin e saj të vazhdueshëm. Po të marrim parasysh disa koncepte thelbësore, krimi kibernetik dhe përdorimi i sistemeve kompjuterik për veprimtari antiligjore mund të parandalohet dhe të zbulohet shumë më lehtë. Më poshtë po përmendim disa prej tyre:

- Teknologjia e informacionit është e tashmja por më shumë e ardhmja dhe për këtë arsye stafi policor duhet të trajnohet më shumë mbi teknologjinë e sulmet kibernetike.
- Teknologjia dhe pajisjet e përdorura nga Policia e Shtetit duhet të jenë të gjeneratës së fundit, për të zbuluar krimet kibernetike dhe parandaluar sulmet kibernetike.
- Bashkëpunimi me institucionet e tjera dhe me kompanitë që ofrojnë shërbimet e internetit apo kompanitë celulare duhet të jetë më konkret , më efikas dhe në kohë reale. Kjo për arsye të dinamikës së shpejtë që këto sulme kibernetike zhvillohen.
- Komunikimi me publikun, për të sensibilizuar çdo person, për dëmet që mund të shkaktojnë sulmet kibernetike dhe keqpërdorimi i sistemeve kompjuterike. Në një botë që sa vjen dhe bëhet më e kompjuterizuar e më inovatore,fushatat mbi ndërgjegjësimi e personave, organizatave, bizneseve janë shumë të nevojshme, për të bërë prezent rreziqet që i kanosen çdokujt.
- Hetimi i krimeve kompjuterike në mënyre profesionale duke shfrytëzuar praktikat më të mira botërore.

Përpjekjet e vazhdueshme të policisë dhe angazhimi i saj në zgjidhjen e këtyre dukurive moderne që lidhen me sistemet kibernetik dhe me kriminalitetin e zhvilluar nëpërmjet tyre , është e konsiderueshme. Por duhet të theksojmë që sfidat e Policisë së Shtetit janë të mëdha në të ardhmen duke analizuar rritjen e përdorimit të teknologjisë së informacionit nga të gjithë.

## 4. Përfundime

Për një mbrojtje efikase duhen kuptuar shkaqet nga se vijnë këto sulme kibernetike , cilat sisteme kompjuterike përdoren më së shumti. Qëllimi dhe motivi i personave që merren me veprimtari antiligjore, metodat që ata përdorin. Mbas analizimit të gjithë faktorëve dhe pasojave që vijnë nga këto sulme, do të jemi më të përgatitur për të ndërhyre në mënyre më të shpejt dhe efikase në parandalim dhe në zbulimin e autorëve. Hakerat kanë një shumëllojshmëri mënyrash për të goditur, ndërhyre në mënyrë të paautorizuar apo vjedhur të dhëna të klasifikuara, informacione të rëndësishme. Gjithashtu persona të thjeshtë mund të zhvillojnë veprime kriminale duke përdorur teknologjinë që kanë në dispozicion. Është detyra e të gjithëve të bëjmë maksimumin për të zbutur pasojat që vijnë nga këto sulme e krime kibernetik.

Masat për të parandaluar këto kërcënime varjojnë, por bazat e sigurisë janë të njëjtat; çdo person, organizatë apo institucion, duhet të dijë:

- të mbajë sistemin, bazën e të dhënave (*database*-in) dhe antivirusin të përditësuar;
- të trajnojë punonjësit për sigurinë që duhet dhe masat që duhen marrë;
- të konfigurojnë *firewall*-et që të identifikojnë portat dhe *host*-et specifike, që të mund të aksesojnë të dhënat apo informacionet;
- të krijojnë *password* të fortë dhe me karaktere të ndryshëm, si dhe ta ndryshojnë shpesh;
- të bëjnë *backup*-e, në mënyre të rregullt dhe shpeshherë;

- të kontrollojnë sistemin në mënyrë të përhershme, për aktivitete të dyshimta nga përdorues të ndryshëm.

Një vëmendje e veçantë duhet treguar ndaj fëmijëve dhe adoleshentëve, një praktikë e mirë do të ishte sensibilizimi nëpër shkolla me raste të ndodhura e shembuj konkretë. Në këtë mënyrë do të përfitonim ndërgjegjësimin e tyre mbi rreziqet e përdorimit të teknologjisë. Prindërit, nga ana tjetër, duhet gjithashtu, të informohen mbi veprimtarinë kriminale që zhvillohet nga persona të ndryshëm, për të qenë më vigjilent ndaj fëmijëve të tyre. Sulmet kibernetike prekin të gjithë, pa dallim, çdokush mund të bie viktimë e tyre dhe kostot, si ekonomike edhe personale e psikologjike, janë shumë të mëdha. Policia e Shtetit e ka detyrë kryesore mbrojtjen e çdo shtetasi shqiptar nga veprimtaritë joligjore. E ardhmja e kriminalitetit do të zhvendoset gjithmonë e më shumë drejt sistemeve kompjuterike, si mjeti më i mirë për të fshehur implikimin direkt të autorëve. Përfitimet dhe mundësitë që të ofron teknologjia e informacionit janë të shumëllojshme, por nga ana tjetër kostoja është shumë e madhe, në qoftë se kjo teknologji përdoret nga njerëzit e gabuar. E për këtë arsye, fokusi kryesor duhet të përqendrohet në krijimin e kapaciteteve të mirëfillta, në trajnimet e vazhdueshme, në rekrutimin e personelit të specializuar në këto fusha, për ta bërë sa më efikas parandalimin dhe zbulimin e krimit kibernetik. Bashkëpunimi me institucionet e tjera shtetërore, dhe jo vetëm, por me organizatat e ndryshme, si dhe me biznesin e kompanitë që ofrojnë shërbime të teknologjisë së informacionit duhet forcuar, pasi vetëm në këtë mënyrë Policia e Shtetit mund t'ju vijë në ndihmë më së miri shoqërisë dhe qytetarëve.

## Bibliografi


1. Brenner, Susan. *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara, California: ABC-CLIO, 2010.
2. Baldwin, John, Mackenzie Baldwin. *Almost Gone: Twenty-Five Days and One Chance to Save Our Daughter*. New York: Simon and Schuster, 2017.
3. Santos, Omar. *Developing Cybersecurity Programs and Policies*. London: Pearson Education, 2018.
4. Diogenes, Yuri, Erdal Ozkaya. *Cybersecurity – Attackand Defense Strategies*. Birmingham: Packt Publishing, 2018.
5. Dragoti, Edmond, Emanuela Ismaili. *Raport studimor: Studim kombëtar mbi bullizmin dhe ekstremizmin e dhunshëm në sistemin arsimor shqiptar*. Tiranë: Këshilli i Evropës, 2017.
6. Kodi Penal i Republikës së Shqipërisë.
7. Qendra e Publikimeve Zyrtare. Ligj nr. 8888, datë 25.4.2002: "Për ratifikimin e Konventës për krimin në fushën e kibernetikës". *Fletorja Zyrtare e Republikës së Shqipërisë*, nr. 18, maj 2002.
8. Ministria e Mbrojtjes, RSH. *Strategjia për Mbrojtjen Kibernetike, 2018 2020* . Versioni elektronik: http://www.mod.gov.al/images/PDF/2017/Strategjia_Mbrojtjen_Kibernetike_2018_2020.
9. https://www.akep.al/.
10. U. S. Department of Health and Human Services. "Bullying Prevention". *Federal government website*. Washington, D.C. : https://www.stopbullying.gov/.


ACADEMIA E SIGURIMI
AS
1972

*~ Sesioni III ~*

# Aspekte ligjore, ekonomike e psikosociale të krimeve kibernetike

# Legjislacioni material shqiptar, në fushën e krimit kibernetik - përqasja me Konventën e Budapestit: problematikat

■**Magjistrat Elsa MIHA**
*Prokuroria pranë Gjykatës së Rrethit Gjyqësor, Tiranë*
*elsamiha@yahoo.it*

**Abstrakt**

*Gjatë dekadave të fundit, ashtu sikundër kudo në botë edhe në vendin tonë, teknologjia ka përparuar në përmasa të jashtëzakonshme. Paralelisht me të mirat që sjell ky zhvillim teknologjik në fusha të ndryshme të jetës, është zhvilluar edhe aktiviteti kriminal që kryhet nëpërmjet dhe kundër teknologjisë. Këto tregues të kriminalitetit kibernetik, e ndërgjegjësuan legjislatorin shqiptar për nevojën e parashikimit të këtyre veprimeve shoqërisht të rrezikshme, si vepra penale në kodin tonë penal. Në këtë punim do të trajtohet legjislacioni penal material në fushën e krimit kibernetik në Shqipëri, përputhshmëria e tij me parashikimet e Konventës së Budapestit dhe disa problematika dhe mangësi që ka diktuar praktika në këtë drejtim. Do të analizohen gjithashtu, disa nocione bazë lidhur me elementë teknikë ose jo, që gjenden pothuaj në të gjitha dispozitat kompjuterike dhe për të cilat u vlerësua të jenë të rëndësishme për kuptueshmërinë e drejtë të tyre. Një analizë e hollësishme do të kryhet në këtë punim për dy kategori të krimit kompjuterik dhe konkretisht: për krimet e lidhura me kompjuterët [1] dhe ato të lidhura me përmbajtjen [2], referuar parashikimeve të Konventës së Budapestit dhe legjislacionit të brendshëm. Në përfundim të punimit, do të paraqiten në trajtë konkluzionesh apo sugjerimesh, nevoja e përmirësimit dhe plotësimit të legjislacionit të brendshëm në fushën e krimit kibernetik, si dhe nevoja e trajnimit të vazhdueshëm të strukturave ligjzbatuese, për shkak të natyrës dinamike të këtij lloj krimi.*

**Fjalëkyçe:**
**legjislacioni material shqiptar, krimi kibernetik, mashtrimi kompjuterik, Konventa për Krimin Kibernetik, dispozita kompjuterike.**

## 1. Legjislacioni penal material shqiptar lidhur me krimin kompjuterik, parë nga një këndvështrim krahasues me dispozitat e Konventës së Budapestit

Ndërsa në Europë iniciativat legjislative në drejtim të krimit kibernetik, kanë nisur në vitet 1970[3], në vendin tonë këto iniciativa janë ndërmarrë relativisht vonë. Dispozitat e para penale në fushën e teknologjisë, në Kodin Penal të Republikës së Shqipërisë, janë parashikuar më datë 24.1.2001 me ligjin nr. 8733, "*Për disa shtesa dhe ndryshime në Ligjin Nr. 7895, datë 27.1.1995 Kodi Penal i Republikës së Shqipërisë*", me të cilin u parashikuan si vepra penale: *"Ndërhyrja në transmetimet kompjuterike"*[4], parashikuar nga neni 192/b, si dhe, *"Përdorimi i paligjshëm i teknologjisë së lartë"*[5], parashikuar nga neni 286/a i Kodit Penal. Është e qartë se këto dy parashikime ligjore nuk i përgjigjeshin nevojës gjithnjë e në rritje për mbrojtje nga veprimtaria e paligjshme kibernetike, ndaj

[1] Mashtrimi kompjuterik, (neni 143/b K.P) dhe "Falsifikimi Kompjuterik" (neni 186/a i K. Penal).
[2] Pornografia me fëmijë (neni 9 i Konventës)dhe Pornografia (neni 117 K.P.)
[3] Iniciativa e parë në lidhje me krimin kompjuterik në Europë, ishte Konferenca e Këshillit të Europës, "Mbi aspektet kriminalistike të krimit ekonomik", në Strasburg, në vitin 1976. Në këtë konferencë u prezantuan për herë të parë disa kategori të krimit kompjuterik si dhe u përkufizua krimi kompjuterik si çdo akt i paligjshëm në të cilin kompjuteri është një mjet apo objekt i krimit.
[4] Ndërhyrja në transmetimet kompjuterike sanksiononte ndërhyrjen në çdo formë, në transmetimet dhe programet kompjuterike, ku si rrethanë cilësuese e dispozitës paraqitej ardhja e pasojave të rënda. Me ligjin nr. 9686, datë 26.2.2007 është ndryshuar paragrafi i parë i dispozitës duke u hequr fjalët përbën kundërvajtje penale dhe me ligjin nr. 10023, dt. 27.11.2008 është ndryshuar tërësisht, madje edhe në titullin e saj (hyrje e paautorizuar kompjuterike) për të qenë në harmoni me parashikimet e Konventës së Budapestit.
[5] Dispozita e "Përdorimit të paligjshëm të teknologjisë së lartë" e kufizonte paligjshmërinë e përdorimit të teknologjisë vetëm për veprat penale të parashikuara nga nenet 283 deri në nenin286/a të K. Penal si dhe për të mundësuar ose lehtësuar konsumimin e lëndëve narkotike dhe psikotrope ose për të transmetuare përhapur njoftime për përdorimin, trafikimin, prodhimin apo tregtimin e lëndëve narkotike.

një vit më vonë, me ligjin nr. 8888, datë 25.4.2002, vendi ynë do të ratifikonte Konventën e Budapestit për Krimin Kibernetik, duke marrë kështu përsipër, detyrimin për ta bërë atë, pjesë të legjislacionit të brendshëm.

Konventa mbi Krimin Kibernetike e Këshillit të Europës (Konventa e Budapestit)[6] është aktualisht instrumenti më i rëndësishëm evropian, sa i përket normimit të veprimtarisë kriminale në fushën e krimit kibernetik. Kjo konventë, e cila u konsiderua si një arritje historike në luftën kundër krimit kibernetik u hap për nënshkrim në një konferencë në Budapest, më 23 nëntor 2001 dhe hyri në fuqi si e tillë, me 1 korrik 2004. Po kështu, me ligjin nr. 9262 datë 29.7.2004, vendi ynë ratifikoi edhe Protokollin shtesë të Konventës për Krimin Kibernetik, "*Për penalizimin e akteve me natyrë raciste dhe ksenofobe të kryera nëpërmjet sistemeve kompjuterike*".

Ndërkohë që, konventa, është ratifikuar në vitin 2002 dhe ka hyrë në fuqi në vitin 2004, implementimi i saj në Kodin Penal të Republikës së Shqipërisë, është bërë vetëm 4 vjet me vonë, me ligjin nr. 10023, datë 27.11.2008[7]. Në të njëjtën kohë u reflektuan në legjislacionin e brendshëm edhe parashikimet e Protokollit shtesë të Konventës, "Për penalizimin e akteve me natyrë raciste dhe ksenofobe të kryera nëpërmjet sistemeve kompjuterike"[8]. Parashikimi i veprave penale kompjuterike në legjislacionin tonë të brendshëm, është rrjedhojë e detyrimit që ka ardhur për legjislatorin shqiptar, për shkak të ratifikimit të Konventës së Budapestit dhe formulimi i dispozitave është pothuajse identik me dispozitat e konventës, me disa përjashtime, të cilat do të trajtohen në vijim të këtij punimi.

Është për t'u evidentuar fakti, që Konventa, në nenin 42 të saj, parashikon të drejtën e shteteve ratifikuese, për të paraqitur rezervat e tyre ligjore ndaj dispozitave të caktuara të saj[9]. Dispozitat ndaj të cilave mund të paraqitet rezervë, janë të përcaktuara shprehimisht, në mënyrë shteruese në konventë, duke mos lejuar paraqitjen e ndonjë rezerve tjetër shtesë nga shtetet palë. Këto të fundit, nëpërmjet një procedure të caktuar, kanë të drejtën të tërhiqen më pas nga rezerva e paraqitur[10]. Po kështu, në përmbajtje të dispozitave të veçanta konventalë në diskrecionin e shteteve palë, të parashikojnë ose jo, elementë të caktuar të dispozitës në fjalë të cilat i referohen sipas rastit anës objektive apo subjektive të veprës, apo edhe të rrisin standardin e vendosur prej saj duke shtuar elementë kryesisht të karakterit subjektiv[11].

### *1.1 Rezervat ligjore që ka paraqitur vendi ynë lidhur me Konventën e Budapestit*

Në mbështetje të nenit 42 të konventës, Republika e Shqipërisë ka rezervuar të

[6] Konventa e Budapestit është nënshkruar dhe ratifikuar edhe nga shtete që nuk janë anëtare të Këshillit të Europës, sikundër janë Australia, Shtetet e Bashkuara të Amerikës apo Japonia.

[7] "Mashtrimi kompjuterik" (neni 143/b), "Falsifikimi kompjuterik" (neni 186/a), "Hyrja e paautorizuar kompjuterike" (neni 192/b), "Përgjimi i paligjshëm i të dhënave kompjuterike" (neni 293/a), "Ndërhyrja në të dhënat kompjuterike" (neni 293/b), "Ndërhyrja në sistemet kompjuterike" (neni 293/c), "Keqpërdorimi i pajisjeve" (neni 293/ç).

[8] Shpërndarja kompjuterike e materialeve pro gjenocidit ose krimeve kundër njerëzimit (neni 74/a K.P); Kanosja me motive racizmi dhe ksenofobie nëpërmjet sistemit kompjuterik (neni 84/a K.P); Shpërndarja e materialeve raciste ose ksenofobie nëpërmjet sistemit kompjuterik (neni 119/a K.P);Fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik (neni 119/b K.P).

[9] Nëpërmjet një njoftimi me shkrim drejtuar Sekretarit të Përgjithshëm të Këshillit të Europës, çdo Shtet, në momentin e nënshkrimit ose të depozitimit të instrumentit të ratifikimit, pranimit, aprovimit ose anëtarësimit mund të deklarojë se i lejon vetes rezervën (at) e parashikuara në nenin 4 paragrafi 2, neni 6 paragrafi 3, neni 9 paragrafi 4, neni 10 paragrafi 3, neni 11 paragrafi 3, neni 14 paragrafi 3, neni 22 paragrafi 2, neni 29 paragrafi4 dhe neni 41 paragrafi 1. Nuk mund të bëhet asnjë rezervë tjetër.

[10] Neni 43 i Konventës së Budapestit.

[11] Në mënyrë të detajuar do të flitet në pjesën kur të analizohen dispozitat e veçanta materiale të krimit kibernetik.

drejtën për të mos parashikuar përgjegjësi penale, në rrethana të kufizuara, sipas paragrafëve 1 dhe 2, të nenit 10 të konventës, me kusht që të parashikohen zhdëmtime të tjera, të cilat nuk shmangin përgjegjësinë ndaj dëmit të shkaktuar dhe nuk e shmangin Republikën e Shqipërisë nga detyrimet ndërkombëtare, të parashikuara në instrumentet ndërkombëtare, përmendur në dispozitën e lartpërmendur[12]. Pra, vendi ynë rezulton të ketë paraqitur një rezervë të vetme ligjore, lidhur me nenin 10 të Konventës së Budapestit, i cili i referohet veprave penale, të lidhura me dhunimin e të drejtës së autorit dhe së të drejtave të tjera të lidhur me të[13].

Ajo që vihet re, është se dispozitat për të drejtat e autorit nuk janë prekur në vitin 2008, kur u bënë shtesat e veprave penale kibernetike për shkak të Konventës së Budapestit. Këto dispozita vazhdojnë të kenë të njëjtin formulim që u është bërë që nga viti 2001 me ligjin nr. 8733, datë 24.1.2001[14]. Megjithatë ndërsa do të analizojmë dispozitat materiale kibernetike në veçanti, do të vëmë re se pavarësisht se e vetmja rezervë ligjore e vendit tonë është e lidhur me nenin 10 të konventës, rezulton të ketë disa mangësi në legjislacionin e brendshëm lidhur me dispozita të veçanta kompjuterike që gjejnë rregullim në konventë[15]. Rezulton gjithashtu, që në disa nene, të mos jenë parashikuar elemente të anës objektive, apo subjektive, referuar parashikimeve të tyre në konventë, edhe pse nuk janë nga ato elemente, që konventa i ka lënë në diskrecionin e shteteve nënshkruese[16].

Këto mangësi kanë krijuar diskutime tek ligjzbatuesit nëse gjatë interpretimit dhe zbatimit të dispozitave të atilla, do të duhet t'i qëndrojnë strikt formulimit të dispozitës sipas legjislacionit shqiptar, apo do ta interpretojnë atë sipas Konventës së Budapestit. Ky diskutim, shtrohet në kushtet kur kjo konventë është një akt ndërkombëtar i ratifikuar, e që si i tillë, ka epërsi mbi ligjet e vendit, kur këto të fundit bien në kundërshtim me të. Kushtetuta jonë parashikon shprehimisht se, *çdo marrëveshje ndërkombëtare e ratifikuar, përbën pjesë të sistemit të brendshëm juridik pasi botohet në Fletoren Zyrtare dhe zbatohet në mënyrë të drejtpërdrejtë, përveç rasteve kur nuk është e vetëzbatueshme dhe zbatimi i saj, kërkon nxjerrjen e një ligji*[17]. *Nga* ana tjetër parashikohet se një marrëveshje ndërkombëtare e ratifikuar me ligj, ka epërsi mbi ligjet e vendit që nuk pajtohen me të.

Vlerësohet se nuk do të mund t'i referohemi drejtpërdrejt Konventës së Budapestit, pasi kjo e fundit nuk është konceptuar si e tillë. Me nënshkrimin e saj palët anëtare marrin përsipër detyrimin që parashikimet e saj t'i bëjnë pjesë të legjislacioneve të brendshme. Duke u kthyer te parashikimi kushtetues i paraqitur më sipër, rezulton që Konventa e Budapestit të bëjë përjashtim nga vetëzbatueshmëria, në kushtet ku zbatimi i saj kërkojnë nxjerrjen e një ligji[18]. Megjithatë, gjykoj se kjo nuk duhet t'i pengojë organet ligjzbatuese që t'i referohen Konventës lidhur me përkufizime të termave kryesisht teknikë, terma të cilët rezultojnë qartë se janë huazuar në legjislacionin e brendshëm pikërisht nga Konventa e Budapestit. Edhe praktika gjyqësore, ka treguar se në rastet kur dispozita në konventë dhe normat e brendshme, ndryshojnë apo vendosin standarde të ndryshme, ligjzbatuesit në çdo rast të analizimit të elementeve të

[12] Shih nenin 2 të ligjit nr. 8888, datë 25.4.2002 për ratifikimin e Konventës.
[13] Shih nenin 10 të Konventës së Budapestit,
[14] Shih nenet 148, 149, 149/a të Kodit Penal të Republikës së Shqipërisë.
[15] Pornografia me të mitur.
[16] Falsifikimi kompjuterik.
[17] Neni 122 i Kushtetutës së Republikës së Shqipërisë.
[18] Po aty.

veprës, i janë referuar dispozitave të legjislacionit të brendshëm dhe standardit të vendosur prej tyre. Përjashtim këtu, bën vetëm vepra penale e "Falsifikimit kompjuterik", e cila do të trajtohet më hollësisht në vijim.

### *1.2 Përkufizime të disa termave teknike në veprat penale kompjuterike*

Pavarësisht përpjekjes së legjislatorit për të kryer një formulim të qartë të dispozitave të krimit kompjuterik, për vetë natyrën e kësaj kategorie veprash, është e pamundur që në formulimin e tyre, të mund të evitohet përdorimi i termave teknike, sikundër janë"*e dhëna kompjuterike*" apo "*sistemi kompjuterik*". Në këtë kuptim, para se të analizohen elementët objektivë dhe subjektivë të veprave kompjuterike, është e nevojshme që para së gjithash të kemi një kuptueshmëri të qartë të këtyre termave. Në legjislacionin tonë nuk kemi një përkufizim të tyre, ndaj do të duhet që për këtë qëllim t'i referohemi Konventës së Budapestit[19].

Sipas konventës, "*Sistem kompjuterik*" do të thotë çdolloj pajisje, apo grup i ndërlidhur, ose pajisje të lidhura, ku një ose më shumë prej të cilave, vazhduese të një programi, kryejnë procesime automatike së të dhënave. Ndërkohë, "*e dhënë kompjuterike*", do të thotë çfarëdolloj përfaqësimi faktesh, informacioni apo konceptesh, në një formë të përshtatshme për procesim në një sistem kompjuterik, që përfshijnë një program të përshtatshëm për punën e një sistemi kompjuterik, për të kryer një funksion.

Të dhënat kompjuterike, nga ana e tyre ndahen në: "*të dhëna të përmbajtjes*" dhe "*të dhëna të trafikut"*, por konventa gjen me vend të përkufizojë vetëm të dhënat e trafikut[20], duke i konsideruar ato si çdo lloj të dhënash kompjuterike, të lidhura me komunikimin nëpërmjet një sistemi kompjuterik të prodhuara nga një sistem kompjuterik që përfaqëson një pjesë, në zinxhirin e komunikimit, duke treguar origjinën e komunikimit(eve) destinacionin, rrugën, kohën, datën, kohëzgjatjen apo tipin e shërbimit.

Ndërkohë, me *të dhënat e përmbajtjes,* duhet kuptuar përmbajtja e komunikimit, si p.sh. kuptimi ose domethënia e komunikimit, ose mesazhi apo informacioni që po transmetohet me anë të komunikimit. Një përkufizim, lidhur me to, gjendet në raportin shpjegues të konventës[21], ku të dhënat e përmbajtjes përcaktohen si çdo e dhënë e transmetuar në komunikim, që nuk përbën të dhënë trafiku. Pra, me të dhënë përmbajtjeje, duhet kuptuar çdo informacion që ka të bëjë me thelbin apo substancën e vetë komunikimit[22].

## 1.6 Organizimi i dispozitave materiale kompjuterike

Ajo që konstatohet para së gjithash në legjislacion tonë penal, është që veprat penale kompjuterike të sipërcituara, dhe të implementuara në vitin 2008[23], nuk janë të vendosura në një krè të veçantë, por janë të shpërndara nëpër seksionet ekzistuese në varësi të objektit juridik të mbrojtur. Legjislatori ynë, ka vlerësuar se krimi kibernetik nuk mbron një të mirë të re juridike, por vetëm sa paraqet një forme të re, të shfaqjes së

[19] Shih nenin 1 të Konventës së Budapestit.
[20] Council of Europe, European treaty Series-No.185. Explanatory Report to the Convention on Cybercrime, f. 40.
[21] Po aty.
[22] Relacioni shpjegues i Konventës bën sqarime të mëtejshme të pjesëve përbërëse të një sistemi kompjuterik, të procesimit automatik së të dhënave, apo të termit i përshtatshëm për procesim.
[23] Me ligjin nr. 10023, datë 27.11.2008 "Për disa shtesa në K. Penal të R.SH".

veprave penale ekzistuese, të cilat mbrojnë objektet juridike ekzistuese si: prona, rendi publik apo dinjiteti. Të njëjtën mënyrë sistemimi, si vendi ynë, kanë ndjekur edhe Italia, Gjermania, Austria, Zvicra, ndërkohë që disa vende të tjera, sikundër janë Franca apo edhe Kosova, në legjislacionin e tyre të brendshëm u kanë dhënë një krè të veçantë veprave penale në fushën e krimit kibernetik. Këto të fundit bazohen në doktrinën se e mira juridike, që mbrohet nga krimi kompjuterik, është një e mirë e re e ndryshme nga ekzistueset, ku përmenden koncepte të tilla si "e mirë juridike kompjuterike", "banesë kompjuterike" apo "liri kompjuterike". Sipas kësaj doktrine, prezantimi i normave të reja në fushën e teknologjisë, është bazuar pikërisht në nevojën për të mbrojtur këto interesa të reja juridike[24].

Konventa nga ana e saj i ka pozicionuar krimet kompjuterike në varësi të formës së shfaqjes së tyre, ndërsa i ka ndarë në:

krimet e lidhura me kompjuterët[25];

veprat penale të lidhura me përmbajtjen;

krime kundër integritetit së të dhënave dhe sistemeve kompjuterike;

Objekt analize në këtë punim janë përzgjedhur të jenë dy kategoritë e para, gjykuar nga përhapja që ato kanë në vendin tonë, por edhe problematikat ligjore që paraqesin.

### *1.7 Krimet e lidhura me kompjuterët*

Doktrina ka pranuar, se krim i lidhur me kompjuterët, konsiderohet çdo lloj krimi ku përfshihen kompjuterët, por Konventa e Budapestit ka përfshirë në këtë kategori, vetëm mashtrimet dhe falsifikimet kompjuterike.

#### *1.7.1 Mashtrimi kompjuterik*

Mashtrimi kompjuterik, është një vepër penale e parashikuar nga neni 143/b i K. Penal dhe i vendosur në kreun e veprave penale kundër pasurisë dhe në sferën ekonomike. Është një dispozitë e shtuar në kodin tonë penal, me ligjin nr. 10023, datë 27.11.2008 "Për disa shtesa dhe ndryshime në K. Penal të R.Sh*",* e cila parashikon shprehimisht se:

"*Futja, ndryshimi, fshirja ose heqja e të dhënave kompjuterike apo ndërhyrja në funksionimin e një sistemi kompjuterik, me qëllim për t'i siguruar vetes apo të tretëve, me mashtrim, një përfitim ekonomik të padrejtë apo për t'i shkaktuar një të treti pakësimin e pasurisë, dënohen me burgim nga gjashtë muaj deri në gjashtë vjet.*

*Po kjo vepër, kur kryhet në bashkëpunim, në dëm të disa personave, më shumë se një herë ose kur ka sjellë pasoja të rënda materiale, dënohet me burgim nga pesë deri në pesëmbëdhjetë vjet".*

Vlen të përmendet, se "Mashtrimi kompjuterik", është një nga veprat penale më të përhapura në praktikë, dhe përgjithësisht, për nga mënyra sesi konsumohet ka karakter ndërkombëtar. Në këtë kontekst penalizimi i saj, është një hap shumë i rëndësishëm në luftën ndaj krimit kibernetik. Parë edhe nga seksioni ku është pozicionuar *objekti* i kësaj figure krimi, janë marrëdhëniet juridike, të vendosura për të garantuar të drejtën e pronës apo edhe interesat pasurore, nga veprimet apo mosveprimet kriminale. Gjithashtu, si objekt dytësor i saj, vijnë edhe mbrojtja dhe funksionimi i rregullt i sistemeve

[24] Mario A. Cattaneo, "*Pena e diritto e dignita umana. Saggio sulla filosofia del diritto penale*", Giappichelli, Torino, 1998.

[25] Në krimet e lidhura me kompjuterët futen "Mashtrimi kompjuterik", (neni 143/b K.P) dhe "Falsifikimi Kompjuterik", (neni 186/a i K.P).

kompjuterike, apo ruajtja e të dhënave kompjuterike.

*Ana objektive* e veprës gjendet në mënyrë përshkruese në dispozitë dhe konsiston në hyrjen, ndryshimin, fshirjen ose heqjen e të dhënave kompjuterike ose ndërhyrjen në funksionimin e një programi apo sistemi kompjuterik. Për të përcaktuar nëse ndodhemi para konsumimit të anës objektive të kësaj vepre penale, do të duhet të kemi të qartë se çfarë do të nënkuptojmë me gjithsecilin prej këtyre veprimeve, gjë që jo gjithmonë është e thjeshtë, për shkak të karakterit teknik të tyre.

Duke qenë se, *futja, ndryshimi, fshirja apo ndërhyrja* në të dhëna, apo sisteme kompjuterike, janë nocione që gjenden në disa nga veprat penale kibernetike, vlerësohet me rëndësi të prezantohet një përkufizim për secilin prej tyre, referuar interpretimeve që u janë bërë në doktrinë dhe veçanërisht në relacionin shpjegues të Konventës së Budapestit. *Me* "ndërhyrje" në funksionimin e programit apo sistemit kompjuterik do të kuptohen veprime të tilla si manipulimi i pajisjeve, veprime që ndalojnë printimet apo akte që ndikojnë në regjistrimin, apo rrjedhjen e të dhënave, ose sekuencën në të cilën veprojnë programet[26].

"*Futja*" e të dhënave kompjuterike, nënkupton futjen e të dhënave të atilla, qofshin këto të sakta ose jo, në mënyrë që ato të ndikojnë në sistem. Ndërkaq, "*ndryshimi*" i referohet modifikimeve, apo ndryshimeve të pjesshme së të dhënave kompjuterike. Dy konceptet e tjera: "*fshirja*" dhe *"heqja*", për vetë kuptimin që paraqesin në gjuhën shqipe, duken si sinonime të njëra-tjetrës, por në terma kompjuterikë, kanë kuptime të ndryshme. "Fshirja" nënkupton largimin e të dhënave nga një medium, ndërsa "heqja", konsiston në fshirjen përfundimtare te tyre.

Në rastin e mashtrimeve kompjuterike nuk është e nevojshme që sistemi të jetë i mbrojtur me masa sigurie, por mjafton ndërhyrja. *Ana subjektive* e veprës penale, është me dashje direkt dhe me qëllimin për t'i siguruar vetes apo të tretëve, me mashtrim, një përfitim ekonomik të padrejtë, apo për t'i shkaktuar një të treti pakësimin e pasurisë.

Diskutim ka pasur në praktikë, fakti, nëse pjesë e anës objektive të veprës, do të ishte dhe ardhja e pasojës, pra përfitimit të padrejtë. Sipas raportit shpjegues të konventës, përfitimi i padrejtë është elementi kryesor i kësaj vepre penale. Sipas tij mashtrimet kompjuterike dënohen vetëm nëse prodhojnë një humbje të drejtpërdrejtë ekonomike. Nga mënyra sesi është formular neni 143/b i K. Penal, mjafton që vetëm të veprohet për qëllimin e përfitimit të padrejtë dhe pavarësisht nëse vjen apo jo pasoja, vepra penale do të quhet e konsumuar. Edhe në praktikën tonë gjyqësore janë mbajtur qëndrime të ndryshme lidhur me këtë. Në disa raste realizimi i qëllimit të padrejtë, pra ardhja e pasojës së dëshiruar, vlerësohet të jetë pjesë e domosdoshme e anës objektive të veprës, ndërsa në raste të tjera, vepra quhet e konsumuar pa qenë e nevojshme të vijë pasoja ekonomike. Kështu, në një rast gjykata e ka gjetur të drejtë kualifikimin e bërë nga akuza, si, mashtrim kompjuterik në bashkëpunim dhe më shumë se një herë, ku i pandehuri S.B kishte shkuar në disa bankomate të bankës X, dhe kishte përdorur disa karta të klonuara, por nuk kishte mundur të tërhiqte të holla[27]. Ndërkohë, në një

[26] Council of Europe, European treaty Series-No.185. Explanatory Report to the Convention on Cybercrime, f. 15.

[27] Shih vendimin nr. 4639, dt 23.12.2015 të Gjykatës së Shkallës së Parë, Tiranë, ku arsyetohet: *"organi i akuzës e ka vlerësuar drejt atë, pasi në funksion të provueshmërisë së faktit penal, provat e sipërcituara dhe sipër analizuara, veçanërisht procesverbalet e këqyrjes së kamerave të sigurisë si edhe ato të sekuestrimit të kartave bankare gjetur të pandehurit, që nuk i përkasin atij por subjekteve të ndryshme dhe të përdorura prej tij si në mënyrën e sipër treguar, njohja dhe vlera e të cilave konfirmohen prej vetë të pandehurit, i sjellin bindje kësaj gjykate në fajësinë e të pandehurit S.B. për veprën penale për të cilën ai akuzohet, për të cilën ai duhet të ndëshkohet penalisht."*

vendim tjetër, po të Gjykatës së Shkallës së Parë, Tiranë[28], është arsyetuar se: *"ardhja e pasojës është një element esencial material që vepra të konsiderohet e konsumuar. Në të vërtetë është pikërisht përfitimi ekonomik i padrejtë apo dëmi i shkaktuar një të treti ajo që dallon mashtrimin kompjuterik nga llojet e tjera të krimeve kompjuterike".*

Një tjetër diskutim që është evidentuar në praktikë, ka qenë edhe rasti i përdorimit të kartave të klonuara të kreditit në ATM-të e bankave, nëse do të kualifikohej si "Mashtrim kompjuterik" apo "Vjedhje e bankave dhe arkave të kursimit"[29]; kjo, pasi në interpretim të vendimit unifikues nr. 3/2015 të Kolegjeve të Bashkuara të Gjykatës së Lartë, rezulton që edhe ATM-të, janë pasuri në pronësi dhe në përdorim të bankës[30]. Diskutimi lidhur me kualifikimin konsiston në atë që në rastin konkret do t'i jepet prioritet vendit ku ka ndodhur hedhja në dorë e përfitimit të paligjshëm që është banka, apo mënyrës së kryerjes së saj, nëpërmjet teknologjisë.

Në praktikë hasen diskutime gjithashtu edhe lidhur me kualifikimin e duhur juridik të rasteve të mashtrimit nëpërmjet dërgimit të email-ëve të rremë, të cilat janë edhe rastet më të shpeshta të mashtrimit që gjenden në hetim apo në gjykim. Kazusi është pothuaj i njëjtë në të gjitha rastet. Viktimës, i mbërrijnë mesazhe në postën elektronike nga subjekte që përgjithësisht paraqiten si përfaqësues shoqërish tregtare serioze, që tregtojnë pikërisht produktet për të cilat viktima është i interesuar. Mes këtij të fundit dhe autorit të veprës penale, zhvillohet një komunikim normal, i besueshëm, biznesi, çka bën që i dëmtuari të mos ketë dyshime për vërtetësinë e komunikimit. Pasi ka fituar besimin e viktimës, subjekti i veprës penale avancon në kërkimin e shumës së parave në këmbim të produkteve të ofruara. Viktima, në kushtet e mirëbesimit, pranon, dhe dërgon paratë në vendin dhe mënyrën e propozuar nga autori i veprës. Vetëm pasi produktet e paguara nuk mbërrijnë tek blerësi dhe komunikimet mes këtij të fundit dhe të prezantuarit si shitës ndërpriten, viktima ndërgjegjësohet mbi mashtrimin e ndodhur.

Diskutimi që lind në këtë rast, konsiston në faktin nëse do të gjendemi para veprës penale "Mashtrimi", parashikuar nga neni 143 i K. Penal apo "Mashtrim Kompjuterik", parashikuar nga neni 143/b i K.P. Objekti dhe ana subjektive e të dy veprave është e njëjtë, ndaj për dallimin mes tyre do t'i referohemi anës objektive të veprës penale. Në rastin e mashtrimit kompjuterik, ndryshe nga mashtrimi, veprimet nuk shtrihen mbi personin (subjektin pasiv), por mbi sistemin kompjuterik nëpërmjet manipulimit të këtij sistemi[31]. Në rastin e mashtrimit kompjuterik, subjekti pasiv i kësaj vepre nuk është një person, i cili shtyhet në gabim, me anë të gënjeshtrës apo shpërdorimit të besimit por sistemi në të cilin bëhet një ndërhyrje e paligjshme. Bëhet fjalë, për një vepër që konsiston në tërheqjen në gabim (mashtrim) të një operatori elektronik, me qëllim nxjerrjen e një përfitimi ekonomik (për vete apo të tjerët), në dëm të një subjekti të tretë.

Në dallim nga mashtrimi, që kufizohet vetëm tek elementët *gënjeshtër* apo *shpërdorim besimi,* ndërhyrja në mashtrimin kompjuterik mund të bëhet në çdo mënyrë përmes

[28] Shih vendimin nr. 2617, dt. 5.11.2014 të Gjykatës së Shkallës së Parë Tiranë.

[29] Shih neni 136 i Kodit Penal të R.SH.

[30] Në vendimin unifikues nr. 3/2015 përcaktohet se: "Kriteret që mund të ndiqen janë dy llojesh: kriteri material ose hapësinor, sipas të cilit kërkohet përkatësia e mjedisit në raport me bankën, kundrejt ambienteve të tjera që e rrethojnë atë. Kriteri kualitativ ose funksional, sipas të cilit kërkohet përkatësia e mjedisit në raport me bankën të jetë e destinuar për zhvillimin e aktivitetit të bankës me të gjitha mjediset e lidhura me të. Sipas kriterit të dytë, në mjediset e bankës përfshihen edhe godinat ku banka ushtron aktivitetin e saj, përfshirë këtu zyrat, magazinat dhe ambientet e tjera shërbyese, por edhe mjetet e tjera në dispozicion të saj, siç janë edhe automjetet me të cilat banka operon. Ky kriter ndiqet për faktin se, edhe këto ambiente janë mjedise të bankës që përmbajnë dhe përbëjnë pasuri të saj, të cilat janë në pronësi/përdorim po të bankës, ku person pasiv i veprës penale do të ishte po banka."

[31] Corte di Cassazione, Sezione VI Penale, Sentenza 4 ottobre 1999, n. 3065.

ndryshimeve të brendshme apo të jashtme, në *software* ose *hardware*, mjafton që të modifikohet qëllimi për të cilin është destinuar sistemi. Duke qenë se sistemit kompjuterik, i mungon aspekti psikologjik që shoqëron individin, inkriminohen ndërhyrjet në funksionim dhe futjet pa të drejtë në përmbajtje, përmes të cilave arrihet të sigurohet një përfitim.

Në këtë kontekst, rastet e sipërcituara kur personat mashtrohen për shkak të komunikimit me persona nën identitet të rremë, vlerësohet se nuk duhet të kualifikohen si mashtrim kompjuterik. Në këtë rast veprimet kriminale janë shtrirë drejt personit, mbi psikologjinë e këtij të fundit, duke e bërë atë të bjerë në lajthim dhe në këtë mënyrë vullnetarisht t'i sigurojë autorit përfitimin e padrejtë. Nuk rezultojnë ndërhyrje në sistem apo futje e fshirje të dhënash kompjuterike, të atilla që ato të modifikojnë qëllimin për të cilin është destinuar sistemi. Pra viktima ka rënë në mashtrim për shkak të gënjeshtrës që i është bërë nga autori, duke u hequr si një person tjetër dhe jo për shkak së të dhënave të ndryshuara që do të gjeneronte një sistem kompjuterik i manipuluar, e thënë ndryshe, për shkak të "gënjeshtrës" së diktuar nga operatori kompjuterik.

*1.7.2 Falsifikimi kompjuterik*

Falsifikimi kompjuterik është një vepër penale e parashikuar nga neni 186/a i K. Penal, që ashtu sikurse veprat e tjera kompjuterike, është shtuar në kodin tonë penal me ligjin nr. 1002 datë 27.11.2008. Parashikimi i kësaj vepre penale, u bë i domosdoshëm në kushtet kur të dhënat zyrtare ose jo, gjithmonë e më shumë nuk po ruheshin më në letër, por në mënyrë elektronike. Ashtu sikundër falsifikimi i dokumenteve (në letër), rezultoi e nevojshme të merreshin në mbrojtje edhe dokumentet elektronike, në të cilat mund të ndërhyhej gjithashtu, duke paraqitur të dhëna të rreme. Ky qëllim, i parashikimit të kësaj dispozite, duhet konsideruar dhe pasur parasysh, edhe në interpretimin që i bëhet asaj rast pas rasti.

Neni 186/a i Kodit Penal, është formuluar si më poshtë:

"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."*

Formulimi i kësaj dispozite duket se vjen në përputhje të asaj çka është parashikuar në nenin 7 të Konventës së Budapestit[32], por ndryshe nga kjo e fundit që kërkon përdorimin e të dhënave për qëllime jo ligjore, dispozita e mësipërme mjaftohet vetëm me faktin e krijimit së të dhënave të rreme me qëllim përdorimin e tyre si autentike. Këtu vlen të theksohet fakti se Konventa e Budapestit nuk e ka lënë në diskrecion të palëve, parashikimin ose jo në dispozitë të rrethanës së përdorimit së të dhënave për qëllime jo ligjore. Nga ana tjetër, vendi ynë nuk ka paraqitur ndonjë rezerve ligjore

[32] Neni 7 i Konventës - Falsifikimet e lidhura me kompjuterët:*"Çdo Palë do të adaptojë legjislacion të tillë dhe masa të tjera që mund të jenë të nevojshme të përcaktojnë si vepra penale sipas ligjit të brendshëm, kur kryhet me qëllim dhe pa të drejtë, futja e të dhënave, ndryshimi, fshirja, apo heqja e të dhënave kompjuterike që rezultojnë në të dhëna joautentike, me qëllim që ato të konsiderohen apo të veprohet mbi to për qëllime ligjore sikurse ato të ishin autentike, pavarësisht nëse të dhënat janë të lexueshme apo të kuptueshme direkt. Një Palë mund të kërkojë synimin për të mashtruar ose një synim të ngjashëm të pandershëm përpara lindjes së përgjegjësisë penale."*

lidhur me këtë dispozitë, apo elemente të caktuara të saj.

Nën logjikën e këtij arsyetimi, kjo rrethanë[33] do të duhej të ishte parashikuar në dispozitën e brendshme të falsifikimit kompjuterik, si një detyrim ligjor që rrjedh për shkak të nënshkrimit të Konventës së Budapestit. Kjo e fundit u jep mundësinë palëve vetëm që ta rrisin standardin e vendosur prej saj, duke parashikuar edhe synimin për të mashtruar ose një synim të ngjashëm të pandershëm[34], por jo për ta ulur më tej atë, duke hequr elementë që vlerësohet të jenë thelbësore për qenësinë e veprës. Duke i qëndruar korrekt interpretimit fjalë për fjalë të dispozitës së falsifikimit kompjuterik, nxirret përfundimi se mjafton që futja, ndryshimi apo heqja e të dhënave në mënyrë të padrejtë, të bëhen me qëllim paraqitjen e tyre si autentike, dhe vepra penale, të quhet e konsumuar. Kjo ka bërë që më herët të kualifikohen si "Falsifikim kompjuterik" edhe rastet e hapjes së *profileve të rremë* në rrjetet sociale[35]. Tashmë praktika gjyqësore ka ndryshuar dhe rastet kur krijohen dhe përdoren profile të rreme në rrjete të ndryshme sociale[36], nuk janë kualifikuar më si "Falsifikim kompjuterik", por në varësi të rrethanave të faktit si "Ndërhyrje të padrejta në jetën private", (neni 121 i K.P), "Fyerje", (neni 119 K.P) apo dhe "Shpifje", (neni 120 K.P)[37]. Rasti i veprës penale të "Falsifikimit kompjuterik"është një nga rastet e vetme, ku ligjzbatuesit në njëfarë mënyre e kanë tejkaluar parashikimin e dispozitës së brendshme duke iu referuar parashikimit të Konventës së Budapestit. Është e rëndësishme të kuptohet që qëllimi i kësaj dispozite nuk është dhe nuk duhet të jetë për penalizimin e rasteve të atilla[38].

Në raportin shpjegues të konventës, sqarohet se qëllimi i këtij neni, është të krijojë një vepër paralele me falsifikimin e dokumenteve "të prekshme"[39]. Kjo dispozitë synon mbushjen e hapësirave apo boshllëqeve, që mund të krijohen në të drejtën penale, në lidhje me falsifikimin tradicional, i cili kërkon dokumente të materializuara, lexueshmëri vizuale apo deklarime të mishëruara në një dokument, gjë që nuk mund të zbatohet për të dhënat e ruajtura në mënyrë elektronike.

Termi *për qëllime ligjore*[40], i referohet transaksioneve ligjore dhe dokumenteve, të cilat kanë një vlerë ligjore. Pra sipas konventës, të dhënat e falsifikuara duhet të jenë të atilla që marrin një vlerë apo efekt juridik, të dhëna që janë ekuivalente me një dokument publik apo privat, i cili pas, sjell efekte juridike.

Edhe praktika ndërkombëtare ka shkuar po në këtë drejtim. Madje në disa vendek praktika gjyqësore ka evoluar edhe më tej, ndërsa kërkon që përveçse "dokumenti" të ketë vlerë juridike, pjesë e aktit, të ishte edhe nënshkrimi elektronik, si një kusht ligjor që garanton besueshmërinë e të dhënave.

### *1.8 Veprat penale lidhur me përmbajtjen*

Në këtë kategori të krimeve kompjuterike, përfshihen veprat penale në të cilat paligjshmëria qëndron në përmbajtjen e tyre dhe ku rrjeti apo kompjuteri përdoren si mjet për realizimin e tyre apo edhe për të lehtësuar kryerjen e tyre. Vepra tipike në këtë

[33] Qëllimi të veprohet mbi të dhënat për qëllime ligjore.
[34] Një Palë mund të kërkojë synimin për të mashtruar ose një synim të ngjashëm të pandershëm përpara lindjes së përgjegjësisë penale."
[35] Vendim nr. 485, datë 23.04.2013 i Gjykatës së Rrethit Gjyqësor Tiranë.
[36] Këto raste janë më të shumtat në numër.
[37] Vendim mosfillimi dt. 07.05.2018 lidhur me kallëzimin penal nr5198/2018.
[38] Në praktikën ndërkombëtare ky lloj veprimi kategorizohet si impersonifikim apo "identity theftë" (vjedhje identiteti).
[39] Council of Europe, European Treaty Series - No. 185, Explanatory Report to the Convention on Cybercrime, f.14.
[40] Po aty.

kategori do të ishte ajo e pornografisë me fëmijë. Zhvillimi i teknologjisë e ka bërë më të thjeshtë posedimin, shpërndarjen apo publikimin e pornografisë me fëmijë. Kjo ka bërë që Konventa e Budapestit, në nenin 9 të saj, të kërkonte nga shtetet palë që të parashikojnë si figurë të veprës penale të kryer nëpërmjet teknologjisë edhe "Pornografinë me fëmijë"[41]. Pavarësisht se kjo konventë është ratifikuar nga vendi ynë, duke marrë përsipër kështu detyrimin për zbatimin tërësor të saj[42], nuk rezulton që parashikimet e saj të jenë implemetuar në legjislacionin e brendshëm, lidhur me këtë vepër penale.

*1.8.1 Pornografia me të mitur (neni 9 i Konventës së Budapestit)*

Pornografia me të mitur, është një nga dispozitat më të qarta të Konventës së Budapestit, e parashikuar në nenin 9 të saj, ku në pikën 1 të tij parashikon shprehimisht se:

Çdo palë do të adaptojë legjislacion të tillë dhe masa të tjera, që mund të jenë të nevojshme të përcaktojnë si vepra penale sipas ligjit të brendshëm, kur kryhet me qëllim dhe pa të drejtë, në drejtimet e mëposhtme:

a) prodhimin e pornografisë me fëmijë, me qëllimin e shpërndarjes së tij nëpërmjet një sistemi kompjuterik;

b) ofrimi apo vënia në disponim e pornografisë për fëmijë nëpërmjet një sistemi kompjuterik;

c) shpërndarja apo transmetimi i pornografisë për fëmijë nëpërmjet një sistemi kompjuterik;

d) prokurimi i pornografisë për fëmijë nëpërmjet një sistemi kompjuterik për vete apo për një tjetër;

e) zotërimi i pornografisë për fëmijë nëpërmjet një sistemi kompjuterik apo në një mjet të memorizimit së të dhënave kompjuterike.

Konventa e Krimit Kibernetik, në përmbajtje të këtij neni, paraqet gjithashtu një përkufizim të asaj se çfarë do të konsiderohet "*pornografi me fëmijë*", për qëllime të kësaj dispozite[43]. Sipas këtij përkufizimi, "pornografi me fëmijë", do të përfshijë çdo material pornografik që dallon nga ana pamore:

a) *një minoren, i cili angazhohet në drejtime të qarta seksuale;*

b) një person, i cili duket që është minoren, i angazhuar në drejtime të qarta seksuale;

c) imazhe realiste që prezantojnë një minoren të angazhuar në drejtime të qarta seksuale.

Konventa, në vijim përkufizon edhe termin"*minoren*"[44] nga ku rezulton të konsiderohen të tillë, të gjithë personat *nën moshën 18 vjeç*. Ajo megjithatë lë në diskrecionin e shteteve, ta ulin këtë kufi, duke vendosur një limit moshe më të vogël, e cila gjithsesi nuk duhet të jetë më pak se 16 vjeç.

Konventa e Budapestit u ka dhënë mundësi shteteve palë, të rezervojnë të drejtën, të mos aplikojnë në tërësi apo pjesërisht paragrafin 1(d), 1(e) dhe 2 (c)[45], të cilët i referohen konsumimit të veprës penale nëpërmjet prokurimit të pornografisë për fëmijë, nëpërmjet një sistemi kompjuterik, për vete apo për një tjetër 1(d), zotërimit të pornografisë për fëmijë nëpërmjet një sistemi kompjuterik apo në një mjet të memorizimit së të dhënave kompjuterike 1 (e), si dhe konsiderimin si pornografi me

[41] Shih nenin 9 të Konventës së Budapestit.
[42] E vetmja rezervë e paraqitur ka qenë lidhur me nenin 10 të Konventës së Budapestit.
[43] Neni 9, prg. 2 i Konventës së Budapestit.
[44] Neni 9, prg. 3 i Konventës së Budapestit.
[45] Neni 9, prg. 4 i Konventës së Budapestit.

fëmijë, edhe të imazheve realiste që prezantojnë një minoren të angazhuar në drejtime të qarta seksuale 2 (c).

*1.8.2 Pornografia (neni 117 i Kodit Penal të R.Sh)*

Ligji nr. 10023, datë 27.11.2008, me të cilin u shtuan në Kodin Penal të Republikës së Shqipërisë veprat penale në fushën e krimit kibernetik, në zbatim të Konventës së Budapestit, nuk ndryshoi dispozitën e "Pornografisë", që ishte e parashikuar tashmë dhe as nuk shtoi ndonjë dispozitë tjetër lidhur me të.

Në fakt, "Pornografia" është nga dispozitat më të hershme në kodin tonë penal. Kjo vepër ka qenë e pasqyruar edhe në kodet penale të viteve 1952[46] dhe1977[47] dhe mandej në atë të vitit 1995[48]. Në kodin penal aktual, dispozita e pornografisë ka pësuar ndryshime me ligjin nr. 9859, datë 21.01.2008, me të cilin është shtuar paragrafi i dytë[49] dhe ndryshimet e fundit i ka pësuar me ligjin nr. 144/2013, me këtë përmbajtje:

"Prodhimi, shpërndarja, reklamimi, importimi, shitja e botimi i materialeve pornografike në mjediset ku ka fëmijë, me çdo mjet ose formë, përbëjnë kundërvajtje penale dhe dënohen me burgim deri në dy vjet. Prodhimi, importimi, ofrimi, vënia në dispozicion, shpërndarja, transmetimi, përdorimi ose posedimi i pornografisë së fëmijëve, si dhe krijimi i aksesit në mënyrë të vetëdijshme në të, me çdo mjet ose formë, dënohet me burgim nga tre deri në dhjetë vjet.

*Rekrutimi, përdorimi, shtrëngimi, ose bindja e një fëmije, për të marrë pjesë në shfaqje pornografike, ose marrja pjesë në shfaqje pornografike që përfshijnë fëmijët, dënohet me burgim nga pesë deri në dhjetë vjet".*

Në rastin më të parë që ligjzbatuesi ndeshet më këtë dispozitë, do t'i duhet të ketë të qartë se çfarë do të kuptojë me *"Fëmijë"* dhe *"Pornografi me fëmijë"*. Këto janë koncepte bazë, paqartësia mbi të cilat mund të krijojë praktika dhe kualifikime të gabuara, ndërkohë që në legjislacionin e brendshëm nuk gjejmë përkufizime lidhur me to. Në dispozitë përdoret termi "fëmijë" dhe ligjzbatuesi mbetet i paqartë se çfarë do të kuptojë me të, pasi ligji penal shqiptar në dispozita të tjera, përdor termin *"i mitur*", ndërsa Konventa e Budapestit e quan "minoren". A është termi "fëmijë" i njëjtë me "i mitur" apo "minoren", dhe nëse po, a mund t'i referohemi drejtpërdrejt përkufizimit që Konventa e Budapestit ka kryer për minorenin[50]? I njëjti diskutim krijohet edhe lidhur me atë se çfarë do të konsiderohet "Pornografi me fëmijë", në kuptim të nenit 117 të K. Penal të Republikës së Shqipërisë.

Pyetja që shtrohet është, nëse për këtë qëllim do të mund t'i referohemi përkufizimit që Konventa e Budapestit i ka bërë pornografisë me të mitur[51]. Këto diskutime bëhen akoma më konkrete, kur në praktikë gjendemi para rasteve që viktima duket si e mitur,

[46] Neni 293 i KP 1952: "Prodhimi, shpërndarja dhe reklamimi i veprave, botimeve, figurave, ose sendeve të tjera pornografike, si dhe tregtia e tyre, ose mbajtja e tyre me qëllim shitjeje ose shpërndarjeje dënohen me burgim gjer në tre vjet..."

[47] Neni 136 i KP 1977: "Prodhimi, shpërndarja dhe reklamimi i veprave, i botimeve, i figurave dhe i sendeve të tjera pornografike, si edhe tregtimi i tyre ose mbajtja e tyre me qëllim shitjeje ose shpërndarjeje, dënohen me heqje të lirisë gjer në tre vjet."
188 Neni.

[48] Neni 117 i K.P të vitit 1995:"Prodhimi, shpërndarja, reklamimi, importimi, shitja e botimi i materialeve pornografike në ambientet e të miturve, përbëjnë kundërvajtje penale dhe dënohen me gjobë ose me burgim gjer në dy vjet".

[49] Paragrafi i shtuar ka këtë përmbajtje:"Përdorimi i të miturit për prodhimin e materialeve pornografike, si dhe shpërndarja ose publikimi i tyre në internet apo në forma të tjera, dënohet me burgim nga një deri në pesë vjet dhe me gjobë nga një milion deri në pesë milionë lekë".

[50] Neni 9, prg. 3 i Konventës së Budapestit.

[51] Neni 9, prg. 2 i Konventës së Budapestit.

por nuk mund të përcaktohet mosha e saj, apo para imazheve pornografike që prezantojnë një të mitur, por që nuk i referohen një personi konkret. Sipas Konventës së Budapestit, në këto raste kemi pornografi me të mitur[52], ndërkohë praktika gjyqësore në vend tregon që ligjzbatuesi shqiptar nuk i ka cilësuar të tilla, duke mos iu referuar kështu përkufizimit të bërë nga Konventa e Budapestit.[53] Janë të pakta rastet e dërguara për gjykim[54] për këtë vepër penale dhe ajo që konstatohet, është se një nga arsyet më të shpeshta të pushimit të këtyre çështjeve, është fakti i pamundësisë së përcaktimit të moshës së viktimës[55].

Sikundër është përmendur edhe më herët në këtë punim, vendi ynë e ka ratifikuar Konventën e Budapestit dhe nuk ka paraqitur rezervë ligjore lidhur me dispozitën e pornografisë me të mitur. Po kështu nuk ka paraqitur rezervë ligjore as për elementë të caktuar të dispozitës që vetë Konventa ka lënë në diskrecion të shteteve dhe që janë cituar më sipër[56]. Pra si rregull parashikimet ligjore të Konventës lidhur me pornografinë e të miturve duhet të ishin bërë pjesë e legjislacionit të brendshëm, në sajë të detyrimit të marrë përsipër pas ratifikimit të saj.

Referuar ndryshimeve që ka pësuar dispozita e pornografisë, kohës kur janë kryer dhe termave të përdorur, rezulton qartë që kjo dispozitë është produkti Konventës së Këshillit të Europës, për Mbrojtjen e Fëmijëve Kundër Shfrytëzimit dhe Abuzimit Seksual, e njohur ndryshe si Konventa e Lanzarotes[57]. Në këtë konventë gjenden edhe emërtimet që hasim në dispozitën tonë të brendshme: "fëmijë" apo"pornografi me fëmijë", madje edhe përkufizimet lidhur me to[58]. Ajo që vihet re është se si në Konventën e Lanzarotës, edhe në Konventën e Budapestit, përkatësisht me "fëmijë" dhe "minoren", do të kuptohet çdo person nën moshën 18 vjeç.[59]

### *1.9 Konkluzione dhe rekomandime*

Legjislacioni penal shqiptar, në fushën e krimit kibernetik, vlerësohet të jetë një legjislacion bashkëkohor dhe përgjithësisht në përputhje me Konventën për Krimin Kibernetik (Konventa e Budapestit), e cila është edhe akti ndërkombëtar më i rëndësishëm aktualisht për krimin kibernetik.

Sikundër është evidentuar gjatë këtij punimi, ka dispozita të Konventës së Budapestit apo elementë objektivë dhe subjektivë të dispozitave të caktuara, të cilat nuk janë parashikuar si të tilla, në legjislacionin e brendshëm, duke e vënë në vështirësi ligjzbatuesin shqiptar mbi dispozitën së cilës do të duhet t'i referohen, në rastin konkret. Konventa e Budapestit është konceptuar në atë mënyrë, që detyron shtetet palë ta bëjnë atë pjesë të legjislacionit të brendshëm, çka e bën atë, një akt ndërkombëtar jo të vetëzbatueshëm[60]. Pra ligjzbatuesi shqiptar, që të mund të zbatojë parashikimet e Konventës së Budapestit, i duhet që ato t'i gjejë të pasqyruara në legjislacionin e brendshëm. Është detyrë e

[52] Neni 9, prg. 2 i Konventës së Budapestit.
[53] Një pjesë e madhe e procedimeve penale në vendin tonë pushohen me arsyetimin se nuk provohet fakti që viktima është i mitur.
[54] Vendim nr. 1048, datë 5.4.2016 i Gjykatës së Rrethit Gjyqësor Tiranë.
[55] Vendim për Pushimin e çështjes penale nr. 8782, datë 15.11.2016 i Prokurorisë pranë Gjykatës së Shkallës së Parë Tiranë.
[56] Neni 9, prg. 4 i Konventës së Budapestit.
[57] Ratifikuar nga vendi ynë me Ligjin nr. 10 071, datë 9.2.2009.
[58] Neni 3/a i Konventës së Lanzarotës parashikon se për qëllime të kësaj konvente fëmijë është çdo person nën moshën 18 vjeç.
[59] Konventa e Budapestit u lë mundësi shteteve palë edhe ta ulin kufirin e moshës deri në 16 vjeç.
[60] Shih nenin 122 të Kushtetutës së R.Sh.
[61] Shih nenin 43 të Konventës së Budapestit.

legjislatorit të bëjë pjesë të legjislacionit të brendshëm gjithë parashikimet ligjore të Konventës së Budapestit, përveç rezervës ligjore të paraqitur në momentin e ratifikimit të saj, duke parë edhe mundësinë të heqë dorë nga kjo e fundit sipas procedurave që vetë konventa parashikon[61].

Një tjetër konstatim që vlerësohet më rëndësi për t'u evidentuar në këtë pjesë të fundit, është edhe vështirësia që krijohet tek ligjzbatuesi shqiptar lidhur me kuptueshmërinë e dispozitave kompjuterike, për shkak të karakterit teknik të tyre. Pothuaj të gjitha dispozitat kompjuterike kanë në përmbajtjen e tyre elemente teknike, elemente të cilat është e rëndësishme të kuptohen drejt, duke qenë se lidhen drejtpërdrejt me anën objektive të veprave penale konkrete dhe për pasojë, me vetë ekzistencën e tyre. Lidhur me këto elemente, do të duhej të kishte përkufizime të qarta në legjislacionin e brendshëm, me qëllimin që termat teknike të "*përkthehen*" në një gjuhë të thjeshtë dhe të kuptueshme për të gjithë. Parë karakterin ndërkombëtar që ka krimi kompjuterik, vlerësohet të jetë me rëndësi që këto terma dhe koncepte, të jenë të unifikuara apo të gjithëpranuara.

## Bibliografi


1. Konventa për Krimin Kibernetik (Konventa e Budapestit).
2. Konventa e Këshillit të Europës për Mbrojtjen e Fëmijëve Kundër Shfrytëzimit dhe Abuzimit Seksual (konventa e Lanzarotës).
3. Relacioni shpjegues i Konventës së Krimit Kibernetik (Council of Europe, European Treaty Series - No. 185, Explanatory Report to the Convention on Cybercrime).
4. Kushtetuta e Republikës së Shqipërisë, e ndryshuar.
5. Kodi Penal i Republikës së Shqipërisë, i ndryshuar.
6. Ligji nr. 9859, datë 21.91.2008 "Për disa ndryshime në K. Penal të R.SH".
7. Ligji nr. 144/2013 "Për disa ndryshime në K. Penal të R.SH".
8. Ligji nr. 8733, datë 24.1.2001 "Për disa ndryshime në K. Penal të R.SH".
9. Ligji nr. 9262,datë 29.7.2004 "Për ratifikimin e protokolleve shtesë të Koventës së Budapestit".
10. Ligji nr. 8888, datë 25.4.2002 "Për ratifikimin e Konventës së Budapestit".
11. Ligji nr. 9686, datë 26.2.2007 "Për disa ndryshime në K. Penal të R.Sh".
12. Mario A. Cattaneo, "*Pena e diritto e dignita umana. Saggio sulla filosofia del diritto penale*", Giappichelli, Torino, 1998.
13. Vendim unifikues nr. 3/2015 i Kolegjeve të Bashkuara të Gjykatës së Lartë.
14. Vendim nr. 1048, datë 5.4.2016 i Gjykatës së Rrethit Gjyqësor Tiranë.
15. Vendim nr. 6639, datë 23.12.2015 i Gjykatës së Rrethit Gjyqësor, Tiranë.
16. Vendim nr. 2617, datë 5.11.2014 i Gjykatës së Shkallës së Parë, Tiranë.
17. Vendim nr. 485, datë 23.4.2013 i Gjykatës së Rrethit Gjyqësor, Tiranë.
18. Vendim për Pushimin e çështjes penale nr. 8782, datë 15.11.2016 i Prokurorisë pranë Gjykatës së Shkallës së Parë Tiranë.

# Mashtrimet e bizneseve, keqpërdormi i kartave bankare dhe përdormi i sigurt i internetit

■**MSc. Visar PACOLLI**
*Sektori për hetimin e krimeve kibernetike,*
*Policia e Kosovës*
*visar.pacolli@kosovopolice.com*

**Abstrakt**

*Teknologjia, interneti, përdorimi i ATM-ve (bankomatëve) si dhe pagesat online nga bizneset, ka marrë vendin e tij, krahas zhvillimi të teknologjisë informative si një pjesë e rëndësishme e jetës së njerëzve. Konsumatorët përdorin bankomatët, POS terminalet dhe internetin për blerje online, dhe të investojnë online. Shumica e konsumatorëve si dhe bizneset në ditët e sotme përdorin, karta krediti ose debiti, për tërheqje parash dhe për të bërë pagesa të ndryshme online, duke mos parashikuar rreziqet të cilat ju kanosen gjatë kryerjes së këtyre shërbimeve. Shumica e këtyre mekanizmave kërkojnë përfshirjen e një pale të tretë, për të shërbyer si një ndërmjetësues në transaksione. Varësisht nga mekanizmi, ndërmjetës mund të ketë një marrëdhënie kontraktuale me blerësin, shitësin, ose të dyja. Përparësitë kryesore të metodave të pagesës online janë komoditeti dhe efikasiteti. Për shembull, një shërbim i pagesës online, mund t'i mundësojë një blerësi për të blerë mallra nga një individ nga kredit-karta, duke bërë që shitësi t'i transportojë mallrat menjëherë, në vend që të vonohen disa ditë ose javë. Disa prej këtyre shërbimeve i kanë tarifat shumë të larta, që janë të krahasueshme, - krahas disave që kushtojnë ndonjëherë edhe më lirë. Megjithëse institucionet financiare, respektivisht shërbimet bankare, bëjnë të pamundurën për të siguruar përdorimin e kartave, si online ashtu edhe për të bërë pagesa, prapëseprapë të drejtat e blerësit dhe të shitësit, janë të kontrolluara përgjithësisht nga kushtet e çdo ofruesi. Në këtë punim, do të trajtohen disa nga rreziqet e tërheqjes së parave nga bankomatët, vjedhja e të dhënave personale bankare, klonimi i kartave dhe mënyrat e klonimit, shfrytëzimi i tyre, blerja online dhe format më të reja të mashtrimit të bizneseve si dhe disa mënyra se si të mbrohemi nga ato rreziqe.*

**Fjalëkyçe:**
**ATM, klonim kartash, mashtrim, pagesa *online*, bankomat.**

## 1. Hyrje

Teknologjia, interneti, përdorimi i ATM-ve (bankomatëve) si dhe pagesat *online* nga bizneset, ka marrë vendin e tij, krahas zhvillimi të teknologjisë informative si një pjesë e rëndësishme e jetës së njerëzve. Konsumatorët përdorin bankomatët, POS terminalet dhe internetin për blerje *online*, dhe të investojnë *online*. Shumica e konsumatorëve si dhe bizneset në ditët e sotme përdorin, karta krediti ose debiti, për tërheqje parash dhe për të bërë pagesa të ndryshme *online,* duke mos parashikuar rreziqet të cilat ju kanosen gjatë kryerjes së këtyre shërbimeve. Shumica e këtyre mekanizmave kërkojnë përfshirjen e një pale të tretë, për të shërbyer si një ndërmjetësues në transaksione. Varësisht nga mekanizmi, ndërmjetës mund të ketë një marrëdhënie kontraktuale me blerësin, shitësin, ose të dyja.

Përparësitë kryesore të metodave të pagesës *online* janë komoditeti dhe efikasiteti. Për shembull, një shërbim i pagesës *online,* mund t'i mundësojë një blerësi për të blerë mallra nga një individ nga kredit-karta, duke bërë që shitësi t'i transportojë mallrat menjëherë, në vend që të vonohen disa ditë ose javë. Disa prej këtyre shërbimeve i kanë tarifat shumë të larta, që janë të krahasueshme, - krahas disave që kushtojnë ndonjëherë edhe më lirë.

Megjithëse institucionet financiare, respektivisht shërbimet bankare, bëjnë të pamundurën për të siguruar përdorimin e kartave, si *online* ashtu edhe për të bërë pagesa, prapëseprapë të drejtat e blerësit dhe të shitësit, janë të kontrolluara përgjithësisht nga kushtet e çdo ofruesi. Në këtë punim, do të trajtohen disa nga rreziqet e tërheqjes së parave nga bankomatët, vjedhja e të dhënave personale bankare, klonimi i kartave dhe mënyrat e klonimit, shfrytëzimi i tyre, blerja *online* dhe format më të reja të mashtrimit të bizneseve si dhe disa mënyra se si të mbrohemi nga ato rreziqe.

## 2. Klonimi i kartave bankare në ATM (bankomat) dhe keqpërdorimi i tyre

Klonimi i kartave bankare bëhet në ATM, kur aty vendosen disa pajisje të cilat bëjnë leximin e shiritit magnetik si dhe një pajisje tjetër, që vendoset mbi pjesën ku shtypet *pin code*. Pasi i sigurojnë të dhënat, ato të dhëna dekodohen dhe bëhen funksionale dhe kartat janë të gatshme për përdorim. Ato mund të përdoren për blerje *online* si dhe për transferime të ndryshme të parave, si për shembull në *Uestern Union, Mony Gram* etj. Gjatë klonimit të kartave bankare në bankomat, ata përdorin disa pajisje speciale që bëhen të ngjashme me tipin e ATM-së që të mos jenë të dukshme për përdoruesit e ATM-ve. Në ditët e sotme kjo dukuri është shumë e shpeshtë në të gjithë botën, e ku këtu, bën pjesë edhe vendi ynë.

Figura 2: Pajisje për leximin e shiritit magnetik.

Figura 1: Pajisje për leximin e shtypjes së "pin code".

Figura 3: Bankomati në të cilin është vendosur pajisja për klonim të kartave bankare.

Për klonimin e kartave bankare në ATM, ka pajisje shumë specifike dhe kjo gjë, bëhet nga disa persona në grup, duke i ndarë rolet e tyre për vjedhjen e dhënave të kartave bankare në ATM. Këto pajisje janë pajisje që kanë role të ndryshme: te një pjesë vendoset kamera për incizimin, e cila incizon shtypjen e "pin code"-it, ose edhe mikrofona të vegjël për incizimin e zërit gjatë shtypjes së "pin code"-it, si dhe pjesa tjetër për leximin e shiritit magnetik. Më pas, ato të dhëna bashkohen, dhe krijohet karta funksionale si për përdorim *online* ose edhe duke i shtypur ato të dhëna në karta *Blanko;* dhe më pas i përdorin për blerje të ndryshme në dyqane ose pompa benzine.

Leximi i të dhënave nga pajisja e cila bën leximin e shiritit magnetik, është shumë i vështirë pasi aty ka një kriptim (shifrim) shumë të lartë dhe shumë herë, është e pamundur që ne të vërejmë se sa të dhëna të kartave bankare përmban ajo vetë; ndërsa ekzaminimi i pajisjes, e cila bën incizimin gjatë shtypjes se "pin code"-it, është më lehtë. Gjithashtu, krijuesit e këtyre pajisjeve, vendosin disa pjesë shtesë për leximin e këtyre, që, edhe nëse

arrihet sekuestrimi i këtyre pajisjeve, të mos ketë mundësi të leximit nga ana e zyrtarëve policorë.

Kartat bankare, gjithashtu mund të keqpërdoren nga keqbërësit, të cilët krijojnë programe ose skripte[1] të ndryshme dhe ua dërgojnë klientëve të ndryshëm kinse rastësisht, ku ata duhet të japin të dhënat e tyre, për të marrë pjesë në ndonjë lojë shpërblyese ose për ndonjë arsye tjetër. Kjo dukuri, njihet ndryshe në teknologjinë informative, edhe si *phishing* [2], dhe dëmet materiale nga kjo dukuri janë shumë të mëdha. Kohët e fundit, viktima të këtyre mashtrimeve kanë rënë një numër i madh njerëzish, të cilët përdorin kartat e tyre dhe sistemin *e-Banking*. Ky lloj mashtrimi është i quajtur edhe si *Nigerian Letter*. Shumë njerëz zgjedhin të bëjnë blerje *online* sepse mund të gjejnë oferta më të mira apo për të shmangur radhët e gjata. Fatkeqësisht, ka ueb-faqe të cilat përpiqen të bëjnë mashtrime të ndryshme duke shitur produkte joorigjinale, duke vjedhur informacionet e kartës së kreditit, apo duke mos dërguar asgjë nga ato që blihen.

Zakonisht, duhet pasur parasysh që kur të zgjidhet një ueb-faqe për të blerë produktet e dëshiruara, duhet pasur kujdes nga ato ueb-faqe të cilat ofrojnë çmim shumë më të ulët se sa ueb-faqet e tjera. Mbase arsyeja e këtij çmimi kaq të ulët është se, pasi të keni bërë blerjen, ju vjen me postë një produkt joorigjinal, i vjedhur ose asgjë fare.

Disa të dhëna që tregojnë që një ueb-faqe është e rreme, janë:

- nuk ka një numër telefoni që mund ta përdorni në lidhje me blerjen apo për të bërë pyetje;

- emri i *domain*-it të ueb-faqes ndryshon nga emri i *domain*-it që përdor për adresat e *email*-it apo kontakteve të tjera;

- ueb-faqja është e shkruar keq apo me gabime;

- ueb-faqja është kopje ekzakte e një ueb-faqeje të njohur, që keni përdorur në të kaluarën, por emri i *domain*-it të ueb-faqes ose vet emri i ueb-faqes është ndryshe.

Duhet pasur parasysh që, edhe pse faqja e internetit duket profesionale, nuk do të thotë që është e ligjshme. Nëse vetëm një aspekt i ueb-faqes duket i çuditshëm, duhet

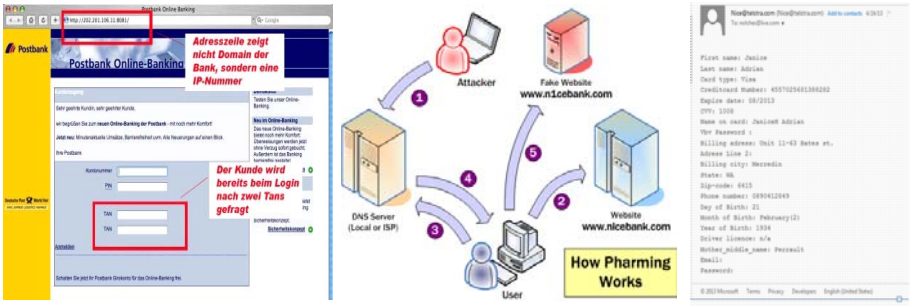



**Figura 4: Ueb-faqe mashtruese për vjedhjen e të dhënave.**

[1] Skript / "scripting", Një virus *web scripting* është një lloj i sigurisë kompjuterike përmes faqeve që thyen sigurinë e shfletuesit e internetit. Kjo lejon që sulmuesit të injektojnë skriptimin në anën e klientit në faqen e internetit. Ajo mund të anashkalojë kontrollet e qasjes, të vjedhë informacionin tuaj nga shfletuesi juaj i internetit.

[2] "Phishing", është akti mashtrues i marrjes së informacioneve private dhe të ndjeshme, të tilla si numrat e kartave të kreditit, identifikimi personal dhe emrat e përdoruesve të llogarisë dhe fjalëkalimet. Duke përdorur një grup kompleks të teknikave të inxhinierisë sociale dhe ekspertizës së programimit kompjuterik, faqet e internetit të *phishing* tërheqin pranuesit e postës elektronike dhe përdoruesit e internetit duke besuar se një faqe interneti e mashtruar është e ligjshme dhe e vërtetë. Në fakt, viktima *phishing* më vonë zbulon identitetin e tij personal dhe informacione të tjera jetike janë vjedhur dhe ekspozuar.

shikuar çdo detaj tjetër me shumë kujdes. Për shembull, te pjesa "kontakt" mund të merret numri i telefonit dhe të konfirmohet nëse është i vlefshëm. Mund të bëhet kërkimi i emrit të ueb-faqes apo URL-së së saj në një motor kërkimi, dhe mund të shohim se çfarë kanë thënë persona të tjerë për atë ueb-faqe në të kaluarën.

Nëse ka ende dyshime që kjo ueb-faqe nuk është e ligjshme, atëherë është më mirë të përdoret një ueb-faqe e besueshme mundësisht, të cilën ju, familja apo miqtë tuaj e kanë përdorur në të kaluarën. Çmimet mund të mos jenë aq të mira, por do të merrni një produkt më të besueshëm dhe do të jetë më pak e mundur që t'ju mashtrojnë.

## 3. Siguria e kompjuterit prej nga bëhet blerja

Përveç blerjes në ueb-faqe të ligjshme, duhet siguruar që kompjuteri i cili përdoret për blerje *online* të jetë i sigurt. Nëse kompjuteri është i infektuar, një kriminel kibernetik diku në botë, mund të identifikojë shtypjet e butonave në tastierë dhe mund të marrë gjithashtu informacionet tjera të rëndësishme. Kjo do ta mundësonte të përdorë emrin e përdoruesit të kompjuterit dhe fjalëkalimin për blerje *online*, apo të merrte informacion mbi kartën e kreditit dhe informacion bankar, si dhe të dhëna të tjera të tjera konfidenciale.


Figura 5: Kompjuter të zakonshëm.

Pra, duhet siguruar që kompjuteri të cilin e përdorim të jetë i kontrolluar dhe i lidhur me një rrjet të sigurt. Kjo do të thotë që së paku të kemi të instaluar përditësimet më të fundit mbi sigurinë dhe një program të përditësuar antivirus. Zakonisht nëse në shtëpi kemi fëmijë, do të ishte mirë të kishim dy kompjuterë, një për fëmijët dhe një për të rriturit. Fëmijët janë shumë kureshtarë për shfrytëzimin e teknologjinë, dhe si rrjedhojë, mund ta infektojnë kompjuterin. Nëse përdorim një kompjuter tjetër vetëm për transaksione *online*, si *e-banking* dhe blerje, ulim rrezikun e infektimit të kompjuterit tonë. Nëse nuk është e mundur të kemi dy kompjuterë, atëherë së paku duhet të kemi llogari të ndryshme dhe të sigurohemi që fëmijët ose të tjerët që hyjnë në kompjuterin tonë të mos kenë të drejta administrimi.

Përveç, sigurisë së kompjuterit personal, duhet siguruar gjithashtu, që dalja në internet të jetë po aq e sigurt. Pra, për një rrugëtim të sigurt në internet përdoren shumë protokolle që sigurojnë punën tonë dhe blerjen tonë në internet.

## 4. Pagesat, blerjet *online*

Pagesat *online* mund të bëhen duke përdorur dy sisteme kryesore: sistemi i të hollave

në sportele të institucioneve financiare, si për shembull, banka dhe sistemi i llogarive elektronike.

Sistemi i bazuar në llogari, lejon pagesën nëpërmjet një llogarie ekzistuese të personalizuar (zakonisht një llogari bankare), ndërsa sistemi i të hollave elektronike, lejon pagesën, thjeshtë nëse paguesi ka sasinë e duhur së të hollave elektronike. Më pas, ekzistojnë disa forma të ndryshme të pagesave *online,* përmes sistemit të bazuar në llogari: kartat e kreditit, kartat e debitit, sistemet e ndërmjetësimit, pagesa përmes celularit, duke përdorur llogarinë *e-banking* dhe pagesat përmes sistemit bankar *online*.

Mirëpo, më së shumti përdoret mënyra e pagesës përmes kartës së kreditit dhe kartës së debitit. Pasi vendosim që të bëjmë blerje nëpërmjet kartës së kreditit, ne duhet të tregohemi të zgjuar. Kjo do të thotë, që të kontrollojmë faturën e kartës së kreditit për të identifikuar pagesat e dyshimta. Fatura duhet kontrolluar të paktën një herë në muaj. Disa ofrues të kartave të kreditit ofrojnë edhe mundësinë e njoftimit me *email* apo mesazh në telefon në rast pagese nga karta, ose nëse është bërë një pagesë mbi një shumë të caktuar.

Kështu që, nëse ne mendojmë se gjatë pagesës na kanë mashtruar, atëherë mund të kontaktojmë ofruesin tonë të kartës dhe të shpjegohemi me të, për problemet që kemi hasur. Nga kjo gjë, del edhe arsyeja që është më mirë që të përdorim një kartë krediti, për blerje *online,* se sa një kartelë debiti. Sepse me kartat e debitit marrin paratë direkt nga llogaria bankare, dhe në rast mashtrimi, është shumë më e vështirë për të rimarrë paratë.

Së fundi, përdoren edhe disa karta krediti që ofrojnë mundësinë e krijimit të një numri unik për çdo blerje *online* ose ndoshta mund të përdorin shërbime si *PayPal* ku nuk duhet të ekspozohet karta e kreditit për çdo blerje *online*.

Përdorimi i kartelës së kreditit për blerje *online,* shton rrezikun që informacione delikate të kompromentohen, të vidhen ose të përdoren për të bërë blerje nga një palë e tretë, e paautorizuar. Ndaj gjithmonë duhet pasur parasysh që kartelën e kreditit, ta përdorim vetëm në ueb-faqet e sigurta që kanë prefiksin "*https*". Shkronja "s" në fund tregon se faqja që është përdorur, në esencë përdor një protokoll të sigurt për të enkriptuar komunikimin e informacionit në mes nesh dhe ueb-faqes. Ky protokoll përdoret në faqet *online* të bankave dhe faqet e blerjeve, të cilat llogariten që përmbajnë informacione të ndjeshme. Nëse nuk shikohet ky prefiks, atëherë shanset që të dhënat tona të rrezikohen, janë tepër të larta.

## 5. Siguria gjatë përdorimit të kartelës bankare për pagesa në POS-terminale

Gjatë përdorimit të kartelës në POS-terminale, duhet të kemi shumë kujdes pasi ekzistojnë pajisje shumë të vogla, për të cilat klonimi i kartës tonë mund të jetë shumë i lehtë dhe i thjeshtë. Mjafton që karta jonë, të kalojë nëpër shiritin magnetik të pajisjes për leximin e shiritit magnetik.

Kartat të cilat keqpërdoren ditët e sotme, janë kryesisht kartat amerikane dhe australiane pasi standardi në këto shtete ju mundëson përdorimin e kartave pa "pin code" dhe klonimi i këtyre kartave është shumë i thjesht nga keqbërësit. Ndërsa kartat, të cilat kanë një siguri më të madhe se ato me *chip* është shumë më e vështirë të klonohen dhe më pas të keqpërdoren, pasi keqbërësi duhet të ketë shumë më shumë të dhëna, për ta bërë një kartë të klonuar funksionale. Kartat bankare mund të klonohen

Figura 6: MSR (pajisje elektronike)

nga një MSR e cila bënë leximin e shiritit magnetik dhe më pas mund edhe të shkruhet në atë shirit magnetik të asaj kartele bankare.

## 6. Funksionimi i një grupi kriminal dhe rolet e anëtarëve gjatë klonimit të kartave bankare dhe përdorimit të tyre – praktika nga hetimet e rasteve

Secili nga anëtarët e një grupi kriminal, i ka të ndara rolet gjatë sigurimit së të dhënave të kartave bankare, klonimit të tyre dhe përdorimit të tyre në treg, ose për të kryer blerje me ato karta. Disa nga anëtarët e këtyre grupeve kriminale, kanë për detyrë sigurimin e të dhënave nga interneti duke klonuar ueb-faqe të ndryshme, duke dërguar reklama të ndryshme në *email*-e njerëzve të zakonshëm. Sigurimin e këtyre *email*-ve e bëjë në mënyra të ndryshme, duke sulmuar dyqane *online* që kanë adresa *email* të klientëve të tyre si dhe të dyqaneve me serverë ose me të dhëna të klientëve, të cilët kanë karta të lojalitetit, ku shumica nga këta klientë kanë të plotësuar të dhënat si: *email* dhe numër telefoni. Zakonisht, këta më pas pranojnë *email*-e, me reklama po nga këto biznese. Gjithashtu, klonime u bëhen edhe ueb-faqeve të bankave. Këto ueb-faqe bëhen aq mirë në dizajn, sa që klientët e kanë shumë të vështirë për ta vërejtur se kjo ueb-faqe nuk është një origjinale, e bankës ku ata janë klientë, dhe më pas, klientëve u kërkohet që ata t'i konfirmojnë të dhënat e tyre bankare. Shumica nga këta klientë, nga mungesa e njohurive të këtyre mashtrimeve *online*, i japin ato të dhëna të cilat kërkohen, pa e kontaktuar bankën e tyre, dhe me pas, bien pre e mashtrimeve të ndryshme ku ato karta, përdoren për qëllime të ndryshme.

Hakerët këto *email*-e i dërgojnë në grupe shumë të mëdha, duke përdorur serverë të ndryshëm, të cilët ju mundësojnë për të dërguar viruse *spam*[3]. Klientëve, pasi i pranojnë këto *email*-e, u kërkohet që t'i plotësojnë disa të dhëna e zakonisht këto të dhëna janë të dhëna bankare që kërkohet për tu plotësuar. Hakerët pasi t'i sigurojnë këto të dhëna të kartave bankare, ati u epen anëtarëve të tjetrë të grupit, të cilët e kanë për obligim klonimin e këtyre kartave bankare, me pajisje të ndryshme ose me pajisjen e cila zakonisht përdoret për klonimin ose mbishkrimin e këtyre kartave banke, pajisje kjo, që njihet

[3] SPAM - Spam i referohet përdorimit të sistemeve të mesazheve elektronike për dërgimin e mesazheve të padëshiruara ose të padëshiruara në masë.

me emrin MSR[4]. Pasi të shkruhen këto të dhëna në shiritin magnetik të kartave bankare dhe ato të jenë funksionale, të gatshme për përdorim, ato ju kalojnë anëtarëve të tjerë të grupit që kanë për detyrë t'i përdorin ato në dyqane (shitore) të ndryshme, për të kryer blerje me ato karta te klonuara (falsifikuara) bankare.

Pasi të kryhet blerja e mallit me karta të klonuara, anëtarët e këtij grupi të cilët janë përgjegjës për shitjen e këtij malli të blerë, e shesin atë mall, dhe të hollat të cilat i kanë fituar nga kjo veprimtari kriminale, i ndajnë varësisht nga funksioni anëtarëve të grupit. Padyshim, që rolin më të madh në grup, e kanë anëtarët të cilët sigurojnë të dhënat e kartave bankare *online* duke krijuar dhe përdorur viruse të ndryshme.

Lidhur me të dhënat e siguruara të kartave, hakerët tani kanë gjetur një mënyrë për t'ua vështirësuar punën e hetuesve të këtyre veprave, duke përdorur adresa IP të ndryshme, ose duke përdorur softuer të ndryshëm që bëjnë ndërrimin e adresave IP në kohë të ndryshme dhe e fshehin vendndodhjen hakerëve. Ata porositin *online* sende të ndryshme dhe i dërgojnë në adresa të ndryshme, ose shpeshherë edhe në adresat e tyre reale. Mirëpo disa nga bizneset të cilat operojnë *online,* tani kërkojnë edhe verifikimin e këtyre pagesave qoftë me email ose në forma tjera.

## 7. Mashtrimet e bizneseve dhe pagesat që bizneset i kryejnë *online*

Në ditët e sotme, shumica e bizneseve, për t'i kryer shërbimet e tyre dhe për ta ulur koston e transferimit në sportele bankare, duke kursyer kohën dhe siguruar mallin në kohë sa më të shkurtër e me kosto sa më të lirë, shumicën e shërbimeve janë duke i kryer *online*. Gjatë këtyre pagesave, këto biznese nuk marrin parasysh kërcënimet të cilat ju vijnë nga përdorimi jo i sigurt i internetit dhe nga mungesa e përvojës. Sot, bizneset u kushtojnë shumë pak rëndësi teknologjisë informative apo edhe vetë pajisjeve teknologjike të cilat i përdorin. Sot bizneset janë duke u mashtruar në masë të madhe, ata janë duke rënë pre e mashtruesve *online* duke bërë pagesa në mënyrë jo të sigurt. Bizneset fillimisht janë duke u shënjuar në mënyra të ndryshme dhe më pas duke u infektuar me viruse të llojeve të ndryshme (*malwer* [5], *spam*, *key loger* [6] etj.), pasi bizneset infektohen atyre ju merret komplet qasja (kontrolli) i kompjuterit dhe adresave *email* të cilat ata i përdorin për të kryer pagesa partnerëve të cilëve ata bashkëpunojnë.

Në këto ndërhyrje, fillimisht krijohen *email-e* të paverifikuara nga ueb-sajte të ndryshme ose edhe duke e ndërruar një shkronjë të vetme në email, si për shembull: agron@gmail.com në: agr0n@gmail.com. Pasi të merret kontrolli nga hakerët në *email* ata ndërhyjnë dhe bëjnë ndryshimin e faturës të cilën veç biznesi e ka pranuar në *email*. Në fatura, ndërhyhet kryesisht duke ndërruar *SIFT Code* si dhe numrin e llogarisë

[4] MSR - Magnetic Stripe Reader, Një lexues me shirit magnetik është një pajisje e dizajnuar për të lexuar informacionin e depozituar brenda shiritit magnetik të kartave të posaçme si kartat e kreditit të cilat përdoren në ATM. Shirit magnetik zakonisht gjendet në anën e pasme të kartës ose simbolit dhe përmban detajet e llogarisë së personit që zotëron kartën. Ky informacion pastaj vërtetohet në kohë reale me emetuesin e kartës.

[5] MALWARE - Malware ose softuer me qëllim të keq, është ndonjë program ose skedar që është i dëmshëm për një përdorues kompjuteri. Malware përfshin viruset kompjuterike, krimbat, kuajt e Trojës dhe spyware. Këto programe me qëllim të keq mund të kryejnë një sërë funksionesh, duke përfshirë vjedhjen, encryptimin ose fshirjen e të dhënave të ndjeshme, ndryshimin ose rrëmbimin e funksioneve bazë të informatikës dhe monitorimin e aktivitetit kompjuterik të përdoruesve pa lejen e tyre

[6] KEY LOGGER - Një keylogger është një teknologji që ndjek dhe regjistron goditje të njëpasnjëshme të tastierës. Për shkak se informatat e ndjeshme si përdoruesit dhe fjalëkalimet futen në tastierë, një keylogger mund të jetë një teknologji shumë e rrezikshme. Keyloggers shpesh janë pjesë e malware, spyware ose një virus i jashtëm.

bankare; kryesisht për këto raste janë përdorur llogari nga shtete të ndryshme si: Poloni, Angli, Rumani e vende të tjera.

Është shumë i vështirë kthimi i mjeteve sepse bizneset zakonisht e vërejnë këtë gjë, shumë kohë më vonë, - përafërsisht një muaj kohë. Më pas, është shumë e vështirë që të kthehen mjetet mbrapa nga këto mashtrime, sepse ato mjete të cilat janë transferuar ndahen në shumë llogari të tjera *online*, me llogari *e-Banking*, dhe është i pamundur kthimi i tyre sepse ato, shumë shpesh përfundojnë në vende të tilla, si Nigeria, Vietnami dhe vende tjera, ku nuk ka mbulesa sigurimi bankar. Një nga faqet të cilat janë përdorur një kohë të gjatë nga hakerët për të krijuar *email*-e të kësaj natyre, për t'i mashtruar bizneset, ka qenë *www.emkei.cz* ; dhe sigurimi i të dhënave, është shumë i vështirë pasi kompania nuk shkëmben të dhëna.

Mashtrime të kësaj natyre janë gjithnjë e më të theksuara. Në vendin tonë ka disa biznese të cilat kanë rënë prè e këtyre mashtrimeve. Punonjësit që janë përgjegjës për financën dhe që komunikojnë me partnerë të ndryshëm për kryerjen e pagesave, nuk i kushtojnë rëndësi *email*-ve me bashkëngjitje të dokumenteve të ndryshme, e që në shikim të parë, janë si dokumente të zakonshme, mirëpo ato janë dokumente të infektuar me virus, ku më pas merret edhe kontrolli i kompjuterit dhe bëhet monitorimi i vazhdueshëm i komunikimeve. Mungesa e njohurive dhe mungesa e programeve kompjuterike, si antivirus, gjithashtu edhe përditësimi i tyre, është shumë i theksuar. Hakerët presin momentin e caktuar të komunikimeve, ndërmjet bizneseve dhe ndërhyjnë me programe speciale dhe bëjnë ndryshimin e të dhënave bankare në faturën të cilën e kanë të bashkangjitur në *email*. Zyrtarët që kryejnë këtë komunikim, edhe pse kanë një kohë të gjatë bashkëpunimi me kompaninë, nuk kontaktojnë qoftë edhe përmes telefonit, ose ndonjë faksi, për konfirmim nga kompania: nëse është bërë ndërrimi i të dhënave të llogarisë bankare. Por, ata kryejnë pagesën pa konfirmim shtesë. Gjithashtu, ata nuk i kushtojnë rëndësi shikimit të *email*-ve me të cilët kanë komunikuar se mos është ndonjë ndryshim eventual në adresa *email*-i ose në tekstin e shkruar, ku shpeshherë hakerët e bëjnë përkthimin në ueb-faqe të ndryshëm, sepse nuk kanë njohuri të mjaftueshme të gjuhës.

Të dhënat të cilat mbesin si dëshmi për hetimin e këtyre rasteve, janë të dhënat ne *header*-in e adresës së *email*-it, e cila është përdorur për mashtrim dhe shkëmbim të *email*-ve. Në *header* mund të gjenden të dhënat për *email*-in si dhe rruga e përshkruar nga ai *email*, si:

- adresa IP,
- data dhe koha e dërgimit të *email*-it;
- *Mail server* i kompanisë dërguese,
- ID-ja e mesazhit.

Të gjitha këto informata ndihmojnë në identifikimin e krijuesit dhe dërguesit të një *email*-i te pranuesi (nga pika A tek B). Disa kompani kanë ndërruar politikat e tyre të funksionimit dhe të sigurisë, duke mos treguar burimin e dërguesit (adresën IP), mirëpo vendosin një adresë IP të rrjetit të brendshëm të tyre (IP private) të kompanisë. Me këtë veprim, kompanitë në fjalë, e vështirësojnë hetimin dhe zgjatin gjurmimin për identifikimin te dërguesit të këtij *email*-i mashtrues.

## 8. Përfundimi

Në këtë punim u përshkruan, në mënyrë të shkurtër disa nga rreziqet dhe se si

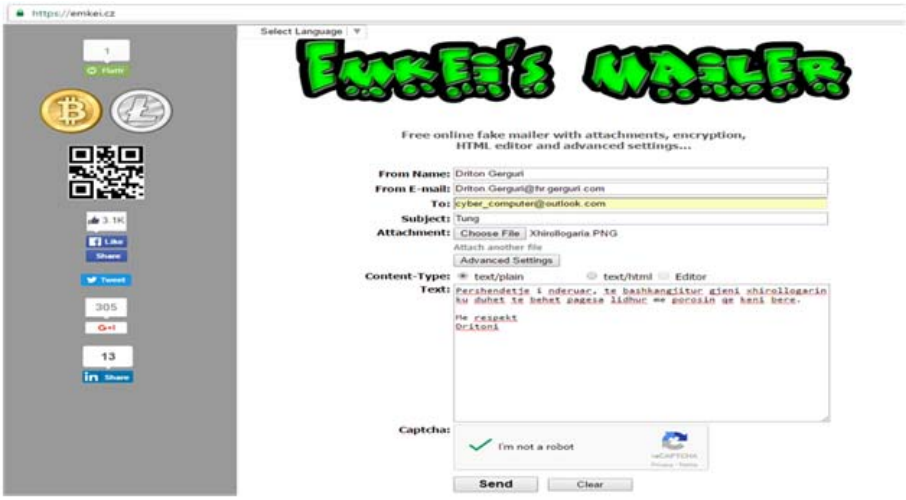



**Figura 7: Ueb faqe e *emkei.cz***

```
Header Email - Notepad
File  Edit  Format  View  Help
Received: from VI1PR08MB0317.eurprd08.prod.outlook.com (10.162.12.12) by
 AM2PR08MB0307.eurprd08.prod.outlook.com (10.161.235.144) with Microsoft SMTP
 Server (TLS) id 15.1.447.15 via Mailbox Transport; Wed, 30 Mar 2016 08:51:04
 +0000
Received: from HE1PR08CA0035.eurprd08.prod.outlook.com (10.161.112.45) by
 VI1PR08MB0317.eurprd08.prod.outlook.com (10.162.12.12) with Microsoft SMTP
 Server (TLS) id 15.1.447.15; Wed, 30 Mar 2016 08:51:03 +0000
Received: from HE1EUR01FT047.eop-EUR01.prod.protection.outlook.com
 (2a01:111:f400:7e1f::208) by HE1PR08CA0035.outlook.office365.com
 (2a01:111:e400:5097::45) with Microsoft SMTP Server (TLS) id 15.1.447.15 via
 Frontend Transport; Wed, 30 Mar 2016 08:51:02 +0000
Received: from SNT004-MC1F40.hotmail.com (10.152.0.55) by
 HE1EUR01FT047.mail.protection.outlook.com (10.152.1.5) with Microsoft SMTP
 Server (TLS) id 15.1.453.6 via Frontend Transport; Wed, 30 Mar 2016 08:51:01
 +0000
Received: from emkei.cz ([46.167.245.72]) by SNT004-MC1F40.hotmail.com with Microsoft SMTPSVC(7.5.7601.23143);
         Wed, 30 Mar 2016 01:50:59 -0700
Received: by emkei.cz (Postfix, from userid 33)
        id 50751D5665; Wed, 30 Mar 2016 10:55:39 +0200 (CEST)
To: "GjokÃ« Gashi" <el-com@hotmail.com>
Subject: R: Ordine OV16-01127
From: Elena - Metalli Stampati Cavaletto <elena@cgcavaletto.com>
Errors-To: elena@cgcavaletto.com
Reply-To: Elena - Metalli Stampati Cavaletto <elena@cgcaveletto.com>
Content-Type: text/html; charset="utf-8"
Message-ID: <20160330085540.50751D5665@emkei.cz>
Date: Wed, 30 Mar 2016 10:55:39 +0200
Return-Path: elena@cgcavaletto.com
X-OriginalArrivalTime: 30 Mar 2016 08:50:59.0276 (UTC) FILETIME=[47DFB8C0:01D18A61]
X-MS-Exchange-Organization-Network-Message-Id: 80d7fa31-6670-48fa-42a4-08d358786c7d
X-EOPAttributedMessage: 0
X-EOPTenantAttributedMessage: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0
X-MS-Exchange-Organization-MessageDirectionality: Incoming
CMM-sender-ip: 46.167.245.72
CMM-sending-ip: 46.167.245.72
CMM-Authentication-Results: hotmail.com; spf=none (sender IP is
 46.167.245.72) smtp.mailfrom=elena@cgcavaletto.com; dkim=none
 header.d=cgcavaletto.com; x-hmca=none header.id=elena@cgcavaletto.com
CMM-X-SID-PRA: elena@cgcavaletto.com
CMM-X-AUTH-Result: NONE
CMM-X-SID-Result: NONE
CMM-X-Message-Status: sF:n
CMM-X-Message-Delivery: Vj0xLjE7dXM9MDtsPTA7YT0wO0Q9MTtHRD0xO1NDTD0w
CMM-X-Message-Info: NhFq/7gR1vQ7S/L7wqKE599fDfWBE2gsWAH+hCnN9tPNigoUYTXGjj0dAWoc2FLGcGryS4/RaU72OYINOuUQTZK8jNxAMHE1MA
+cNLnBnS3AoafNppoIpIrfG9QNF0VHRJV3MzoWpwcZ6tP10S0e5QYo8O7qVzWPwNEHxO/e+RgjIURjcpwM=
```

**Figura 8: Header nga email-i i dërguar nga *emkei.cz*.**

klonohen kartat tona, si në bankomat, në POS gjatë blerjeve *online* si dhe disa nga mundësitë e shmangies së atyre rreziqeve. Pra, kuptuam që, së pari, gjatë hulumtimit në internet për blerje të ndryshme, ne mund të biem prè e ueb-faqeve të ndryshme dashakeqe, të cilat mund të na mashtrojnë në lidhje me produktet të cilat dëshirojmë t'i blejmë, më lirë dhe me cilësi më të lartë. Kështu, kuptuam që është më mirë të blejmë një produkt nga një ueb-faqe që e kemi përdorur më herët, edhe pse çmimi është më i lartë.

Është më mirë që të bëhen blerje me kartë të krediti, se sa me kartë debiti. Sepse me kartë krediti, mundësia e kthimit së të hollave nga ndonjë mashtrim, është më e madhe në krahasim me blerjet me karta të debitit të cilat i marrin të hollat drejtpërdrejtë nga llogaria jonë bankare. Gjithashtu, të dhënat tona të ndjeshme, si detajet e kartës së kreditit, asnjëherë mos t'i shkruajmë në një ueb-faqe e cila nuk përdor nivelin e sigurisë "https".

Përveç këtyre mashtrimeve, në të cilat mund të biem prè pa dashje, e rëndësishme është që edhe kompjuteri prej të cilit bëjmë blerje, të jetë i sigurt. Ai duhet të përdorë antivirus të ndryshëm si dhe duhet të jetë i përditësuar, si dhe gjatë përdorimit të bankomatit, të vendosim dorën gjatë kohës kur shtypim kodin tonë, e jo ta pështpëritim atë me zë, pasi pajisjet e përdorura nga keqbërësit shpeshherë kanë edhe mikrofona.

## Bibliografia


1. Ligj për parandalimin dhe luftimin e krimit kibernetikë ligji nr. 03/l-166.
2. Council of europe electronic evidence guide, 20 july 2012.
3. Raste nga praktika e hetimeve.
4. http://www.techopedia.com/definition/2387/cybercrime.
5. https://www.techopedia.com/definition/1716/spam.
6. https://www.techopedia.com/definition/14458/magnetic-stripe-reader.
7. https://www.investopedia.com/terms/a/atm.asp.
8. https://www.techopedia.com/definition/26649/point-of-sale-terminal-pos-terminal.
9. http://touque.ca/EC/students/DubeyR/ics_minor_project.html.
10. https://searchsecurity.techtarget.com/definition/malware.
11. https://www.techopedia.com/definition/4000/keylogger.

# Krimi kibernetik dhe mbrojtja e konsumatorëve

■**Prof. Asc. Dr. Ersida TELITI**
*Fakulteti i Drejtësisë, Universiteti i Tiranës*
*ersida.teliti@fdut.edu.al*

■**MSc. Ketjona KAÇUPI**
*Qendra "Konsumatori shqiptar"*
*ketjonakacupi@gmail.com*

**Abstrakt**

*Zhvillimi i teknologjisë së informacionit dhe bota e internetit kanë thyer rregullat dhe kufijtë e tregtisë së brendshme dhe tradicionale. Në ditët e sotme, përgjigjet në kohë reale, blerjet si dhe kontaktet mundësohen nëpërmjet internetit.*

*Ka lindur dhe është zhvilluar koncepti i konsumatorit virtual, i cili realizon blerje si dhe kryen pagesa drejtpërsëdrejti nga interneti. Kontratat elektronike janë kontratat tipike, me palë shitës dhe blerës, që nuk e njohin njëri – tjetrin por kryejnë transaksione financiare. Të gjithë këto veprime juridike të kryera online kanë krijuar një sërë problemesh në fushën e mbrojtjes së të drejtave të konsumatorëve. Në këtë marrëdhënie juridike, konsumatori është pala më e dobët, si nga pikëpamja e pushtetit, informacionit dhe sigurisë. Për pasojë krimi kibernetik drejtohet tek ai, ndonëse pala që synohet të jetë drejtpërdrejtë është tregtari. Duke dëmtuar konsumatorin, nëpërmjet kësaj vepre penale, cenohet imazhi dhe siguria e tregtarit.*

*Ky artikull do të trajtojë në këndvështrimin teorik dhe praktik, krimin kibernetik dhe ndikimin e tij tek konsumatori, cenimi i të dhënave personale, shfrytëzimi i tyre, si dhe pasiguria e konsumatorit në tregtinë online. Një vëmendje e veçantë do t'i kushtohet kuadrit ligjor shqiptar, si dhe hapësirave ligjore, në aspektin civil dhe penal.*

*Në përfundim të punimit, autorët do të japin rekomandimet përkatëse për përmirësimin e kuadrit ligjor dhe institucional për të krijuar në mjedis sa më të sigurt për konsumatorin virtual në Shqipëri.*

**Fjalëkyçe:**

**konsumator, krim kibernetik, të dhëna personale, kontrata elektronike.**

"As the world is increasingly interconnected,
everyone shares the responsibility of securing cyberspace."
- Newton Lee.

## 1. Hyrje

Krimi kibernetik i referohet të gjitha veprimtarive kriminale të kryera nëpërmjet përdorimit të kompjuterëve, internetit dhe *world wide web*. Ende sot nuk ka një përkufizim për krimin kibernetik, por vetëm disa objektiva të parashikuara pothuajse nga çdo Kod Penal, të cilat synojnë mbrojtjen e informacionit, pajisjeve kompjuterike, kompjuterëve dhe çdo pajisjeje tjetër komunikimi nga aksesi i paautorizuar dhe përdorimi i padrejtë i tyre nga persona/individë që nuk kanë të drejtë ligjore për t'i përdorur, modifikuar apo edhe shkatërruar ato.

Zhvillimi i teknologjisë dhe përdorimit masiv të internetit, ka ndikuar në përhapjen e krimit kibernetik në të gjithë botën. Në ndryshim nga veprat e tjera penale, ky krim ka shtruar diskutime në lidhje më përcaktimin e shtetit i cili ka juridiksionin dhe kompetencën për të shqyrtuar këtë lloj vepre penale. Një gjë e tillë nënkupton që një transaksion i zakonshëm përfshin minimalisht tre juridiksione të ndryshme: a) ligji i shtetit në të cilin banon përdoruesi; b) ligji i shtetit në të cilin ndodhet server, me anë të së cilit realizohet transaksioni; si dhe c) ligji i shtetit, shtetësinë e të cilit ka personi/biznesi/konsumatori me të cilin realizohet transanksioni.

Hapësira kibernetike ndodhet nën presionin e spiunëve kibernetikë, vjedhësve së të dhënave personale (hakerave) dhe sekreteve tregtare; apo subjekteve të cilët

vandalizojnë faqet e internetit, shkatërrojnë apo modifikojnë të dhëna specifike apo sisteme të ndryshme, apo që kanë synim të realizojnë transaksione mashtruese në dëm të personave fizike apo juridike. Motivi më i zakonshëm i krimit kibernetik është përfitimi ekonomik, dhe rrallë herë kryhet për motive hakmarrjeje apo argëtimi. Rritja e përdorimit të internetit ka ndikuar në zhvillimin e mëtejshëm të tregtisë elektronike (e-commerce). Për konsumatorët, kryerja e transanksioneve në një kohë më të shkurtër, ulja e kostove të realizimit të tyre, si dhe shkurtimi i distancave është shoqëruar me rritjen e numrit të krimeve që realizohen nëpërmjet rrjetit kompjuterik, si: mashtrimet me kartat e kreditit, serverët bankarë, manipulimet e kompjuterëve, hakime të ndryshme, pastrimin e parave, etj.

Çdo ditë mund të identifikohen lehtësisht raste në të cilat kemi shitjen e produkteve të ndryshme, të cilat nuk plotësojnë kushtet minimale, të cilësisë, sasisë, apo karakteristika të tjera të kërkuara nga konsumatorët. Praktikisht është e vështirë për të kontrolluar apo parandaluar një person që nëpërmjet një faqe internet të tregtojë produkte të ndryshme, sidomos kur këto produkte mund të jenë substanca kimike të ndaluara, barna pa recetë, apo produkte që ndikojnë në përmirësimin e shëndetin e konsumatorëve. Kjo situatë paraqet rrezik potencial për jetën, shëndetin dhe sigurinë e konsumatorëve (pacientëve), të cilët gjenden në pamundësi për t'u informuar dhe mbrojtur interesat e tyre të ligjshëm përballë personave të cilët si qëllim kryesor kanë mashtrimin dhe përfitimin në mënyrë të padrejtë.

Dërgimi i një *email*-i, kryerja e një transferimi bankar, rezervimi i fluturimit *online*, realizohen gjithmonë e më lehtë dhe më shpejtë në ditët e sotme. Sa të sigurt janë konsumatorët përballë një veprimtarie të tillë, e cila është vështirë të kontrollohet nga institucionet publike shtetërore? Studimet tregojnë se konsumatorët ndihen gjithmonë e më të pambrojtur dhe të pasigurt në lidhje me mënyrën e përdorimit së të dhënave personale të tyre. Kjo sjell uljen e nivelit të besimit gjatë realizimit të transaksioneve të ndryshme me tregtarët mbi mënyrën se si ai (tregtari) mund të përdorë të dhënat përkatëse të konsumatorëve. Siguria Kibernetike merr një rëndësi themelore në ditët e sotme, ndikuar nga numri i lartë i shkeljeve së të drejtave nëpërmjet përdorimit të rrjetit kompjuterik. Cenimi i sigurisë kibernetike, përbën shqetësim jo vetëm për tregtarët, të cilët duhet të kujdesen për ta ruajtur këtë siguri nëpërmjet departamentit të tyre të IT-së; por njëkohësisht cenon konsumatorët, të cilët ndryshe nga tregtarët janë tërësisht të pambrojtur ndaj sulmeve të ndryshme kibernetike. Kjo kërkon një nivel më të lartë të mbrojtjes së të drejtave të konsumatorëve, duke ofruar më shumë siguri tek këta të fundit gjatë realizimit të transaksioneve në mënyrë elektronike. Synimi kryesor është gjetja e një ekuilibri midis rrezikut, risive në teknologji dhe kostove që sjell krimi kibernetik.



## 2. Fenomeni i krimit kibernetik dhe evolucioni i tij

Zhvillimi i teknologjisë ndikon paralelisht në rritjen e numrit të kërcënimeve në internet. Aktualisht nuk janë gjetur mënyra për të parashikuar kërcënimin e ardhshëm. Historia tregon ngjarje të rëndësishme të sigurisë kibernetike që kanë luajtur një rol të rëndësishëm në formësimin e botës së sotme dhe *World Wide Web.* Për herë të parë historia e *cybercrime* mendohet të ketë filluar në vitin 1964, kur AT&T spiunonte telefonata. Që atëherë, teknologjia ka bërë një rrugë të gjatë, ashtu dhe për përdoruesit[1].

[1] Hanif Mehmood, "A detailed history of cybercrimes", artikull, 25 tetor 2017. https://www.purevpn.com/blog/history-of-cybercrimes/

Teknologjia e sotme ka ecur në drejtim të mbrojtjes së privatësisë së përdoruesve të internetit, sigurisë dhe anonimitetit. Pavarësisht kësaj, duhet që përdoruesit e internetit të jenë inteligjentë dhe të përdorin teknologjinë për të mbrojtur veten kundër shumë të papriturave që ndodhen në rrugët e errëta në internet.

Fillesat e krimit kibernetik datojnë më herët se ekzistenca e internetit dhe përfshinin vjedhjen e të dhënave. Historia dhe evolucioni i krimit kibernetik janë të lehta për t'u ndjekur dhe përkojnë me evolucionin e vetë Internetit[2]. Krimet e para ishin natyrisht hakime të thjeshta për të informuar nga rrjetet lokale, por ndërsa përhapja e internetit u bë më e madhe dhe e shpejtë në kohë, të tilla u bënë edhe "sulmet" kibernetike[3].

Vala e parë e madhe e krimit kibernetik erdhi me përhapjen e email-it gjatë fundit të viteve 80-të. Një gjë e tillë lejoi që një mori mashtrimesh të dërgoheshin në postën elektronike të pothuajse çdo konsumatori[4]. Rritja e përdoruesve të internet-it gjatë viteve të mëvonshme ndikoi drejtpërdrejtë në rritjen e krimit kibernetik. Gjatë kësaj periudhe mbrojtja nga viruset kompjuterike ishte shumë e vogël, çka mundësonte dërgimin e tyre nëpërmjet lidhjeve të internetit duke shkaktuar ngadalësimin e kompjuterëve, dërgimin e reklamave të paautorizuara etj.

Në vitet '90-të, përhapja masive e *web browser* dhe *email*-it nënkuptonte përdorimin e mjeteve të reja për hakerat për t'u shfrytëzuar. Këto të fundit mund të transmetojnë kodin e virusit nëpërmjet internetit në këto përdorues të rinj, shumë të prekshëm, duke marrë atë që kishin mësuar më parë me synimin për ta përshtatur në mënyrë të tillë që të vepronin lirisht në internet, me rezultate shkatërruese[5]. Nuk ishte më e nevojshme për ta (hakerave) të angazhoheshin direkt me persona të veçantë, pasi mund të mashtronin miliona përdorues në të njëjtën kohë. Informacion i siguruar nga hakerat, i shoqëruar me mungesën e vetëdijes së sigurisë në internet nga publiku i gjerë lejoi ata që të kryejnë të gjitha llojet e mashtrimeve financiare si: hapja e llogarive bankare dhe karta krediti në emër të të tjerëve.

Në fillim të viteve 2000, kur media sociale erdhi në jetë dhe mori zhvillim, përhapja e krimit kibernetik u bë edhe më e madhe[6]. Mundësia për vjedhjen e të dhënave dhe informacionit personal, apo edhe rastet e vjedhjes së identiteteve të përdoruesve u bënë më të shpeshta, pasi tashmë hakerat kishim më shumë mundësi të realizonin qëllimin e tyre nëpërmjet hyrjes në llogaritë bankare të konsumatorëve, të kartave të kreditit, apo edhe nëpërmjet mashtrimeve të tjera financiare që realizoheshin lehtësisht nëpërmjet rrjetit kompjuterik. Kjo industri kriminale globale sjell një dëm të konsiderueshëm prej pothuajse gjysmë trilion dollar në vit, në të cilën hakerat zgjedhin të përdorin metoda të mirëpërcaktuara për të arritur përfitime personale maksimale nga kryerja e kësaj

[2] "Where Does Cyber Crime Come From? The origin and evolution of cybercrime". https://www.le-vpn.com/history-cyber-crime-origin-evolution/

[3] Gerhart Morgan, "The Evolution of Cybercrime and What It Means for Data Security", artikull, 27 korrik 2017 https://www.imperva.com/blog/2017/06/the-evolution-of-cybercrime-and-what-it-means-for-data-security/

[4] Për të vërtetuar këtë aspekt, vlen të përmendim mashtrimin e realizuar nga princi Nigerian, nëpërmjet dërgimit të email-eve në drejtim të konsumatorëve, për t'i mashtruar këta të fundit. Për më tepër:
*Nigerian Prince scam*:
"Greetings, I am a down-and-out prince from Nigeria. I need help getting millions out of my country and all you have to do is send me some money first to set-up the transfer. Once done I'll share my millions with you".

[5] Packt Editorial Staff, "The evolution of cybercrime", artikull, 29 mars 2018. https://hub.packtpub.com/the-evolution-cybercrime/

[6] "Where Does Cyber Crime Come From? The origin and evolution of cybercrime". https://www.le-vpn.com/history-cyber-crime-origin-evolution/

veprimtarie të paligjshme[7].

Doktrina vazhdimisht është përpjekur të japë një përkufizim të unifikuar në lidhje me termin krim kibernetik[8], por dhënia e një përkufizimi apo jo nuk përbën shqetësim për legjislacionet e ndryshme kombëtare, të cilët kryesisht përdorin termat "krime kompjuterike"[9], "komunikime elektronike"[10], "teknologji informacioni"[11], ose "krim i teknologjisë së lartë"[12]. Pavarësisht hapësirës në përkufizimin e termave, krimi kibernetik është një nga veprat penale të kohëve moderne që po tronditin shtetet dhe shtetasit e tyre.

## 4. Tregtia elektronike dhe krimi kibernetik

Zhvillimi i shoqërisë dhe industrisë elektronike ka nxitur forma të reja të tregtisë. Marrëdhënia juridike midis tregtarëve ndërmjet tyre, apo tregtar-konsumator nuk nënkupton domosdoshmërish praninë tipike të dy palëve. Tregtia elektronike kryesisht përbëhet nga tërësia e transaksioneve të tregtisë elektronik në lidhje me blerjen dhe shpërndarjen e mallrave dhe shërbimeve[13]. Autorë të ndryshëm pohojnë se a elektronike përfshin vetëm transferimin elektronik të parave, megjithatë duhet pranuar se kjo e fundit përfshin tërësinë e transaksioneve elektronike, qoftë blerje me çek, qoftë me telefon apo mjete të tjera elektronike. Tregtia elektronike përfshin tregtinë me pakicë në mes të biznesit dhe konsumatorët (B2C) si dhe tregtinë biznes-biznes (B2B)[14]. *E-commerce* tani është duke u përdorur në të gjitha llojet e biznesit, duke përfshirë kompanitë prodhuese, dyqanet e shitjes me pakicë, dhe firmat e shërbimit, duke i bërë proceset e biznesit më të besueshme dhe më efikase. Rrjedhimisht, tregtia elektronike është tani thelbësore për tregtarët që të jenë në gjendje të konkurrojnë në

[7] Për më shumë informacion rreth zhvillimit dhe përhapjes së krimit kibernetik në vite:
"- 1971 - *John Draper*, një *phone phreak*, zbuloi se një bilbil i dhënë si një çmim për konsumatorët në kutitë e *Cap'n Crunch Cereal,* prodhonte të njëjtin tingull si telefonat celularë. Duke kuptuar këtë gjë, John ndërton një *"blue box"*me fishkëllimë, që do i lejonte atij të realizonte thirrje falas në distance të largëta. Më pas botoi udhëzime se si të realizohej një mashtrim i tillë.
- 1973 - Një tregtar në një bankë lokale të Nju Jorkut përdori një kompjuter për të përvetësuar mbi 2 milionë dollarë.
- 1978 - Sistemi i parë elektronik i buletinit elektronik erdhi në internet dhe shpejt u bë një metodë e preferuar e komunikimit për botën kibernetike. Kjo lejoi shkëmbimin e shpejtë të njohurive, duke përfshirë këshilla dhe truket për *hacking* në rrjetet kompjuterike.
- 1981 - Ian Murphy, i njohur si kapiten Zap për tifozët e tij, ishte personi i parë i dënuar për një krim në internet. Ai hakoi rrjetin e brendshëm të "AT & T".
- 1982 - Elk Cloner, një virus, është krijuar si një shaka nga një fëmijë 15 vjeçar. Ky është një nga viruset e parë të njohur dhe më të përhapur, i cili sulmoi sistemet operative të Apple II dhe u përhap nga *floppy disk*.
- 1983 - Filmi i "Lojërave të Luftës", përshkruan një djalë adoleshent që hyn në një sistem kompjuteri qeveritar përmes një derë të pasme dhe gati e çon botën në Luftën e Dytë Botërore.
- 1986 - Kongresi kalon Aktin e Mashtrimit të Kompjuterit dhe Abuzimit, duke e bërë piraterinë dhe vjedhjen e paligjshme.
- 1988 - Robert T. Morris jr., një student i diplomuar në Cornell, lëshoi një *worm* vetëpërsëritur në Departamentin e Mbrojtjes APRANET. ARPANET është pararendës i internetit siç e njohim sot. *Worm-at* infektuan më shumë se 600 000 kompjuterë të lidhur në rrjet.
- 1989 - Rasti i parë i një numri të madh të *ransomware* që është raportuar. Virusi paraqitet si një quiz mbi virusin AIDS dhe pasi shkarkohej, mbante të dhëna kompjuterike peng për 500 dollarë. Në të njëjtën kohë një grup tjetër është arrestuar duke vjedhur të dhënat e qeverisë dhe të sektorit privat të SHBA dhe duke ua shitur ato KGB-së.
- 1990 - "Legjioni i dënimit" dhe "zotërinjve të mashtrimit", dy banda të bazuara në internet, angazhohen të fillojnë një luftë *online*. Ata në mënyrë aktive bllokojnë lidhjet e njëri-tjetrit, hakojnë kompjuterët dhe vjedhin të dhëna.
- 1993 - Kevin Poulson është kapur dhe dënuar për sulme në sistemet telefonike. Ai mori kontrollin e të gjitha linjave telefonike që shkonin në një stacion radio në LA për të garantuar fitimin e një konkurrimi në thirrje.
- 1994 - Është hapur World Wide Web, duke lejuar hakerat për të lëvizur informacionin e tyre mbi produktin nga

një treg global[15].

Me zhvillimin e teknologjisë së informacionit, një numër i madh konsumatorësh është ekspozuar ndaj rreziqeve të reja të cilat burojnë nga hapësira kibernetike. Ky zhvillim nuk ecën në të njëjtat ritme me mbrojtjen e konsumatorëve, duke ndikuar në përhapjen e krimit kibernetik. Në treg gjenden konsumatorë të frikësuar për t'iu drejtuar blerjeve *online*. Për të rregulluar këtë problem në treg, tregtarët të cilët zgjedhin t'i ofrojnë mallrat edhe shërbimet e tyre *online*, duhet të marrin të gjitha masat e nevojshme, në mënyrë të tillë që të rritin besimin e konsumatorit gjatë realizimit të blerjeve *online*. Masat e marra duhet të jenë në përputhje me respektimin dhe ruajtjen e të dhënave apo informacionit personal të konsumatorëve[16].

Një nga aspektet pozitive të tregtisë elektronike është promovimi nëpërmjet internetit të mallrave dhe shërbimeve të ndryshme. Studimet tregojnë se në momentin që konsumatorët shohin reklama të ndryshme *online*, ka një probabilitet të lartë që ata të bëhen pjesë e një blerjeje në internet. Kjo shpjegon arsyen pse tregtarët shpenzojnë shuma të konsiderueshme të hollash për të vendosur mesazhet e tyre promocionale në faqet e internetit me një numër të lartë klikimesh[17].

Një studim i Qendrës për Inovacionin e Qeverisjes Ndërkombëtare, në bashkëpunim me OKB- në, pohon se konsumatorët në mbarë botën po bëhen më të kujdesshëm ndaj transaksioneve në internet për shkak të rritjes së krimit në internet dhe shkeljeve të privatësisë. Përpos kësaj, edhe pse shqetësimet rreth rritjes së mashtrimit në internet janë shtuar ndjeshëm, nuk ka shenja se tregtia elektronike po ngadalësohet. Kjo ka çuar në një konkurrencë teknologjike për të luftuar krimin kibernetik pasi të dy palët, konsumatorët dhe tregtarët përballen me rreziqe të papërjetuara më parë[18]. Sa më

---

sistemet e vjetra të buletinit në faqet e tyre të internetit. Një student në Britani të Madhe përdor informacionin për të hakuar programin bërthamor të Koresë, NASA-s dhe agjencive e tjera të SHBA duke përdorur vetëm një kompjuter "Commodore Amiga" dhe një program "blueboxing" të gjetur në internet.

- 1995 - Shfaqen makroviruset. Makroviruse janë viruse të shkruara në gjuhët kompjuterike të përfshira brenda aplikacioneve, të cilat funksionojnë kur aplikacioni hapet, siç janë dokumentet e përpunimit të tekstit dhe që janë një mënyrë e lehtë për hakerët që të dorëzojnë *malware*. Kjo është arsyeja pse përhapja e të dhënave të panjohura në *email* mund të jetë shumë e rrezikshme. Macrovirus-et janë ende të vështirë për të zbuluar dhe janë një shkak kryesor i infeksionit kompjuterik.

- 1999 - "*Melissa Virus"* është lëshuar. Ajo bëhet infeksioni më i keq i kompjuterëve deri më sot, si një nga një makro-viruset e lëshuara me qëllim të vjedhjes së llogarive të postës elektronike dhe dërgimit të postimeve në masë.".

[8] "Comprehensive Study on Cybercrime", Draft, United Nations Office On Drugs And Crime, Vienna February 2013.

[9] Malaysia, Computer Crimes Act 1997; Sri Lanka, Computer Crime Act 2007; Sudan, Computer Crimes Act 2007.

[10] Albania, Electronic Communications in the Republic of Albania, Law no. 9918 2008; France, Code des postes et des communications électroniques (version consolidée) 2012; Tonga, Communications Act 2000

[11] India, The Information Technology Act 2000; Saudi Arabia, IT Criminal Act 2007; Bolivarian Republic of Venezuela, Ley Especial contra los Delitos Informáticos 2001; Vietnam, Law on Information Technology 2007.

[12] Serbia, Law on Organization and Competence of Government Authorities for Combating High-Tech Crime 2010.

[13] Collao Villanueva Vanessa; "I contrati conclusi in internet", Giuffre editore, Milano 2014, f. 165-170.

[14] Patel Mayur, Patel Neha, Ganatra Amit, Kosta Yogesh, "E-Commerce and Attached E-Risk with Cybercrime", Computer / Information Technology Department Charotar Institute of Technology, Charotar University of Science and Technology – Changa. At Changa-388 421, Ta Petlad, Dist Anand, article of 3 janary 2015.

[15] Për efekt të këtij punimi, do analizojmë vetëm ndikimit të krimit kibernetik në kontratat elektronike tregtar-konsumator.

[16] International Journal of Engineering Sciences & Emerging Technologies, October 2013. Volume 6, Issue 2, ©IJESET; Das Sumanjit, Nayak Tapaswini; "Impact of cyber crime: Issues and challenges", tetor 2013, f. 150.

[17] Kratchman, Stan, J. Smith, and L.M.Smith., Perpetration and Prevention of Cyber Crimes. Internal Auditing", Vol. 23, No. 2 (March-April), 2008, f. 3-12.

[18] Dautner Mike, "As ECommerce Accelerates, So Too Does The Risk Of Cyber Crime", artikull, 10 maj 2017. https://paymentweek.com/2017-5-10-as-ecommerce-accelerates-so-too-does-the-risk-of-cyber-crime/ "Shitjet në internet (*online*) në SHBA, janë duke u rritur me më shumë se 9 për qind në vit dhe janë planifikuar të arrijnë në 523 miliardë dollarë deri në vitin 2020. Një rritje pesëvjeçare prej 56 për qind, pa asnjë shenjë të rënies në numër të këtyre transaksioneve. Vetëm në SHBA, 90 për qind e të gjithë përdoruesve të internetit bëjnë të paktën një blerje në internet çdo muaj."

shumë të përhapet dhe fuqizohet tregtia elektronike dhe sa më shumë konsumatorë të bëhen pjesë e transanksioneve *online* për blerjen e mallrave dhe shërbimeve të ndryshme, aq më shumë rritet mundësia për mashtrimin në internet dhe përhapjen e krimit kibernetik[19].

Problematikat kryesore që lidhen me tregtinë elektronike, kryesisht në kontratat B2C, ku njëra nga palët e kontratës janë konsumatorët, të cilët për arsye të ndryshme zgjedhin të jenë pjesë e një kontrate të lidhur në mënyrë elektronike, mund të konsiderohen:

a) Siguria e pagesave në internet dhe celular. Kjo do të thotë se hakerat në këtë rast e kanë më të lehtë të ndikojnë nëpërmjet sistemeve të ndryshme komjuterike me qëllim vjedhjen e pagesave dhe rritjen e përfitimit material të tyre.

b) Siguria e të dhënave dhe mashtrimet në internet, vjedhjet e identitetit dhe mashtrimet.

c) Shërbimi ofrohet nga tregtarët anonim. Mosnjohja e palës tjetër të kontratës dhe mos krijimi i marrëdhënies së besueshmërisë ndërmjet palëve që marrin pjesë në kontratë, shton rastet, në të cilët në rolin e tregtarit anonim të qëndrojë një *hacker*, i cili i mbuluar nën maskën e tregtarit synon të rrisë përfitimin e tij duke përdorur rrjetin kompjuterik.

d) Mbrojtja e të dhënave personale dhe privatësisë[20].

Duke u nisur nga zhvillimet teknologjike dhe për t'iu përshtatur nevojave të reja, kuadri ynë ligjor për tregtinë elektronike është pasuruar në vazhdimësi me një sërë ligjesh dhe vendimesh[21]. Kjo pasi parimet dhe rregullat e të drejtës kontraktore tradicionale, rezultojnë jo të përditësuara për t'u përdorur për lidhjen e kontratave elektronike[22]. Sipas përkufizimit të dhënë nga ligji nr. 10128, datë 11.05.2009 "Për tregtinë elektronike", i ndryshuar, tregtia elektronike përkufizohet si:

*"kryerja nga subjektet e këtij ligji të një veprimtarie, nëpërmjet shkëmbimit të dokumenteve elektronike, për tregtimin e mallrave dhe/ose shërbimeve"*[23].

Pra, sipas këtij përkufizimi, çdo veprimtari për realizimin e tregtimit dhe shkëmbimit të mallrave dhe/ose shërbimeve nëpërmjet përdorimit të dokumenteve elektronike, përfshihet në sferën e tregtisë elektronike[24]. Qëllimi i ligjit është garantimi i të drejtave të palëve gjatë realizimit të transaksioneve *online*, si mënyrë e tërthortë mbrojtjeje edhe ndaj krimit kibernetik.

## 5. Mënyrat e shfaqjes së krimit kibernetik

Një numër të madh kontratash lidhen pothuajse çdo ditë mes konsumatorëve nga

[19] Si më sipër.
[20] United Nations Conference on Trade and Development, "Consumer protection in electronic commerce", 24 April 2017. http://unctad.org/meetings/en/SessionalDocuments/cicplpd7_en.pdf
[21] - Ligji nr. 10128, datë 11.05.2009 "Për tregtinë elektronike", i ndryshuar.
- Ligji nr. 10273, datë 29.04.2010 "Për dokumentet elektronike".
- Ligji nr. 9918, datë 19.05.2008 "Për komunikimet elektronike"/ i ndryshuar nga ligji nr. 102/2012, datë 24.10.2012 "Për disa shtesa dhe ndryshime në ligjin nr. 9918, datë 19.05.2008 "Për komunikimet elektronike".
- Ligji nr. 9880, datë 25.02.2008, " Për nënshkrimin elektronik", i ndryshuar nga ligji nr. 10178, datë 29.10.2009 "Për miratimin e aktit normative, me fuqinë e ligjit, nr. 8, datë 30.092009 të Këshillit të Ministrave "Për një ndryshim në ligjin nr. 9880, datë 25.02.2008, " Për nënshkrimin elektronik".
[22] Malltezi Argita, Rystemaj Jonida, Pelinku Lealba; "Aspekte të së drejtës së biznesit në Shqipëri", Mediaprint, Tiranë 2013, f. 476-485.
[23] Ligji nr. 10128, datë 11.05.2009 "Për tregtinë elektronike", i ndryshuar, neni 3.
[24] Malltezi Argita, Rystemaj Jonida, Pelinku Lealba; vep. e cit., f. 480.

njëra anë dhe tregtarëve nga ana tjetër nëpërmjet përdorimit të internetit. Një përhapje e madhe e këtyre kontratave favorizon edhe hakerat, të cilët nëpërmjet mashtrimeve të ndryshme arrijnë të nxjerrin përfitime të padrejta për vetën e tyre apo për të tretë, në dëm të konsumatorëve[25].

Sa të sigurta janë këto kontrata për konsumatorët? Sa të mbrojtur janë këta të fundit nga krimi kibernetik?

Informacioni që kemi për përhapjen e krimit kibernetik dhe shkeljen e të drejtave të konsumatorëve vjen kryesisht nga vëzhgimet e drejtpërdrejta të studiuesve. Ndonëse është e vështirë të përcaktohet me saktësi përqindja e konsumatorëve të prekur nga ky krim për shkak të mënyrës së realizimit të tij dhe vështirësisë që ekziston për rruajtjen e sigurisë në internet[26]. Në ditët e sotme pranohet që të paktën 0.4% e popullsisë bie "pre" e mashtrimeve *online* apo krimit kibernetik[27]. Janë realizuar shumë sondazhe për të bërë një vlerësim sa më konkret në lidhje me ndikimin e krimit kibernetik. Gjatë anketimit të konsumatorëve në mbarë botën, të realizuar nga *Symantec*, rreth 54% e tyre rezultojnë të kenë rënë pre e hakimeve të ndryshme përgjatë një viti[28].

Disa nga llojet më të përhapura të krimit kibernetik, të cilat më së shumti sjellin dëme tek konsumatorët janë:

a) vjedhja e identitetit dhe të dhënave personale në përgjithësi, duke u dhënë mundësi hakerave të hyjnë lirisht në llogaritë bankare të konsumatorëve të dhënat e të cilëve kanë përvetësuar në mënyrë të padrejtë;

b) vjedhja e *email*-ve dhe kërkimi i vlerave monetare të konsiderueshme për kthimin e tyre;

c) mashtrime të ndryshme në internet në lidhje me kontratat elektronike të lidhura, ku mallrat e blera nuk dorëzohen, ose nuk janë në cilësinë dhe sasinë e rënë dakord nga palët në momentin e lidhjes së kësaj kontrate;

d) pamundësia për të përdorur shërbime të ndryshme në internet, siç janë shërbimet bankare, për shkak të sulmeve kibernetike dhe hakimeve të ndryshme[29].

e) vjedhja e shërbimeve të telekomunikacionit. Të ashtuquajturit "phone phreakers"[30] janë ata që në mënyrë të padrejtë marrin të dhënat e konsumatorëve nga qarqet dial-in/deal-out, e më pas i përdorin ato për të dërguar thirrje vetë ose për t'i shitur këto të fundit. Ky lloj krimi shkon edhe më tej në momentin kur hakerat që kanë qasje në centralin përkatës, arrijnë të përvetësojnë nëpërmjet mashtrimit kodin e hyrjes së punonjësve përkatës, duke përdorur *software*-in dhe internetin, për të realizuar si produkt përfundimtar falsifikimin ose riprogramimin e paligjshëm të vlerës së mbetur nga kartat telefonike[31].

f) përdorimi masiv i mjeteve të komunikimit. Ashtu sikurse bizneset e ligjshme që operojnë në sektorin publik dhe atë privat, ashtu edhe aktiviteti i organizatave

[25] Bohme Rainer, Moore Tyler; "How Do Consumers React to Cybercrime ?", article, November 2012, f.1.
[26] T. Moore, R. Clayton, and R. Anderson, "The economics of *online* crime," Journal of Economic Perspectives, vol. 23, no. 3, Summer 2009, f. 3–20.
[27] D. Florencio and C. Herley, "Evaluating a Trial Deployment of Password ^ Re-Use for Phishing Prevention," in eCrime Researchers Summit, ser. ACM International Conference Proceeding Series, L. F. Cranor, Ed., vol. 269. ACM, 2007, f. 26–36.
[28] Symantec Corporation, "Norton 2011 cybercrime report," 2011, http://www.symantec.com/content/en/us/home homeoffice/html/ cybercrimereport/
[29] Bohme Rainer, Moore Tyler; "How Do Consumers React to Cybercrime ?", article, November 2012, f. 5.
[30] Das Sumanjit, Nayak Tapaswini; "Impact of cyber crime: issues and challenges", International Journal of Engineering Sciences & Emerging Technologies, October 2013. ISSN: 22316604 Volume 6, Issue 2, ©IJESET, tetor 2013, f.142-153.
[31] Grabosky, Peter Smith, Russell "Crime in the Digital Age" Sydney: Federation Press, 1998.

kriminale është zgjeruar nëpërmjet përhapjes dhe rritjes së ndikimit të teknologjisë. Pajisjet e telekomunikacionit sot, përdoren për të lehtësuar punën e këtyre organizatave, sidomos aktivitetit të paligjshëm që ato ushtrojnë, siç mund të jetë pastrimi i parave, prostitucioni, trafikimi i drogës, etj. Duke qenë se informacioni në ditët e sotme përhapet me fuqinë e dritës, konsumatorët janë të parët që rrezikohen dhe vuajnë pasojat e veprimeve të tilla.

g) pirateria në fushën e telekomunikacionit. Teknologjia digjitale lejon riprodhimin deri diku perfekt dhe shpërndarjen e lehtë e të printimit, të grafisë, zërit dhe kombinimeve të tjera multimediale. Këtu shfaqet tendenca e hakerave për të riprodhuar materialin, të drejtën e autorit të së cilës e kanë individë të tjerë. Një gjë e tillë sjell humbje financiare të konsiderueshme dhe frikën që ka çdo person ose konsumator për krijimtarinë personale të tij[32].

h) shpërndarja e materialeve fyese. Përdorimi i të dhënave personale, fotove të ndryshme, materialeve të tjera me kontekst të pakëndshëm ekziston masivisht në hapësirën kibernetike. Kjo është më negative kur bëhet në formën e kërcënimit ndaj një ose më shumë personave, kur bëhet për marrjen e përfitimeve me natyrë të ndryshme nga hakerat që e realizojnë një veprimtari të tillë. Për pasojë, përdoruesit e internetit (konsumatorët) janë gjithmonë në rrezik ndaj veprimeve të tilla, të cilat sjellin jo vetëm dëme ekonomike, por edhe morale tek ta.

i) pastrimi elektronik i parave dhe shmangia e taksave. Nëpërmjet zhvillimit të teknologjisë është bërë e mundur gjetja e mënyrave të posaçme për të ndihmuar në fshehjen e të ardhurave apo në shmangien nga pagimi i taksave nga autoritetet tatimore përkatëse[33].

j) mashtrimet në shitje dhe investime. Një numër i konsiderueshëm konsumatorësh bëhen "pre" e hakerave, të cilët gëzojnë një qasje të drejtpërdrejtë me konsumatorët dhe me kosto minimale. Synimi në këto raste është nxjerrja e një përfitimi material, nëpërmjet mashtrimit të konsumatorëve të cilët kanë qëllim të blejnë mallra me cilësi dhe sasi të caktuara, që në të vërtetë nuk ekzistojnë dhe që përdoren vetëm për t'i manipuluar ata dhe për t'i nxitur të realizojnë blerje të tilla fiktive[34].

k) mashtrimi elektronik në shumat që transferohen[35]. Gjatë realizimit të transaksioneve, të dhëna konfidenciale të kartave të kreditit merren në mënyrë të paligjshme, falsifikohen dhe përdoren kundër vullnetit të konsumatorit që realisht e disponon kartën dhe të ardhurat e gjendura në brendësi të saj[36].

## 6. Ndikimi i krimit kibernetik tek të drejtat e konsumatorëve

Ligji nr. 9902/2008, "Për mbrojtjen e konsumatorëve", i ndryshuar liston të drejtat

[32] Each year, it has been estimated that losses of between US$15 and US$17 billion are sustained by industry by reason of copyright infringement (United States, Information Infrastructure Task Force 1995, 131).
[33] Kharouni, L. (2012) "Automating *online* banking fraud, automatic transfer system, the latest cyber crime toolkit feature, trend micro incorporated research paper". Për më tepër: http://www.trendmicro.com.br/cloud-content/us/pdfs/security-intelligence/white-papers/wp_auto mating_*online*_banking_fraud.pdf.
[34] International Journal of Engineering Sciences & Emerging Technologies, October 2013. ISSN: 22316604 Volume 6, Issue 2, ©IJESET; Das Sumanjit, Nayak Tapaswini; "Impact of cyber crime: issues and challenges", tetor 2013, f. 147.
[35] Dopuk (2013), "Bank distributed denial of service (DDoS) attacks strikes could presage Armageddon. DoS Protection UK"; për më tepër: http://www.dos-protection.co.uk/?p=152
[36] Si më sipër.

që ka çdo person në rolin e tij si konsumator[37]. Këto të drejta duhet të respektohen në të gjitha marrëdhëniet juridike konsumatore. Një nga mënyrat se si shfaqet kjo marrëdhënie janë kontratat elektronike[38].

Një nga të drejtat bazë të konsumatorëve është *mbrojtja e interesave ekonomike* të tyre. Kjo e drejtë cenohet më shumë nga krimi kibernetik. Pavarësisht kësaj, është më e lehtë të përcaktohen se cilat janë disa nga mënyrat efektive për të parandaluar shkeljen e kësaj të drejtë në kontratat konsumatore, të cilat realizohen me praninë fizike të palëve[39]. Kjo, sepse është e vështirë të identifikosh palën tjetër të kontratës, vendqëndrimin e tij/saj, në mënyrë që të realizohet më pas ndjekja penale dhe dëmshpërblimi i konsumatorëve të dëmtuar, në rastin e kontratave elektronike.

*E drejta e ankimit* përbën gjithashtu një nga të drejtat që i'u garantohen konsumatorëve. Si persona fizikë, këtë të drejtë e gëzojnë nga Kushtetuta e RSH-së[40], nga Konventa Europiane e të Drejtave të Njeriut (KEDNJ)[41] dhe nga ligji nr. 9902/2008, "Për mbrojtjen e konsumatorëve" (i ndryshuar), i cili përcakton se cilat janë të drejtat e tyre, ashtu edhe organet publike shtetërore para së cilave mund të paraqesin ankesat[42].

Por si realizohet kjo e drejtë e konsumatorëve, në rastin e kontratave elektronike?

Vështirësia në këtë rast nuk qëndron në identifikimin e krimit kibernetik e as në parashikimet ligjore ndëshkuese të bëra në Kodet Penale të vendeve të ndryshme, por në identifikimin e personave të cilët do të mbajnë përgjegjësi për këto veprime të paligjshme.

Një nga të drejtat bazë të konsumatorëve është e drejta e edukimit, e cila mbrohet në nivel kushtetues, në nivel europian dhe më pas në nivel ligjor. Kushtetuta e RSH-së[43] është burimi i parë që e konsideron të drejtën për edukim si të drejtë themelore, duke ia dhënë këtë të drejtë çdo individi, në lidhje me marrjen e njohurive dhe dijeve në secilën prej fushave që ata dëshirojnë. Përveç Kushtetutës, një rol i rëndësishëm, të drejtës së edukimit i kushtohet edhe nga Traktati Themelor për Funksionimin e Bashkimit Europian[44]. Ky i fundit synon rritjen e nivelit të mbrojtjes së konsumatorit dhe në

---

[37] Neni 4, Të drejtat e konsumatorëve, Ligji nr. 9902/2008 "Për mbrojtjen e konsumatorëve".

[38] Prof. Asc. Dr. Teliti Ersida; Doktoratura "Kontratat Konsumatore (Kredia konsumatore dhe kontrata e paketave turistike)", Tiranë, maj 2013, f. 43. Për më tepër:
"Të gjitha kontratat konsumatore janë marrëdhënie juridike që rregullohen mbi bazën e një ligji të veçantë, ligjit "Për mbrojtjen e konsumatorëve". Ky ligj bën një rregullim të përgjithshëm të kontratave konsumatore, të cilat detajohen më tej me akte të tjera nënligjore të nxjerra nga Këshilli i Ministrave apo nga organe të tjera qendrore si: Banka e Shqipërisë. Ato specifika të veçanta të marrëdhënieve juridike konsumatore, që nuk rregullohen nga këto norma juridike, disiplinohen nga Kodi Civil, si një akt me karakter të përgjithshëm që rregullon marrëdhëniet juridike pasurore dhe personale jopasurore ndërmjet subjekteve të së drejtës."

[39] Guidelines for Consumer Protections, UN Department of International Economic and Social Affairs, A/RES/39/248 (1986), University of Minessota, Human right library.
http://hrlibrary.umn.edu/links/consumerprotection.html

[40] Kushtetuta e Republikës së Shqipërisë, Neni 42/2, parashikon:
"Kushdo, për mbrojtjen e të drejtave, lirive dhe interesave të tij kushtetuese dhe ligjore, ose në rastin e akuzave të ngritura kundër tij, ka të drejtën e një gjykimi të drejtë dhe publik brenda një afati të arsyeshëm nga një gjykatë e pavarur dhe e paanshme e caktuar me ligj".

[41] KEDNJ-ja në nenin 13 të saj parashikon: "Çdokush të çilit i janë shkelur të drejtat dhe liritë e garantuara në këtë Konventë, ka të drejtë të bëjë ankim efektiv tek një organ i vendit të tij, edhe kur shkelja është kryer nga persona që veprojnë në përmbushje të funksioneve të tyre zyrtare".

[42] Kreu V, neni 56, Ligji nr. 9902/2008, "Për mbrojtjen e Konsumatorëve", i ndryshuar.

[43] Kushtetuta e Republikës së Shqipërisë, neni 57, paragrafi 1, parashikon:
"Kushdo ka të drejtën për arsimim..."

[44] Neni 153 TFBE, parashikon:
"Me qëllim që të përkrahen interesat e konsumatorëve dhe të sigurohet një nivel i lartë i mbrojtjes së tyre Komuniteti synon... promovimin e të drejtave të tyre për informim, edukim..."

kuadër të realizimit të këtij qëllimi duhet garantuar e drejta e edukimit të konsumatorëve. Një edukim i cili mund të merret në rrugë formale dhe joformale[45].

Për të garantuar dhe realizuar të drejtën e edukimit, nevojitet ndërmarrja e programeve informuese të cilat zhvillojnë dhe inkurajojnë edukimin e përgjithshëm të konsumatorëve duke pasur parasysh traditat kulturore të këtyre personave që kanë cilësinë e konsumatorit[46]. Qëllimi i programeve të tilla është që konsumatorët të ndërgjegjësohen në lidhje me të drejtat dhe përgjegjësitë e tyre[47]. Ky edukim do të ishte më efektiv nëse do të bëhej pjesë e programit mësimor, si një komponent shtesë krahas lëndëve ekzistuese. Megjithatë, procesi i edukimit duhet të nisë që nga edukatorët, gazetarët, si dhe Qendrat e Këshillimit të cilët ndikojnë në jetën e përditshme të çdo konsumatori. Konsumatorët duhet të njohin se çfarë është krimi kibernetik dhe rrezikshmërinë që mund t'ju vijë atyre si pasojë e materializimit të këtij krimi. Dhënia e një informacioni të plotë në kuadër të informimit dhe ndërgjegjësimit të konsumatorëve rreth krimit kibernetik dhe masave që duhet të merren me synim parandalimin e tij është një mundësi e mirë për të zvogëluar rastet e kryerjes me sukses së kësaj vepre penale.

Në bazë të ligjit "Për mbrojtjen e konsumatorëve", konsumatorët gëzojnë të drejtën për t'u dëmshpërblyer[48], në rastet kur i shkaktohet një dëm.

Kur një konsumator lidh një kontratë elektronike dhe ka pësuar një dëm, kujt do t'i kërkojë dëmshpërblim ai, kur është i pamundur identifikimi i palës tjetër në kontratat elektronike?

Parashikimet ligjore e mbrojnë konsumatorin nga pikëpamja formale, por nuk ofrojnë një zgjidhje praktike. Direktiva 2013/40/EU[49] parashikon se Shtetet Anëtare duhet të vendosin penalitetet dhe ndëshkimet e duhura për të parandaluar krimin kibernetik, por nuk përcakton se cilat mund të jenë ato masa efikase për të ndaluar krimin kibernetik të sjellë pasoja tek konsumatorët[50].

Për të realizuar mbrojtjen e të drejtave të konsumatorëve, gjatë realizimit të kontratave elektronike duhet të zbatohet ligji nr. 9887, datë 10.03.2008, ndryshuar me ligjin nr. 48/2012 "Për mbrojtjen e të dhënave personale", sipas së cilit përcaktohen rregullat për mbrojtjen dhe përpunimin e të dhënave personale të konsumatorëve[51]. Ligji synon të garantojë të drejtat dhe liritë themelore të personave gjatë përpunimit të të dhënave të tyre personale[52]. Mbrojtja e të dhënave personale të konsumatorëve duhet të bazohet në përpunimin e drejtë dhe të ligjshëm së të dhënave të tyre dhe

[45] Dr. Teliti Ersida, "Një vështrim krahasues mbi të drejtat e konsumatorëve në Shqipëri", Revista: Studimet Juridike, 2011, f. 127.

[46] Guidelines for Consumer Protections, UN Department of International Economic and Social Affairs, A/RES/39/248 (1986), University of Minessota, Human right library.
http://hrlibrary.umn.edu/links/consumerprotection.html

[47] Në zhvillimin e programeve të tilla, vëmendje e veçantë duhet t'i kushtohet nevojave të konsumatorëve në disavantazh, si p.sh konsumatorëve në zonat rurale apo ehe atyre me të ardhura të ulëta.

[48] Neni 31 Ligji nr. 9902/2008 "Për mbrojtjen e konsumatorëve" parashikon dëmshpërblimin si një e drejtë e konsumatorit.

[49] Direktiva 2013/40 /EU e Parlamentit Europian dhe Këshillit, e 12 Gushtit 2013, "Mbi sulmet ndaj sistemeve të informacionit dhe zëvendësimin e Vendimit Kornizë të Këshillit 2005/222 / JHA".

[50] Direktiva 2013/40 /EU, Preambula e Direktivës, pika 10.

[51] Ligji nr. 9887, datë 10.03.2008, ndryshuar me ligjin Nr. 48/2012 "Për mbrojtjen e të dhënave personale", neni 3, paragrafi i 1-rë.
"Të dhëna personale" është çdo informacion në lidhje me një person fizik, të identifikuar ose të identifikueshëm, direkt ose indirekt, në veçanti duke iu referuar një numri identifikimi ose një a më shumë faktorëve të veçantë për identitetin e tij fizik, fiziologjik, mendor, ekonomik, kulturor apo social.

[52] Ligji nr. 9887, datë 10.03.2008, ndryshuar me ligjin nr. 48/2012 "Për mbrojtjen e të dhënave personale", neni 2.

vetëm për aq sa është e nevojshme. Zbatimi i drejtë i këtij ligji, është një mënyrë e mirë për të zvogëluar përhapjen e krimit kibernetik dhe për të rritur mbrojtjen e konsumatorëve gjatë transaksioneve *online*.

Tregtia elektronike ofron mundësi të mëdha për zhvillimin e biznesit në të gjithë botën, duke shmangur çdo kufizim të mundshëm që paraqet tregtia joelekronike. Bashkë me të mirat e saj ka edhe anë negative, siç është krimi kibernetik. Studimet e fundit tregojnë se korporatat e mëdha marrin rreth 3000 kërcënime çdo muaj[53]. Pasojat shtrihen drejtpërdrejtë tek shoqëritë tregtare dhe tërthorazi prekin edhe konsumatorët, si pala tjetër në realizimin e një transaksioni të formës B2C[54]. Të gjithë përdoruesit e tregtisë *online*, qofshin tregtarë apo konsumatorë duhet të marrin masa të përbashkëta sigurie, në mënyë që të mbrojnë të dhënat e tyre financiare. Një gjë e tillë mund të realizohet nëpërmjet disa mënyrave, ndër të cilat janë:

a) Server i sigurt - siguria e pajisjes (serverit) që na mundëson lidhjen me internetin dhe më pas mundësinë për të realizuar transaksione *online* ;

b) Mbrojtja e të dhënave personale, - mosekspozimi i të dhënave personale, konfidenciale për të gjithë individët, duke marrë gjithmonë parasysh mundësinë e mashtruesve kompjuterike (hakerave), për t'i përdorur këto të dhëna në mënyrë të paautorizuar, për qëllime përftimi material.

c) Përdorimi i *password*-eve/ fjalëkalimeve të forta, - duke qenë se ka një sërë programesh kompjuterike që përdoren nga hakerat, si: Brutus, Rainbow-crack, wfuzz, Kain dhe Abel, THC Hydra, OphCrack, Aircrack-NG, Medusa dhe John the Ripper, që shërbejnë për të gjetur fjalëkalime të ndryshme, rekomandohet vendosja e *password*-ëve të kombinuar ndërmjet alfabeteve, numrave dhe karaktereve të tjera të ndryshme.

d) Siguria gjatë qenies *online* - çka do të thotë se identiteti i individëve duhet të mbrohet gjatë kohës që qëndron *online*; dhe e njëjta gjë duhet të ndodhë edhe në rastin e medieve sociale, siguria e llogarive të së cilave duhet të kontrollohet rregullisht, duke shmangur pasqyrimin në to të informacioneve private dhe të ndjeshme.

e) Përditësimi i Sistemit dhe Programeve kompjuterike - në këtë rast përdoruesit e internetit duhet të përmirësojnë sistemet e tyre *software* për të shmangur shkeljet e sigurisë[55].

Nga sa më sipër, arrijmë në përfundimin se krimi kibernetik sjell pasoja të konsiderueshme tek konsumatorët, të cilët cenohen ndjeshëm për shkak të humbjeve financiare dhe mungesës së besueshmërisë në lidhje me transaksionet që realizohen *online*[56]. Nëse konsumatorët dëmtohen si pasojë e kryerjes së një krimi kibernetik, këta të fundit do të zvogëlojnë pjesëmarrjen në transanksionet që realizohen *online*[57]. Kjo nuk sjell vetëm dëmtimin e konsumatorit dhe të ardhurave financiare të tij, por çon edhe në falimentimin e bizneseve që kanë zgjedhur të realizojnë veprimtarinë e tyre *online* sipas të gjitha kushteve që kërkohen nga legjislacioni i shtetit ku ata operojnë apo

[53] Ali Liaqat, Ali Faisal, Surendran Priyanka, Bindhya Thomas; "The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services";12 gusht, 2016, f. 71.

[54] Malltezi Argita, Rystemaj Jonida, Pelinku Lealba; "Aspekte të së drejtës së biznesit në Shqipëri", Mediaprint, Tiranë 2013, f. 476-485.

[55] International Journal of e-Education, e-Business, e-Management and e-Learning, Volume 7, Number 1, March 2017; Ali Liaqat, Ali Faisal, Surendran Priyanka, Thomas Bindhya ; "The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services", published mars 2017, f. 70-74. Për më tepër: http://www.ijeeee.org/vol7/414-IM023.pdf

[56] The Deloitte Consumer Review; Fenech Celine, Hamilton Lisa; "Consumer data under attack: The growing threat of cyber crime", UK, Artikull, nëntor 2015, f. 5-12.

[57] Bohme Rainer, Moore Tyler; "How Do Consumers React to Cybercrime?", article, November 2012, f. 7.

janë regjistruar[58]. Një konsumator jo domosdoshmërish mund të jetë viktimë e krimit kibernetik, e për pasojë të heqë dorë nga tregtia elektronike dhe kryerja e transaksioneve *online*. Megjithatë, shqetësimet si pasojë e këtij krimi, si dhe publikimi në media e lajme, e bëjnë konsumatorin të hezitojë dhe të mos ketë besim në realizimin e transaksioneve *online*.

Çdo ndërveprim, nga një transaksion i thjeshtë në një bashkëpunim kompleks mund të jetë i suksesshëm vetëm nëse ekziston një nivel i mjaftueshëm besimi ndërmjet palëve të marrëdhënies juridike që krijohet. Një nga komponentët më të rëndësishëm të një besimi reciprok është bashkëpunimi i tillë ndërmjet palëve, në mënyrë të tillë që të mbrohet privatësia e konsumatorit. E njëjta gjë funksionon edhe në hapësirën kibernetike[59]. Që një konsumator të blejë një mall ose shërbim nëpërmjet internetit, duhet që fillimisht të krijojë një lloj besimi të padyshimtë tek pala tjetër e kontratës, e cila duhet të jetë e aftë të garantojë mbrojtjen e privatësisë së transaksionit. Ky është aspekti kryesor që prek krimi kibernetik, i cili cenon si çështjet e besimit ashtu edhe të privatësisë së konsumatorëve[60].

Në ditët e sotme synohet të krijohen modele formale besimi[61] që iu përkasin çështjeve të ndryshme (p.sh. besimi tek subjekti të cilit i përkasin të dhënat, besimi tek subjekti që do i përdorë këto të dhëna, etj.). Rritja e sigurisë së mjeteve elektronike që përdoren për të garantuar privatësinë dhe besimin tek konsumatorët gjatë realizimit të ndërveprimeve *online*, në mënyrë të tillë që të shmangen vjedhjet e identitetit të konsumatorëve apo të dhëna të tjera konfidenciale të tyre. Ajo që synohet të arrihet, në funksion të mbrojtjes së konsumatorëve dhe privatësisë së tyre gjatë kryerjes së transaksioneve elektronike, është:

a) Monitorimi, vlefshmëria e politikave të privatësisë dhe zhvillimi i politikave që do të kontribuojnë në garantimin e saj, si mënyrë mbrojtje e konsumatorëve nga krimi kibernetik.

b) Licencimi i personave që autorizohen nga konsumatorët për të përdorur të dhënat e tyre personale dhe konfidenciale.

c) Gjetja e mënyrave të efektshme për sigurimin e anonimatit nëpërmjet fshehjes dhe mbrojtjes së informacionit personal të konsumatorëve, duke filluar nga garantimi i vendndodhjes, fshehjen e burimit të mesazhit, etj. Në këtë mënyrë bëhet e vështirë për hakerat të gjejnë e më pas të manipulojnë të dhënat personale të konsumatorëve[62].

Nga ana tjetër "pre" e krimit kibernetik, nuk janë vetëm konsumatorët. Edhe vetë tregtarët mund të dëmtohen si pasojë e veprimeve të ndryshme të kryera nga hakerat, të cilët është e vështirë për t'i identifikuar. Një nga gjërat më të rëndësishme që çdo biznes apo korporatë përpiqet të ruajë është *reputacioni* apo *imazhi* përballë

[58] Riek Markus , Bohme Rainer; "Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries"; University of Innsbruck, Department of Computer Science Innsbruck, Austria, Working Paper, f. 5-7.

[59] Chen Kuanchin Western Michigan University, USA; Fadlalla Adam Cleveland State University, USA; "*Online* Consumer Protection: The teories of Human Relativism"; Information Science Reference (an imprint of IGI Global), USA 2009, f. 87.

[60] Lilien Leszek Western Michigan University, USA; Bhargava Bharat Purdue University, USA; "Privacy and Trust in *Online* Interactions"; Information Science Reference (an imprint of IGI Global), USA 2009, f. 89.

[61] Bhargava, B., Lilien, L., Rosenthal, A., & Winslett, M. (2004); "Pervasive trust", IEEE Intelligent Systems, 19(5), Purdue University, UTET 2004, f. 74-77.

[62] Bhargava, B., Farkas, C., Lilien, L., & Makedon, F.; "Trust, privacy, and security"; summary of a workshop breakout session at the national science foundation information and data management (IDM) workshop held in Seattle, Washington (Tech. Rep. No. 2003-34). West Lafayette, IN: Purdue University, Center for Education and Research in Information Assurance and Security (CERIAS); 14-16 shtator, 2003.

konsumatorëve dhe bizneseve të tjera konkurruese[63]. Dëmtimi i këtij reputacioni do të sillte për pasojë humbje të konsiderueshme në të ardhura, më pak blerës, derisa biznesi të arrijë drejt falimentimit. Një pasojë e tillë mund të shkaktohet shumë lehtë nëpërmjet krimi kibernetik. Një nga mënyrat nëpërmjet të cilave mund të shmanget ky lloj krimi është përvetësimi i njohurive menaxheriale nga ana e biznesit. Pasja e sa më shumë njohurive *Know - How* nga ana e biznesit, rrit jo vetëm konkurrueshmërinë e tij në treg, por gjithashtu shërben edhe si mbrojtje nga krimi kibernetik, sepse zvogëlon mundësinë e hakerave të ndryshëm për të hyrë dhe për të përdorur të dhënat konfidenciale të biznesit[64].

"Loja" ndërmjet krimit kibernetik dhe luftës për ta parandaluar atë, nuk do të ketë fund asnjëherë. Megjithatë mund të vendoset një balancë ndërmjet hakerave nga njëra anë dhe mbrojtësve nga ana tjetër. Synimi është të ulet numri i konsumatorëve që bëhen viktima të krimit kibernetik dhe rritja e besueshmërisë së tyre për realizimin e transaksioneve *online*[65].

## 7. Konkluzione

- Krimi kibernetik i referohet të gjitha veprimtarive kriminale të kryera duke përdorur kompjuterët, internetin, hapësirën kibernetike dhe *world wide web*.

- Hapësira kibernetike krijon mjedis të përshtatshëm për hakerat, të cilët synojnë vjedhjen e të dhënave personale dhe sekreteve tregtare, dërgojnë viruse kompjuterike, kryejnë transaksione mashtruese, etj.

- Zhvillimi i tregtisë elektronike sjell si pasojë rritjen dhe përsosjen e krimeve në hapësirën kibernetike, duke rrezikuar të ardhurat materiale të një numri të madh konsumatorësh.

- Lidhja e kontratave elektronike B2C ka nxitur përhapjen e krimit kibernetik. Nëpërmjet hapësirës kibernetike, hakerat përvetësojnë të dhënat personale dhe informacione private të konsumatorëve, duke u shkaktuar këtyre të fundit dëme ekonomike, si dhe humbjen e besimit.

- Në rastin e krimit kibernetik është e vështirë të garantohen të gjitha të drejtat e konsumatorëve, sepse është e vështirë të gjendet burimi i hakimit, personit/personave që e kanë kryer këtë krim duke e bërë të pamundur procesin e dëmshpërblimit të konsumatorëve.

- Krimit kibernetik dëmton bizneset, të cilët tregtojnë në përputhje me rregullat ligjore të përcaktuara nga legjislacioni në fuqi në vende të ndryshme, duke sjellë në shumë raste falimentimin e këtyre bizneseve.

- Rritja e aksesit në internet të konsumatorëve nxit përmirësimin e mjeteve dhe teknikave nëpërmjet të cilave realizohet krimi kibernetik, të cilat synojnë krijimin e programeve të sofistikuara nga hakerat.

- Legjislacioni i BE-së synon të shtyjë Shtetet Anëtare të marrin masat e posaçme që të ketë një kufizim të numrit të krimeve të kësaj natyrë, por nuk parashikon se cilat janë këto masa ku duhet të mbështeten Shtetet Anëtare në mënyrë që të arrihen rezultate pozitive në parandalimin dhe uljen e numrit të kësaj vepre penale.

- Krimi kibernetik cenon të drejtat e konsumatorëve duke u bërë thirrje shteteve për hartimin dhe zbatimin e parashikimeve ligjore në funksion të rritjes së sigurisë së konsumatorëve në transaksionet *online*.

- Kostot e krimit kibernetik rriten në mënyrë të shpejtë, duke shtruar detyrën për

gjetjen e mënyrave alternative për parandalimin e kësaj vepre penale dhe identifikimin e personave përgjegjës dhe marrjen e tyre në përgjegjësi penale.

## 8. Rekomandime

- Konsumatorët duhet të përdorin serverë të sigurt në realizimin e transaksioneve *online*.

- Tregtarët duhet të krijojnë sisteme të sofistikuara dhe të fuqishme për të monitoruar dhe parandaluar sa më shumë aktivitetin e mashtruesve kompjuterike, si dhe për të rritur sigurinë gjatë kryerjes se transaksioneve *online*.

- Konsumatorët duhet të mirë-edukohen rreth metodave dhe mjeteve që duhet të përdorin dhe si ti përdorin ato në mënyrë që të realizojnë transaksione të sigurta *online* dhe njëkohësisht të ruajnë të paprekura të dhënat dhe informacionin e tyre personal.

- Rekomandohet ndërmarrja e politikave ndërgjegjësuese për konsumatorët në lidhje me rrezikshmërinë nga kërcënimet *online* dhe pasojat që krimi kibernetik sjell tek të ardhurat ekonomike të tyre.

- Rekomandohet që në amendamentet e ardhshme të ligjit 9902, datë 17.4.2008 "Për mbrojtjen e konsumatorit", i ndryshuar, të parashikohet një krè kushtuar krimit kibernetik dhe rikuperimit të dëmeve.

- Shtetet Anëtare duhet të rrisin bashkëpunimin në hapësirën kibernetike në kuadër të identifikimit të personave përgjegjës dhe vendosjen e tyre përpara përgjegjësisë.

- Duhet të identifikohen dhe monitorohen personat që realizojnë përpunimin e të dhënave të konsumatorëve dhe tregtarëve në përputhje me legjislacionin në fuqi.

- Në kuadër të sensibilizimit duhet të merren një plan masash nga institucionet publike me kompetencë në këtë fushë në mënyrë që të mos cenohet tregtia elektronike.

## Bibliografia


1. Ali Liaqat, Ali Faisal, Surendran Priyanka, Bindhya Thomas; "The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services"; August 12, 2016.
2. Bohme Rainer, Moore Tyler; "How Do Consumers React to Cybercrime ?", article, November 2012.
3. Bhargava, B., Lilien, L., Rosenthal, A., & Winslett, M.; "Pervasive trust", *IEEE Intelligent Systems*, 2004.
4. B., Farkas, C., Lilien, L., & Makedon, F.; "Trust, privacy, and security"; Seattle, Washington, September 14-16,2003.
5. Collao Villanueva Vanessa; "I contrati conclusi in internet", Giuffre Editore, Milano 2014.
6. Chen Kuanchin Western Michigan University, USA; Fadlalla Adam Cleveland State University, USA; "Online Consumer Protection: The teories of Human Relativism"; *IGI Global*, USA 2009.
7. Dautner Mike, "As ECommerce Accelerates, So Too Does The Risk Of Cyber Crime", article of 10 may 2017.
8. Dopuk; "Bank distributed denial of service (DDoS) attacks strikes could presage Armageddon", *DoS Protection* UK, 2013.
9. D. Florencio and C. Herley, "Evaluating a Trial Deployment of Password ^ Re-Use for Phishing Prevention," in *eCrime Researchers Summit*, *ser. ACM International Conference Proceeding Series*, L. F. Cranor, Ed., vol. 269. ACM, 2007.
10. Gerhart Morgan, "The Evolution of Cybercrime and What It Means for Data Security", article, 27 july 2017.
11. Gottschalk Petter, "Policing cyber crime", Germany, Ventus Publishing ApS, 2010.
12. Grabosky Peter and Smith Russell, "Crime in the Digital Age" Sydney: Federation Press, 1998.
13. Hanif Mehmood, "A detailed history of cybercrimes", article, 25 October 2017.
14. *International Journal of e-Education, e-Business, e-Management and e-Learning*, Volume 7, Number 1; Ali


[63] Gottschalk Petter, "Policing cyber crime", 2010, Germany, Ventus Publishing ApS, f. 66-73.
[64] Vep. e Cit., f. 74-95.
[65] Van Ommeren Erik, Borrett Martin, Kuivenhoven Martin; "Staying Ahead in the Cyber Security Game"; *line up* boek en media bv, Groningen, the Netherlands, prill 2014, f. 19-25.

Liaqat, Ali Faisal, Surendran Priyanka, Thomas Bindhya; "The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services", March 2017.
15. *International Journal of Engineering Sciences & Emerging Technologies,* Volume 6, ©IJESET, Das Sumanjit, Nayak Tapaswini; "Impact of cyber crime: issues and challenges", October 2013.
16. Kharouni, L., "Automating *online* banking fraud, automatic transfer system, the latest cyber crime toolkit feature, trend micro incorporated research paper", 2012.
17. Kratchman, Stan, J. Smith, and L.M.Smith., "Perpetration and Prevention of Cyber Crimes. Internal Auditing", Vol. 23, No. 2 (March-April), 2008.
18. Lilien Leszek Western Michigan University, USA; Bhargava Bharat Purdue University, USA; "Privacy and Trust in *Online* Interactions"; IGI Global, USA 2009.
19. Mallteзi Argita, Rustemaj Jonida, Pelinku Lealba, *Aspekte të së drejtës së biznesit në Shqipëri*, Mediaprint, Tiranë 2013.
20. Packt Editorial Staff, "The evolution of cybercrime", article, 29 march 2018.
21. Patel Mayur, Patel Neha, Ganatra Amit, Kosta Yogesh, "E-Commerce and Attached E-Risk with Cybercrime", article of 3 janary 2015.
22. Riek Markus, Bohme Rainer; "Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries"; University of Innsbruck, Department of Computer Science Innsbruck, Austria, Working Paper, 2012.
23. Teliti Ersida, "Një vështrim krahasues mbi të drejtat e konsumatorëve në Shqipëri", *Revista: Studimet Juridike*, Tiranë 2011.
24. Teliti Ersida; *Kontratat Konsumatore* (Kredia konsumatore dhe kontrata e paketave turistike), Tezë doktorature, Tiranë, maj 2013.
25. The Deloitte Consumer Review; "Consumer data under attack: The growing threat of cyber crime", Article, 2016.
26. T. Moore, R. Clayton, and R. Anderson, "The economics of *online* crime," *Journal of Economic Perspectives*, vol. 23, no. 3, Summer 2009.
27. United Nations Conference on Trade and Development, "Consumer protection in electronic commerce", 24 April 2017.
28. Van Ommeren Erik, Borrett Martin, Kuivenhoven Martin; "Staying Ahead in the Cyber Security Game"; Groningen, the Netherlands, april 2014.

**Legjislacion**

1. Bolivarian Republic of Venezuela, Ley Especial contra los Delitos Informáticos 2001;
2. "Comprehensive Study on Cybercrime", Draft, United Nations Office on Drugs and Crime, Vienna February 2013.
3. Direktiva 2011/83/EU "Mbi të drejtat e konsumatorëve".
4. Direktiva 2013/40 /UE E PARLAMENTIT EVROPIAN DHE E KËSHILLIT, e 12 Gushtit 2013, "Mbi sulmet ndaj sistemeve të informacionit dhe zëvendësimin e Vendimit Kornizë të Këshillit 2005/222 / JHA".
5. Electronic Communications in the Republic of Albania, Law no. 9918 2008.
6. France, Code des postes et des communications électroniques (version consolidée) 2012.
7. Guidelines for Consumer Protections, UN Department of International Economic and Social Affairs, (1986), University of Minessota, Human right library.
8. India, The Information Technology Act 2000.
9. Kushtetuta e Republikës së Shqipërisë
10. Konventa Europiane e të Drejtave të Njeriut.
11. Ligji nr. 9902/2008 "Për mbrojtjen e konsumatorëve".
12. Ligji nr. 10128, datë 11.5.2009 "Për tregtinë elektronike", i ndryshuar.
13. Ligji nr. 10273, datë 29.4.2010 "Për dokumentet elektronike".
14. Ligji nr. 9918, datë 19.5.2008 "Për komunikimet elektronike"/ i ndryshuar nga ligji nr. 102/2012, datë 24.10.2012 "Për disa shtesa dhe ndryshime në ligjin nr. 9918, datë 19.05.2008 "Për komunikimet elektronike".
15. Ligji nr. 9880, datë 25.2.2008, " Për nënshkrimin elektronik", i ndryshuar nga ligji nr. 10178, datë 29.10.2009 "Për miratimin e aktit normative, me fuqinë e ligjit, nr. 8, datë 30.092009 të Këshillit të Ministrave "Për një ndryshim në ligjin nr. 9880, datë 25.2.2008, " Për nënshkrimin elektronik".
16. Ligji nr. 9887, datë 10.3.2008, ndryshuar me ligjin nr. 48/2012 "Për mbrojtjen e të dhënave personale".
17. Malaysia, Computer Crimes Act 1997.
18. Sri Lanka, Computer Crime Act 2007.
19. Serbia, Law on Organization and Competence of Government Authorities for Combating High-Tech Crime 2010.
20. Sudan, Computer Crimes Act 2007.
21. Saudi Arabia, IT Criminal Act 2007.
22. Tonga, Communications Act 2000.
23. Traktati për Funksionimin e Bashkimit Europian.
24. Vietnam, Law on Information Technology, 2007.

**Website**

1. https://www.le-vpn.com/history-cyber-crime-origin-evolution/
2. http://www.symantec.com/content/en/us/home
3. homeoffice/html/ cybercrimereport/
4. http://hrlibrary.umn.edu/links/consumerprotection.html

# Hetimi i krimit kompjuterik në Shqipëri

■**Dr. (proc) Armand GURAKUQI**
*Prokuroria pranë Gjykatës së Shkallës së Parë, Tiranë*
*gurakuqiarmand@yahoo.com*

**Abstrakt**

*Për shkak të tipareve të veçanta që karakterizojnë krimin kompjuterik edhe hetimi i tij paraqet problematika që dallojnë nga hetimi i veprave penale tradicionale. Krimi kompjuterik mund të realizohet në një kohë mjaft të shpejtë, ndërkohë që elementet përbërës të figurave të veprave penale në fushën e teknologjisë së informacionit, mund të jenë të përhapura në vende të ndryshme. Natyra ndërkombëtare e kriminalitetit kibernetik bën të detyrueshëm zhvillimin e veprimtarisë hetimore në disa shtete. Nivelet e bashkëpunimit ndërkombëtar ndryshojnë në varësi të legjislacionit të brendshëm dhe vullnetit të shteteve në të cilat shtrihet vepra penale. Suksesi apo dështimi i hetimeve me shtrirje ndërshtetërore të krimeve në fushën e teknologjisë, është i lidhur ngushtë me kryerjen ne kohë dhe përmbushjen e të gjitha veprimeve hetimore nga secili prej shteteve pjesëmarrëse në hetim. Veç sa më lart, problematika në hetimet e krimeve kompjuterike është e lidhur me faktin se organet e hetimit, në kuadër të përmbushjes së procedurave ligjore, nevojitet të ndërmarrin veprime të lidhura me pajisjet kompjuterike, në të cilat, veç gjurmëve të veprës penale, mund të gjenden edhe të dhëna që përfshihen në jetën private të individit. Ky moment ngre para organit procedues detyrimin për të siguruar të gjitha garancitë e nevojshme, me qëllim respektimin e jetës private të personit. Në këtë punim do të trajtohen parashikimet ligjore që normojnë hetimin e krimeve kompjuterike në Shqipëri, duke bërë një analizë krahasuese me instrumentet ligjore ndërkombëtare. Njëkohësisht, do të prezantohen dhe vështirësitë dhe problematikat që hasen në kuadër të hetimit të kësaj kategorie të veprave penale.*

**Fjalëkyçe:**
**hetim, kompjuterik, krim, ndërkombëtar, bashkëpunim.**

## 1. Hyrje

Zhvillimet e shpejta teknologjike janë shoqëruar me ndryshime të rëndësishme të së gjitha aspekteve të veprimtarisë së njeriut. Tashmë shoqëria njerëzore është afruar duke shmangur pengesat e krijuara nga distancat gjeografike, për shkak të mundësive dhe lehtësive të shumta të ofruara nga evoluimi i shkencës. Ndërveprimi mes institucioneve shtetërore, individëve apo shoqërive tregtare, në nivel kombëtar e ndërkombëtar, realizohet duke u mbështetur në komunikimet kompjuterike. Ruajtja e të dhënave dhe përpunimi i tyre, e si pasojë edhe veprimtaria e subjekteve shtetërore e private, i besohet jo më materies fizike, por sistemeve teknologjike. Pajisjet kompjuterike gjejnë përdorim në të gjitha fushat e jetës njerëzore si: mjekësia, arsimi, sporti, arti, ekonomia etj. Mund të thuhet që funksionimi i shoqërisë dhe i strukturave shtetërore, është i varur nga teknologjia sa që e bën të vështirë të mendohet se mund të realizohet në mungesë të saj.

Ekzistenca e një raporti kaq të ngushtë ndërmjet risive kompjuterike dhe individit, organizmave shtetërore apo enteve private, ka prezantuar një terren mjaft tundues edhe për shkelësit e ligjit, të cilët në vazhdimësi kërkojnë mjete e mënyra për të përfituar në mënyra të paligjshme ose për të dëmtuar interesa të ligjshme të së tretëve. Lehtësitë që teknologjia e informacionit ofron për veprimtaritë legjitime, shfrytëzohen edhe nga personat me prirje kriminale. Këto të fundit kanë mundësi të përmbushin aktivitetin kriminal duke u shmangur nga mënyrat tradicionale të kryerjes së veprave penale, nëpërmjet evitimit të realitetit fizik dhe elementeve përbërës të tij si koha, vendi, mjeti, veprimi apo mosveprimi. Autori i një aktiviteti kriminal në fushën kompjuterike e ka të panevojshme të gjendet fizikisht në vendin e kryerjes së krimit, të kryejë një veprim konkret në atë ambient, duke shuar çdo mundësi për të lënë gjurmën fizike që do ta

lidhte me veprën penale. Individit në fjalë do t'i mjaftonte, veç aftësive në fushën informatike, një sistem kompjuterik dhe lidhja me rrjetet kombëtare apo ndërkombëtare të komunikimeve informatike, për të realizuar veprimin e paligjshëm të synuar prej tij. Mundësitë e fshehjes së lidhjes mes veprës penale dhe autorit të saj, në terrenin virtual, janë në përmasa mjaft të gjëra.

Anonimati i ofruar nga lidhjet në rrjet, programet kompjuterike që mundësojnë zhvendosjen e pozicionit të autorit nga vendndodhja reale e tij, përshtatja me hapa të ngadaltë të infrastrukturës shtetërore në raport me nevojat për hetimin e krimeve kompjuterike, janë disa nga rrethanat që mund të përmenden si faktorë që ndikojnë në reagimin jo në nivelin e duhur të organeve ligjzbatuese e për pasojë edhe në rezultate të ulëta të luftës ndaj kriminalitetit kompjuterik.

Natyra ndërkombëtare e kriminalitetit kibernetik bën të detyrueshëm zhvillimin e veprimtarisë hetimore në disa shtete. Nivelet e bashkëpunimit ndërkombëtar ndryshojnë në varësi të legjislacionit të brendshëm dhe vullnetit të shteteve në të cilat shtrihet vepra penale. Suksesi apo dështimi i hetimeve me shtrirje ndërshtetërore të krimeve në fushën e teknologjisë, është i lidhur ngushtë me kryerjen në kohë dhe përmbushjen e të gjitha veprimeve hetimore nga secili prej shteteve pjesëmarrëse në hetim. Veç sa më lart, problematika në hetimet e krimeve kompjuterike është e lidhur me faktin se organet e hetimit, në kuadër të përmbushjes së procedurave ligjore, nevojitet të ndërmarrin veprime të lidhura me pajisjet kompjuterike në të cilat veç gjurmëve të veprës penale, mund të gjenden edhe të dhëna që përfshihen në jetën private të individit. Ky moment ngre para organit procedues detyrimin për të siguruar të gjitha garancitë e nevojshme, me qëllim respektimin e jetës private të personit.

Në këtë punim do të trajtohen parashikimet ligjore që normojnë hetimin e krimeve kompjuterike në Shqipëri, duke bërë një analizë krahasuese me instrumentet ligjore ndërkombëtare. Njëkohësisht, do të prezantohen vështirësitë dhe problematikat që hasen në kuadër të hetimit të kësaj kategorie të veprave penale.

## 2. Mjetet e kërkimit të provës në krimet kompjuterike

Në vitin 2008, në Kodin e Procedurës Penale të Republikës së Shqipërisë, u bënë ndryshime në lidhje me mjetet e kërkimit të provave në rastet e veprave penale në fushën e teknologjisë së informacionit[1]. Për vepra të tilla u parashikuan dispozita specifike në të cilat konstatohet një shtim i rolit kontrollues të gjykatës. Edhe në vitin 2017 ligji procedural penal pati ndryshime sa i takon veprimeve hetimore në lidhje me provat kompjuterike, konkretisht në lidhje me procesin e kontrollit të tyre.

Në rregullat procedurale të shtuara në vitin 2008[2] lidhur me të dhënat apo pajisjet kompjuterike, parashikohet zbatimi i tyre në rastin e procedimeve për veprat penale në fushën e teknologjisë së informacionit, por nuk përcaktohet se cilat do të përfshihen në këtë kategori veprash. Një moment i tillë paraqet rëndësi pasi në varësi të kategorizimit apo jo të veprës penale si pjesë e fushës së teknologjisë së informacionit, do të përzgjidhet edhe baza përkatëse ligjore për tu zbatuar. Lidhur me këtë moment është e vlefshme të trajtohet diskutimi nëse të tilla do të konsiderohen vetëm ato vepra penale që drejtohen

[1] Shih ligjin nr. 10 054, datë 29.12.2008 "Për disa shtesa dhe ndryshime në ligjin nr. 7905, datë 21.3.1995 "Kodi i Procedurës Penale i Republikës së Shqipërisë", të ndryshuar.

[2] Shih nenet 191/a "Detyrimi për paraqitjen e të dhënave kompjuterike", 208/a "Sekuestrimi i të dhënave kompjuterike" etj, të Kodit të Procedurës Penale të Republikës së Shqipërisë.

ndaj sistemit kompjuterik[3] apo të dhënës kompjuterike[4] apo edhe ato vepra në të cilat sistemi apo e dhëna kompjuterike përdoren si prova apo mjete për konsumimin e tyre. "Konventa për Krimin në Fushën e Kibernetikës"[5], si një nga instrumentet ndërkombëtare më të rëndësishme në këtë fushë, ka strukturuar veprat penale në disa kategori, konkretisht:

1) kundër konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave dhe sistemeve kompjuterike[6];

2) krimet e lidhura me kompjuterët[7];

3) veprat penale të lidhura me përmbajtjen[8];

4) veprat penale të lidhura me dhunimin e të drejtës së autorit dhe të drejtave të tjera të lidhura me të.

Nisur nga përmbajtja e dispozitave penale orientuese për shtetet palë konstatohet se Konventa e Budapestit nuk aplikohet vetëm për faktet penale që drejtohen ndaj sistemeve apo të dhënave kompjuterike. Veprat e lidhura me përmbajtjen dhe ato që cenojnë të drejtat e autorit janë përfshirë në Konventë, kur realizohen më anë të një sistemi kompjuterik, pra kur ky i fundit ka cilësinë e mjetit të kryerjes së faktit penal. Në lidhje me sferën e zbatimit të dispozitave procedurale Konventa e Budapestit ka përcaktuar që palët të aplikojnë këto norma për veprat penale të përcaktuara në Konventë; vepra të tjera penale të kryera nëpërmjet një sistemi kompjuterik dhe për mbledhjen e fakteve në formë elektronike të një vepre penale[9]. Duke u bazuar në këto përcaktime normative konkludohet se do të përfshihen në fushën e teknologjisë së informacionit si veprat penale të drejtuara ndaj të dhënave apo sistemeve kompjuterike ashtu edhe veprat në të cilat të dhënat apo sistemet përdoren si mjete për kryerjen e tyre. Për pasojë në këto raste duhet të përdoren dispozitat procedurale të parashikuara specifikisht për këtë kategori shkeljesh penale.

Siç është trajtuar më lart në këtë punim, në hetimet e krimeve kompjuterike është shtuar roli kontrollues i gjykatës. Rritja e rolit të gjyqësorit në këtë fazë të procesit është e lidhur me nevojën për të ruajtur privatësinë e personave të lidhur me procedimin. Në kushtet kur veprimtaria njerëzore është shumë e lidhur me pajisjet kompjuterike, në këto të fundit përmbahen të dhëna të konsiderueshme me natyrë personale, të cilat nuk janë të lidhura me hetimin e veprës penale. Për të siguruar paprekshmërinë e këtyre të dhënave ligjvënësi ka rritur nivelin kontrollues të mjeteve të kërkimit të provës, duke ia besuar gjykatës këtë mision.

### *2.1 Detyrimi për paraqitjen e të dhënave kompjuterike[10]*

Gjykata është organi kompetent për të autorizuar jo vetëm veprimtarinë hetimore të lidhur me gjetjen dhe marrjen e përmbajtjes së sistemeve apo të dhënave kompjuterike

[3] Në nenin 1 të "Konventës për krimin në fushën e kibernetikës", ratifikuar me ligjin nr.8888, datë 25.4.2002 jepet përkufizimi: "Sistem kompjuterik" do të thotë çdo lloj pajisje apo grup i ndërlidhur ose pajisje të lidhura, një ose më shumë prej të cilave, vazhduese të një programi kryejnë procesime automatike së të dhënave".

[4] Në nenin 1 të "Konventës për krimin në fushën e kibernetikës", ratifikuar me ligjin nr.8888, datë 25.4.2002 jepet përkufizimi: "Të dhëna kompjuterike" do të thotë çfarëdolloj përfaqësimi i fakteve, informacioni apo konceptesh në një formë të përshtatshme për procesim në një sistem kompjuterik, që përfshijnë një program të përshtatshëm për punën e një sistemi kompjuterik për të kryer një funksion.

[5] Në vijim Konventa e Budapestit.

[6] "Ndërhyrja në të dhënat", "Ndërhyrja në sisteme", "Keqpërdorimi i pajisjeve".

[7] "Falsifikimet e lidhura me kompjuterët", "Mashtrimet e lidhura me kompjuterët".

[8] "Veprat penale të lidhura me pornografinë e fëmijëve".

[9] Shih nenin 14 të "Konventës për krimin në fushën e kibernetikës", ratifikuar me ligjin nr.8888, datë 25.4.2002.

[10] Shih nenin 191/a të Kodit të Procedurës Penale të Republikës së Shqipërisë.

por edhe për marrjen e të dhënave të përdoruesit si gjeneralitetet e tij, numrin e telefonit, të dhënat e lidhjes me internetin. Vlerësohet se të dhënat e përdoruesit nuk kanë të njëjtën natyrë me përmbajtjen e komunikimeve kompjuterike[11], pasi ndryshe nga këto të fundit ku individi ushtron jetën e tij private, ato, pra të dhënat e përdoruesit, paraqesin rrethana që shërbejnë për identifikimin e personit apo të lidhjes që ai ka krijuar me internetin. Për këtë arsye vlerësohet i papërshtatshëm kufizimi ligjor sipas të cilit edhe administrimi i këtyre të dhënave duhet të autorizohet nga gjykata. Një kufizim i tillë përfaqëson qasje të kundërt me raste të tjera të ngjashme si administrimi i të dhënave telefonike të individit nga shoqëritë e telefonive celulare, veprim ky që nuk është i detyruar të vlerësohet dhe lejohet nga gjykata por realizohet mbi bazën e kërkesës së dërguar nga ana e prokurorit.

Marrja e të dhënave të përdoruesit pranë mbajtësit apo kontrolluesit të të dhënave kompjuterike, urdhërohet nga gjykata mbi bazën e kërkesës së prokurorit apo viktimës[12]. Prokurori mund të hartojë një urdhër të tillë vetëm në raste të ngutshme dhe urdhri duhet të vlerësohet nga gjykata brenda 48 orëve.

Procesi i grumbullimit të të dhënave të përdoruesit është i shtrirë jo vetëm në territorin shqiptar. Në një pjesë të konsiderueshme të rasteve hetimore ai zhvillohet nëpërmjet kërkimeve në shtete të tjera. Kjo ndodh për shkak se shoqëritë më të mëdha të ofrimit të shërbimeve të internetit[13] ndodhen në ato shtete. Shoqëri të tilla mund të përmenden *Facebook Inc, Microsoft, Google, Yahoo* etj..., të cilat janë ndër subjektet më të mëdha që ofrojnë shërbime si komunikimet nëpërmjet postës elektronike, ndërveprimin nëpërmjet rrjeteve sociale etj[14]. Kompanitë e mësipërme janë të regjistruara në Shtetet e Bashkuara të Amerikës dhe realizojnë ruajtjen e informacionit në atë shtet apo në vende të tjera të ushtrimit të veprimtarisë. Për këto arsye edhe marrja e të dhënave të përdoruesit realizohet vetëm nëpërmjet bashkëpunimit ndërkombëtar.

Sipas Kodit të Procedurës Penale, mekanizmi i vetëm për marrjen e provave jashtë vendit është letërporosia për jashtë shtetit[15]. Ky proces, për vetë numrin e lartë të organeve që kanë kompetencë për ta trajtuar, ezauron një kohë shumë të gjatë e për këtë arsye nuk i përgjigjet natyrës së krimit kompjuterik dhe nevojës për shpejtësi të veprimtarisë hetimore të lidhur me të. Për këto arsye përdorimi i letërporosisë për marrjen e të dhënave të përdoruesit është një mjet i papërshtatshëm procedural.

Mungesa e efiçencës së aplikimit të letërporosive ishte një arsye që është marrë në konsideratë nga Këshilli i Europës gjatë miratimit të Konventës së Budapestit, në të cilën janë parashikuar mënyra më të shpejta veprimi për marrjen e një kategorie të dhënash kompjuterike, në të cilat përfshihen edhe ato të përdoruesit. Ky akt ndërkombëtar ka parashikuar se një palë nënshkruese, pa marrë autorizimin nga pala tjetër, mund të hyjë ose të marrë, nëpërmjet një sistemi kompjuterik në territorin e tij, të dhënat e regjistruara në kompjuter tek një palë tjetër, nëse pala kërkuese merr lejen e ligjshme dhe të vullnetshme të personit që ka kompetencën ligjore t'i njoftojë të dhënat palës nëpërmjet sistemit kompjuterik[16]. Një rregullim i tillë ka krijuar mundësinë për palët nënshkruese të Konventës që t'i drejtohet, duke përdorur komunikimet kompjuterike, një shoqërie

[11] Me email apo programe të ndryshme komunikimi kompjuterik.
[12] Shih nenin 191/a të Kodit të Procedurës Penale të Republikës së Shqipërisë.
[13] Në vijim ISP (Internet Service Provider).
[14] Shih https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
[15] Shih nenin 500 të Kodit të Procedurës Penale të Republikës së Shqipërisë.
[16] Shih nenin 32/b të "Konventës për krimin në fushën e kibernetikës", ratifikuar me ligjin nr.8888, datë 25.4.2002.

që ruan të dhëna kompjuterike në një shtet tjetër dhe të kërkojë të dhënat e përdoruesit. Për këtë qëllim nevojitet marrja e lejes nga personi të cilit i është ngarkuar kompetenca përkatëse ligjore. Personi "ligjërisht i autorizuar" për të dorëzuar të dhënat mund të ndryshojë në varësi të rrethanave, natyrës së personit dhe ligjit të zbatueshëm. Për shembull adresa e e-malit të një personi mund të jetë e ruajtur në një vend tjetër nga një ofrues shërbimi interneti ose një person qëllimisht mund të ruajë të dhëna në një vend tjetër. Këto persona mund të tërheqin të dhënat dhe kur kanë autoritetin ligjor t'i dorëzojnë vullnetarisht ato tek organet ligjzbatuese[17].

Marrja e të dhënave të përdoruesit nga një shoqëri ofruese shërbimesh interneti e huaj, realizohet duke aplikuar normat procedurale penale shqiptare dhe ato të mundësuara nga Konventa e Budapestit. Kështu së pari përfaqësuesi i akuzës i drejtohet me kërkesë gjykatës dhe kur kjo e fundit pranon kërkesën dhe lejon marrjen e të dhënave, vendimi gjyqësor dërgohet nëpërmjet komunikimeve kompjuterike të sigurta të krijuara mes shoqërive dhe organeve ligjzbatuese. Praktika e përditshme është shoqëruar me problematika të ndryshme në lidhje me këtë mekanizëm procedural. Siç u trajtua më lart, marrja e të dhënave në zbatim të Konventës së Budapestit, nga ofruesit e huaj të shërbimit të internetit, zhvillohet mbi baza vullnetare, parim ky që ka krijuar diskrecionin për të pranuar ose jo dorëzimin e të dhënave. Për këto arsye, shoqëri të ndryshme ndërkombëtare, në raport me shtete të ndryshme, nuk mbajnë politika të njëjta në lidhjen me dorëzimin e të dhënave.

Shoqëria "Facebook" Inc. në vazhdimësi ka pranuar të dërgojë të dhënat e përdoruesit në zbatim të vendimeve gjyqësore shqiptare. Kështu në kuadër të procedimit penal nr. 3771 të vitit 2016, të regjistruar për kryerjen e veprës penale "Përndjekja", ajo shoqëri ka dërguar të dhënat e përdoruesit të llogarisë së hapur në rrjetin social "Facebook", të përdorur nga personi i dyshuar, të cilat kanë mundësuar kryerjen e veprimeve të tjera hetimore në lidhje me të[18]. Të njëjtin qëndrim ka mbajtur subjekti "Facebook" Inc edhe në procedime të tjera penale[19]. Ndërkohë kjo qasje nuk prezantohet në marrëdhëniet me shoqëri të tjera të mëdha të ofrimit të shërbimeve të internetit, të cilat shfrytëzojnë diskrecionin për të vendosur refuzimin e kërkesave për të dhëna kompjuterike. Ky qëndrim pengon ecurinë e hetimeve të krimeve në fushën e teknologjisë, pasi vetëm nëpërmjet atij informacioni mund të identifikohet personi i dyshuar dhe të mundësohen mjetet e tjera të kërkimit të provës. Për këto arsye vlerësohet se diskrecioni i parashikuar për ISP, për dorëzimin ose jo së të dhënave kompjuterike, është një parim që nuk i përgjigjet nevojave të hetimit të krimit kompjuterik.

### *2.2 Sekuestrimi i të dhënave kompjuterike*[20]

Për të vendosur aplikimin ose jo të sekuestrimit të të dhënave apo sistemeve kompjuterike, ashtu siç u trajtua dhe në rastin e marrjes së të dhënave të përdoruesit, nevojitet të vlerësohet nëse rasti objekt hetimi përfshihet ose jo në kategorinë e krimeve

[17] "Explanatory Report to the Convention on Cybercrime", faqe 53. I disponueshëm në https://rm.coe.int/16800cce5b, në datë 10.09.2018.

[18] Shih vendimin dt.24.05.2017 të pushimit të çështjes penale nr.3771 të vitit 2016, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.

[19] Shih vendimin dt. 01.03.2017 të pezullimit të hetimeve paraprake të procedimit penal 5778 të vitit 2016, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë; vendimin dt. 10.03.2018 të pezullimit të hetimeve paraprake të procedimit penal nr. 6730 të vitit 2017, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.

[20] Shih nenin 208/a të Kodit të Procedurës Penale të Republikës së Shqipërisë.

që lidhen me teknologjinë e informacionit. Veç këtij kriteri, sekuestrimi i të dhënave kompjuterike, nuk është i lidhur me asnjë kusht tjetër ligjor[21]. Pavarësisht nga ky fakt, në praktikë, prokuroria në kërkesë dhe gjykata në vendimin e saj, merr në konsideratë lidhjen e objektit të sekuestrimit, pra së të dhënës apo sistemit kompjuterik, me faktin objekt hetimi.

Në vendimin gjyqësor përcaktohen të drejtat për të hyrë, kërkuar dhe marrë të dhënat kompjuterike në sistemin kompjuterik, si dhe ndalimi për kryerjen e veprimeve të mëtejshme. Lidhur me këtë parashikim ligjor konstatohen problematika pasi nga ana e gjykatës nuk saktësohen të drejtat e hyrjes dhe kërkimit së të dhënave në sistem, duke krijuar në këtë mënyrë mundësinë për organet e hetimit, për të aksesuar të gjithë pajisjen kompjuterike dhe duke rrezikuar të dhënat me karakter privat. Kështu në rastin e procedimit penal nr. 8774 të vitit 2014, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë, gjykata ka disponuar: "Lejimin e sekuestrimit e kontrollit së të dhënave dhe sistemeve kompjuterike si njësi qendrore, usb, telefona mobile, IPAD, TABLETA, CD, hard disqe të jashtëm apo të brendshëm, apo çdo forme tjetër memorieje kompjuterike, në pronësi, posedim, apo administrim të shtetasit K.G.; Të lejohet hyrja, kërkimi dhe marrja e të dhënave kompjuterike në sistemet kompjuterike objekt sekuestrimi, duke përfshirë, ndër të tjera, komunikimet elektronike si *email*, *Chat*, sms dhe çdo komunikim nëpërmjet programeve kompjuterike të tjera, në të cilat përmbahen të dhëna të dobishme për hetimin"[22]. Për të garantuar privatësinë e individit si organi i akuzës ashtu edhe gjykata kanë detyrimin për të kufizuar kërkesat apo vendimet e hartuara, vetëm në të dhënat dhe sistemet kompjuterike të lidhura me rrethanat objekt hetimi.

Veç sistemit kompjuterik të lidhur drejtpërdrejt me veprën penale të dyshuar, sekuestrimi dhe kërkimet shtrihen dhe në sisteme të tjera kompjuterike apo pjesë të tyre, kur ekzistojnë shkaqe të arsyeshme për të menduar se të aty janë memorizuar të dhënat e kërkuara kompjuterike[23]. Prokurori ose oficeri i policisë gjyqësore i deleguar, merr masa për të ndaluar kryerjen e veprimeve të mëtejshme ose për të siguruar sistemin kompjuterik, vetëm të një pjese të tij ose të një mjeti tjetër memorizimi të dhënash; për të nxjerrë dhe marrë kopje së të dhënave kompjuterike; për të penguar hyrjen në të dhënat kompjuterike, ose për t'i hequr këto të dhëna nga sistemet kompjuterike me të drejtë hyrjeje; ç) për të siguruar paprekshmërinë e të dhënave përkatëse, të memorizuara[24]. Në kryerjen e këtyre veprimeve organi procedues mund të asistohet nga eksperti përkatës.

Procedura e sekuestrimit të sistemeve apo të dhënave kompjuterike e parashikuar në legjislacionin shqiptar nuk është në përputhje të plotë me rregullimet normative të Konventës së Budapestit[25].

Në Konventë përcaktohet që hyrja apo kërkimi realizohet në një sistem kompjuterik apo të dhëna të tilla, kur ato janë memorizuar aty. Kodi procedural shqiptar nuk e ka

[21] Në nenin 208/a, prg.1 të Kodit të Procedurës Penale të Republikës së Shqipërisë parashikohet: "Në rastin e procedimeve për krime që lidhen me teknologjinë e informacionit, gjykata, me kërkesën e prokurorit, urdhëron sekuestrimin e të dhënave ose sistemeve kompjuterike. Në këtë vendim gjykata përcakton të drejtën për të hyrë, kërkuar dhe marrë të dhënat kompjuterike në sistemin kompjuterik, si dhe ndalimin për kryerjen e veprimeve të mëtejshme apo sigurimin e të dhënave ose të sistemit kompjuterik".

[22] Shih vendimin dt. 04.04.2018 të pezullimit të hetimeve paraprake të procedimit penal nr. 8774 të vitit 2014, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.

[23] Shih nenin 208/a, prg.2 të Kodit të Procedurës Penale të Republikës së Shqipërisë.

[24] Shih nenin 208/a, prg.3 të Kodit të Procedurës Penale të Republikës së Shqipërisë.

[25] Shih nenin 19 të "Konventës për krimin në fushën e kibernetikës", ratifikuar me ligjin nr.8888, datë 25.4.2002.

parashikuar një rrethanë të tillë, duke lejuar në këtë mënyrë që sekuestrimi të kryhet edhe për të dhëna që janë memorizuar në një vend tjetër, siç mund të jenë adresat e e-mailit dhe materialet përkatëse, të cilat ruhen në shtetin ku ushtron aktivitetin shoqëria që ofron shërbimin përkatës. Pavarësisht se këto materiale mund të aksesohen dhe administrohen nga territori shqiptar, memorizimi i tyre realizohet jashtë këtij territori. Për këto arsye sekuestrimi i këtyre të dhënave do të binte në kundërshtim me parimin e sovranitetit duke ngritur në këtë mënyrë diskutime mbi vlefshmërinë e veprimeve apo përdorshmërinë e provave. Nisur nga kjo analizë vlerësohet se dispozita procedurale mbi sekuestrimin e provave kompjuterike duhet të plotësohet, duke kufizuar kryerjen e veprimit vetëm për të dhënat të cilat janë memorizuar në territorin e Shqipërisë.

### *2.3 Kontrollet e provave kompjuterike* [26]

Në vitin 2017 pësoi ndryshime edhe procedura e kontrollit, në rastet kur këtij veprimi është e nevojshme t'i nënshtrohet një sistem informatik ose telematik[27]. Kështu kur ka arsye të bazuara se të dhënat, informacionet, programet informatike ose gjurmë të tyre, gjenden në një nga sistemet e mësipërme, edhe kur janë të mbrojtur me masa sigurie, gjykata merr vendim për kontrollin, duke urdhëruar masa teknike të përshtatshme, të cilat sigurojnë ruajtjen e të dhënave origjinale dhe nuk lejojnë ndryshimin e tyre. Vendimi i kontrollit duhet të përcaktojë llojin e informacionit që kërkohet dhe mënyrën e marrjes së tij[28]. Një rregullim i tillë ligjor duhet të merret në konsideratë në rastet e kryerjes së veprimeve hetimore në pajisjet e ndryshme elektronike.

Në praktikën e deritanishme, në rastin e nxjerrjes së të dhënave nga telefonat e lëvizshëm është përdorur këqyrja si mjet i kërkimit të provës. Këto sende janë sisteme kompjuterike sepse përmbushin përkufizimin e dhënë nga Konventa e Budapestit për të tilla sisteme, pasi janë pajisje që kryejnë procesime automatike së të dhënave[29]. Deri më tani marrja e të dhënave nga objektet e mësipërme realizohej nëpërmjet këqyrjes, ku përmbajtja e tyre verifikohej dhe administrohej nga organi hetimor më anë të dhënies së komandave të ndryshme të kërkimit dhe konstatimit viziv të informacionit të ruajtur. Një procedurë e tillë shoqërohet me problematika lidhur me integritetin e provës. Sistemi kompjuterik është një provë tejet e ndjeshme dhe çdo veprim i kryer në të shkakton ndryshim të vlerës "hash" të tij[30].

Një fakt i tillë krijon mundësinë e vënies në dyshim të vërtetësisë së provës dhe mund të shfrytëzohet nga personi i dyshuar për ta kundërshtuar atë dhe për të ngritur pretendime për shtimin, fshirjen apo ndryshimin e të dhënave informatike. Për të shmangur këtë mundësi nevojitet që përpunimi i telefonave të lëvizshëm, ashtu si edhe për llojet e tjera të sistemeve kompjuterike, të realizohet nga persona të specializuar dhe të pajisur me aparaturat dhe programet e nevojshme që mundësojnë administrimin e të dhënave duke mos cenuar integritetin e provës.

[26] Shih nenin 202/a, prg.2 të Kodit të Procedurës Penale të Republikës së Shqipërisë.
[27] Telematika është fusha e teknologjisë që merret me dërgimin e informacionit dixhital në distanca të gjata, duke përdorur forma komunikimi pa tel. Shih "Cambridge English Dictionary". I disponueshëm në datë 17.09.2018 në https://dictionary.cambridge.org.
[28] Shih nenin 202/a, prg.2 të Kodit të Procedurës Penale të Republikës së Shqipërisë.
[29] Shih nenin 1 të "Konventës për krimin në fushën e kibernetikës", ratifikuar me ligjin nr.8888, datë 25.4.2002.
[30] "Hash" është një algoritëm që kthen një sasi të ndryshme teksti në një vlerë të vogël, me gjatësi të pandryshuar. Shih https://encyclopedia2.thefreedictionary.com/Hash+(computer+science). Aksesuar në datë 17.09.2018.

## 2.4 Përgjimi në krimet kompjuterike[31]

Një tjetër mjet i kërkimit të provës që lidhet me sistemet dhe të dhënat kompjuterike është përgjimi. Ky veprim është i lejuar për çdo vepër penale me dashje kur kryhet me anën e mjeteve të telekomunikimit apo përdorimit të teknologjive informatike ose telematike[32]. Ndërkohë përgjimi i komunikimeve të zhvilluara me anë të kompjuterit është i lejuar në raste të tjera për krimet e kryera me dashje, për të cilat parashikohet dënim me burgim jo më pak, në maksimum, se shtatë vjet. Në lidhje me përgjimet e komunikimeve kompjuterike janë të zbatueshme të gjitha standardet e aplikuara edhe për llojet e tjera të përgjimit privat. Veprimi është i lejuar me vendim të gjykatës, mbi bazën e kërkesës së prokurorit. Ky i fundit ka të drejtë të autorizojë përgjimin në rastet kur nga vonesa shkaktohen dëme të rënda për hetimet dhe brenda 24 orëve duhet të kërkojë vleftësimin nga gjykata. Kjo e fundit duhet të shprehet brenda 24 orëve nga depozitimi i kërkesës[33].

Edhe lidhur me mjetin hetimor të përgjimit, kur komunikimet zhvillohen ndërmjet personave të ndodhur jo vetëm në Shqipëri por edhe jashtë vendit, nevojitet të analizohet parimi i sovranitetit. Sipas Konventës së Budapestit palët nënshkruese duhet të përcaktojnë në ligj që mjetet teknike të përgjimeve kompjuterike të ndodhen në territorin e brendshëm. Nëpërmjet tyre të realizohet mbledhja apo regjistrimi i përmbajtjes, në kohë reale, i shoqëruar me komunikimet e specifikuara në territorin e palës, të transmetuara me anë të një sistemi kompjuterik. Ndryshe nga rasti i sekuestrimit së të dhënave kompjuterike, ku, siç u trajtua më lart, në Konventë përcaktohet se duhet të jenë memorizuar brenda territorit të palës, një parashikim i tillë nuk është aplikuar lidhur me përgjimin. Një qëndrim i tillë është i lidhur me faktin se komunikimet që përgjohen zhvillohen në kohë reale, janë të aksesueshme dhe transmetohen në një sistem kompjuterik të ndodhur në territorin e shtetit autorizues të përgjimit. Për këto arsye vlerësohet se lejimi i përgjimit të komunikimeve kompjuterike, edhe pse mund të zhvillohet ndërmjet Shqipërisë dhe vendeve të tjera, nuk cenon sovranitetin e këtyre të fundit.

### *2.5 Ruajtja e përshpejtuar dhe mirëmbajtja e të dhënave kompjuterike* [34]

Shtete të ndryshme kanë afate të ndryshme të ruajtjes së të dhënave kompjuterike lidhur me përdoruesin e shërbimeve të internetit apo trafikut të komunikimit. Nga momenti i konstatimit të faktit penal dhe bërja e kallëzimit nga personat e interesuar, mund të kalojë një periudhë e gjatë. Gjithashtu për procedurat e marrjes së këtyre të dhënave mbi bazën e vendimit gjyqësor apo me anë të letërporosisë është e nevojshme një kohë e konsiderueshme. Këto rrethana përbëjnë shkaqe për kalimin e afateve ligjore të memorizimit së të dhënave të mësipërme duke shkaktuar humbjen e përhershme të tyre. Për këto arsye, ligjvënësi ka parashikuar procedurën e ruajtjes së përshpejtuar të tyre, e cila është kompetencë e prokurorit. Ky i fundit, mund të urdhërojë ruajtjen e përshpejtuar të së dhënave kompjuterike të caktuara, duke përfshirë të dhënat e trafikut, kur ka shkaqe të mjaftueshme për të besuar se të dhënat mund të humbasin, dëmtohen

[31] Shih nenin 221 të Kodit të Procedurës Penale të Republikës së Shqipërisë.
[32] Shih nenin 221/1, pika "b" të Kodit të Procedurës Penale të Republikës së Shqipërisë.
[33] Po aty.
[34] Shih nenin 299/a të Kodit të Procedurës Penale të Republikës së Shqipërisë.

ose ndryshohen[35].

Për disponimin e urdhrit të ruajtjes, organi i akuzës duhet të vlerësojë ekzistencën, ose jo, të rrezikut të humbjes, dëmtimit, apo ndryshimit të së dhënave. Vetëm kur konstatohet një rrezik i tillë, prokurori mund të urdhërojë personin që ka në zotërim, ose në kontroll të dhënat, që t'i ruajë dhe t'i mirëmbajë ato për 90 ditë, afat ky i cili mund të shtyhet vetëm një herë[36]. Ky parashikim ligjor është në përputhje të plotë me rregullimin e normuar në Konventën e Budapestit lidhur me ruajtjen e përshpejtuar së të dhënave[37]. Veç ruajtjes dhe paprekshmërisë së të dhënave, personi i ngarkuar është i detyruar t'i sigurojë prokurorisë, ose oficerit të policisë gjyqësore të autorizuar, zbulimin e një sasie të mjaftueshme së të dhënave të trafikut, në mënyrë që të mundësohet identifikimi i dhënësit të shërbimit dhe shtegu nëpërmjet të cilit komunikimi është transmetuar[38].

Palët nënshkruese të "Konventës për krimin në fushën e kibernetikës" kanë të drejtë që të kërkojnë ruajtjen e përshpejtuar së të dhënave edhe nga palët e tjera. Kështu, mund të kërkohet ruajtja e përshpejtuar e të dhënave të regjistruara nëpërmjet një sistemi kompjuterik, i cili ndodhet brenda territorit të palës së kërkuar. Një veprim i tillë realizohet, me kushtin që pala dërguese të shprehë vullnetin se do të bëjë një kërkesë për ndihmë të ndërsjellë, për të kërkuar hyrje të ngjashme, ngrirje, sigurim të ngjashëm, ose hapje së të dhënave[39]. Ruajtja e përshpejtuar e të dhënave është një mjet shumë efikas procedural, pasi garanton paprekshmërinë e të dhënave kompjuterike të dobishme për hetimin, pavarësisht kalimit të periudhave të gjata kohore.

## 3. Bashkëpunimi ndërkombëtar për krimin kompjuterik

Elementet e figurave të veprave penale të krimit kompjuterik, në një pjesë të konsiderueshme, shtrihen në dy ose më shumë shtete. Për këtë arsye, hetimi i tyre është i pamundur në mungesë të bashkëpunimit ndërkombëtar mes autoriteteve hetimore dhe të drejtësisë. Procedura e zakonshme, për realizimin e bashkëpunimit me qëllim marrjen e provave jashtë territorit shqiptar, është letërporosia për jashtë shtetit[40]. Me anë të kërkesës për ndihmë juridike në fushë penale, kërkohet kryerja e veprimeve të ndryshme hetimore, si: pyetja e personave që kanë dijeni për rrethanat e hetimit, pyetja e personave të dyshuar, këqyrja dhe marrja e dokumenteve, sekuestrimi dhe kontrolli i pajisjeve kompjuterike, ekspertimi i tyre dhe veprime të tjera të nevojshme.

Konventa e Budapestit parashikon që shtetet palë të ofrojnë bashkëpunim me njëritjetrin në masën më të gjerë të mundur, në rastet e çështjeve penale të lidhura me sistemet apo të dhënat kompjuterike ose për mbledhjen e provave në formë elektronike për një vepër penale[41]. Nëse ekzistojnë kushtet e urgjencës shtetet nënshkruese mund të kërkojnë dhe ofrojnë ndihmë juridike nëpërmjet mënyrave të sigurta të komunikimit elektronik. Emergjenca, mund të lidhet me rrezikun e zhdukjes së të dhënave kompjuterike, apo me veprat penale, që dëmtojnë rëndë pronën, apo jetën e personit[42].

[35] Shih nenin 299/a të Kodit të Procedurës Penale të Republikës së Shqipërisë.
[36] Shih nenin 299/a, prg.2 të Kodit të Procedurës Penale të Republikës së Shqipërisë.
[37] Shih nenin 16 të "Konventës për krimin në fushën e kibernetikës", ratifikuar me ligjin nr.8888, datë 25.4.2002.
[38] Shih nenin 299/b të Kodit të Procedurës Penale të Republikës së Shqipërisë.
[39] Shih nenin 29 të "Konventës për krimin në fushën e kibernetikës", ratifikuar me ligjin nr.8888, datë 25.4.2002.
[40] Shih nenin 509 të Kodit të Procedurës Penale të Republikës së Shqipërisë.
[41] Shih nenin 25 të "Konventës për krimin në fushën e kibernetikës", ratifikuar me ligjin nr.8888, datë 25.4.2002.
[42] "Explanatory Report to the Convention on Cybercrime", faqe 44. I disponueshëm në https://rm.coe.int/16800cce5b, në datë 10.09.2018.

Një mekanizëm shumë i vlefshëm për realizimin e bashkëpunimit ndërkombëtar, është rrjeti 24/7[43]. Konventa e Budapestit, përcakton detyrimin për shtetet palë, që të vendosin një person kontakti, që të punojë në mënyrë të pandërprerë. Synimi i këtij rrjeti është dhënia e ndihmës së menjëhershme për qëllimet e hetimeve, ose gjykimeve për veprat penale, në lidhje me sistemet dhe të dhënat kompjuterike, ose, për marrjen e provave në formë elektronike për një vepër penale[44]. Ndihma e ofruar nëpërmjet rrjetit 24/7, konsiston në dhënien e asistencës teknike, ruajtjen e përshpejtuar së të dhënave dhe marrjen e provave[45], duke dhënë informacion ligjor, dhe vendndodhjen e personave të dyshuar[46].

Lidhur me zbatimin e letërporosive, konstatohen probleme të ndryshme, si: vullneti jo në nivelin e duhur për të ofruar bashkëpunimin mes shteteve, zgjatja për kohë të konsiderueshme e ekzekutimit të veprimeve të kërkuara, mospërmbushja e kërkesave për marrjen e provave për shkak të numrit të lartë të letërporosive në drejtim të shteteve të caktuara, ekzekutimi i pjesshëm kërkesave për ndihmë juridike, apo mungesa e përgjigjeve në lidhje me to. Kështu, nga disa shtete nuk ekzekutohet letërporosia, madje mungon tërësisht korrespondenca në lidhje me to[47]. Ndër këto shtete, mund të përmenden Republika e Nigerisë dhe Republika Popullore e Kinës. Në mjaft procedime penale të tjera, rezulton se kthimi i përgjigjeve për letërporositë, bëhet pas një periudhe të gjatë kohore, fakt ky që shkakton zvarritje të procesit, rrezikon humbjen e provave dhe uljen e efektivitetit të hetimit. Kështu, në kuadër të procedimit penal nr. 7345, të vitit 2014, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë, të regjistruar për veprën penale "Mashtrimi kompjuterik", kthimi i përgjigjes nga autoritetet e drejtësisë së Mbretërisë së Bashkuar është realizuar rreth dy vite pas dërgimit të kërkesës për ndihmë juridike[48]. Vlen të përmendet gjithashtu se në shumë procedime të tjera penale, edhe pse zhvillohet korrespondencë me autoritetet partnere, plotësimi i kërkesave për ndihmë juridike bëhet pjesërisht, duke mos siguruar të dhënat e nevojshme për provueshmërinë e faktit objekt hetimi[49].

Një problem specifik që rezulton nga praktika e përditshme, është mos ekzekutimi i letërporosive nga autoritetet e drejtësisë së SHBA-së, në rastet e veprave penale me rrezikshmëri të ulët, si: "Përndjekja"[50], apo "Ndërhyrja në të dhëna kompjuterike"[51]. Në këto raste, ato autoritete shprehen se, për shkak të numrit të madh të kërkesave të tilla, prej tyre, është përcaktuar përparësi për trajtimin e veprave penale të lidhura me veprimtari terroriste, akte korruptive, krime ndaj jetës, apo vepra të tjera me rrezikshmëri të lartë, e për këto arsye, institucionet e drejtësisë së SHBA-së procedojnë me arkivimin

[43] Shih nenin 35 të "Konventës për krimin në fushën e kibernetikës", ratifikuar me ligjin nr.8888, datë 25.4.2002.
[44] Po aty.
[45] Në nenin 25 të "Konventës për krimin në fushën e kibernetikës" parashikohet që marrja e provës realizohet me anë të kërkesës për ndihmë juridike e për pasojë nëse ky veprim realizohet nëpërmjet rrjetit 24/7, në respektim të së njëjtës dispozitë, ky proces mund të kryhet vetëm në kushtet e urgjencës.
[46] "Explanatory Report to the Convention on Cybercrime", faqe 54. I disponueshëm në https://rm.coe.int/16800cce5b, në datë 10.09.2018.
[47] Shih vendimin dt. 15.04.2015 të pezullimit të hetimeve paraprake të procedimit penal nr. 8779 të vitit 2014, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.
[48] Shih vendimin dt. 14.07.2017 të pezullimit të hetimeve paraprake të procedimit penal 7345 të vitit 2014, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.
[49] Shih vendimin dt. 14.07.2017 të pezullimit të hetimeve paraprake të procedimit penal nr. 7347 të vitit 2014, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë; Shih vendimin dt. 30.10.2017 të pezullimit të hetimeve paraprake të procedimit penal nr. 2610 të vitit 2016, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë; Shih vendimin dt. 03.05.2018 të pezullimit të hetimeve paraprake të procedimit penal nr. 31 të vitit 2015, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.
[50] Shih nenin 121/a të Kodit Penal të Republikës së Shqipërisë.

e letërporosive të lidhura me krime të lehta[52].

Mosfunksionimi në nivelin e duhur, i bashkëpunimit mes autoriteteve të drejtësisë së shteteve të ndryshme, dëmton mjaft rëndë ecurinë e hetimeve të veprave penale në fushën e teknologjisë. Në mungesë të këtij bashkëpunimi është i pamundur identifikimi i autorit të veprës penale. Për këto arsye, nevojitet ngritja e nivelit të kooperimit mes trupave hetimore dhe gjyqësore të vendeve të ndryshme, me qëllimin për t'iu përgjigjur nevojave për një hetim të shpejtë dhe efikas të krimit kompjuterik.

## 4. Bashkëpunimi i organeve hetimore me sektorin privat

Shërbimet e internetit, në pjesën më të madhe të tyre, ofrohen nga subjektet private. Janë këto të fundit që organizojnë, kontrollojnë dhe ruajnë të dhënat që lidhen me veprimtarinë e kryera në rrjet nga individët. Për këto arsye organi procedues mund të sigurojë informacionin apo provat e nevojshme për hetimin vetëm me anë të bashkëpunimit me sektorin privat.

Ofruesit e shërbimit të internetit, kanë detyrimin për të ruajtur për një periudhë 2 vjeçare, të dhënat në lidhje me pajtimtarët. Konkretisht, ISP ruan të dhënat e nevojshme për ndjekjen dhe identifikimin e burimit/origjinës të komunikimit; identitetin e pajtimtarit (*user* ID) dhe numrin e telefonit të caktuar për komunikimet që hyjnë në rrjetin publik telefonik; emrin dhe adresën e pajtimtarit, ose përdoruesit të regjistruar, të cilit i është caktuar një adresë IP; identitetin e përdoruesit (user ID), ose numrin e telefonit të caktuar gjatë kohës së komunikimit; të dhëna të nevojshme për identifikimin e destinacionit të komunikimit, në rastin e telefonisë në internet; identitetin e përdoruesit (user ID), ose numrin e telefonit të numrit të thirrur, në rastin e postës elektronike ose telefonisë në internet; emrin dhe adresën e pajtimtarit ose përdoruesit të regjistruar dhe identitetin e përdoruesit (user ID) të marrësit të synuar të komunikimit; të dhëna të nevojshme për identifikimin e datës, kohës dhe kohëzgjatjes së komunikimit; datën dhe orën e lidhjes (*log in*), dhe shkëputjes (*log off*) të shërbimit të aksesit në internet, sipas orës lokale; adresën IP, duke përcaktuar nëse është dinamike apo statike, të caktuar nga ofruesi i shërbimit internet; identitetin e pajtimtarit ose përdoruesit të regjistruar të shërbimit të aksesit në internet[53].

Bashkëpunimi me sektorin privat prezanton një gamë të gjerë problematikash, ekzistenca e të cilave vështirëson, e madje në disa raste e bën të pamundur, identifikimin e autorit të veprës penale. Pavarësisht detyrimit ligjor për ruajtjen e të dhënave të lartpërmendura deri në identifikimin individual të pajtimtarit apo përdoruesit të internetit, për shkak të pamjaftueshmërisë së infrastrukturës së nevojshme teknike, ISP-të, në një numër të konsiderueshëm rastesh, nuk kanë mundur t'i ruajnë dhe t'i vënë këto të dhëna në dispozicion të organeve hetimore. Për shkak të numrit të kufizuar të adresave IP[54] shoqëritë ofruese të shërbimit të internetit përdorin teknologjinë

[51] Shih nenin 292/b të Kodit Penal të Republikës së Shqipërisë.

[52] Shih vendimin dt. 10.03.2016 të pezullimit të hetimeve paraprake të procedimit penal nr. 8797 të vitit 2014, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.

[53] Shih nenin 101 të ligjit Nr.9918, datë 19.5.2008 " Për Komunikimet Elektronike në Republikën e Shqipërisë" (I ndryshuar).

[54] Shkronjat "IP" janë shkurtim i fjalëve "Internet Protocol" (protokolli i internetit). Internet Protocol është seti i rregullave që rregullojnë mënyrën e transmetimit të paketave në një rrejt. https://www.lifewire.com/internet-protocol-explained-3426713. Aksesuar në datë 18.09.2018.

NAT[55], duke mundësuar përdorimin e rrjetit nga një numër i madh pajtimtarësh, nëpërmjet përdorimit të së njëjtës IP. Për këtë arsye ISP, në një numër të madh rastesh, nuk mundësojnë identifikimin e të dyshuarit që ka kryer veprën penale[56]. Në këto kushte është e nevojshme që shoqëritë ofruese të shërbimit të internetit, në respektim të detyrimeve ligjore që normojnë veprimtarinë e tyre, të ndërmarrin masat e nevojshme për përmirësimin e infrastrukturës teknike, me qëllimin për të mundësuar ruajtjen e të dhënave të pajtimtarëve, apo të përdoruesve të internetit.

## 5. Përfundime

1. Të dhënat e përdoruesit, vlerësohet se nuk kanë të njëjtën natyrë me përmbajtjen e komunikimeve kompjuterike, pasi ndryshe nga këto të fundit, ku individi ushtron jetën e tij private, ato, pra, të dhënat e përdoruesit, paraqesin rrethana që shërbejnë për identifikimin e personit, apo të lidhjes që ai ka krijuar me internetin. Për këtë arsye, vlerësohet i papërshtatshëm, kufizimi ligjor sipas të cilit administrimi i këtyre të dhënave, duhet të autorizohet vetëm nga gjykata.

2. Diskrecioni i parashikuar për ISP të huaja, për dorëzimin, ose jo, së të dhënave kompjuterike, është një parim që nuk i përgjigjet nevojave të hetimit të krimit kompjuterik.

3. Për të evituar diskutimet mbi vërtetësinë e të dhënave dhe sistemeve kompjuterike, nevojitet, që përpunimi i tyre, të realizohet nga persona të specializuar dhe të pajisur me aparaturat dhe programet e nevojshme, që mundësojnë administrimin e të dhënave, duke mos cenuar integritetin e provës.

4. Dispozita procedurale mbi sekuestrimin e provave kompjuterike, duhet të plotësohet, duke kufizuar kryerjen e veprimit vetëm për të dhënat të cilat janë memorizuar në territorin e Shqipërisë.

5. Lejimi i përgjimit të komunikimeve ndërkombëtare kompjuterike, edhe pse zhvillohet ndërmjet Shqipërisë dhe vendeve të tjera, nuk cenon sovranitetin e këtyre të fundit.

6. Ruajtja e përshpejtuar e të dhënave është një mjet shumë efikas procedural, pasi garanton paprekshmërinë e të dhënave kompjuterike të dobishme për hetimin, pavarësisht kalimit të periudhave të gjata kohore.

7. Mosfunksionimi në nivelin e duhur, i bashkëpunimit mes autoriteteve të drejtësisë së shteteve të ndryshme, dëmton mjaft rëndë ecurinë e hetimeve të veprave penale në fushën e teknologjisë. Në mungesë të këtij bashkëpunimi, është i pamundur identifikimi i autorit të veprës penale. Për këto arsye nevojitet ngritja e nivelit të kooperimit mes trupave hetimore dhe gjyqësore të vendeve të ndryshme, me qëllimin për t'iu përgjigjur nevojave për një hetim të shpejtë dhe efikas të krimit kompjuterik.

8. Është e nevojshme, që shoqëritë ofruese të shërbimit të internetit, në respektim të detyrimeve ligjore që normojnë veprimtarinë e tyre, të ndërmarrin masat e nevojshme për përmirësimin e infrastrukturës teknike, me qëllim që të mundësojnë ruajtjen e të dhënave të pajtimtarëve, apo përdoruesve të internetit.

[55] Përkthyesi i adresës së rrjetit (NAT) është një funksion shpërndarës që mundëson lidhje rrjeti dhe lejon komunikim përmes një adrese të vetme IP. NAT përdoret si një zgjidhje efektive në kohë për trafikun e rëndë të rrjetit. Shih https://www.techopedia.com/definition/4028/network-address-translation-nat. Aksesuar në datë 18.09.2018.

[56] Shih vendimin dt. 01.04.2017 të pezullimit të hetimeve paraprake të procedimit penal nr. 5772 të vitit 2016, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.

# Bibliografi


1. Ligji nr. 10 054, datë 29.12.2008 "Për disa shtesa dhe ndryshime në ligjin nr. 7905, datë 21.3.1995 "Kodi i Procedurës Penale i Republikës së Shqipërisë", i ndryshuar.
2. "Konventa për krimin në fushën e kibernetikës", ratifikuar me ligjin nr. 8888, datë 25.4.2002.
3. Ligji nr. 7905, datë 21.3.1995, "Kodi i Procedurës Penale i Republikës së Shqipërisë", i ndryshuar.
4. Ligji Nr. 9918, datë 19.5.2008 "Për Komunikimet Elektronike në Republikën e Shqipërisë" (I ndryshuar).
5. "Explanatory Report to the Convention on Cybercrime".
6. Vendimi dt. 24.05.2017 i pushimit të çështjes penale nr. 3771 të vitit 2016, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.
7. Vendimi dt. 01.03.2017 i pezullimit të hetimeve paraprake të procedimit penal nr. 5778 të vitit 2016, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë;
8. Vendimi dt. 10.03.2018 i pezullimit të hetimeve paraprake të procedimit penal nr. 6730 të vitit 2017, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.
9. Vendimi dt. 04.04.2018 i pezullimit të hetimeve paraprake të procedimit penal nr. 8774 të vitit 2014, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.
10. Vendimi dt. 15.04.2015 i pezullimit të hetimeve paraprake të procedimit penal nr. 8779 të vitit 2014, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.
11. Vendimin dt. 14.07.2017 i pezullimit të hetimeve paraprake të procedimit penal nr. 7345 të vitit 2014, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.
12. Vendimi dt. 14.07.2017 i pezullimit të hetimeve paraprake të procedimit penal nr. 7347 të vitit 2014, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.
13. Vendimi dt. 30.10.2017 i pezullimit të hetimeve paraprake të procedimit penal nr. 2610 të vitit 2016, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.
14. Vendimi dt. 03.05.2018 i pezullimit të hetimeve paraprake të procedimit penal nr. 31 të vitit 2015, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.
15. Vendimi dt. 10.03.2016 i pezullimit të hetimeve paraprake të procedimit penal nr. 8797 të vitit 2014, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.
16. Vendimi dt. 01.04.2017 i pezullimit të hetimeve paraprake të procedimit penal nr. 5772 të vitit 2016, të Prokurorisë pranë Gjykatës së Shkallës së Parë, Tiranë.
17. "Cambridge English Dictionary". I disponueshëm në https://dictionary.cambridge.org.
18. https://encyclopedia2.thefreedictionary.com/Hash+(computer+science).
19. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
20. https://www.lifewire.com/internet-protocol-explained-3426713.
21. https://www.techopedia.com/definition/4028/network-address-translation-nat.

# Rëndësia e të mësuarit *mikro* në organizatë


**Prof. Asc. Gaqo TANKU**
*Universiteti "Aleksandër Moisiu", Durrës*
*gaqotanku@hotmail.com*

**Dr. Piro TANKU**
*Universiteti "Aleksandër Moisiu", Durrës*

**MSc. Aida DELIU**
*Universiteti "Aleksandër Moisiu", Durrës*



**Abstrakt**

*Mikromësimi është një qasje gjithëpërfshirëse për mësimin e bazuar në aftësi, në edukimin, i cili ka për objekt njësi relativisht të vogla të të mësuarit. Ai përfshin strategjitë afatshkurtra veçanërisht për kuptimin e aftësive, të mësuarit dhe edukimit. Mësimi "mikro" i referohet mikroperspektivave të të mësuarit, arsimit, trajnimit dhe zhvillimit të aftësive. Qasjet e ndjekura për vlerësimin e të mësuarit mikro janë shumëdimensionale dhe gjithëpërfshirëse, në natyrë dhe në nevoja të bazuara në raste të veçanta. Kjo është një qasje ideale mësimore për shumë situata, sidomos në arsimin e lartë, për zhvillimin e aftësive, kompetencave dhe punësimit të nxënësve (shkollat profesionale) apo studentëve. Teknikat e mikromësimit ndihmojnë që punonjësit apo studentët që janë të ngadalshëm në përvetësimin e dijes, të përballojnë më lehtë sfidat. Pa u kujdesur për mikroperspektiva në kontekstin e të mësuarit, edukimit, trajnimit dhe zhvillimit të aftësive, arsimi i bazuar në kompetenca nuk mund të transmetohet në mënyrë efektive. Ky hulumtim ka të bëjë me mikromësimin në organizatë. Ne jemi një vend që po zhvillohet edhe në përdorimin e teknologjisë. Tema kryesore e punimit: është qasja në përkufizimin e të mësuarit mikro, si ndihmon në organizatë, si mund të ndikojë tek punonjësit, si mund të ndikojë në rritjen e përdorimit të teknologjisë në kompani? A do të shkaktojë rritje të kostos për organizatën? A do të jetë kjo negative për kompanitë, pasi ne e dimë se një nga prioritetet e kompanive është minimizimi i kostove.*



**Fjalëkyçe:**
**të mësuarit mikro, kompani, organizatë, teknologji, produkti.**

## 1. Hyrje

Në fushën e ndryshimeve të mëdha të *eLearning*, mikromësimi është një arritje e re dhe i përgjigjet nevojës urgjente për të treguar vëmendje të madhe mjeteve dhe metodave të *eLearning*, parë nga këndvështrimi i të mësuarit dhe jo nga këndvështrimi teknologjik. Agjenda e mikromësimit kryesisht fokusohet te mësimi informal dhe që shikohet si një meteor në ngjitje në arsimimin Europian, përfshi dhe politikat e trajnimit (Pappas, 2017).

Sot nuk është shumë e lehtë për të gjetur një punë të mirë, ku mund të mësosh më shumë dhe të japësh sa më shumë dije. Gjate procesit të intervistimit, disa punonjës të kompanive që merren me eksportin, e konsideronin mundësi të madhe dhe pjesë e atij vendi pune që quhet "krem i kremit të biznesit". Fillimisht ata kishin informacion të përgjithshëm. Kompania është shoqëri aksionare me 100% kapital shqiptar dhe ndërvepron me shumë shtete europiane dhe aziatike.

Veprimtaria kryesore është përqendruar në importimin, eksportimin, prodhimin dhe shitjen me shumicë dhe pakicë të artikujve me prodhim druri dhe metale e nënprodukteve të tyre si mobilie, pajisje zyrash, spitalesh dhe objekte të tjera publike. Këto marrëdhënie kanë bërë të mundur njohjen në treg si firmë me shumë eksperiencë, duke qene aktive në një treg dinamik dhe në përballjet me konkurrentet ndërkombëtar. Shitjet bazohen në ndërtimin e marrëdhënieve të forta dhe afatgjata me klientët, furnizuesit dhe stafin. Më konkretisht kompania "Shpiragu GGH LTD "ofron produkte si vegla dore, ndriçim dhe materiale elektrike, hidraulike, ndërtimi, mobilie dhe dekorime (brenda dhe jashtë) etj. Në këtë mënyrë plotësojnë të gjitha kërkesat, jo vetëm për nevoja familjare, por edhe të bizneseve dhe institucioneve.

Disa të intervistuar që punonin në sektorët financiarë, port ë rinj në profesion mendonin se puna e tyre do të ishte e vështirë për shkak të numrit të madh të punonjësve me përvojë, të cilët kanë vite dhe janë të mirëtrajnuar profesionalisht. Struktura e kompanisë përbëhet nga departamente si financa, marketingu, zyra juridike, burimet njerëzore dhe shitjet. Secili punon duke qenë pjesëtar i strukturave të kompanisë, por e ndjejnë sikur të jetë pjesë e një makine të madhe, që kurrë nuk ndalon të punojë dhe të prodhojë vetëm. Këtu CEO ka një moto për çdo punonjës: mos kini frikë nga dështimi, ai është pjesë e punës. Nëse dështoni herën e parë, do të arrish suksesin patjetër herën e dytë. Eksperienca e kompanive të ndryshme në vendin tonë, tregon se ka edhe eksperienca jo pozitive, ku në rast gabimi punonjësit nuk i jepet një mundësi e dytë, e akoma më keq i largojnë nga puna. Sa më i lartë b/punimi midis njësive, aq me e lartë do të jetë edhe performanca e organizatës. Ekzistenca e barrierave midis njësive të ndryshme të prodhimit pengon komunikimin, çka ndikon në performancë. Në kompaninë objekt studimi presidenti dhe zyra e tij janë të hapura për stafin. Nëse ka diçka për të thënë, ata janë të hapur për çdo problem, familjar, shëndetësor apo të punës. Në këtë mënyrë krijojnë marrëdhënie si në familje.

## 2. Çfarë është *mikromësimi*?

Mikromësimi është një qasje gjithëpërfshirëse për mësimin, bazuar në aftësi, në arsimin, i cili merret me njësi relativisht të vogla të të mësuarit. Mikromësimi është të mësuarit në një grup të vogël, për një periudhë kohore 5-15 minuta e duke marrë "fidbek" rreth performancës. Do të jetë gabim ta trajtosh çështjen e mikromësimit si çështje e edukimit formal, e trajnimit nga mësuesit apo nga këndvështrimi pedagogjik (Jomah et al, 2016:104).

Mikromësimi përfshin strategjitë afatshkurtra të dizajnuara dhe të mbështetura në kuptimin e aftësive dhe mësimnxënies. Mësimdhënia i referohet mikroperspektivave të të mësuarit, trajnimit dhe zhvillimit të aftësive. Qasjet për vlerësimin e mikromësimit janë shumëdimensionale dhe gjithëpërfshirëse, me synim gjetjen e zgjidhjeve në raste të veçanta. Kjo është një qasje ideale mësimore për shumë situata, sidomos në arsimin e lartë, me qëllim zhvillimin e aftësive për punësimin e studentëve. Teknika është mjaft e mirë për të përballuar sfidat që lidhen me ata që përparojnë ngadalshëm. Kjo teknikë është e gjithanshme jo vetëm për edukimin bazuar në aftësitë e individit, por edhe për zhvillimin e qëndrueshëm socio-ekonomik. Pa marrë parasysh mikroperspektivat në kontekstin e të mësuarit, arsimit, trajnimit dhe zhvillimit të aftësive, arsimimi dhe dija nuk mund të transmetohet në mënyre efektive.

Në një kuptim të gjerë, mikromësimi mund të kuptohet si një metaforë, e cila i referohet aspekteve mikro të një shumëllojshmërie të modeleve, koncepteve dhe proceseve të mikromësimit. Në varësi të kuadrit dhe kontekstit të referencës, që mund të jenë të nivelit mikro, mesatar dhe makro, të aspekteve të ndryshme me variacionet e tyre të cilat janë koncepte të ndërlidhura njëra me tjetrën, p.sh: në kontekstin e mësimit të gjuhës, mund të mendohet për aspektet mikro në kuptimin e fjalive, frazave, të cilat do t'i dalloni nga situatat, episodet dhe specifikat socio-kulturore. Në një diskutim në rrafsh të gjerë procesi i të mësuarit, përfshin dallimin mes të mësuarit në mënyrë individuale, të mësuarit në grupe, të mësuarit në organizatë apo të mësuarit që bëjnë gjeneratat/shoqëritë. Tre arsye për të lëvizur drejt mikromësimit sipas Peter A. Bruck, janë: ulja e ngarkesës dhe kompleksitetit të informacionit, strukturimi dhe ndarja për

zbatim në pjesëza dhe linja të vogla; ulja e informacionit duhet parë nga perspektiva e personit që do të përballet me këtë shumësi informacioni për ta mësuar; individët të lejohen ta zgjedhin vetë kohën, vendin dhe hapësirën e të mësuarit, ndërkohë që kjo kërkon që tu sigurohet teknologjia e duhur (Peter A. Bruck, 2012:22).

Për më tepër, mikromësimi shënon një kalim nga modelet e zakonshme të të nxënit, drejt mikroperspektivave dhe mikrodimensioneve në procesin e të mësuarit. Fokusi në rritje në aktivitetet e mikromësimit, mund të shihet nga aktivitetet e përdoruesve të internetit, të cilët shënojnë postimet e tyre në *blog*-e dhe rrjetet sociale me termin "mikromësim". Si një teknologji mësimore, mikromësimi fokusohet në dizajnimin e aktiviteteve të tij, përmes hapave mikro në mjediset e medies digjitale, e cila tashmë është një realitet i përditshëm për punëtorët me dije. Këto aktivitete mund të përfshihen në rolin dhe detyrat e përditshme. Ndryshe nga qasjet tradicionale të mësimit elektronik, mikromësimi shpesh tenton nxitjen përmes teknologjisë, kryesisht asaj të medieve, dije e cila kërkon më pak energji për tu përvetësuar. Mikromësimi, me pak fjalë, është një përvojë digjitale për të mësuar që të jesh efektivë, i angazhuar por duke marrë edhe kënaqësinë.

## 3. Karakteristikat e mikromësimit

Proceset e të mësuarit mikro, shpesh rrjedhin nga ndërveprimi me përmbajtjen mikro, që ndodh si në ambiente të përcaktuara (*e-learning*) ose në strukturat mikro. Kjo lidhet me përmbajtjen e momentit, si postimet në *blog*-e ose programe të rrjeteve sociale në *World Wide Web*. Të mësuarit mikro, mund të jetë një supozim për kohën e nevojshme për të zgjidhur një detyrë mësimore, p.sh. duke iu përgjigjur një pyetje, monitoron një informacion ose një burim që të nevojitet. Proceset e quajtura "të mësuarit mikro" mund të kërkojnë një hapësirë kohore prej disa sekondash (p.sh. të mësimit në celular) deri në 15 minuta apo më shumë.

Ekziston një lidhje me termin mikromësimdhënie, e cila është praktikë e krijuar në fushën e përgatitjes se mësuesve. Mikromësimi mund të kuptohet si proces i aktiviteteve në vijim, pra e të mësuarit në një kohë të shkurtër. Kjo ndodh nëpërmjet ndërveprimit me objektet e mikropërmbajtjes në afate të shkurtra kohe. Në këtë rast, dizajnimi, përzgjedhja, reagimi dhe shpejtësia e detyrave (proceseve) të përsëritura, ndryshe "të lidhur me zinxhirë" të mikromësimit del në pah. Në një kuptim më të gjerë, mikromësimi është term që mund të përdoret për të përshkruar mënyrën se si gjithnjë e më shumë, njerëzit mësojnë përmes të mësuarit joformal, duke fituar njohuri në mjedise me përmbajtje mikro, veçanërisht ato që bazohen në teknologjinë e transmentimit wireless (Giurgiu, 2017).

## 4. Dimensionet e mikromësimit

Dimensionet e mëposhtme mund të përdoren për të përshkruar ose dizajnuar aktivitetet e mikromësimit:

*Koha*: përpjekje relativisht e shkurtër, shpenzimet operative, shkalla e konsumimit të kohës, koha e matshme, koha subjektive etj.

*Përmbajtja*: njësi të vogla ose shumë të vogla, tema të ngushta, çështje shumë të thjeshta etj.

*Kurrikula*: pjesë e vogël e vendosjes kurrikulare, pjesë të moduleve, elemente të

mësimit joformal, etj.

*Formulari*: fragmente, aspekte, episode, "copëza dijesh", elemente aftësie, etj.

*Procesi*: veprimtari të veçanta, aktuale, të vendosura/të integruara, metoda interaktive, menaxhimi i vëmendjes, ndërgjegjësimi (futja në ose duke qenë në proces) etj.

*Mënyrat*: ballë për ballë, mediet e shkruara, mediet elektronike, mediet multimediale, multimedia, format e ndërmjetësuara (inter-), objekte informuese, vlerat simbolike, kulturat bazike, etj.

*Lloji mësimor:* përsëritës, aktivist, reflektues, pragmatist, konceptualist, konstruktivist, lidhës, sjellës; gjithashtu mësimi përmes veprimit, mësimi në klasë, mësimi i korporatave etj (Hug 2005: 152-175).

## 5. Përparësitë e mikromësimit

1. *Personalizimi dhe autonomia*. Secili aset i mikromësimit është i përcaktuar për krijimin e të dhënave që duhen. Njerëzit mund të gjejnë lehtë atë dije që i nevojitet për të kryer detyrat e lidhura me punën. Kjo nxit autonominë, nxit më shumë interesin dhe motivimin. Ka më shumë gjasa të aplikojnë dijet në punë dhe të kërkojnë akoma më shumë zhvillimin e tyre.

*2. Të mësuarit në kohë (Just in time).* Mikromësimi mbështet punonjësit kur kanë më së shumti nevojë për informacion. Për shkak se asetet janë kompakte, ata kanë më shumë mundësi të investojnë kohën e nevojshme për t'i përdorur ato në kontekstin e punës. Më tej, dijet e zhvilluara dhe të shoqëruara nga një shumëllojshmëri e gjerë e pajisjeve, i lejon t'i përdorin kur dhe ku është më e dobishme. Si rezultat, mikromësimi bën të mundur që personeli të fitojë njohuri të reja, në kohë të shkurtër, duke përmbushur nevojat e menjëhershme.

*3. Mësim efektiv dhe i larmishëm.* Mikromësimi mbështetet nga një shumëllojshmëri e modaliteteve të ndryshme, të cilat krijojnë përvojat e trajnimit efektiv dhe shumë të ndryshme në fushën e mësimdhënies. Dijet e përfituara nga mikromësimi janë kompakte dhe të fokusuara në objektiva specifike. Përdorimi në mënyrë më specifike bën që trajnimi të jetë më efektiv. Efektiviteti dhe shumëllojshmëria e përvojave të trajnimit, rrisin angazhimin e pjesëmarrësve.

*4. Përparësitë e trajnerëve.* Mikromësimi ofron lehtësi të mëdha për trajnerët dhe departamentet e mësimit dhe zhvillimit. Nisur nga madhësia e tyre e vogël, asetet e mikromësimit mund të jenë më të lehta dhe të përballueshme për tu prodhuar dhe ruajtur. Megjithatë, mund të përdoren lehtësisht edhe për qëllime të tjera, si komponentë për ndërmarrjen e iniciativave më të mëdha në fushën e trajnimit, si mjete komunikimi etj.

*5. Grackat e mundshme të mikromësimit.* Ndërsa mikromësimi ofron përparësi të dukshme, ndjekja e një strategjie trajnimi që mbështetet shumë te mikromësimi, mund të sjellë pengesa. Për shkak se mikromësimi rezulton në shumë pjesë të vogla trajnuese, lehtësisht personeli ndjehet sikur u mungon pamja e madhe, apo ajo që u krijon një përvojë jokonsistente në praktikat e trajnimit. Prof. Erich Neuhold, thekson sfidat me të cilat përballet mikromësimi si: ndërveprimi që shkon përtej "vazhdo në hapin tjetër"; të mësuarit personal nuk duhet të pengohet nga standardet dhe metodat; integrimi i fidbekut në një proces kompleks të mësuari; karakteri i të cilit ende nuk është kuptuar mjaftushëm; aspektet sociale të të mësuarit individual përmes bashkëpunimit në procesin

e punës në ekip dhe integrimi i *eLearning* në organizatë (Erich Neuhold, 2005:27).

Praktikat më të mira që do të ndihmojnë në shmangien e këtyre kurtheve përfshijnë:

Ndërto lidhjet mes aseteve të ndryshme të mikromësimit. Ndërtimi i lidhjeve midis aseteve të mikromësimit dhe aseteve të trajnimit. Përcakto standarde të qarta, që krijojnë qëndrueshmëri në zhvillimin e mikromësimit. Përdorni në mënyrë strategjike fjalët, imazhet dhe parimet kryesore në tëre procesin e mikromësimit. Identifikimi i trajnimeve të lidhura ngushtë me asetet e mikromësimit, duke krijuar lidhje midis mjeteve tuaja të trajnimit e vendosur standarde të qarta për nevojat dhe përvojën e përdoruesve, duke i përdorur ato të dhëna për të ndihmuar personelin të gjej burime që lidhen me trajnimin. Në këtë mënyrë do të krijohet një eksperiencë kohezive dhe konsistente, e cila ndihmon personelin të kuptoj tablonë e madhe.

## 6. Metodologjia

Metodologjia siguron mbështetje teorike për të kuptuar se cila metodë, grup metodash ose praktika të mira, mund të zbatohen në rastin në shqyrtim. Ne kemi shumë mënyra për të bërë një kërkim shkencor, specifik për organizatën. Mund të përdorim resurse të ndryshme, si të dhëna primare, sekondare dhe terciare. Në organizatë mund të përdorim informacione të ndryshme nga interneti, *software* të reja për programe të reja. Pjesëmarrësit përdorin teknika si intervistat, ditarët ose fokus grupet, ku mund të analizohen të dhënat mbi të cilat analisti reflekton duke u fokusuar në opinionin e përgjithshëm e bazuar në përvojat e pjesëmarrësve. Analiza është ajo që balancon përshkrimin fenomenologjik me një kuptim të qartë e të thellë të interpretimit, duke i ndërlidhur këto interpretime me ato të pjesëmarrësve.

## 7. Aspekte praktike të mikromësimit në organizatë

Aktivitetet e mikromësimit si definicion, mbështeten te aksesi i burimeve për të mësuar, të cilat mund të ndodhin në kohën e pushimit ose hapësirat që krijohen gjatë ditës së punës (aktivitetit të përditshëm). Në këto kushte, mikromësimi është forma më tipike e të mësuarit kudo dhe në çdo kohë (Fox 2016:116).

Më sipër u trajtuan aspekte teorike të mikromësimit. Le të shikojmë në vijim aspekte praktike. Gjate procesit të intervistimit një nga punonjësit u shpreh se kur erdhi në fillim nuk kishte dijet e plota. Ishte fillestar dhe me praktikë zero. Presidenti e prezantoi si pjesëtarë te stafi i departamentit të financës. Në fillim u trondit, u ul në karrigen e punës dhe pa vetëm kompjuterin dhe shumë dosje. Nuk dinte nga ta fillonte dhe shkoi te CEO, ku theksoi se e kishte të vështirë. Ndërkohë CEO vajti në zyrën e ekonomistëve dhe u tha se duhet ta trajnonin për të bërë punën.

Një tjetër i intervistuar, theksoi se kolegët më me eksperiencë, shkruanin në një fletore gjithçka që ai kishte nevojë, p.sh. si skedarët të vendoseshin në rregull, si të plotësoheshin faturat, si të kryenin transferimet bankare. Ky ishte një proces që mori kohën e tij, por i domosdoshëm për të gjithë ata që janë të rinj në këtë punë.

Marrja e faturave për konsumatorët nuk është aq e lehtë sa mendojmë. Duhen bërë shumë llogari për t'u marrë me çmimin që dëshirojmë. Kur marrim porosi me *email* dhe na thonë se klientët kanë nevojë për një ofertë nga kompania, se duan çmimet më të ulëta që ofrohen. Në këto kushte, duhet të bëjmë gati porosinë, ta dërgojmë në departamentin e shitjeve dhe të fillojmë negociatat.

I intervistuari tjetër, theksoi se në rastet e blerjeve për furnizuesit që janë jashtë shtetit, negociatat fillojmë përmes blerjeve të produkteve aq të lira sa munden, pasi kur produktet vijnë nga jashtë, ka një sërë kostosh si Tatimi mbi Vlerën e Shtuar (TVSH), Tatimi Doganor (CT), etj. Në këtë rast, ky i intervistuar, vlerëson trajnuesin e tij pasi ishte negociues shumë i mire dhe me eksperiencë. Fleksibiliteti dhe efikasiteti i tij ishte modeli më i mirë.

Për të thelluar akoma më shumë dijet, është e domosdoshme njohja e programeve ekonomike si *Financa* 5, *Alpha* etj, të kesh kompjuterët e duhur, si të kërkosh në internet, programi për llogaritë bankare, që është një program i veçantë, i cili lejon të shikosh transferimet, gjendjen e llogarisë dhe xhiron e brendshme të bankës. Programi Financa 5, është programi kryesor, pasi i shërben të gjithë operatorëve të biznesit sipas funksioneve që ata kryejnë në kompani si shitjet, të cilat janë niveli më i lartë i vendimmarrjes lidhur me administrimin dhe menaxhimin financiar. Organizimi i punës me Financën 5 funksionon sipas moduleve, ku e drejta e përdorimit të sistemit është e kufizuar ose e lejuar sipas funksionit që kryen çdo operator i programit. Në vijim të procesit të intervistimit, një specialist theksoi se trajneri e mësoi si të kryente transfertat bankare dhe si t'i kontrollonte ato. Fillimisht e mësoi si të futej në sistem, të shkonte te skedari i bankës dhe të klikonte.

Si punohet me *Alpha Web Series,* – duke mbajtur kontakt, pavarësisht distancës. Mjafton që të ketë lidhje interneti dhe në këtë mënyrë zgjidhen edhe problemet e komunikimit me degët e largëta; *Alpha Platinium* ofrohet për raportet financiare me standardet e reja kombëtare të kontabilitetit dhe raportet menaxheriale; Special *Alpha Solutions*, përdoret më shumë për dyqanet, personelin e barit, menaxhimin e projekteve dhe institucionet publike; Kontabiliteti *Alpha*, është i lehtë për t'u përdorur dhe ofron një gamë të gjerë funksionesh. Ka module të ndryshme (prodhimi, qendrat e kostos, amortizimi i aseteve etj). Këto integrohen në një *software* (Bower et al, 2017).

Mësimi i programeve nuk është shumë i vështirë, por trajnuesi duhet të jetë shumë i duruar për t'i mësuar si punonjësit të kryejnë vetë veprimet. Kjo është pjesë e pandashme e mikromësimit. Kur jemi në një drejtori finance, mësojmë si të jemi fleksibël me departamentet e tjerë, pasi gjithçka është e lidhur me financën. Nëse departamenti i marketingut dëshiron të krijojë reklamë tregtare në TV, duhet të shkojmë te financa për të rënë dakord me vlerën që kompania do të shpenzoj për një reklamë. Nga ana tjetër, departamenti i burimeve njerëzore lidhet me financën për pagesat e personelit. Kur një punonjës dëmtohet në punë, burimet njerëzore informohen për të paguar sigurimet shëndetësore dhe rrogën deri sa të shërohet.

E rëndësishme është të dimë se çdo gjë është kosto. Për ta mësuar, duhet të përpiqemi të gjejmë produktet cilësisht më të mira. Është e rëndësishme të mësojmë si të plotësosh një TVSH, pasi një faturë e TVSH-së është një shitje e faturës tatimore, ku çdo produkt ka 20% shtesë në çmim, dhe ku 20% është ajo që i jepet shtetit. Në momentet fillestare ka edhe ngutje e gabime, ndaj kërkohet organizim më i mirë. Në këtë kontekst, çdo punonjës në kompaninë e tij ruan dosjet e punës në kompjuterin e punës. Detaje të tilla si shpenzimet e firmave, blerjet që bëjnë, doganat, pagat, janë nga gjërat e para që duhet të mësoj punonjësi i ri. Gjatë procesit të intervistimi, punonjësi që ishte menaxher i shitjeve, theksoi se për të qenë i suksesshëm, duhet të dish gjithçka rreth produkteve që shet, si materialin e produktit, përmasat e tij, sa ngjyra ju mund të gjeni te produkti dhe më e rëndësishmja: si të ndikoni tek blerësi.

Për ata që janë të rinj në detyrë, ka edhe procedura të tilla si trajnim një mujor dhe

nëse arrin performancën, do të jesh pjesë e personelit. Përmes aplikimit të teorisë së modelit, kandidatët vështronin si menaxheri i departamentit të shitjes vepronte me klientët, si fliste, si u soll me ta, si reklamohej malli. Një nga pjesët më të rëndësishme ishte komunikimi, i cili realizohej elektronikisht. Ndërkohë, kandidatët gjithçka që u nevojitej e kishin të shkruar.

## 8. Strategjitë e mikromësimit

Shumica e dijeve që marrin të rriturit ndodh jashtë mësimit formal. Kjo i korrespondon nevojave të individit, i cili kërkon të zhvillohet profesionalisht, kërkon aftësi dhe dije të reja e t'i përditësoj ato, që motivohet duke ndryshuar kushtet ose rrethanat në jetë (p.sh. parapërgatitja për një punë të re). Kjo bazohet në aspektet specifike të detyrave, të cilat kërkojnë informacion specifik dhe jo dije në tërësi. Kjo me qëllim mbështetjen e vendimmarrjes për arritjen e një aftësie (Tough, A. (1971).

Mikromësimi duhet konsideruar kështu si një proces i të mësuarit gjatë tërë jetës, i cili është shumë efektiv kur realizohen aktivitete të tilla si: ndërtimi i dijes, gjetja e zgjidhjeve të ndryshme të problemeve ose krijimi i lidhjeve midis eksperiencave të kaluara dhe të tanishme; bashkëbisedim midis botës që na rrethon me qenien tonë (si në refleksione, eksperimente në vende të ndryshme dhe interpretimi i rezultateve); punonjësi kontrollon në vazhdimësi tërë ciklet e eksperimentit dhe reflekton (Livingstone, D.W (2001).

Mikromësimi ka strategjinë e tij si:

- *Strategjia e të mësuarit social*; mund të mësoni nga grupi i njerëzve me të cilët punoni. Në rast se punoni në zyrë mëson nga kolegët e tu, p.sh. shpjegimin e librave të bilancit, kontabilitetit, hyrjen dhe daljen e produktit, si bëhet zhdoganimi i mallrave, si përpilohet deklarata etj.

- *Mësimi i bazuar në lojë;* ju mund të mësoni duke e "bërë punën si lojë", pra keni "misionin për të përfunduar punën".

- *Të mësuarit përmes veprimit*; ju ndihmon për të mësuar më shumë nga aktivitetet që merrni pjesë.

- *Të mësuarit nga gabimet*; zakonisht mësojmë nga gabimet, por në kompani do të mësojmë më shumë nga problemet që dalin, p.sh. problematika të organizimit-mosfunksionimi dhe porosia në kohën e duhur.

- *Mësimi i bazuar në punë;* mësojmë nga bashkëpunëtoret tanë. Kjo është mënyra më e mirë e të mësuarit për kompaninë.

- *Praktikë në hapësirë kohore*; është një strategji mësimi, ku praktika ndahet në një sërë seancash të shkurtra – por për një periudhë më të gjatë kohore.

- *Të mësuarit me mjete të vogla elektronike*; procesi i të mësuarit kalon përmes konteksteve të shumëfishta, nëpërmjet ndërveprimeve sociale dhe përmbajtjes, duke përdorur mjete elektronike personale, p.sh. përdorim fjalët kyçe, imazhet dhe parimet midis aseteve të mësimit mikro, - kur duam të bëjmë pjesën tonë të punës, por jemi konfuz, (p.sh. për të plotësuar një faturë për një klient dhe nuk dimë çfarë të shkruajmë në të). Në kompaninë objekt–studimi, shiten materiale ndërtimi dhe ekzistojnë 5000 materiale dhe me përbërës të ndryshëm. Në këtë rast do të ishte një zgjedhje shumë e mirë, nëse shikojmë imazhet e produktit në një katalog *online*, me fjalë kyçe dhe produktet që klientët kërkojnë.

## 9. Përfundime dhe rekomandime

Qëllimi i këtij punimi është paraqitja dhe analiza e teknikës se mikromësimit, e cila ofron mundësi për zhvillimin e punonjësve gjatë tërë jetës. U pasqyruan në këtë punim, mjetet, teoritë dhe metodat për realizimin e mikromësimit, si dhe rastet konkrete për realizimin dhe zbatimin e tyre. Në këto kushte, institucionet e niveleve të ndryshme (organizatat) janë duke implementuar edhe konceptet e mikromësimit. Në të ardhmen, në dobi të mikromësimit do të jetë edhe organizimi i trajnimeve në organizatë, duke shpjeguar mundësitë që të krijon për zhvillimin e burimeve njerëzore. Sipas literaturës, mikromësimi është një teknikë e *eLeraning*, e cila gjithmonë e më shumë po fiton terren në organizata, pasi realizohet përmes rrjeteve sociale, mësimit joformal (mësohet edhe nëpërmjet celularit).

Shkaku për interesin në rritje të mikromësimit buron nga fakti se jetojmë në epokën e informacionit. E ardhmja po e kërkon gjithnjë e më shumë varësinë nga teknologjia e informacionit, duke filluar nga më e thjeshta (celulari). Koha kërkon të mësuarit e shpejtë, në kohën e duhur deri dhe marrjen e informacionit për shoqërinë përmes celularit.

Kryerja e trajnimeve dhe kurseve afatshkurtra, mund të organizohet si nga institucionet publike dhe ato private. Është e domosdoshme që trajnuesit të jenë të përgatitur, me përvojën e duhur për të pasur një proces të suksesshëm të mikromësimit. Rekomandohet në fillim që kurset të jenë programe pilot, në të pastajmen të implementohen në organizatë. Mikromaterialet e krijuara/përzgjedhura, mund të përditësohen e përshtaten lehtësisht për tiu përgjigjur më mirë nevojave në rritje të organizatave. Hulumtimet tregojnë se mikromësimi mund të përdoret gjerësisht në institucionet publike dhe private.

Vlerësimi dhe analiza e herëpashershme, konsiderohet e nevojshme për të bërë ndryshimet në raport me kërkesat e kohës. Nisur nga fakti se është një teknikë e re e të mësuarit, ka më shumë hapësira për realizimin e studimeve shkencore si për institucionet publike dhe ato private.

## Bibliografi


1. Bower, M., Lee, M. J., & Dalgarno, B. (2017). Collaborative learning across physical and virtual worlds: Factors supporting and constraining learners in a blended reality environment. *British Journal of Educational Technology*, *48*(2), 407-430. Retrieved from https://www.researchgate.net
2. Theo Hug, Institute of Educational Sciences, University of Innsbruck (Austria) Microlearning: A Neë Pedagogical Challenge, RSA Studio eLearning Environments (Innsbruck, Austria), p.14).
3. Peter A. Bruck, Research Studios Austria (Salzburg/Vienna), General Manager Microlearning as strategic research field: An invitation to collobarate (Introductory Note), p.22).
4. Erich Neuhold, Darmstadt University of Technology (Germany), Professor of Computer Science Fraunhofer Institute for Integrated Publication and Information Systems / IPSI (Germany), Director Emeritus Quo Vadis, eLearning? (Introductory Note) p.27).
5. Jomah, O., Masoud, A. K., Kishore, X. P., & Aurelia, S. (2016). Micro learning: A modernized education system. *BRAIN. Broad Research in Artificial Intelligence and Neuroscience*, *7*(1), 103-110.
6. Tough, A.(1971). The Adults Learning Projects: A Fresh Approach to Theory and Practise in Adult Learning. Toronto: OISE).
7. Livingstone, D.Ë (2001) Adults Informal Learning, Toronto, 2002).
8. Giurgiu, L. (2017). Microlearning an Evolving Elearning Trend. Scientific Bulletin, 43(1), 18-23. Retrieved from https://www.degruyter.com/downloadpdf/j/bsaft.2017.22.issue-1/bsaft-2017-0003/bsaft-2017-0003.pdf
9. Fox, A. (2016, April). Microlearning for effective performance management. *Talent Development, 70*(4), 116-117. Retrieved from https://search-proquestcom.ezproxy.uned.es/docview/1782244841?accountid=14609.
10. Pappas, C. (2017, December 29). 10 Adult Learning Facts and Stats That eLearning Pros Need to Know. https://elearningindustry.com/adult-learning-facts-stats-elearningpros-need-know.

# Krimi kompjuterik në Shqipëri: baza ligjore dhe statistikat në vite

**MSc. Artan DASHI**
*Sektori i hetimit të krimit kompjuterik,*
*Policia e Shtetit*
*artan.dashi@asp.gov.al*

**Abstrakt**

*Që nga viti 2009 deri në vitin 2018 interneti është zgjeruar 10 herë apo e më shumë, krimi kompjuterik është tani një nga sfidat më të mëdha ligjore. Në nivel global, digjitalizimi gjithë përfshirës, i veprimtarisë ekonomiko – shoqërore, sociale e më gjerë në çdo aspekt të shoqërisë njerëzore ku, aktualisht rreth 4 miliard njerëz janë online. Hapësira Kompjuterike sot është një nga sfidat më të mëdha ligjore e cila ka nxitur një formë tjetër të krimit, duke krijuar një mjedis për metodat e reja të krimit. Tani pothuajse të gjitha krimet mund të kryhen me përdorimin e kompjuterëve dhe sistemeve kompjuterike. Duke parë rëndësinë aktuale të këtij fenomeni në shkallë kombëtare, duke pasur parasysh rritjen e shpejtë të krimit kompjuterik në Shqipëri ne 10 vitet e fundit dhe mungesën e interpretimeve analitike statistikore për veprat penale në fushën e krimeve kompjuterike dhe kibernetike që prekin shoqërinë, individin, sipërmarrjen dhe kompanitë private në vendin tonë dhe më gjerë, vendosa të bëj një kërkim shkencor mbi krimin kompjuterik, bazat ligjore, kërkesa dhe nevoja për përmirësime, interpretimin analitik të statistikave të krimeve kibernetike në vendin tonë në 10 vitet e fundit. Qëllimi i këtij studimi është analizimi i situatës aktuale në Shqipëri, në lidhje me standardet ligjore, nevoja për përmirësimet ligjore, mekanizmat për hetimin dhe ndjekjen penale të krimit kompjuterik, dhe evidentimin e problematikave dhe sfidave kryesore me të cilat hasen hetuesit, prokurorët, policia dhe shteti shqiptar në parandalimin dhe luftimin e krimit kompjuterik në Shqipëri. Në fund të këtij punimi janë paraqitur dhe disa rekomandime për një qasje dhe një analizë statistikore ndërgjegjësuese sa më të mirë të krimit kibernetik në Shqipëri.*

**Fjalëkyçe:**
**vepër penale, krim kompjuterik, standardet ligjore, mekanizmat për hetim, sulm kibernetik.**

## 1. Hyrje

Fillimet e tij, hetimi i krimi kompjuterik, në vendin tonë e ka në qershor 2009, duke u krijuar sektori i krimit kompjuterik në Drejtorinë e Përgjithshme të Policisë së Shtetit, sektori për ekzaminimet e pajisjeve kompjuterike pranë Institutit të Policisë Shkencore, Tiranë si dhe në korrik 2010 seksioni për hetimin e krimit kompjuterik në Drejtorinë Vendore të Policisë Tiranë po edhe specialist të hetimit të krimit kompjuterik në drejtoritë vendore të policisë të emëruar apo në organik në sektorë të tjerë po që ndiqnin dhe hetimin e krimit kompjuterik.

Me ngritjen e strukturave, përshtatjet dhe implementimi ligjor në Kodin Penal dhe Kodin e Procedurës Penale, filluan dhe regjistrimet e para të kallëzimeve dhe referimet e para në Prokuroritë vendore nga shtetas të ndryshëm dhe qytete te ndryshme të vendit.

Ky numër ishte minimal në fillim por me zhvillimin e teknologjisë, akseset e afruara, publiciteti i bërë, ka çuar që raportimi, kallëzimet e më pas referimet të rriten në numër, por akoma më shumë ky zhvillim teknologjik, do të çoj në rritjen e përfituesve(autorëve apo shkelësit e ligjit) të këtij zhvillimi teknologjik dhe "viktimat" (të dëmtuarit) e këtij zhvillimi teknologjik.

*Digjitalizimi në Shqipëri*

Popullsia e Shqipërisë në 1 janar 2018, rezulton 2.870.324 banorë (INSTAT); 65% e popullsisë kanë akses në internet; mbi 130 subjekte të shpërndarjes së internetit në vend; 3 kompani telefonike celulare, që japin shërbimin e internetit nëpërmjet sistemit 3G; akses falas në internet në shkolla e universitete, zyra postare etj.

*Konventa për krimin kibernetik*

Me ligjin nr. 8888 datë 25.4.2002, Parlamenti Shqiptar ka ratifikuar Konventën e Këshillit të Europës, "Për krimin kibernetik", miratuar më 23 nëntor 2001 në Budapest. Ajo parashikon: përkufizime për sistemet kompjuterike, të dhënat kompjuterike, subjektet e shërbimeve kompjuterike, të dhënat; masat që duhen marrë në nivel kombëtar (ligji penal, ligji procedural, juridiksioni); bashkëpunimin ndërkombëtar (ekstradimi, ndihma e ndërsjellët juridike, shkëmbimi i informacioneve, ruajtja e përshpejtuar dhe vënia në dispozicion e të dhënave kompjuterike, aksesimi i të dhënave të sekuestruara, përgjimi i të dhënave kompjuterike etj.); rrjetin 24/7; harmonizimin e elementëve të veprave penale të ligjit penal vendas dhe parashikimeve të saj në fushën e krimit kompjuterik; të sigurojë fuqitë e nevojshme për ligjin e brendshëm procedural penal, për ndjekjen penale dhe hetimin e veprave penale kompjuterike, apo dhe të atyre të kryera nëpërmjet sistemeve kompjuterike; ngritjen e një regjimi të shpejtë dhe efektiv të bashkëpunimit kombëtar dhe ndërkombëtar.

## 2. Harmonizimi në legjislacion

Në *Kodin Penal të Republikës së Shqipërisë* (ligji nr. 10023, datë 27.11.2008) janë parashikuar dhe nenet përkatëse të krimit kompjuterik:

- neni 143/b, "Mashtrimi kompjuterik", masa e dënimit për këtë vepër penale e parashikuar në Kodin Penal është (6 muaj-6 vjet dhe nga 5 vjet-15 vjet);
- neni 186/a, "Falsifikimi kompjuterik", masa e dënimit për këtë vepër penale e parashikuar në Kodin Penal është (6 muaj-6 vjet dhe nga 3 vjet-10 vjet );
- neni 192/b, "Hyrja e paautorizuar kompjuterike", masa e dënimit për këtë vepër penale e parashikuar në Kodin Penal është (gjobë-3 vjet si dhe nga 3-10 vjet);
- neni 293/a, "Përgjimi i paligjshëm i të dhënave kompjuterike", masa e dënimit për këtë vepër penale e parashikuar në Kodin Penal është (3 vjet-7 vjet-15 vjet);
- neni 293/b, "Ndërhyrja në të dhënat kompjuterike", (6 muaj-3 vjet dhe 3 vjet-10 vjet);
- neni 293/c, "Ndërhyrja në të dhënat kompjuterike" masa e dënimit për këtë vepër penale e parashikuar në Kodin Penal është (3 vjet-7 vjet dhe 5 vjet-15 vjet);
- neni 293/ç, "Keqpërdorimi i pajisjeve" masa e dënimit për këtë vepër penale e parashikuar në Kodin Penal është (6 muaj-5 vjet);
- neni 137/a, "Vjedhja e rrjetit të komunikimeve elektronike" (ligji 144/2013 neni 34 deri masa e dënimit për këtë vepër penale e parashikuar në Kodin Penal është 3 vjet dhe në bashkëpunim 3 vjet-7 vjet).

Në *Kodin i Procedurës Penale* (ligji nr. 10053 datë 29.12.2008) janë parashikuar dhe veprimet procedurale për krimin kompjuterik; disa nga këto janë:

- neni 191/a, "Detyrimi për paraqitjen e të dhënave kompjuterike";
- neni 208/a, "Sekuestrimi i të dhënave kompjuterike";
- neni 299/a, "Ruajtja e përshpejtuar dhe mirëmbajtja e të dhënave kompjuterike";
- neni 299/b, "Ruajtja e përshpejtuar dhe zbulimi i pjesshëm i të dhënave kompjuterike".

*Protokolli shtesë*

- Me ligjin nr. 9262, datë 29.7.2004, Parlamenti Shqiptar ka miratuar "Protokollin

shtesë të Konventës së Krimit Kibernetik, për penalizimin e akteve me natyrë raciste dhe ksenofobe të kryera nëpërmjet sistemeve kompjuterike".

- Ky protokoll ka si qëllim: harmonizimin e legjislacionit penal vendas me elementët dhe përkufizimet e parashikuara në këtë protokoll, për kriminalizimin e akteve raciste dhe ksenofobe të kryera nëpërmjet rrjetit kompjuterik, duke përfshirë prodhimin, ofrimin, shpërndarjen e materialeve dhe mesazheve me përmbajtje të tillë nëpërmjet rrjeteve kompjuterike; plotësimin e parashikimeve të Konventës së Krimit Kibernetik lidhur me kriminalizimin e akteve të racizmit dhe ksenofobike të kryera nëpërmjet sistemit kompjuterik.

*Kodi Penal (ligji nr. 10023, datë 27.11.2008):*

- neni 74/a, "Shpërndarja kompjuterike e materialeve pro gjenocidit ose krimeve kundër njerëzimit";
- neni 84/a, "Kanosja me motive racizimi dhe ksenofobie nëpërmjet sistemit kompjuterik";
- neni 119/a, "Shpërndarja e materialeve raciste ose ksenofobike nëpërmjet sistemit kompjuterik";
- neni 119/b, "Fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik".

*Konventa e Lanzarotit*

Kjo konventë ka si qëllim të parandalojë dhe të luftojë abuzimin seksual të fëmijëve; të mbrojë të drejtat e fëmijëve viktima të shfrytëzimit seksual dhe të abuzimit seksual; të nxisë bashkëpunimin kombëtar dhe ndërkombëtar kundër shfrytëzimit seksual dhe abuzimit seksual të fëmijëve.

## 3. Format më kryesore të krimeve kompjuterike

Format më kryesore të krimeve kompjuterike të evidentuara janë:

- mashtrimet nëpërmjet internetit:
- krijimi dhe përdorimi i faqeve të internetit mashtruese, me qëllim marrjen e të dhënave personale dhe financiare të përdoruesve të internetit, për përfitim të paligjshëm, metoda *phishing*.
- përfitimi me mashtrim i shumave të parave, duke përdorur të dhëna kompjuterike të rreme nëpërmjet përdorimit të adresave të postës elektronike mashtruese, duke u paraqitur si subjekt tregtar në një shtet të huaj.

*Mashtrimet me karta bankare:* përdorimi i paligjshëm i të dhënave të kartave bankare të vjedhura për prenotimin e biletave të udhëtimit, akomodimit në hotel, prenotimin për organizimin e ceremonive; vjedhja e të dhënave të kartave bankare nëpërmjet programeve kompjuterike të këqija.

*Falsifikimet kompjuterike:* janë evidentuar raste kur janë falsifikuar të dhëna të ruajtura në rrjetet sociale në internet.

*Ndërhyrjet e paligjshme kompjuterike:* ndërhyrja e paligjshme në faqet zyrtare të internetit të subjekteve publike dhe private me qëllim mosfunksionimin e tyre dhe prishjen e imazhit; hyrja e paligjshme në adresat e postës elektronike të përdoruesve të internetit; thyerja e masave të sigurisë së sistemeve apo programeve kompjuterike, për vjedhjen e të dhënave personale dhe financiare.

## 4. Veprat penale kryesore të krimit kompjuterik, në vite

Më poshtë po paraqesim në formë grafike veprat penale kryesore të krimit kompjuterik të evidentuara në vite.

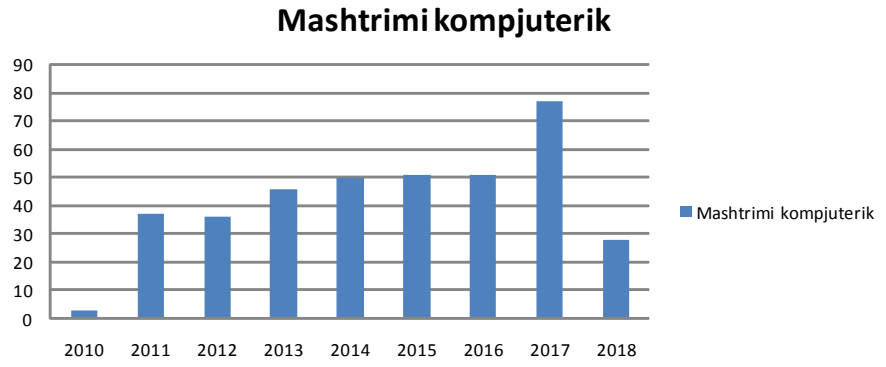
**Tabela 1: Veprat penale të krimit kompjuterik ndër vite**

| Vepra Penale | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 |
|---|---|---|---|---|---|---|---|---|
| Mashtrimi kompjuterik 143/b | 3 | 37 | 36 | 46 | 50 | 51 | 51 | 77 |
| Falsifikimi kompjuterik 186/a | 8 | 17 | 11 | 23 | 27 | 12 | 29 | 49 |
| Ndërhyrja në të dhënat 293/b kompjuterike | 2 | 3 | 14 | 19 | 6 | 33 | 65 | 56 |
| Pornografia (nëpërmjet sistemeve kompjuterike) 117 | 0 | 0 | 1 | 2 | 40 | 7 | 5 | 4 |
| **Gjithsej** | **17** | **84** | **81** | **108** | **176** | **122** | **175** | **218** |

Nga tabela e mësipërme, rezulton se kemi një rritje të evidentimit të veprave penale të krimit kompjuterik në vite. Nëse në 2010, janë evidentuar 17 vepra penale; më pas për vitin 2011 janë rritur në 84, pra në afërsisht 500% të një vitit më parë. Ky trend i veprave penale, është në rritje nga viti në vit, ku numri më i madh është evidentuar në vitin 2017 në 218 të tilla; po ta krahasojmë me vitin 2010, janë rritur me 1282 %. Më konkretisht, të ndara në vepra penale janë si më poshtë.

**Figura 1: Mashtrimi kompjuterik**

| Vepra Penale | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|---|---|---|
| Mashtrimi kompjuterik 143/b | 3 | 37 | 36 | 46 | 50 | 51 | 51 | 77 | 28 |

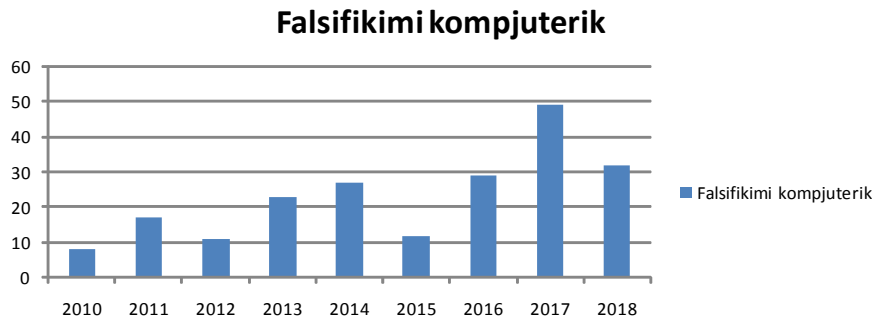



Nga tabela e mësipërme dhe grafiku, rezulton se në 2010, janë evidentuar 3 vepra penale të mashtrimit kompjuterik; ky numër ka ardhur në rritje dhe numri më i madh i kësaj vepre penale është evidentuar në vitin 2017, me 77 mashtrime, ose në përqindje, 2566% në raport me vitin 2010. Është për tu theksuar se për 6-mujorin e parë të 2018-s, ky numër është 28, ose në 933%; kjo ka ardhur si rezultat i një fushate sensibilizuese në mediet kombëtare te shkruara dhe vizive. Kjo fushatë sensibilizuese, është bërë për faktin se nga bizneset të ndryshme po edhe nga persona që kanë dashur të blejnë

automjete *online*, është pësuar një dëm financiar mbi 3 000 000 euro (shifër jo e vogël) që ka ikur jashtë vendit .

**Figura 2: Falsifikimi kompjuterik**

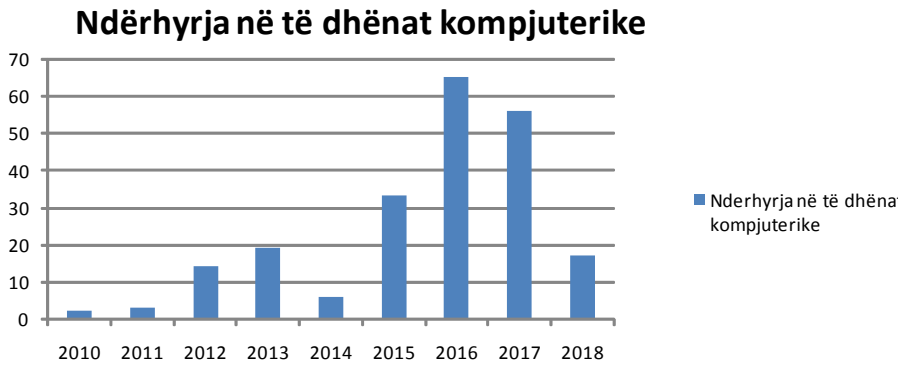
| Vepra Penale | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|---|---|---|
| Falsifikimi kompjuterik 186/a | 8 | 17 | 11 | 23 | 27 | 12 | 29 | 49 | 32 |




Në tabelën e mësipërme së bashku me grafikun përkatës ku evidentimi ka filluar në vitin 2010 ku kemi pasur 8 vepra penale te "Falsifikimit kompjuterik" dhe numri më i madh i kësaj vepre penale është evidentuar në vitin 2017, në 49 të tilla ose në përqindje 612.5 % , në vite kjo vepër penale është prezent dhe ka kurbën e saj të zhvillimit edhe për 6-mujorin e parë të 2018 janë evidentuar 32 vepra penale po ky numër deri në fund të vitit 2018 do jetë në rritje.

**Figura 3: Ndërhyrja në të dhënat kompjuterike**

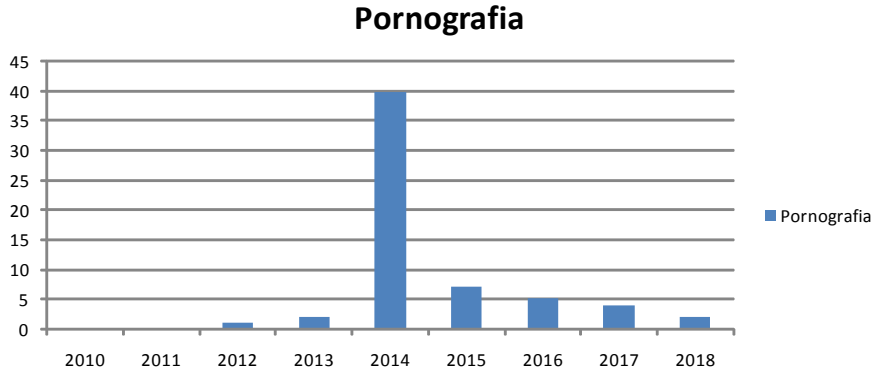
| Vepra Penale | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|---|---|---|
| Ndërhyrja në të dhënat kompjuterike 293/b | 2 | 3 | 14 | 19 | 6 | 33 | 65 | 56 | 17 |



Sipas të dhënave në vite për veprën penale të "Ndërhyrjes në të dhënat kompjuterike" ku në 2010 janë evidentuar 2 vepra penale, ndër vite kjo vepër penale ka qenë prezent ku numrin më të madh të evidentuar është në vitin 2016 në 65 të tilla ose në 3250 % në krahasim me vitin 2010. Për 2018 ky numër si 6-mujor të parë është në 17 vepra penale dhe ky trend nuk mund të jetë më i madh se ai i vitit 2016.

**Figura 4: Pornografia**

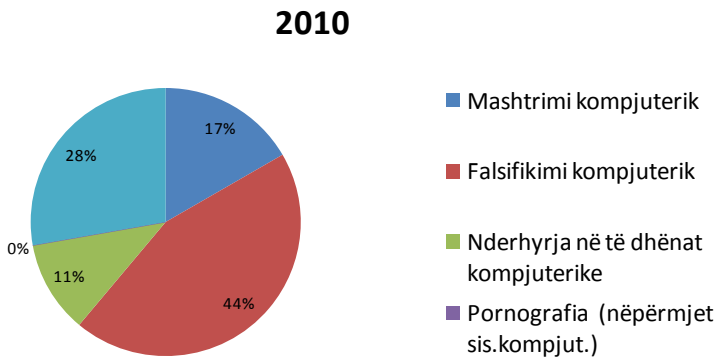
| Vepra Penale | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|---|---|---|
| Pornografia (nëpërmjet sistemeve kompjuterike) 117 | 0 | 0 | 1 | 2 | 40 | 7 | 5 | 4 | 2 |




Jo më pak e rëndësishme është dhe vepra penale e "Pornografisë" ku sipas tabelës dhe grafikut rezulton se në vitin 2014 kjo vepër penale është regjistruar në 40 të tilla dhe më pak në vitet e tjera. Shumica e kësaj vepre penale është evidentuar nga homologet tanë ndërkombëtar si Europol apo Interpol, të cilët kanë struktura të veçanta dhe pajisje të specializuara për këtë vepër penale, duke afruar lidhje (*link*) të ndryshme për adresa të cilat përdorin foto, video apo dhe komunikime me fëmijë, me qëllim për pornografi.

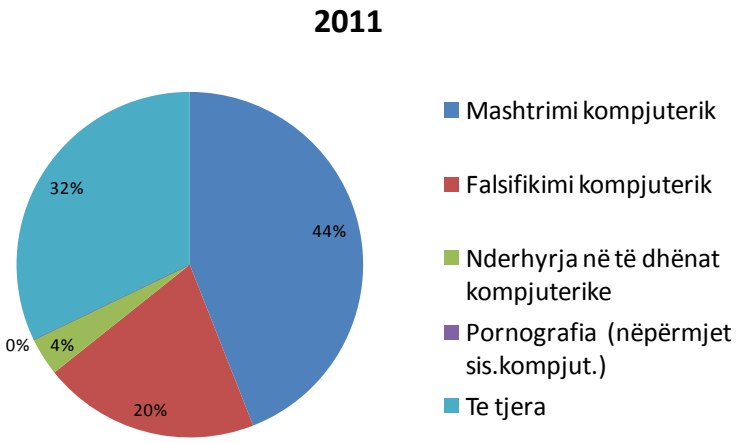
*-Ndarja në përqindje e veprave penale sipas viteve*

**Figura 5: Përqindja e veprave penale 2010**



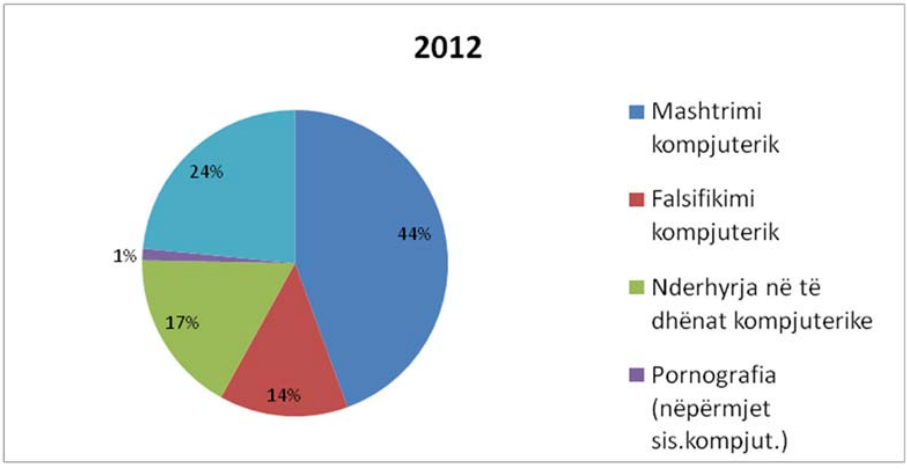
Në vitin 2010 numri më i madh i evidentuar në 44% i përket *falsifikimit kompjuterik*, e më pas *mashtrimit kompjuterik* me 17% dhe *ndërhyrja në të dhënat kompjuterike*, në 11%. Kurse, në vepra penale të tjera, janë 28%, ku aty përfshihen disa vepra si: *përndjekje*, *kanosje në rrjetet sociale*, *ndërhyrje të padrejtë në jetën private* etj.

**Figura 6: Përqindja e veprave penale 2011**



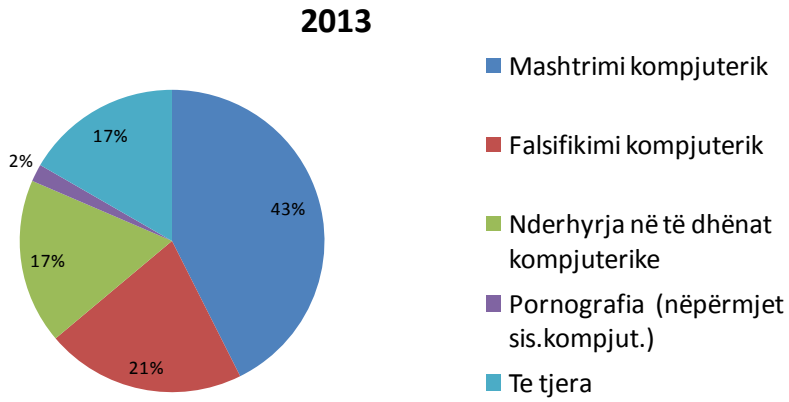

Për vitin 2011 kemi: 44% të veprave penale si *mashtrim kompjuterik*, 20% *falsifikim kompjuterik* dhe 4% *ndërhyrje në të dhënat kompjuterike*; kurse 32% i përkasin *përndjekjes, mashtrimeve të tjera, kanosje në rrjetet sociale* etj.

**Figura 7: Përqindja e veprave penale 2012**



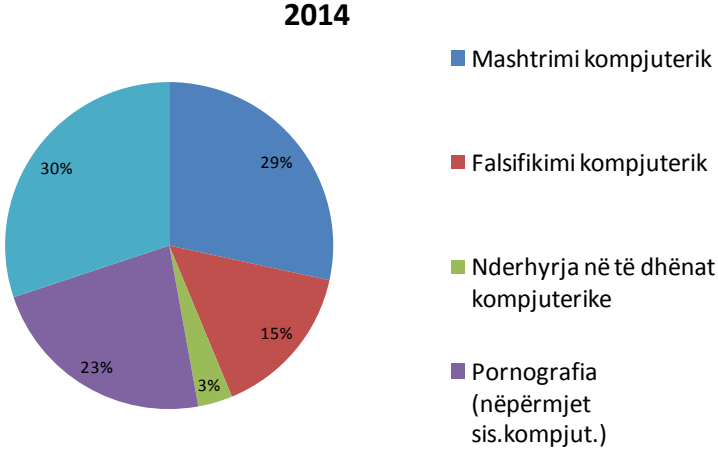

Për vitin 2012 kemi të evidentuara 44% *mashtrime kompjuterike*, 17% *ndërhyrje në të dhënat kompjuterike* dhe 14% *falsifikim kompjuterik*, 1% *pornografi* dhe 24% të tjera i përkasin *përndjekjes, mashtrime te tjera, kanosje në rrjetet sociale* etj.

Figura 8: Përqindja e veprave penale 2013



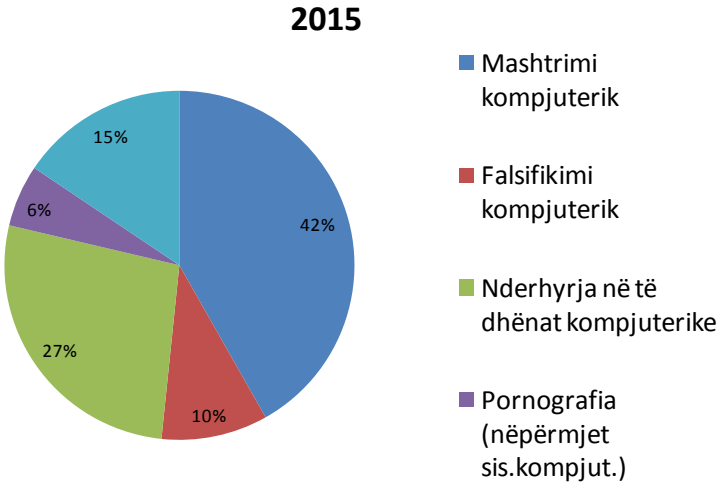

Për vitin 2013 janë evidentuar 43% *mashtrime kompjuterike*, 21% *falsifikime* kompjuterike, 17% *ndërhyrja në të dhënat kompjuterike*, 17% të tjera dhe 2% *pornografi*.

Figura 9: Përqindja e veprave penale 2014



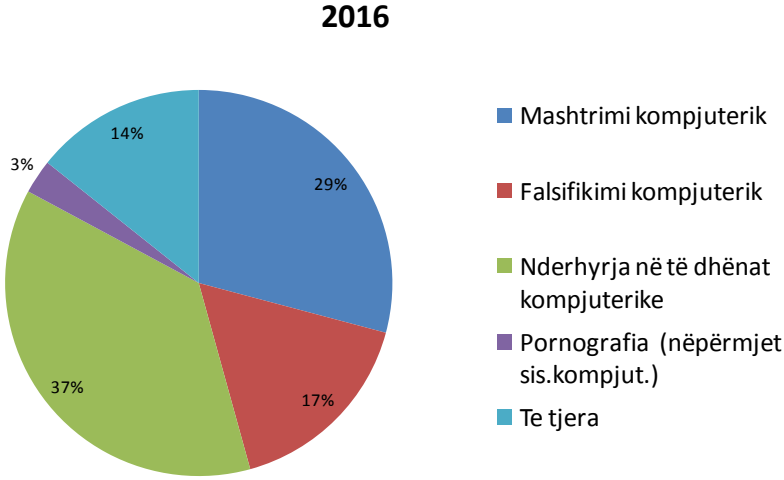

Për vitin 2014 janë evidentuar 29% *mashtrime kompjuterike*, në veçanti edhe me vitet e tjera kemi një rritje për 2014-ën të *pornografisë* me 23%, *falsifikim kompjuterik* në 15%, të tjera 30% dhe 3% *ndërhyrja në të dhënat kompjuterike*.

Figura 10: Përqindja e veprave penale 2015



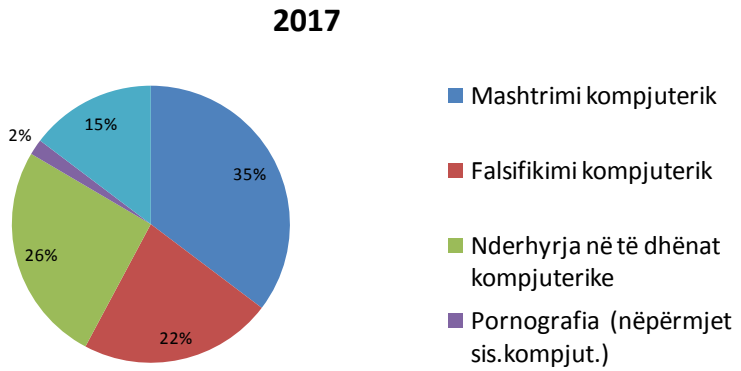

Në vitin 2015 janë evidentuar 42% *mashtrime kompjuterike*, 27% *ndërhyrje në të dhënat kompjuterike*, 10% *falsifikime kompjuterike*, 6% *pornografi* dhe 15 % të tjera.

Figura 11: Përqindja e veprave penale 2016



Në vitin 2016 janë evidentuar 37% *ndërhyrje në të dhënat kompjuterike*, 29% *mashtrime kompjuterike*, 17% *falsifikim kompjuterik*, 3% *pornografi* dhe 14% të tjera.

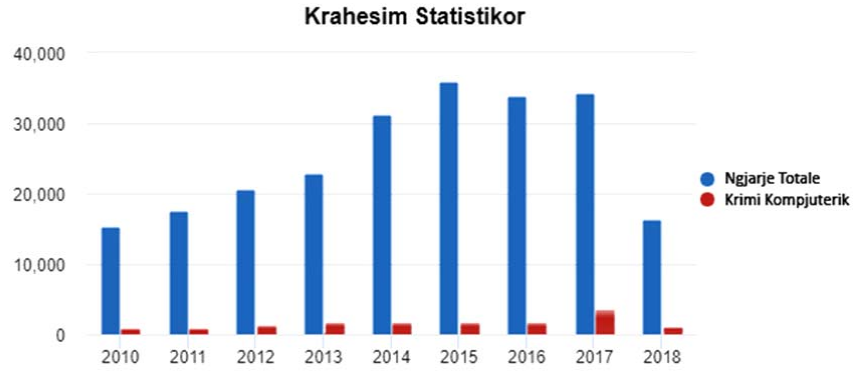
**Figura 12: Përqindja e veprave penale 2017**




Në vitin 2017 janë evidentuar 35% *mashtrime kompjuterike*, 26% *ndërhyrje në të dhënat kompjuterike*, 22% *falsifikim kompjuterik*, 2% *pornografi* dhe 15% të tjera. Më pas është evidentimi i veprave penale të *krimit kompjuterik* në raport me ngjarjet e evidentuara në rang vendi.

**Tabela 2: Krimi kompjuterik në raport me ngjarjet në total**

| Viti | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|---|---|---|
| Ngjarje total | 15249 | 17646 | 20688 | 22816 | 31225 | 35864 | 33808 | 34317 | 16393 |
| Krimi kompjuterik | 17 | 84 | 81 | 108 | 176 | 122 | 175 | 218 | 90 |



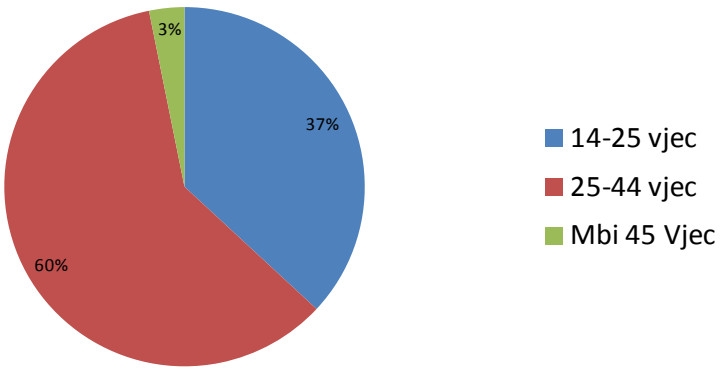
ipas tabelës dhe grafikut te paraqitur më lartë kemi të bëjmë me një numër shumë të madh të veprave penale në vite në përgjithësi, dhe numri i veprave penale të krimit kompjuterik është shumë i vogël për mos të thënë i pakrahasueshëm. Por, impakti në shoqërinë apo mjedisin vendas, që ka çdo vepër penale e krimit kompjuterik, është akoma më i madh se vetë numri i tyre.

*- Autorët e krimeve kompjuterike sipas grupmoshave*

**Tabela 3: Autorët e krimeve sipas grupmoshave**

| Viti | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | Totali |
|---|---|---|---|---|---|---|---|---|---|---|
| **14-25 vjeç** | 2 | 13 | 29 | 36 | 40 | 19 | 33 | 3 | 0 | 175 |
| **25-44 vjeç** | 10 | 87 | 59 | 33 | 46 | 21 | 25 | 3 | 0 | 284 |
| **Mbi 45 vjeç** | 0 | 0 | 0 | 0 | 0 | 11 | 4 | 0 | 0 | 15 |

**Figura 13: Autorët e krimeve sipas grupmoshave**




Pjesë e kësaj analize, janë edhe grupmoshat e autorëve të veprave penale në vite për krimet kompjuterike. edhe pse ishte e vështirë, por u bë një ndarje ku numrin më të madh të autoreve të veprave penale e zë grupmosha 25-44 vjeç me 60%, më pas 14-25 vjeç me 37% dhe mbi 45 vjeç me 3%. Sa për një ndarje sipas gjinisë të autorëve të veprave penale kemi të bëjmë me 95% meshkuj dhe 5% femra.

*- Krime kompjuterike të zbuluara ndër vite*

**Tabela 4: Krime kompjuterike të zbuluara ndër vite**

| Viti | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|---|---|---|
| **Krime të zbuluara** | 9 | 62 | 57 | 63 | 75 | 33 | 50 | 60 | 26 |

Deri më tani, kemi folur për krimet kompjuterike të ndodhura dhe ndarjen e tyre sipas veprave penale në vite, apo dhe grupmosha; me tabelën e mësipërme, kemi paraqitur zbulimin në vite të krimeve kompjuterike. Siç është paraqitur edhe në tabelën e mësipërme, kemi të bëjmë me një zbulim në vite nga 23.4% në 2014, dhe me zbulimin më të mirë në vitin 2011, me rreth 62% apo, në 2013 në 64% për veprat penale të

krimit kompjuterik.

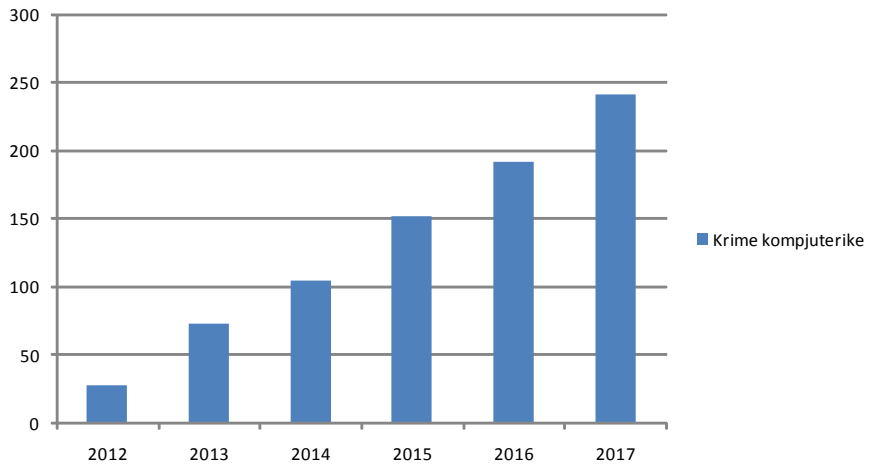
Zbulimi i këtyre veprave penale nuk është domosdoshmërish i lidhur me punën e çdo specialisti, por me kohën apo procedurat që ndiqen për dokumentimin, hetimin, nxjerrjen e vendimeve të gjykatës, dërgimi i *letër porosisë*, ardhja e përgjigjes së *letër porosisë* së dërguar si dhe përgjigjet me shumë vonesë nga kompanitë e internetit në vend (ISP), të cilat në shumicën e rasteve, janë shabllon duke thënë se: "IP është dinamike", apo "me ketë IP janë 1000 abonentë". Të gjitha këto veprime procedurale duan kohë.

*- Numri i krimeve kompjuterike në Republikën e Kosovës*

**Tabela 5: Numri i krimeve kompjuterike në Republikën e Kosovës**

| Viti | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 |
|---|---|---|---|---|---|---|
| Rastet | 11 | 18 | 24 | 34 | 40 | 42 |
| Asistime | 16 | 55 | 80 | 118 | 152 | 199 |
| Totali | 27 | 73 | 104 | 152 | 192 | 241 |

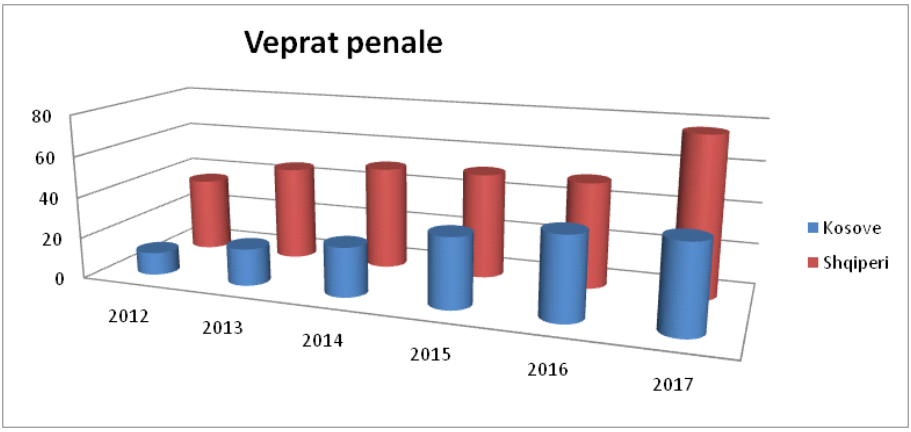
**Figura 14: Numri i krimeve kompjuterike në Republikën e Kosovës**




Për bazë krahasuese për krimin kompjuterik u kërkuan të dhëna edhe për shtetin e Malit të Zi apo të Maqedonisë, të cilat nuk u bë e mundur të siguroheshin. Me të dhënat e siguruara nga homologët e Kosovës, të cilat janë evidentuar më lartë në tabelën dhe grafikun përkatës, kemi një klasifikim paksa ndryshe në, "raste" dhe "asistime". Nuk është objekt i kësaj teme, klasifikimi që bëjnë homologët e Kosovës, por trendi i veprave penale në fushën e krimit kompjuterik, që si në Shqipëri edhe në Kosovë (po edhe në Malin e Zi, Maqedoni e rajon), prirja e veprave penale në fushën e krimeve kompjuterike është në rritje. Duke marrë shkasë nga klasifikimi i kryer nga kolegët e Kosovës, nuk dua të lë pa përmendur edhe qindra raste të evidentuara nga specialistët e hetimit të krimit kompjuterik, ditë pas dite, muaj pas muaji, vit pas viti, ku u është afruar "asistim" për

shtetas të ndryshëm apo edhe marrje kallëzimi penal, dërgim në prokurori për vlerësim (nëse kemi të bëjmë me vepër penale apo jo) të shumë rasteve, të cilat nuk janë evidentuar në të dhënat e mësipërme. Dhe ky numër është i madh!

Figura 15: Krahasim i veprave penale




Në grafikun e mësipërm, me ngjyre të kuqe janë paraqitur veprat penale në fushën e krimit kompjuterik në Shqipëri, dhe me ngjyrë blu, veprat penale në fushën e krimit kompjuterik në Kosovë, ku vihet re qartë se kemi një prirje në rritje, të veprave penale në fushën e krimit kompjuterik. Të dhënat statistikore të lartpërmendura, tregojnë se ka një tendencë pozitive në performancë dhe në përqasjen me këto krime, të cilat janë sfidë e re për Policinë e Shtetit, duke evidentuar punën e mirë të bërë nga strukturat e hetimit të krimeve kompjuterike, kryesisht në Qendër dhe në DPQ Tiranë.

## 5. Rekomandime

- Rritja e numrit të rasteve të evidentuara dhe grupeve kriminale të goditura, me aktivitet në këtë drejtim; trajnimi i strukturave, me qëllim rritjen e treguesve që në procesin e marrjes së informacionit dhe deri në kryerjen e hetimeve cilësore; rritja e bashkëpunimit me sektorin privat do të jenë disa nga objektivat kryesorë për të ardhmen.

- Të dhënat e evidentuara në këtë temë, mbase nga dikush tjetër, mund të ishin parë me këndvështrim tjetër dhe më real, po le të jetë kjo temë, këto të dhëna, një "start" për statistika të tjera, më të hollësishme, më të detajuara e më profesionale.

- Shpejtësia e internetit, përhapja e tij, zhvillimi teknologjik, kanë sjellë deri më sot këto të dhëna, të cilat do kenë trend rritës në vitet në vazhdim. Ky trend rritës duhet të analizohet e përkthehet në vëmendje ndaj sektorit, seksionit, apo specialistëve të krimit kompjuterik në vend: me trajnime, investime në teknologji dhe strukturë organike efikase për kohën që po kalojmë dhe atë që shumë shpejt do të vijë.

## Bibliografi


1. Në këtë temë janë përdorur statistika nga Sektori i Analizes së Informacionit në Drejtorinë e Përgjithshme të Policisë së Shtetit. 2010-2018 ëëë.policia.al
2. Analizat mujore e vjetore për Krimin Kompjuterik. 2010-2018 ëëë.policia.al
3. Bashkëpunimi me Prokurorë të Linjës së Krimit Kompjuterik.
4. *Internet World Statistics*, dhjetor 2017. *https://www.internetëorldstats.com/stats4.htm#europe*
5. Bashkëpunimi me Homologët e Policisë së Kosovës, zimp@KosovoPolice.com
6. Instituti i Statistikave *http://www.instat.gov.al/al/temat/treguesit-demografik%C3%AB-dhe-social%C3%AB/popullsia/publikimet/2018/popullsia-e-shqip%C3%ABris%C3%AB-1-janar-2018/*

# Kiberkriminaliteti dhe kibersiguria publike:

## sindroma *adiktiv ludopatik* dhe nevoja e implementimit të strategjive ndërhyrëse kombëtare të policimit

■**Prof. Asc. Dr. Lindita DURMISHI**
*Universiteti "Aleksandër Xhuvani", Elbasan*
*lindita75@yahoo.com*

■**Dr. (proc.) Silva IBRAHIMI**
*Universiteti i Tiranës*
*silva.ibrahimi@yahoo.it*

**Abstrakt**

*Loja është një instrument themelor dhe i afërt i të nxënit, përmes të cilës njeriu bashkëndan në një pjesë të caktuar me speciet e tjera që nuk kanë zhvilluar një aparat të lartë të funksionalitetit psikik. Kumari dhe lojërat e vendosjes së basteve online janë një nga qëndrimet sjellore më motivuese të kiberkriminalitetit jo vetëm për shoqërinë tonë. Evolucioni i formave të varësisë nga nivelet e ndryshme të kumarit online kërkon njëkohësisht një zhvillim të gjithkahshëm të strukturave akademike, shkencore dhe të sigurisë për depistimin (kontrollin), profilizimin dhe ndërhyrjen efikase sistemike. Ky artikull ka për qëllim të paraqesë një sintezë të punës studimore të zhvilluar në periudhën Janar 2018-Qershor 2018 në një popullatë prej 1500 të rinjsh në grupmoshën 18-24 vjeç në Shqipëri. Metodat e administruara në këtë studim janë "Pyetësori i vlerësimit të sjelljes adiktive South Oaks" dhe studimi i rastit. Rezultatet e përftuara kanë treguar një rritje progresive me rreth 45% të qëndrimit pozitiv dhe tendencës për varësi ndaj kumarit në hapësirën kibernetike ndër të rinjtë. Si përfundim mund të replikojmë për zhvillimin e një dimensioni të kiberkriminalitetit ludopatik adiktiv me karakteristika të veçanta psikologjike, sociale, konjitive dhe të profilit kibernetik në moshën e rritur të re që përbëjnë një fokus specifik të trajtimit për kibersigurinë publike.*

**Fjalëkyçe:**
**çrregullime të shëndetit mendor, e drejta për trajtim, sisteme shëndetësore, shëndeti mendor.**

## 1. Loja në zhvillimin e jetës së përditshme

Loja është një instrument themelor dhe i kahershëm për procesin e të mësuarit, që njeriu e bashkëndan pjesërisht me qeniet e tjera që nuk kanë zhvilluar një aparat psikik të ngjashëm me të. Karakteristikat e lojës janë argëtimi dhe kënaqësia, me funksionalitet kënaqjen e nevojave bazike të individit. Sipas autorëve[1], dimensioni ludik ka krijuar tre përvojat klasike psikologjike të individit: *konjitiven* që zhvillohet sipas vendimmarrjes; *qëllimoren* që fokusohet në vënien e basteve dhe atë *afektive* që ndërthuret me dëshirën për të fituar dhe frikën nga humbja. Pasiguria në rezultatin final dhe rrezikun krijojnë te individi stimulime konjitive, fizike dhe emocionale.

Dëshira për të luajtur përfaqëson rrjedhimisht një formë primitive të mendimit dhe sjelljes, e cila mund të karakterizohet edhe në një tematikë rregulli, kontrolli, zbatimi dhe sjelljeje pak a shumë fikse, një formë sëmundje sociale a individuale, pa kuptuar përse shumë individë në të gjithë botën luajnë dhe e konsiderojnë lojën një sjellje normale dhe të ligjshme. Loja dhe rreziku janë një binom në të gjitha komponentët jetësore, të cilat shpesh kombinohen dhe sjellin sinergji operative në situata të shumëllojshme të jetës së përditshme.

"*Të rrezikosh edhe për një hipotezë*" konsiderohet një formë e vlerësimit në fushat e kërkimit shkencor të dijes dhe më përgjithësisht në fushën e sjelljeve njerëzore, por rreziku është një vlerë pozitive që duhet mbuluar nga shkathtësi konjitive që mbështesin, udhëheqin dhe kontrollojnë proceset dhe vendosin rregulla që kontrollojnë rezultatet. Nevoja për të ditur dhe kontrolluar të ardhmen janë karakteristika të karakterit njerëzor,

[1] Kusyzsyn (1948)The psychology of gambling", *Annals of the American Academy of Political and Social Science*, vol. 474, n.1: 133-145.

thellësisht të shënjuara në natyrën tonë primordiale që ka mësuar të mendojë teksa përpiqet të mbijetojë në kushte të vështirësisë, të paparashikueshme dhe të rrezikshme. Kushtet që kanë formuar dhe strukturuar biologjikisht aparatin psikik njerëzor, për përmirësimin e efikasitetit dhe aftësinë e parashikueshmërisë, për të konceptuar,vlerësuar mundësitë dhe vepruar në varësi të tyre procesin e vendimmarrjes dhe të së mësuarit. Bashkë me trajtimin e "sëmundjes nga loja", qëndron në një rritje e konsumit,si në fushën e publicitet e deri në krijimin e masave përjashtimore të çdo forme të lojës së kumarit[2].

Studiues të tjerë[3] vënë në dukje rritjen e një forme diskursi që promovon ndërmarrjen e rrezikut, hedonizmin dhe kënaqësinë e menjëhershme, si për shembull reklamat e lotarive që nxisin konsumatorin të jetojë të tashmen, që nxisin potencialin e klientit për të "përjetuar momentin" dhe "kapur rastin". Qëndrimi i sistemeve të ndryshme shoqërore ndaj lojërave të fatit ka ndryshuar gjatë rrjedhës së kohës, duke alternuar fazat e lejueshmërisë totale me ato të kufizimit total. Në rrjedhën e shek. të XXI-të, loja ka ndryshuar thellësisht duke u zhvilluar nga aktivitet i paligjshëm dhe i ndaluar në "aktivitet të kohës së lirë"[4], i legalizuar dhe i ofruar publikut në një shkallë të madhe nën kontroll e institucioneve qeveritare[5]. Në një nivel global, të gjitha proceset juridike rregullojnë marrëdhëniet me lojërat e kumarit nëpërmjet ligjeve dhe udhëzimeve e procedurave të ndryshme të licencimit. Kazinotë, lotaritë dhe pikat e baste të llojeve të ndryshme përfaqësojnë sot një fenomen global nga i cili Shqipëria po njeh një rritje eksponenciale jo vetëm në sasi, por sidomos në ndryshim të cilësisë së jetës së popullatave, që e kthejnë këtë veprimtari në stil të jetës; dhe, strukturave të policimit e burimeve njerëzore-financiare, që kërkohen për mbrojtjen e tyre[6] .

Rritja e cilësisë së qëndrimeve adiktive ndaj lojës *online* rrit njëkohësisht cilësinë e sjelljes deviante në hapësirën kibernetike dhe kjo e fundit, forcon kushtet e shfaqjes së sjelljes kriminale si funksion. Shtimi i njërit qëndrim deviant në kushte të favorizimit socioekonomik, siç është *kumari adiktiv*, shton një tërësi të sjelljeve që provokojnë kriminalitet. Me gjithë ndryshimet e rëndësishme të ratifikuara nga Komisioni i Ekonomisë dhe institucionet ligjzbatuese më mars-maj 2018, mbi "Lojërat e Fatit", dhe vendosja e këtyre aktiviteteve në zona periferike dhe larg mjediseve arsimore, ende kemi një situatë që kërkon vëmendje të veçantë dhe trajtim strategjik!

## 2. Cikli i krijimit lojë patologjike dhe *sindromi ludopatik* në hapësirën kibernetike

Sipas studiuesve[7] loja si veprimtari *ludike* ose ekonomike daton përafërsisht 2000 vjet p.e.s. Babilonasit, etruskët, egjiptianët, kinezët, indianët para kolumbianë, grekët, romakët si qytetërime, kanë organizuar forma të lojërave të ndryshme të fatit[8] të cilat



[2] Fea M. (2016), "Gioco d'azzardo: società, istituzioni, servizi", *Gambling newsletter.*
[3] Reith G. (2006), *Research on the social impacts of gambling*, Scottish Executive Social Research, Edinburgh.
[4] Reith G., Dobbie F. (2013), "Gambling careers: a longitudinal, qualitative study of gambling behavior", *Addiction Research and Theory*, vol. 21, n.5: 376- 390. .
[5] McMillen J. (1996), *Gambling Cultures: Studies in History and Interpretation*, Routledge, London/New York: 1-5.; Vaughan Williams L., Siegel D. S. (2013), *The Oxford Handbook of the Economics of Gambling*, Oxford University Press.
[6] Global Betting and and Gaming Consultants – Gbgc - (2017), *Global Gambling Report, 10th edition*.
[7] Becoña E.(1996) *La ludopatia*, Madrid, Santillana.
[8] Fleming A. M. (1978) Something for nothing. A history of gambling, New York, Delacorte Press.

konsideroheshin në antikitet një nga pasionet kryesore të klasës së lartë[9].

Të tjerë autorë[10] e kanë studiuar lojën si një formë e organizimit social që ka marrë edhe vëmendjen e dijetarëve të mëdhenj. Kështu për shembull, Aristoteli,[11] do të lidhte në *Etikën* e tij lumturinë dhe virtytin me lojën duke e konsideruar lojën si një aktivitet i zhvilluar në një plan më të lartë të qenies njerëzore, i lirë nga paraqitja e akteve të tjera të diktuara nga domosdoshmëria. Nga ana tjetër filozofi i shquar gjerman[12], e përcakton lojën si të lidhur me krijimtarinë estetike të njeriut. Po kështu, romantikët[13] do të argumentonin mbi rëndësinë e lojës si një formë të historisë e kulturës, duke pohuar se loja është një manifestim i artit e në veprën e tij "Letra mbi edukimi estetik të njeriut" ai citon: "*vetëm kur luan njeriu është njeri në kuptimin e plotë të fjalës*"[14] (Arancibia Uehara, 2011).

Studiuesi gjerman Max Weber përshkroi disa lloje të veprimeve njerëzore si: tradicionale, emocionale dhe të qëllimshme, racionale. Natyrisht, një kuptimësi e arsyeshme e veprimit shoqëror redukton nevojën për të ndërtuar nga themelet bazike këto aktivitete duke i dalluar ato nga emocionale në tradicionale e të vlerësueshme. Ekonometristët e kanë pranuar dhe transformuar idetë tradicionale të Weber-it si shprehje e racionalizmit në jetën e përditshme duke mbështetur analizën ekonomike e sjelljes njerëzore si bazë për racionalizimin e saj. Maksimizimi i fitimit nga funksioni i përdorimit të së mirave, shpjegon *çdo* formë të sjelljes njerëzore.

Njeriu modern ka një motiv ekonomik dhe kjo duhet të shpjegohet ekonomikisht edhe pse kjo paradigmë nuk sjell një përgjigje mbi koncepte të tejhuazuara, si: lumturia, ndjenja e fatit dhe e rrezikut etj.

Janë identifikuar tri faza të progresit së industrisë së kumarit kibernetik në studimet shkencore[15]:

1."*fëmijëria e madhe* (1946-86)", filloi me hapjen e *skedinës* e cila ka gëzuar një popullaritet të madh në pesë dekadat e fundit, duke u bërë një instrument financiar në duart e shtetit;

2. "*adoleshenca e pakontrolluar*" ku u shfaqën përpjekjet e parë e legalizimit të sistemit të lojërave të fatit (1987-2011);

3. "*tranzicioni në moshën e rritur*" (2012), me përpjekjen e parë për të ndalur përhapjen e lojërave të kumarit. Përmes miratimit të fundit të draft-ligjit të propozuar në Këshillin e Ministrave të Shqipërisë[16], në shtojcë të ligjit të 2015 në Kuvendin e Shqipërisë më 2018, është limituar dhe rregulluar veprimtaria financiare dhe sociale e këtyre subjekteve duke i zhvendosur ato fizikisht përtej qendrave të banuara, shkollave, institucioneve etj. Në nivel Europian, pavarësisht nga mungesa e legjislacionit të veçantë të Komunitetit për Kumarin, Parlamenti i BE ka miratuar në 2013 një rezolutë - 2012/2322 - e cila replikon legjitimitetin e ndërhyrjeve të Shteteve Anëtare për të mbrojtur lojtarët, edhe në mbrojtje të disa parimeve kryesore të së drejtës komunitare, si liria e

[9] Ìàíëîâà, Ä., (2012) Î÷àêâàò ïðèõîäèòå â õàçíàòà îò õàçàðò äà ñå óâåëè÷àò ñ äî 100 ìëí. ëâ. âîäåùîì, Gjendur në "Youth and Gambling" Durmishi. L et al. Knowledge: International Journal of Scientific Papers,vol. 13. 3, f. 425.

[10] Beck U. (2000), *Risikogesellschaft. Auf dem Weg in eine andere Moderne*, Suhrkamp, Frankfurt.

[11] Aristotle (1893 botimi Angl.) The Nicomachean Ethics, M. A. 5th edition London: Kegan Paul, Trench

[12] Kant, I,(1997, botimi Angl.) Lectures on Ethics, Cambridge University Press.

[13] Von Schiller, F. (2004) On the Aesthetic Education of man, Dover Books, UK.

[14] Arancibia U. ( 2011) En busca de sentido:el juego como problema social, Madrid.

[15] Pedroni M. (2014), "The «banker» state and the «responsible» enterprises. Capital conversion strategies in the field of public legal gambling".

[16] Ministria e Financave e Shqipërisë (2018) Projektligj "Për Lojërat e Fatit në Republikën e Shqipërisë", VKM shtojcë e Ligjit për Lojërat e Fatit 2015.

qëndrimit dhe liria sigurimi i shërbimeve[17]. Këto direktiva nga ana tjetër nuk limitojnë të drejtën e agjencive ligjzbatuese për të monitoruar veprimtarinë kiberdeviante të kryer *online*. Vënia e basteve dhe luajtja e kumarit *online* si dukuri socioekonomike shpesh shihet edhe si pjesë e domosdoshme, por veçanërisht e nevojshme për sigurimin e mëtejshëm në industrializimin ekonomik të vetë njeriut.

Është jo rrallë e ndeshur shtrirja e kësaj dukurie si pjesë e stilit të jetës së individëve të "*klasës së lartë", "moderne e mendjehapur", "që ndjekin trendin"* etj.

Industria e kumarit si një komponent zhvillimi i shpejtë dhe vazhdimisht inovativ po aq sa industria e inovacionit progresojnë thuajse me hapa të pandalshme. Edhe pse koncepti i përgjithshëm social mund të "ndëshkojë" sipërfaqësisht sjelljet e lidhura me ndjekjen e kumarit, shpeshherë ky koncept i përgjithshëm "*interneti na ka shpëtuar nga rruga*", "*përjashton sjelljet të rinjve që nuk i bëjnë dëm të tjerëve*", "*që do të largohen nga lojërat kur të rriten dhe të kuptojnë*" apo "*që janë shumë të stresuar dhe nuk kanë sesi të heqin stresin dhe të argëtohen*"![18] Andaj,më tepër sesa tendencë e nivelit personal të individit për tu përfshirë në kumar, kemi të bëjmë me një tendencë psikosociale për të racionalizuar e intelektualizuar sjelljen. Nëse nuk i bën dëm të tjerëve, atëhere nuk ka shumë problem!

Nëse për pjesën më të madhe të njerëzve kumari dhe loja *online* janë vetëm një argëtim, një moment grumbullimi dhe bashkëndarje me të tjerët, për një pjesë tjetër kthehet në një varësi të vërtetë, dukuri e njohur si *kumari patologjik nga loja online a sindromi ludopatik*, i cili në shumë raste krijon pasoja serioze psikologjike, në marrëdhëniet sociale, ekonomike dhe juridike- ligjore.

Kumari *online* mund të nxisë ndryshime në gjendjen mendore dhe fizike, duke stimuluar dhe dhënë energji aspektit psikofizik të lojtarit: të vësh një sasi të caktuar të parave me mundësinë e marrjes e sa më shumë, por edhe për të mbetur pa asgjë, provokon ndjesi që mund të rezultojnë për shumë individë mund të jenë tepër të kënaqshme[19].

Individët edhe më të interesuar ndaj kumarit *online* karakterizohen nga rritja e kërkesës për më shumë kënaqësi nga rreziku dhe vënia e shifrave edhe më të mëdha në lojë. Në këtë rast, pritja për rezultatin do të karakterizohej nga motivacion i lartë dhe rritje e shpresës për fitim çka e shpie individin në tentim për të vendosur baste aty ku rreziku është më i madh[20].

Në literaturë[21]ekzistojnë hipoteza në lidhje me bashkëshoqërime të caktuara mes pacientëve që trajtohen për problemet e lojërave të fatit dhe llojet e lojërave të preferuara.

Literatura psikologjike po kështu ka njohur nevojën e tejkalimit të horizontit të thjeshtë psikopatologjik-kategorik dhe të marrjen në konsideratë të një dimensioni integral dhe të përshtatjes së individit që luan kumar në sistemet dhe marrëdhëniet e tij të shumëfishta sociale. Niveli i përshtatjes integrale i marrë nga individi në moshën e re



[17] Gjykata Supreme UE -Vendim i 22/01/2015

[18] Bashkimi Europian(2012):Plan strategjia e mbrojtjes dhe parandalimit ndaj Kumarit-Direktiva

[19] Bergler E. (1957), *The Psychology of Gambling*, Hill and Wang, New York.

[20] Lesieur H. (1984), *The Chase: career of the Compulsive Gambler*, Schenkman, Cambridge MA; Croce M. (2001), "Il caso del gioco d'azzardo: una droga che non esiste, dei danni che sistono",*Personalità/ Dipendenze*

[21] Petry N. M. (2003), "A comparison of treatment-seeking pathological gamblers based on preferred gambling activity", *Addiction*,; Croce M. (2008), "Typologie et contextes de jeu: hypothèse sur les facteur de risque en relation avec le facteurs de protection", *Prévenir le jeu excessif dans une société addictive? Livre dés résumés*,; Meyer M., Fiebig G., Häfeli J. e Mörsen C. (2011), "Development of an assessment tool to evaluate the risk potential of different gambling types", *International Gambling Studies*, vol. 11,

[22] American Psychiatric Association (2000)The Diagnostic and Statistical Manual on Mental Disorders DSM-IVTr.

është një parashikues i rëndësishëm të sjelljeve të abstinencës në moshën e rritur. Me qëllim përcaktimin më të qartë diagnostik të tipareve dhe karakteristikave të Kumarit Patologjik sipas Manualit Diagnostik Statistikor[22] (DSM-IV TR), e për konkretizimin e qëllimeve të këtij studimi, është përdorur instrumenti i Pyetësorit South-Oaks (SOGS)[23]. Ky pyetësor përbëhet nga 20 pohime të ndara dhe është instrumenti me vlefshmërinë dhe besueshmërinë më të lartë të përdorimit në mjedisin klinik-forens. Përmbajtja e këtyre pohimeve lidhet ndër të tjera me qëndrimet dhe sjelljet që mbajnë individët ndaj kumarit dhe basteve, burimin e marrjes së parave për të luajtur ose për të paguar, sigurinë që përjetojnë nga strukturat ligjzbatuese dhe boshtin emocional të ndërlidhur me to. Në referencë të këtij punimi, ne po paraqesim të dhënat e analizuara nga pyetësori *online* dhe manual i administruar në 1500 të rinj të popullatës moshore 18-24 në periudhën janar-qershor 2018, në vendin tonë.

**Tab.1 Cikli i zhvillimit të *Ludopatisë*. Paraqitje tabelare e analizës së të dhënave të studimit.**

| | |
|---|---|
| ***Faza e Parë:*** | ***Karakteristikat*** |
| ***të fitosh dhe të vazhdosh të ndjekësh.*** | |
| Luan rrallëherë. | Marrje e kënaqësisë së lartë nga loja. |
| Fiton dhe luan më shumë. | Krijon fantazi "të lojtarit të madh" |
| Shtohen fantazitë e "lojtarit të madh" | Optimizëm irracional:mburracak |
| Fillon të mendojë vazhdimisht për kumarin. | Nuk mund të ndalojë të luajë: fitimi ose humbja nuk kanë më rëndësi. |
| ***Faza e Dytë:*** | ***Karakteristikat*** |
| ***të humbësh dhe të vazhdosh të ndjekësh.*** | Kërkojnë para borxh. |
| Shtohen rastet e humbjeve. | Neglizhon mirëqenien e familjes. |
| Fillojnë të mbulojnë humbjet me gënjeshtrat. | Jetë e pakënaqshme në familje. |
| Shpenzon kohë të kotë në punë. | Nuk paguan dot borxhet e marra. |
| Ndryshim karakteri (i ankthshëm, jo i qetë). | Ndikohet reputacioni personal i individit. |
| Vënë para vazhdimisht e më tepër në kumar. | |
| ***Faza e Tretë: Dëshpërimi.*** | ***Karakteristikat.*** |
| Nuk i japin më para borxh. | Ndarje nga familja. |
| Rritet sasia e kohës së kaluar | Ndjesi të fajit dhe të turpit. |
| në kumar dhe dedikimi ndaj saj. | Veprime të paligjshme. |
| Pendesë dhe ndjenja të panikut. | Ide vetëvrasëse dhe vetëvrasje. |
| ***Faza e Katërt: të prekësh fundin.*** | |
| Asnjë shpresë. Ide dhe përpjekje për vetëvrasje. | |
| Probleme me punën dhe humbja e punës. | |
| Denoncime ose ndalim policor. | |
| Shkatërrim në marrëdhënie | |
| inter- dhe intrapersonale. Divorc. | |
| Abuzim dhe varësi nga droga dhe alkooli. | |
| Lënie pas dore e vetes, neglizhencë dhe braktisje. | |

[22] American Psychiatric Association (2000)The Diagnostic and Statistical Manual on Mental Disorders DSM-IVTr.
[23] Lesieur H.R., Blume S.B. (1987), "The South Oaks Gambling Screen (SOGS): A new instrument for the identification of pathological gamblers", *American Journal of Psychiatry*.

Teksa përpiqemi të analizojmë shkakësinë dhe faktorët e sjelljeve të varësisë nga kiberdevianca dhe kriminaliteti, duhet më së pari të ndalemi në burimet psikosociale të problemit. Përtej determinizmit psikik dhe reduksionizmit individual, gjatë studimeve tona të rastit dhe në procesin e intervistave, kemi identifikuar elementët që ndikojnë negativisht në sjelljen e këtyre subjekteve dhe orientimin e tyre ndaj këtyre varësive specifike. Nga intervistat e realizuara gjetëm një shumësi referencash të lidhura me *konfliktet brenda familjes* dhe *krizat emocionale* si dy nga faktorët kryesorë që lehtësojnë kushtet për zhvillimin e sjelljes së varësisë.

Në 30% të rasteve, subjektet e intervistuar kanë tentuar t'i shmangen konflikteve me prindërit a me të tjerët rreth tyre,duke u mbyllur në vetvete dhe s*hmangu*r përballjet e forta psikoemocionale. Dukuria e "*të mos durimit të zënkave dhe debateve*"me njerëzit e dashur i shpie drejt izolimit personal dhe i nxit progresivisht drejt qarqeve të mbyllura afektive. Ky rreth nga ana tjetër rrit presionin e brendshëm, zhgënjimin dhe dëshpërimin, nxit ndjenjat e vetëfajësimeve dhe ul ndjeshëm vetëvlerësimin. *Imazhi* i të riut për veten është thuajse i shpërbërë, ndërsa ndjenja e një identiteti të mirëformuar vihet në dyshim, rritet vulnerabiliteti psikik i individit dhe incidenca për tu prekur nga sjellja deviante. Dhe kompjuteri a pajisja tjetër zëvendësuese shton ndjenjën disfunksionale të sigurisë dhe qetësisë dhe krijon një imazh social të mbivendosur të ri e të pushtetshëm, "*do të loz më shumë, do fitoj dhe do bëhem i Madh*!".

*Rritja e sjelljes deviante kibernetike* është padyshim prelud i sjelljes adiktive jetëkërcënuese.

Të intervistuar të tjerë, rreth 35% e përgjigjeve, na kanë raportuar se *familja* dhe anëtarët e saj nuk i kanë mbështetur dhe ndihmuar si një sistem egombrojtës, që është i nevojshëm në rastet e kumarit patologjik duke i përforcuar atyre ndjeshëm ndjeshmërinë për të rënë prè e kumarit. Elemente të tjerë mjaft interesantë janë edhe *vetmia, koha e tepërt e lirë* dhe *ankthi i shtuar për pavarësi nga familja*, së bashku 20% të totalit së të intervistuarve, që konsiderohen si faktorë rreziku, e sidomos te vajzat. Studimet mbështetëse kanë treguar se vetmia rrit pulsimin ndaj disa sjelljeve të caktuara dhe lehtëson ndjeshmërinë ndaj varësive.

*Pasioni* është një komponent tjetër i rëndësishëm i lojës *online* për të rinjtë pjesëmarrës. Pasioni për sportin e futbollit dhe nxitja e niveleve të ndjenjës së gëzimit e ndjenja e komunitetit që përçohet ka rritur ndjeshëm praninë e të rinjve në pikat e basteve dhe për të hedhur skedina.

Një nga problematikat tona kryesore gjatë analizës së intervistave të individëve ishte edhe marrëdhënia objektive e të rinjve me paranë. Një pjesë e mirë e të rinjve (rreth 35% e totalit) kishin filluar të punonin në moshë të hershme (kamerier, DJ, banakier, operator telefonik), dhe po kështu, kishin pasur të bënin me menaxhimin e parave. Hyrja e shpejtë në botën e punës për një individ që nuk është mësuar me menaxhimin e mirë të të ardhurave dhe të sasive të parave, i bën ata një grup-shënjestër të pëlqyer dhe të preferueshëm për industrinë e bixhozit kibernetik.

Po kaq të përhapura ndër të rinjtë duken edhe perceptimet e "*fitimit të parasë lehtë*", kërkohet një pasurim i shpejtë,një mënyrë për të marrë para shpejt dhe pa punuar.

Ludopatët gjithashtu sfidojnë *kohën.* Ata marrin nxitje nga ndjesia se do të fitojnë shpejt të parët! Nën dritën e përvojave të specialistëve të shëndetësisë (mjekëve, psikoterapistë, psikologëve, punonjësit socialë, etj.), dhe atyre të zbatimit të ligjit, që në dekadat e fundit kanë trajtuar dhe ndihmuar në krijimin e strategjive të mbrojtjes së

qytetarit, për rezultate pozitive të procesit të rehabilitimit, aspekti i *motivacionit* është vendimtar!

Jo vetëm struktura shoqërore, por parësisht dhe fillimisht sistemet ligjzbatuese, duhen nxitur në përpjekjet e përbashkëta për të mbrojtur të rinjtë nga rreziku i kumarit patologjik. Strategji të veçanta të identifikimit të grupeve më të ndjeshme në komunitet dhe mbrojtjes së të rinjve, mund të përvijohen së bashku me oficerët e Policisë së Shtetit për parandalimin e kësaj dukurie; gjithashtu masat shtrënguese për subjektet që lejojnë pjesëmarrjen e të miturve në veprimtari ekonomike të bixhozit, zbatimi i ligjit shtrëngues me efekt prapaveprues dhe mbi të gjitha krijimi i politikave lehtësuese sociale për familjet mund të frenojnë sadopak shpërhapjen ndërnivelore të kësaj dukurie me impakt të fuqishëm në zhvillimin psikologjik e social.

## 3. Roli i strukturave të policisë dhe krijimi i një aksion-plani të gjerë për parandalimin e kiberkriminalitetit *ludopat*

Sindromi ludopatik dhe kumari patologjik janë dy nëntipat më të përhapur të kiberdeviancës kriminale, me fokus lojën. Si të miturit, dhe të rinjtë, dhe më të mëdhenjtë, janë potencialisht të prekur nga ky fenomen i rrezikshëm socioekonomik. Një incidencë e tillë natyrisht që përbën një interes, jo vetëm për shëndetin publik, por mbi të gjitha për sigurinë publike.

Krijimi i një strategjie me bazë të gjerë që do të përfshinte strukturat e larta politikëbërëse dhe organet e Policisë së Shtetit së bashku me organizmat studimore-akademike dhe të mbrojtjes së komunitetit është ndoshta një nga kërkesat më kryesore në forcimin e veprimtarisë së rendit publik.

Nisur nga përvojat e vendeve të tjera të zhvilluara dhe në mbështetje të dhënave të studimit, po parashtrojmë një plan-veprim të koordinuar për të detajuar cilësisht fokusin e Policisë së Shtetit në zgjidhjen e problematikave në komunitet, - këtu të kumarit kibernetik.

- Trajnimi i vazhdueshëm i punonjësve të Policisë së Shtetit e veçanërisht strukturave të reja të BKH/seksioni i krimit kibernetik dhe sigurisë, mbi këtë formë të kiberdeviancës kriminale dhe rritja e bashkëpunimit me agjenci ose struktura të tjera kombëtare dhe ndërkombëtare me këtë fokus.

- Rritja e bashkëveprimit mes strukturave ligjzbatuese dhe operatorëve TIK për evidentimin e grupe-shënjestrave të rrezikuara nga kumari elektronik dhe kiberdevianca patologjike.

- Krijimi i strukturave drejtuese brenda strukturës së detektimit dhe parandalimit të krimit elektronik për kumarin dhe lojën patologjike si pjesë e makropolitikës së sigurisë publike. Përmes zhvillimit të pyetësorëve dhe anketave të vazhdueshme në komunitet, strukturat e policisë mund të mbledhin informacione mbi grup-shënjestrat e përcaktuara dhe t'i pasurojnë ato në fushat e tjera të hetimit.

- Krijimi i programeve *software* dhe përmirësimi i teknologjisë aktuale për ndarjen dhe shkëmbin e informacionit në strukturën e krimit kibernetik në Policinë e Shtetit ose në strukturat e reja të Byrosë Kombëtare të Hetimit, seksioni parandalimit të krimit kibernetik dhe mbrojtja e të miturve.

- Kryerjen e *workshop*-eve trajnues për situatën e krimit kompjuterik dhe kumarit elektronik patologjik në veçanti me pjesëmarrjen e grupeve të interesit si të banorëve të

një komuniteti, drejtorive të shkollave (mësues, nxënës e prindër) dhe përfaqësues të biznesit mbi lojërat elektronike në komunitet.

- Përvijimi i shpejtë i procedurave për trajtim profesional me specialistë psikologë, punonjës socialë të qendrave specifike të trajtimit a Shërbimit Kombëtar Social, në rastet e personave të mitur të ndaluar me tendencë a precedentë të Kumarit patologjik (Ludopatisë).

## 4. Përfundime

Përgjatë shekullit të kaluar qasja e shoqërisë ndaj lojërave të fatit *online* dhe kumarit kibernetik ka ndryshuar në mënyrë progresive. Bashkërendues të këtij procesi të ndryshimit kanë qenë edhe disa ndërhyrje politike dhe ekonomike, në veçanti në makropolitikat e liberalizimit të miratuara në disa shtete që kanë përcaktuar një impuls të fortë për komercializimin e "produktit të kumarit" e sidomos të lojës patologjike në hapësirën kibernetike[24].

Transformimi i kumarit *online* në një veprimtari të zakonshme argëtimi shoqërohet nga një ndryshim i imagjinatës kolektive të motivuar nga simbolet dhe produktet e kumarit në rrjet, gjerësisht të reklamuara dhe të arritshme thuajse nga të gjitha grupmoshat me përdorim të lehtë dhe akses të menjëhershëm nga mediet sociale dhe sitet e dedikuara kumarit *online*. Një proces që normalizon praninë e kumarit në jetë i përditshme dhe e kthen atë në *stil të jetës*.

Pothuajse të gjitha hulumtimet e kryera gjatë viteve të fundit[25] arrijnë në përfundimin se pjesa më e madhe e individëve luajnë kumar gjatë ekzistencës së tyre dhe se numri i lojtarëve e tejkalon atë të jo-lojtarëve.

Shtrirja e kumarit kibernetik në mbarë botën është konsideruar një çështje e rëndësishme për shëndetin publik, dhe sigurinë publike. Në veçanti, kumari patologjik si përhapje e formave të varësisë, ndaj sjelljeve, që të karakterizuara nga përshkrueshmëria e karakterit kulturor, të lidhura me prirjen për tejkalim, me dobësimin e kapaciteteve kritike për të frenuar ambicien për sukses, e deri me nevojën për marrëdhënie, dashuri dhe vëmendje për të ushqyer identitetin e pasigurt, në format e tyre ekstreme, krijojnë vuajtje dhe nxisin patologjinë ludopatike[26].

Ndërhyrjet parandaluese dhe profilaktike sociale për menaxhimin, trajtimin dhe krijimin e paketave të programeve ndaj ludopatisë patologjike kibernetike, ndahen në tri lloje[27]:

a) *parandalimi parësor* (universal),
b) *parandalimi dytësor* (selektiv),
c) *parandalimi tretë*sor (specifik).

Parandalimi *parësor* ka për qëllim që ta bëjë popullsinë të vetëdijshme për rreziqet dhe pasojat e mundshme negative të lidhura me teprimin e kumarit dhe lojës kibernetike. *Parandalimi dytësor* synon të ulë dëmin potencialin të atyre të rrezikuarve, të cilët humbasin kontrollin e tyre vetëm nga loja *online*. *Parandalimi tretësor*, i referohet

[24] Kingma S. F. (2010), *Global gambling: cultural perspectives on gambling Organizations*, Routledge, London.
[25] Calado F., Griffihs M.D. (2016), "Problem gambling worldwide: An update and systematic review of empirical research (2000–2015)", *Journal of Behavioral Addictions*.
[26] Valleuer., M. Y , J. (2005) Las Nuevas Adicciones del siglo XXI. Kap. 5: Prisiones del juego Paidós, Argentina.
[27] Gordon R. S. (1983), "An operational classification of disease prevention", *Public Health Reports*, vol. 98, n. 2: 107–109.

veprimeve që kanë për qëllim kontrollimin dhe përmbajtjen e rezultateve më të mëdha, si: terapinë mbështetëse, programet kombëtare dhe rajonale të mbrojtjes, krijimin e praktikave dhe kurrikulave universitare të integruara etj., për rritjen e sigurisë publike dhe shëndetit publik.

## Bibliografi


1. Kusyzsyn (1948) The psychology of gambling", *Annals of the American Academy of Political and Social Science*, vol. 474, n.1: 133-145.
2. Fea M. (2016), "Gioco d'azzardo: società, istituzioni, servizi", *Gambling newsletter*, http://www.newsletter.federserd.it/.
3. Reith G. (2006), *Research on the social impacts of gambling*, Scottish Executive Social Research, Edinburgh.
4. Reith G., Dobbie F. (2013), "Gambling careers: a longitudinal, qualitative study of gambling behavior", *Addiction Research and Theory*, vol. 21, n.5: 376- 390. .Doi:10.3109/16066359.2012.731116.
5. McM*illen J.* (1996), *Gambling Cultures: Studies in History and Interpretation*, Routledge, London/New York: 1-5.
6. Vaughan Williams L., Siegel D. S. (2013), *The Oxford Handbook of the Economics of Gambling*, Oxford University Press.
7. Global Betting and and Gaming Consultants – Gbgc - (2013), *Global Gambling Report, 10th edition*, http://www.gbgc.com.
8. Becoña E.(1996) *La ludopatia*, Conselleria de Sanidade, Madrid, Santillana.
9. Fleming A. M. (1978) Something for nothing. A history of gambling, New York, Delacorte Press.
10. Ìàíîëîâà, Â., (2012) Î÷àêâàò ïðèõîäèò â õàçíàò ïî õàçàðò äà ñå óâåëè÷àò ñ äî 100 ìëí. ëâ. âîäåøè, Gjendur në "Youth and Gambling" Durmishi.L et al.Knowledge: International Journal of Scientific Papers,vol. 13. 3, fq. 425.
11. Beck U. (2000), *Risikogesellschaft. Auf dem Weg in eine andere Moderne*, Suhrkamp, Frankfurt.
12. Arancibia U.( 2011) En busca de sentido:el juego como problema social, Madrid
13. Aristotle (1893 botimi Angl.) The Nicomachean Ethics, M. A. 5th edition London: Kegan Paul, Trench , Truebner & Co. http://oll.libertyfund.org/titles/903.
14. Kant, I, (1997, botimi Angl.) Lectures on Ethics, Cambridge University Press https://doi.org/10.1017/CBO9781107049512 von Schiller, F. (2004) On the Aesthetic Education of man, Dover Books, UK.
15. Pedroni M. (2014), "The «banker» state and the «responsible» enterprises. Capital conversion strategies in the field of public legal gambling", Rassegna Italiana di Sociologia, vol. 55, n. 1: 71-98.
16. Ministria e Financave e Shqipërisë (2018) Projektligj "Për Lojërat e Fatit në Republikën e Shqipërisë",VKM shtojcë e Ligjit për Lojërat e Fatit 2015.
17. Gjykata Supreme UE -Vendim i 22/01/2015.
18. Bashkimi Europian (2012): Plan strategjia e mbrojtjes dhe parandalimit ndaj Kumarit-Direktiva http://europa.eu/rapid/press-release_IP-12-1135_bg.htm
19. Bergler E. (1957), *The Psychology of Gambling*, Hill and Wang, New York.
20. Lesieur H. (1984), *The Chase: career of the Compulsive Gambler*, Schenkman, Cambridge MA.
21. Croce M. (2001),"Il caso del gioco d'azzardo: una droga che non esiste, dei danni che esistono" *Personalità/ Dipendenze,* n. 2:225-242.
22. Petry N. M. (2003), "A comparison of treatment-seeking pathological gamblers based on preferred gambling activity", *Addiction*, vol. 98, n. 5: 645-655
23. Croce M. (2008), "Typologie et contextes de jeu: hypothèse sur les facteur de risque en relation avec le facteurs de protection", *Prévenir le jeu excessif dans une société addictive? Livre dés résumé*s, Lausanne.
24. Meyer M., Fiebig G., Häfeli J. e Mörsen C. (2011), "Development of an assessment tool to evaluate the risk potential of different gambling types", *International Gambling Studies*, vol. 11,n. 2: 221-236
25. Lesieur H. R., Blume S. B. (1987)"The South Oaks Gambling Screen (SOGS): A new instrument for the identification of pathological gamblers", *American Journal of Psychiatry*, vol. 144, n. 9: 1184-1188.
26. Kingma S. F. (a cura di) (2010), *Global gambling: cultural perspectives on gambling Organization*s, Routledge, London
27. *Calado F., Griffihs M.D. (2016), "Problem gambling worldwide:* An update and systematic review of empirical research (2000–2015)", *Journal of Behavioral Addiction*s, Doi: 10.1556/2006.5.2016.073.
28. Valleuer., M. Y , J. (2005) Las Nuevas Adicciones del siglo XXI. Kap. 5: Prisiones del juego. Paidós,Argentina.
29. Gordon R. S. (1983), "An operational classification of disease prevention", *Public Health Reports*, vol. 98, n. 2: 107–109..

# Siguria në "Internet Banking"


■**Dr. Bitila SHOSHA**
*bitilashosha@yahoo.com*
*Universiteti "Aleksandër Moisiu", Durrës*

■**Dr. Armela ANAMALI**
*financa@hotmail.com*
*Universiteti "Aleksandër Moisiu", Durrës*

■**Dr. Alma ZISI**
*alma_zisi @ yahoo.com*
*Universiteti "Aleksandër Moisiu", Durrës*



**Abstrakt**

*Me zhvillimin ekonomik të vendit, ashtu si në vende të tjera, edhe në vendin tonë, vërë re një rritje dhe një përmirësim të zhvillimit teknologjik. E-Banking, si një nga prirjet dhe inovacionet e fundit në Shqipëri, është adoptuar më së miri si një shërbim i ofruar nga bankat tregtare. Një ndër problemet kryesore, kur konsumatori pranon të paguajë elektronikisht, është siguria. Sipas Kima (2010) siguria e pagesave elektronike varet nga pesë faktorë: faktori sistem, faktorët teknikë dhe të infrastrukturës, implementimi, transaksionet financiare dhe faktorët ligjorë. Në mbrojtje të klientit nga kriminaliteti elektronik, bankat tregtare që ofrojnë E-Banking përdorin sisteme të përparuara sigurie, të cilat kodojnë të gjitha informacionin ndërmjet bankave dhe klientëve të tyre Një prej motiveve kryesore të përdorimit të Internet Banking është marrja e një shërbimi praktik dhe komod duke kursyer kohë dhe para. Teknologjia e Internet Banking, siguron një nga mënyrat më efikase për marrëdhënien e bankave me klientët e tyre, duke ofruar akses në një gamë të gjerë produktesh dhe shërbimesh financiare. Shërbimet e automatizuara të E-Banking ofrojnë mundësi për maksimizimin e fitimeve. Internet Banking ka edhe kosto financiare që lidhen me investime në teknologji. Teknologjia ecën me hapa shumë të shpejta dhe për të arritur ritmin, por edhe për të përmirësuar shërbimin ka kosto. Duke bërë një rishikim literature të thelluar por duke u mbështetur edhe në burime të publikuara lidhur me sigurinë e transaksioneve në mbrojtje te klientit do ta finalizojmë studimin tonë me disa konkluzione dhe rekomandime të rëndësishme.*



**Fjalëkyçe:**
**"Internet banking", "e-banking", "mobile banking", siguria, sisteme kompjuterike, baza e të dhënave, banka tregtare.**

## 1. Hyrje

- Kuptimi i *Internet Banking?*

*E-Banking* e njohur ndryshe si *elektronik-Banking* parashikon përhapjen e produkteve elektronike në tre forma kryesore:

- ATM (*Automatic teller machines*);

- pagesa elektronike të cilat operojnë nëpërmjet kartave të kreditit, debitit apo kartat SMART dhe transferimit të fondeve përmes rrugëve elektronike;

- *Mobile Banking*, *E-Banking* përmes telefonave celularë dhe *E-Banking* përmes internetit.

- Kur dhe si lindi *Internet Banking?*

Përhapja e teknologjive të informacion*it dhe të* komunikimit, rritja e përdorimit të kompjuterëve personalë, lehtësimi i lidhjes me internetin, si dhe përhapja e gjerë e telefonave celularë kanë tërhequr vëmendjen e bankave drejt *internet banking*. Si fillim ai u prezantua në vitet '80, megjithatë vetëm në mesin e viteve '90 u përhap gjerësisht dhe që atëherë ka përparuar shumë. Gjatë dekadës së fundit transaksionet bankare janë rritur në mënyrë marramendëse.

- E ardhmja e *Internet Banking?*

*Internet Banking* ka sjellë pa dyshim një evolucion në sistemin bankar, pasi ka bërë të mundur "krijimin" e një filiali banke në shtëpinë e gjithsecilit dhe është i destinuar të zhvillohet më tej. Megjithatë, historia e viteve të fundit na tregon se shërbimet bankare online, edhe në të ardhmen, do të kenë një funksion plotësues të atyre tradicionale. Aktualisht, modeli më i preferuar duket të jetë ai amerikan, i quajtur modeli "clicks and mortar", i cili nxit klientët të përdorin internet *Banking* për transaksionet bazë, duke i lënë më të lirë punonjësit e bankave për shërbime si, planifikim apo drejtim financiar.

Me kalimin e kohës dhe me afirmimin e shërbimeve bankare *online*, ka gjasa që faqet e internetit të bankave të përdoren po aq sa sportelet dhe ATM-të. Të gjitha këto mënyra, do vazhdojnë të jenë pjesë e një modeli shumëkanalësh, si strategji optimale për t'i garantuar klientëve të tyre më tepër fleksibilitet, prakticitet dhe komoditet[1].

### *1.1 Qëllimi dhe objektivat e punimit*

Qëllimi i punimit është nxjerrja e një panorame sa me të plotë të sistemeve të sigurisë që ofrojnë bankat e nivelit të dytë, në Shqipëri, që përdorin shërbimet *E-Banking*.

Në këtë punim kemi si objektiv kryesor, që duke bërë një rishikim literature të thelluar, por duke u mbështetur edhe në burime të publikuara lidhur me sigurinë e transaksioneve në mbrojtje te klientit, ta finalizojmë studimin tonë me disa konkluzione dhe rekomandime të rëndësishme. Një objektiv tjetër, është që në fund të punimit, t'i japim përgjigje pyetjes: A mendoni se janë të sigurta këto sisteme që ofrohen nga shumica e bankave në Shqipëri?

### *1.2 Metodologjia e punimit*

Ky studim është bazuar në disa etapa të caktuara, të cilat mundësuan njohjen e kontekstit, për trendin e shërbimeve *E-Banking* nga bankat tregtare në Shqipëri. Për këtë arsye, është shfletuar literatura e huaj dhe vendase. Për një kornizë më të plotë dhe qasjen me realitetin në vendin tonë, u panë si të rëndësishme dhe me vlerë, intervista personale dhe takime me specialistë dhe titullarë te institucioneve bankare që ofrojnë shërbimin *E-Banking*; këto takime ndihmuan në mirëpërcaktimin e metodës më të saktë për vlerësimin që u krye. Faza tjetër e rëndësishme ishte mbledhja e të dhënave statistikore dhe raporteve, kryesisht nga Banka e Shqipërisë, të cilat mundësuan një analizë analitike; përcaktimi i pikave të forta dhe të dobëta, - gjithçka bazuar në analizë. Në fund, arrihet në konkluzione, të cilat krahasohen edhe me përfundimet bibliografike të përmendura që në fillim të studimit.

### *1.3 Rishikimi i literaturës*

Pagesat elektronike luajnë një rol të rëndësishëm në zhvillimin e sektorëve bankarë dhe kanë efekte pozitive në ekonominë e një vendi. Studime të ndryshme, tregojnë, që edhe pse këto shërbime nuk janë ato më fitimprurëset që bankat ofrojnë, mund të sigurohen shumë përfitime, nëse ato përdoren siç duhen. Në studimin e tyre, Chakravorti and Emmons (2003) sugjerojnë që strategji të ndryshme të vënies së çmimeve, përmirësojnë mirëqenien në tregje konkurrente. Hasan, De Renzis and Schmiedel (2012), nga kërkimi i tyre, u rezulton që kalimi nga forma e pagesave *cash* në pagesa elektronike, nxiti ekonomitë e tërë vendeve. Zgjerimi i bankave u lehtësua nga progresi i zhvillimit të teknologjisë, si, ATM e POS, të cilat reduktojnë kostot me kalimin e kohës (Berger & DeYoung, 2006).

Disa prej autorëve i kanë kushtuar vëmendje të veçantë jo vetëm marketingut të bërë nga bankat, për pagesat elektronike, por edhe tarifave që paguhen kur kryhen pagesa elektronike. Rochet dhe Tirole (2002), gjykojnë që nëse politikat e vënies së

[1] Publikim nga Banka Qendrore e Shqipërisë "Bankat në epokën e internetit" 2009

çmimeve nuk do të ndryshonin, do të kishim rritje të mirëqenies.

## 2. Siguria në shërbimin e *Internet Banking*

Duke ju referuar mentalitetit të njerëzve një nga hapat më të rëndësishëm të funksionimit dhe të ardhmes së *Internet Banking* është besimi i tyre tek shërbimet *online*. Ekziston gjithmonë e më shumë, nevoja e sigurisë të shërbimeve të transaksioneve që kryhen nëpërmjet *Internet Banking*.

Përdorimi i shërbimeve bankare me anë të internetit, mund të sjellë rrezikun e penetrimit nëpërmjet rrjetit në mënyra të ndryshme: duke përvetësuar kodin sekret të hyrjes, duke ndërmjetësuar, duke kryer veprime bankare në emër të së tjerëve etj.

Në momentin që konsumatori pranon të kryejë pagesa elektronikisht, një nga problemet kryesore, qëndron pikërisht tek siguria e parave gjatë këtij transaksioni. Edhe pse pagesat elektronike kanë avantazhe, kundrejt mënyrës tradicionale të së paguarit, nëpërmjet *cash* apo çeqeve, ato duhet të ofrojnë më shumë siguri për konsumatorin. Kima et al.(2010) identifikoi që siguria e pagesave elektronike varet nga pesë faktorë:

- faktori sistem,
- faktorët teknikë dhe të infrastrukturës,
- implementimi,
- faktorët e transaksionit,
- faktorët ligjorë.

Pavarësisht masave të sigurisë që kanë marrë bankat, edhe në vendet e zhvilluara vazhdojnë të ekzistojnë instrumente të tjerë si, *cash,* apo letra të tjera si, çeqet. Me qëllim rritjen e përdorimit të pagesave elektronike, emëtuesit e bankave kanë shpërndarë programe shpërblimi. Këto programe, llogarisin sasinë e parave elektronike që konsumatorët shpenzojnë në dyqane specifike, dhe për pragje specifike të shpenzimeve të konsumatorëve, këto programe, u kthejnë atyre një sasi shpërblyese të parave elektronike, ose dhurata të ndryshme në dyqanet ku ata kryejnë blerjet.

Hsee et al.(2003) në studimin e tij, tregoi se programet nxitëse të aplikuara, kur konsumatorët kryenin blerjet, në përgjithësi kishin një impakt pozitiv në rritjen e shitjeve. Hayashi and Klee (2003) evidentuan se ndërhyrja e teknologjive të reja, koontribon në rritjen e kënaqësisë së përdorimit të pagesave elektronike. Zbuluan gjithashtu, se vlera e transaksioneve, karakteristikat fizike dhe pikat e shitjes, mund të influencojnë mënyrat e pagesave.

Kennickell and Kwast (1997), zbuluan që niveli i edukimit dhe aseteve financiare, ndikojnë dhe stimulojnë pagesat elektronike. Në mbrojtje të klientit nga kriminaliteti elektronik, bankat që ofrojnë *E-Banking,* përdorin sisteme të përparuara sigurie, të cilat kodojnë të gjithë informacionin që qarkullon mes bankës dhe klientit. Në këtë mënyrë, me anë të procedurave të kriptografisë, bankat i garantojnë klientëve të tyre sigurinë, integritetin dhe disponueshmërinë e produkteve dhe shërbimeve bankare që ato ofrojnë.

Nga ana juaj, ju si klientë mund të bëni diçka për t'u vetëmbrojtur. Mjafton të ndiqni disa këshilla të thjeshta praktike dhe gjithçka do të jetë plotësisht e sigurt[2]:

- bëni kujdes kur të vendosni fjalë kalimin (*password*) e llogarisë tuaj *online*;
- zgjidhni diçka të lehtë për t'u kujtuar, por të vështirë për t'u gjetur nga të tjerët, (mos përdorni emrin, mbiemrin, ditëlindjen, tuaj apo të personave të tuaj të afërm dhe as emrin e ndonjë personazhi publik);
- mos hyni kurrë në llogarinë tuaj *online* nga një kompjuter publik; evitoni të përdorni

kompjuterët e bibliotekave, të shkollave apo të internet-kafeve, pasi disa vendosin *cookies* në kompjuter, që mbledhin informacionin e tyre personal;

- edhe nëse jeni duke përdorur kompjuterin tuaj personal, mos e lejoni faqen e internetit të bankës të "mbajë mend" emrin tuaj të përdorimit apo fjalëkalimin;

- mos u lidhni me faqen e *Internet Banking* nëpërmjet një linku (lidhje) në *email* ose në motorët e kërkimit në internet; më mirë shtypeni vetë adresën elektronike të bankës suaj, për më shumë siguri;

- bëni kujdes nga "*phishers*": këta janë hajdutë të teknologjisë së lartë, të cilët dërgojnë email, duke deklaruar se përfaqësojnë banka apo institucione të tjera financiare dhe se për të përditësuar informacionin që ata kanë mbi klientët e tyre, kanë nevojë për të dhënat tuja personale, përfshirë numrin e llogarisë, emrin e përdoruesit dhe fjalë kalimin; mos u gënjeni nga sofistikimi i këtyre mesazheve dhe mos ju përgjigjni - banka nuk do t'ju kërkojë kurrë një informacion të tillë me email dhe as me telefon;

- kontrollojeni vazhdimisht gjendjen e llogarisë dhe transaksionet tuaja; në rast se vini re gabime apo transaksione të paautorizuara, njoftoni menjëherë bankën;

- mos harroni të s'regjistroheni dhe të mbyllni të gjitha faqet e hapura, pas përfundimit të përdorimit të shërbimit *online*.

### *2.1 Implementi i shërbimit të "Internet Banking" në banka të nivelit të dytë në Shqipëri*

Ndryshimet e vazhdueshme në industrinë e teknologjisë së informacionit, si dhe rritja e problematikave të ndryshme që rrjedhin nga përdorimi i kësaj teknologjie kanë ndikuar në shtimin e vëmendjes dhe investimeve në lidhje me sigurinë e informacionit, nga ana e bankave. Vëmendje e veçantë po i kushtohet rritjes së sigurisë së informacionit dhe monitorimit të vazhdueshëm të rrezikut në lidhje me të. Gjatë vitit 2017, një peshë të madhe të këtyre investimeve kanë zënë investimet për sigurinë kibernetike, e cila është edhe tendenca ndërkombëtare e teknologjisë së informacionit. Në këtë kuadër, gjatë vitit 2017 ka filluar projekti i SWIFT-it (*Client Security Program*), i cili synon rritjen e sigurisë së informacionit (pagesave)[3].

Duke ju referuar raportimeve të tabelës 2.1, shërbimet *E-Banking*, të cilat ofrohen nga bankat tregtare në Shqipëri, në fund të vitit 2017, duke e krahasuar me vitet paraardhëse, tregojnë një tendencë gjithmonë e në rritje. Pjesa më e madhe e produkteve të ofruara nga bankat e nivelit të dytë në Shqipëri, bëjnë pjesë në paketën tradicionale të shërbimeve: depozitime, llogari, transferta.

Ky shërbim ofron kushte maksimale të sigurisë për të ruajtur fshehtësinë e të dhënave të klientit dhe për të ofruar një shërbim sa më të sigurt. Klientët kanë akses për të shlyer detyrimet e tyre mujore për kompanitë utilitare, por sipas bankave, jo çdo kompani është e interesuar. Detyrimet që shlyhen me këtë shërbim janë për: amc, vodafon, albtelekom, tatim taksa, zhdoganimin e mallit[4].

Nga grumbullimi dhe analiza e informacioneve të publikuara nga bankat në faqet e tyre të internetit, rezulton se është rritur prezenca e bankave në disa kanale elektronike të ofrimit të shërbimit për konsumatorët, kanale të drejtpërdrejta si: ATM, Phone *Banking*, Internet *Banking* dhe Mobile *Banking*.

[2] Publikim nga Banka e Shqipërisë "Bankat në epokën e internetit" 2009.
[3] Raport vjetor 2017, Banka e Shqipërisë.
[4] Internet *Banking*: Comptroller's Handbook,1999.

| BANKAT | Kartat Elektronike (debit /kredit) | ATM (Automatik Teller machine) | E- Banking (Electronic Banking) | Mobile SMS Banking | Phone Banking | POS (Point of Sale) | POS Virtual | PayBox |
|---|---|---|---|---|---|---|---|---|
| Raiffeisen Bank | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | I. |
| BKT | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | II. | III. |
| Tirana Bank | ✓ | ✓ | ✓ | ✓ | ✓ | IV. | V. | VI. |
| NBG | ✓ | ✓ | VII. | ✓ | ✓ | VIII. | IX. | X. |
| Alpha Bank | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | XI. | XII. |
| Procredit Bank | ✓ | ✓ | ✓ | ✓ | XIII. | ✓ | XIV. | ✓ |
| Banka e Parë e Investimeve, Albania | ✓ | ✓ | ✓ | ✓ | XV. | XVI. | XVII. | XVIII. |
| Credins Bank | ✓ | ✓ | ✓ | ✓ | XIX. | ✓ | ✓ | XX. |
| Union Bank | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | XXI. | XXII. |
| Banka Societe Generale Albania | ✓ | ✓ | ✓ | ✓ | ✓ | XXIII. | XXIV. | XXV. |
| Banka Intesa Sanpaolo, Albania | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | XXVI. | XXVII. |
| Veneto Bank | ✓ | ✓ | ✓ | XXVIII. | XXIX. | ✓ | XXX. | XXXI. |
| Banka Ndërkombëtare Tregtare | ✓ | ✓ | XXXII. | ✓ | XXXIII. | XXXIV. | XXXV. | XXXVI. |
| Banka Amerikane Einvestimeve | ✓ | ✓ | ✓ | XXXVII. | XXXVIII. | XXXIX. | XL. | XLI. |
| Banka e Bashkuar e Shqipërisë | ✓ | XLII. | XLIII. | XLIV. | XLV. | XLVI. | XLVII. | XLVIII. |

**Tabela 2.1 Shërbimet E-Banking, të cilat ofrohen nga bankat tregtare në Shqipëri në fund te vitit 2017**

**Burimi:**
**Banka e Shqipërisë**

**Tabela 2.2 Produktet elektronike bankare të miratuara nga Banka e Shqipërisë në fund të vitit 2017**

| Produktet elektronike | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2008-2017 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| *Karta debiti* | 3 | 4 | | | | | | | | 1 | 8 |
| *Karta krediti* | 2 | 4 | 1 | | | | | | | | 7 |
| *ATM* | 2 | 2 | | | | | | | | | 4 |
| *POS* | 2 | 1 | | | | | 2 | 1 | | | 6 |
| *Internet Banking* | 3 | 2 | 2 | | | | | | | | 7 |
| *Phone Banking* | 1 | | | | | | | | | | 1 |
| *Mobile Banking /SMS Banking* | 1 | 1 | 1 | 1 | 1 | 2 | 2 | | | 1 | 10 |
| *Prepaid Card* | | | | 1 | | | | | | | 1 |
| *POS Virtual (e-Commerce)* | | | | | | 2 | | | | | 2 |
| *PayBox* | | | | | | | | 1 | | | 1 |

**Burimi: Banka e Shqipërisë**

Siç edhe vihet re në tabelën 2.2, ka pasur një rritje të konsiderueshme të kanaleve alternative të shpërndarjes, në sistemin bankar shqiptar.

## *2.2 Siguria në shërbimin e* internet banking

Përhapja e teknologjive të informacionit dhe komunikimit në vitet e fundit është karakterizuar, përveç të tjerave, nga fenomeni i sulmeve apo shkeljeve informatike. "Sulmet" informatike janë aktivitete të zhvilluara nga palë të treta, të cilët shfrytëzojnë gabime të mundshme, të bëra gjatë fazës së analizës të instrumenteve në fjalë, duke bërë të mundur qasjen te informacioni i ruajtur në kompjuterët tanë, pa dijeninë tonë. Nëse deri para pak vitesh, objektivi kryesor i sulmeve informatike, ishin serverët e organizatave të mëdha dhe informacionet e ruajtura në to, vëmendja e tyre tashmë është përqendruar në aksesimin e kompjuterëve personalë. Arsyet janë disa: sistemet kompjuterike personale janë përgjithësisht më pak të mbrojtur se ato të kompanive, pra më të lehtë për t'u sulmuar me sukses; sistemet e përdoruesve gjithashtu përmbajnë informacione mjaft të dobishme; me zgjerimin e rrjeteve, edhe një kompjuter i vetëm mund të shërbejë si një makinë mjaft e fuqishme për përhapjen e sulmeve.

Sulmet ndaj sistemeve bëhen në forma të ndryshme, por të gjitha kanë një synim të vetëm: vjedhjen e identitetit digjital, që do të thotë, gjithë informacioni i përdorur nga individi për të vërtetuar identitetin e tij në transaksionet e kryera në rrjet; p.sh. kodi identifikues dhe fjalëkalimi i përdorur për të përdorur shërbimin e *internet banking*, të dhënat e kartës së kreditit të përdorura për të kryer blerje *online*, kodin identifikues dhe fjalëkalimin për të përdorur kompjuterët e një kompanie, etj.

Teknikat më të përdorura për vjedhjen e identitetit janë *"phishing* dhe *spyware".*[5]

Teknika e parë e drejton përdoruesin në një web-site, pothuajse identik me atë të përdorur nga përdoruesi, për të kryer disa shërbime (zakonisht flitet për shërbimet *home banking* ose *e-commerce*), duke i kërkuar të kryejë disa veprime ndër të cilat edhe futjen e kodeve të identifikimit, të cilat do të merren dhe do të përdoren ilegalisht.

[5] Deborah Morley, Charles S. Parker "*Understanding Computers*" 14 th, Edition page 371-372

Ndërsa, *spyware* është një program që fshihet brenda një programi tjetër, ose merret nëpërmjet postës elektronike. Kur një përdorues shkarkon këto programe, ose i hap padashje ato, *spyware* aktivizohet automatikisht dhe nga ky moment, është në gjendje të përgjojë çdo veprim që një përdorues mund të kryejë në kompjuterin e tij. Si *spyware* ashtu edhe *phishing,* janë sulme që bazohen mbi një supozim të vetëm: përdoruesit kanë mungesë njohurish informatike, duke e bërë të lehtë mashtrimin e tyre. Vetë suksesi i këtyre sulmeve, tregon se supozimi është i saktë. Sigurisht që informatikanët kanë studiuar kundërmasat e nevojshme për të reduktuar këto sulme, zgjidhje këto që duhet të zbatohen si nga ana e përdoruesve ashtu edhe nga ofruesit e shërbimit të rrjetit.

Masat e zbatueshme nga ana e përdoruesve finalë janë: antivirus, *antispyware* dhe *firewall*-et. Përdorimi i duhur i këtyre instrumenteve bën të mundur: identifikimin në kohë reale të pranisë së viruseve në kompjuter si dhe eliminimin/fshirjen e tyre, identifikimin/kapjen në kohë reale të pranisë së *spyware* në kompjuter, si dhe eliminimin/fshirjen e tyre, si dhe, të identifikojë aktivitete jonormale të kryera në kompjuterë, duke parandaluar forma sulmesh të ndryshme nga viruset dhe spyware-t.

Shërbimet dhe produktet e ofruara nga bankat, veçanërisht ato të ofruara nëpërmjet internetit, duhet të sigurojnë një nivel të lartë të konfidencialitetit, jo vetëm në bankat individuale, por në të gjithë sistemin bankar. Komponentët çelës që ndihmojnë në sigurimin e një niveli konfidencialiteti në një rrjet të hapur përfshijnë[6]:

- siguri,
- autentifikim,
- kontoll aksesi,
- konfidencialitet së të dhënave,
- integritet së të dhënave,
- humbje e reputacionit.

*Siguria:* siguria në internet *Banking* përfshin sigurinë e kompjuterit dhe atë të komunikimit. Qëllimi i sigurisë së kompjuterit është të mbrojë pajisjet kompjuterike nga abuzimi dhe përdorimi i paautorizuar, si dhe të mbrojë të dhënat nga dëmtimet aksidentale dhe ato të qëllimshme.

*Autentifikimi*: është procesi i verifikimit të identitetit të një përdoruesi individual, kompjuteri, komponenti software-ik ose çdo entiteti tjetër. Për shembull, adresa ip identifikon një kompjuter në internet, ashtu si një numër identifikon telefonin. Duhet të sigurohemi që një përdorues i paautorizuar të mos futet në sistem, ose të verifikojmë burimin nga ku merren të dhënat.

*Kontrolli i aksesit*: është një mekanizëm që mundëson kontrollin e aksesueshmërisë në një sistem, si dhe në lehtësirat e tij, nga një përdorues deri në nivelin e nevojshëm për të realizuar punën e tij. Ai siguron një mbrojtje të burimeve të sistemit nga hyrjet e paautorizuara. Në këtë mënyrë, tentativat për hyrje të paautorizuar, mund të iniciohen nga kudo. Hyrja e paautorizuar shkakton shkatërrim, modifikim, vjedhje së të dhënave ose fondeve, kompromet im të konfidencialitetit së të dhënave, etj.

*Konfidencialiteti i të dhënave*: është koncepti i mbrojtjes së të dhënave nga përhapjet e paautorizuara. Për shkak të natyrës së hapur të internetit, të gjithë të dhënat e transmetuara mund të monitorohen ose të lexohen nga të tjerë. Fjalëkalimet dhe metoda të tjera të kontrollit të hyrjes ndihmojnë në konfidencialitetin e të dhënave.

*Integriteti i të dhënave*: siguron që informacioni të mos modifikohet në mënyrë të

[6] Alotaibi, Wald & Argles, 2010 Sun et. al., 2014; Tan, Ko & Holmes, 2013 "*Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications edited by Management Association, Information*" page 389-390

papritur. Humbjet nga integriteti i të dhënave mund të vijnë nga gabimet njerëzore, ngacmime të qëllimshme, madje dhe nga ngjarje katastrofike. Dështimi nga mbrojtja e saktësisë së të dhënave, mund t'i bëjë të dhënat e padobishme, ose më keq, të rrezikshme. Prandaj, duhet të bëhen përpjekje, për të siguruar të dhëna të sakta dhe të përpikta gjatë gjithë kohës. Kontrolli i aksesit, enkriptimi dhe nënshkrimi digjital, janë metodat për të siguruar integritet së të dhënave.

*Humbja e reputacionit*: humbja e reputacionit, nënkupton krijimin e provave të mjaftueshme të origjinës, apo krijimit së të dhënave, me qëllim mbrojtjen e dërguesit kundrejt provave false të marrësit, mbi marrjen e të dhënave. Për të siguruar imponueshmërinë e një transaksioni, duhen të merren masa për të parandaluar palët nga diskutimet mbi vlefshmërinë, refuzimin e të vërtetës, pranueshmërinë e komunikimit apo transaksioneve.

## 3. Konkluzione

Duke ju referuar raportimeve të Bankës së Shqipërisë lidhur me shërbimin bankave të nivelit të dytë, mbi përdorimin e *internet banking* në Shqipëri, tregohet një tendencë në rritje. Vëmë re, se gjatë dekadës së fundit, është shtuar shumë vetëshërbimi bankar si *mobil E-Banking* (me 10 produkte elektronike). Të gjithë bankat kanë ATM-të e tyre (përjashtuar Bankës së Bashkuar të Shqipërisë) dhe pjesa më e madhe, ofron produkte të *E-Banking* apo *mobil E-Banking*.

Një konkluzion i rëndësishëm lidhet me raportin e mosnjohjes së shërbimit dhe aspekte të sigurisë, që do të thotë që, nëse do të kemi një njohje sa më të plotë të *E-Banking* për klientët e bankave si dhe nivele sigurie të larta, tendenca do të jetë gjithmonë e në rritje.

Vihet re nga studime dhe raporte që përdorimi sa më i ulët i shërbimeve *E-Banking*, lidhet me mungesën e besimit të përdorimit të transaksioneve *online*.

Konkluzion i rëndësishëm, është se: investimi i bankave tregtare në kërkim dhe teknologji rrit ndjeshëm edhe përdorimin dhe sigurinë, në përdorimin e shërbimeve *online*, dhe për më tepër, *E-Banking*.

*E-Banking* është burim i rëndësishëm i lidhjes së klientit me bankën, e cila na çon në minimizimin e kostove operative dhe rritjen e eficencës së përdorimit të këtyre shërbimeve dhe rritjen e kënaqësisë së klientëve. *E-Banking* ju siguron konsumatorëve një shpejtësi të lartë veprimesh, kosto më të ulëta dhe kursim kohe.

Duke ju referuar disa këshillave të publikuara nga Banka Qendrore e Shqipërisë, "Bankat në epokën e internetit"(2009), - të cilat janë përmendur edhe tek punimi ynë, - si disa prej masave që mund të marrë klienti, dhe nga ana tjetër kur bankat që ofrojnë *E-Banking* përdorin sisteme të përparuara sigurie, rezulton se, që të dyja palët ndjehen me të sigurta nga kriminaliteti elektronik. Në këtë studim, ne kemi bërë hulumtime të disa autorëve të huaj, por mbështetur në studime dhe raporte në vendin tonë, vihet re një rritje dhe optimizëm për të ardhmen e shqiptarëve në përdorimin e *E-Banking* vitet e fundit.

Gjatë vitit 2017, një peshë të madhe të këtyre investimeve e kanë zënë investimet për sigurinë kibernetike, e cila është edhe tendenca ndërkombëtare e teknologjisë së informacionit. Në këtë kuadër, gjatë vitit 2017 ka filluar projekti i *swift*-it ("client security program"), i cili synon rritjen e sigurisë së informacionit (pagesave).

## 4. Sugjerime për kërkime të mëtejshme

Nga rishikimi i literaturës vëmë re se janë të pakta kërkimet shkencore vendase në këtë fushë. Pjesa më e madhe janë studime, apo raporte, të Bankës së Shqipërisë dhe institucioneve financiare. Kështu, sugjerojmë që t'i kushtohet më shumë rëndësi nga ana e akademikëve, rolit që ka siguria bankare për financat dhe ekonominë e vendit.

Gjithashtu, është e rëndësishme të shohim edhe anën tjetër, atë të përdoruesve të shërbimit bankar. Megjithëse ka kërkesë të lartë që të rritet siguria nga ana e ofruesve, shpesh është mungesa e njohurive dhe kulturës së klientit në fushën e shërbimeve bankare ajo që cenon sigurinë. Prandaj është e rëndësishme të studiohet nëse shoqëria shqiptare është në gjendje të përdorë gjithë këtë mori produktesh elektronike.

## Bibliografi


1. Alotaibi, Wald & Argles, 2010 Sun et. al., 2014; Tan, Ko & Holmes, 2013 "*Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications edited by Management Association, Information*" page 389-390
2. Berger, A. N., DeYoung, R. (1997). "*Problem Loans and Cost Effi ciency in Commercial Banks*." Journal of *Banking* and Finance, Vol. 21, pp. 849-870.
3. By Deborah Morley, Charles S. Parker "*Understanding Computers*" 14 th, Edition 371-372
4. Chakravorti, S. and W. R. Emmons (2003), "*Who Pays for Credit Cards*?" Journal of Consumer Affairs, forthcoming.
5. Hasan, I., Schmiedel, H., and Song, L., 2012, "Retail Payment and Bank Performance," Journal of Financial Services and Research, 41 (3): 163-195.
6. Hayashi, F., Klee, E., 2003. "*Technology adoption and consumer payments: evidence from survey data*". Review of Network Economics 2 (2), 175–190.
7. HERZBERG A., Payments and *Banking* with mobile personal devices, in "*Communications of the ACM*", n. 46/03, pagg. 54
8. Hsee, C. K., Yu, F., Zhang, J., & Zhang, Y. (2003). "*Medium Maximization*". Journal of Consumer Research, 30(1), 1-14.
9. http://www.bankofalbania.org
10. Hyoung shick Kim, Jun Ho Huh, Ross Anderson, On the Security of Internet *Banking* in South Korea, Oxford University Computing Laboratory, CS-RR10-01, 2010. 3.
11. Internet *Banking*: Comptroller's Handbook,1999.
12. Kennickell, Arthur B. and Myron L. Kwast. 1997. "*Who Uses Electronic Banking? Results From the 1995 Survey of Consumer Finances*." Proceedings from the 33rd Annual Conference on Bank Structure and Competition, Federal Reserve Bank of Chicago, pp. 56–75.
13. Mantel, Brian. 2000. "*Why Do Consumers Pay Bills Electronically? An Empirical Analysis.*" Federal Reserve Bank of Chicago Economic Perspectives, Fourth Quarter, pp. 32–47.
14. Publikim nga Banka e Shqipwrisë "*Bankat në epokën e internetit*" 2009
15. Raporti vjetor i Bankes se Shqiperise, 2017
16. Rochet, Jean-Charles, and Jean Tirole (2002). "*Cooperation among Competitors: The Economics of Payment Card Associations.*" Rand Journal of Economics, 33(4), pp. 1–22.
17. Statistikat e publikuara nga Banka e Shqiperise, 2017.

# Krimi kibernetik – vështrim krahasues i legjislacionit

■**MSc. Besnik SHEHAJ**
*Akademia e Sigurisë*
*besnik.shehaj@asp.gov.al*

**Abstrakt**

*Zhvillimet e Teknologjisë së Informacionit (TI) dhe aplikimet gjithnjë e më të shumta të saj në jetën e përditshme, kanë përmirësuar në mënyrë të paimagjinueshme cilësinë e jetës së qenieve njerëzore, siç e kanë bërë atë, edhe më të cenueshme nga ndërhyrjet e palejuara të personave të tretë, në informacionin vetjak të përdorur nëpërmjet TI. Kjo veprimtari e paautorizuar e personave të tretë ka krijuar një fushë të re të aktivitetit kriminal të personave apo grupeve, me shtrirje dhe rrezikshmëri, më të madhe se çdo aktivitet tjetër i krimit konvencional. Ky fakt, është evident kur shikon volumin e krimeve të kësaj kategorie, në raport me kriminalitetin në tërësi, apo dhe për nga pasojat e dëmit të shkaktuar, në vlerë financiare. Të dhënat mund të jenë akoma më të frikshme, po të marrim në konsideratë edhe pjesën e errët të këtij lloj kriminaliteti. Veçoritë e përhapjes së shpejtë, me shtrirje dhe rrezikshmëri të madhe, e bëjnë krimin kibernetik një target të detyrueshëm për shumë agjenci ligjzbatuese, publike e private, që duhet t'i kundërvihen nëpërmjet strukturave të specializuara, të cilat, duhet të jenë të kompletuara me personel të aftë profesionalisht, dhe me njohuri të veçanta në fushën e TI, e me pajisje dhe teknologji të nivelit të lartë, të mirëfinancuara dhe të mirëorganizuara, por mbi të gjitha, të mbështetura me legjislacionin e nevojshëm, strategji dhe plane veprimi specifike. Pikërisht, në këto instrumente të fundit, të luftës ndaj krimit kibernetik, është përqendruar ky punim, duke synuar që nëpërmjet analizës krahasuese midis legjislacionit ndërkombëtar dhe atij vendas, të konkludojmë: nëse është, ky i fundit, në përputhje me Acquis Communautaire; nëse është i plotë, për të luftuar të gjitha format e shfaqjes së krimit kibernetik; nëse duhet t'i paraprijmë, me masa penale shtesë disa formave të shfaqjes së këtij lloj krimi në botë, por ende jo të pranishme në vendin tonë, etj.*

**Fjalëkyçe:**

**hapësirë kibernetike, siguri kibernetike, kërcënim kibernetik, krim kibernetik, krim konvencional, lufta kibernetike, terrorizëm kibernetik, zhvatje kibernetike.**

## 1. Hyrje

Zhvillimet e Teknologjisë së Informacionit (TI), dhe aplikimet gjithnjë e më shumë të saja në jetën e përditshme, kanë përmirësuar në mënyrë të paimagjinueshme cilësinë e jetës së qenieve njerëzore, duke krijuar lehtësi, shpejtësi, komoditet, ndërveprim, eficensë dhe efektivitet, në të gjitha sferat e veprimtarisë njerëzore, por nga ana tjetër, masivizimi i kësaj teknologjie, e ka bërë më të ndjeshëm informacionin vetjak të përdoruesve të TI, nga ndërhyrjet e palejuara të personave të tretë, për qëllime të ndryshme. Kjo veprimtari e paautorizuar e personave të tretë, ka krijuar një fushë të re të aktivitetit kriminal, nga individë apo grupe, me shtrirje dhe rrezikshmëri më të madhe se çdo aktivitet tjetër i *krimit konvencional*. Ky fakt, është evident kur shikon volumin e krimeve të kësaj kategorie, në raport me kriminalitetin në tërësi, apo dhe për nga pasojat e dëmit të shkaktuar në vlerë financiare.

Në një publikim, në faqen zyrtare të agjencisë prestigjioze "Reuters", që i referohet një raporti të Qendrës për Studime Strategjike dhe Ndërkombëtare, thuhet: *"Krimi kibernetik i kushton ekonomisë globale rreth 445 miliardë dollarë çdo vit me dëmtimin e biznesit nga vjedhja e pronës intelektuale, duke tejkaluar humbjen prej 160 miliardë $ për individët nga hakimet... Rreth 40 milionë njerëz në Shtetet e Bashkuara, ose afër 15 për qind e popullsisë, kanë pësuar vjedhje të informacioneve personale nga hakerat, [...] ndërsa nga ndërhyrjet u prekën 54 milionë njerëz në Turqi, 16 milionë në Gjermani dhe më shumë se 20 milionë në Kinë"*[1].

Këto të dhëna, që mund të jenë edhe më të frikshme, duke marrë në konsideratë pjesën e errët të këtij lloj kriminaliteti, e bëjnë *krimin kibernetik,* një target të detyrueshëm

[1] Center for Strategic and International Studies (Reuters 2014)

për shumë agjenci ligjzbatuese, publike e private, që duhet t'i kundërvihen me anë të strukturave të specializuara, të mirëfinancuara dhe të mirëorganizuara, të cilat, duhet të jenë të kompletuara me personel të aftë profesionalisht, dhe me njohuri të veçanta në fushën e TI, të pajisur me teknologji të sofistikuar, por mbi të gjitha, të jenë të mbështetura me legjislacionin e përshtatshëm, strategji dhe plane veprimi specifike.

Në këto veçori të fundit, të luftës ndaj *krimit kibernetik,* është përqendruar ky studim, duke pretenduar të realizojë një vështrim krahasues midis legjislacionit ndërkombëtar dhe atij vendas, me synimin për të dëshmuar, nëse, ky i fundit, është në përputhje me *Acquis Communautaire;* nëse është i plotë, për të luftuar të gjitha format e shfaqjes së *krimit kibernetik*; nëse duhet t'i paraprimë, me masa penale shtesë, disa formave të reja të shfaqjes së këtij lloj krimi në botë, por ende jo të pranishme në vendin tonë, etj.

Metodologjia e përdorur, është ajo e analizës krahasuese midis përmbajtjes së akteve ndërkombëtare për *krimin kibernetik*, kryesisht të BE-së, dhe atyre analoge Shqiptare, si dhe, nëpërmjet interpretimit teorik të tyre me parimet e së drejtës.

## 2. Strategjitë e sigurisë kibernetike

Është me interes të theksohet që në fillim, se, ka një përputhje evidente, midis Strategjisë të Sigurisë Kibernetike të BE-së dhe asaj shqiptare, ku kjo e fundit, duket se i është përmbajtur nocioneve, parimeve, standardeve, metodologjisë dhe rekomandimeve të së parës.

### *2.1. Strategjia e Sigurisë Kibernetike e BE-së*

Kjo strategji është e bazuar në trinitetin: "hapësirë kibernetike *e hapur, e mbrojtur dhe e sigurt" (An Open, Safe and Secure Cyberspace),*[2] që në pamje të parë, të krijon përshtypjen e një kontradikte termash (p.sh. si mund të jetë diçka, e hapur dhe e sigurt?!). Por, pikërisht këtë kundërshti, e neutralizon nocioni *"e mbrojtur"*, që nënkupton se *hapësira kibernetike* ndërkombëtare, duhet, dhe është e mbrojtur, nga jashtë e nga brenda, për të neutralizuar ndërhyrjet e paautorizuara. Pra, jo gjithkush mund të hyjë, ose të lundrojë në këtë hapësirë, pa respektuar disa *protokolle* strikte, të cilat, tentojnë t'i thyejnë persona të paautorizuar, për qëllime të ndryshme.

Gjithashtu, Strategjia e Sigurisë Kibernetike e BE-së, ka për qëllim të standardizojë dhe të unifikojë kundërveprimin e shteteve anëtare, apo dhe më gjerë, ndaj ndërhyrjeve të paautorizuara në rrjetet kibernetike. Kjo, për shkak të veçorisë së *krimit kibernetik,* si krim, që ka shtrirje ndërkombëtare, gjë që e bënë të domosdoshëm bashkëpunimin e bashkëveprimin e shteteve, në luftën ndaj tij, duke eliminuar pengesat që sjellin legjislacionet e veçanta të shteteve, apo mekanizma të tjerë institucionalë.

Parimet në të cilat është e bazuar kjo strategji, janë:

- vlerat thelbësore të BE-së, zbatohen në hapësirën digjitale, njësoj si në botën fizike;[3]
- mbrojtja e të drejtave themelore: liria e shprehjes, të dhënat personale dhe privatësia;[4]
- qasje (*Access*) për të gjithë;[5]
- qeverisje demokratike dhe efikase, me shumë palë të interesuara;[6]

[1] Cybersecurity Strategy of the European Union, faqe1 (EUROPEAN COMMISSION 2013).
[2] Po aty, faqe 3.
[3] Po aty, faqe 4.
[4] Po aty, faqe 4.
[5] Po aty.

- përgjegjësi e përbashkët, për të garantuar sigurinë[7].

Ndërsa 5 prioritetet[8] e kësaj strategjie, janë:

- rikthimi në efiçencë i hapësirës kibernetike, pas çdo ndërhyrje të paautorizuar;
- reduktimi sa më drastik i krimit kibernetik;
- zhvillimi i politikës dhe aftësive të mbrojtjes kibernetike në lidhje me Sigurinë e Përbashkët dhe Politikën e Mbrojtjes (SPPM);
- zhvillimi i burimeve industriale dhe teknologjike për sigurinë kibernetike;
- të krijojë një politikë koherente, ndërkombëtare, për hapësirën kibernetike në Bashkimin Evropian, dhe të promovojë vlerat kryesore të BE-së.

### *2.2. "Dokumenti i politikave për sigurinë kibernetike 2015-2017"*

Ky dokument, i miratuar me Vendimin e Këshillit të Ministrave nr. 973, datë 02.12.2015, përbën instrumentin më të rëndësishëm shtetëror në vendin tonë, sa i përket politikave dhe masave për sigurinë kibernetike, i cili, në përgjithësi, është "...në linjë me Strategjinë për Sigurinë Kibernetike të Bashkimit Evropian: *Hapësirë kibernetike e hapur, e sigurt dhe e mbrojtur...",* [9] përmendur në seksionin 1.1. të këtij studimi.

Në funksion të qëllimit të këtij studimi, Dokumenti i Politikave për Sigurinë Kibernetike (DPSK) 2015 – 2017, përmban:

- përkufizimin e termave të hapësirës dhe sigurisë kibernetike;[10]
- analizën e situatës së hapësirës kibernetike në Shqipëri;[11]
- kuadrin ligjor dhe institucionet përgjegjëse;[12]
- vizionin, parimet dhe objektivat strategjikë;[13]
- politikat për t'u ndjekur[14].

Nga krahasimi i bërë ndërmjet këtyre elementëve të DPSK, me ato të Strategjisë për Sigurinë Kibernetike të Bashkimit Evropian, rezulton se ato janë në përputhje të plotë. Kështu, ka kuptim të njëjtë: për termat e sigurisë kibernetike, për hapësirën kibernetike "të hapur, të mbrojtur dhe të sigurt", për rreziqet që ajo përmban; për parimet dhe objektivat strategjikë; për respektimin e lirive themelore të individit, dhe mbrojtjen e privatësisë nga ndërhyrjet e paautorizuara; për bazën ligjore që duhet përshtatur në lidhje me mbrojtjen e hapësirës kibernetike, dhe krijimin e institucioneve përgjegjëse; për përgjegjësinë e përbashkët të institucioneve shtetërore, dhe sipërmarrjeve private për sigurinë e hapësirës kibernetike, për bashkëpunimin ndërkombëtar, etj.

Vlen të përmendet fakti, se, e njëjta gjë, mund të thuhet edhe për dokumentin analog të Republikës së Kosovës, të quajtur: Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit 2016-2019[15]. "*Kjo strategji është në përputhje me aktet ndërkombëtare që rregullojnë fushën e sigurisë kibernetike, Strategjinë e Sigurisë Kibernetike të Bashkimit Evropian "Hapësirë e hapur, e sigurt dhe e mbrojtur kibernetike (2013)"; Udhëzuesin e ENISA për Strategjitë Shtetërore të Sigurisë Kibernetike (2012);*

[6] Po aty
[7] Po aty, faqe 4-5
[8] Dokumenti i Politikave për Sigurinë Kibernetike 2015 – 2017, faqe 10. (QBZ 2015)
[9] Po aty, faqe 7-8
[10] Po aty, faqe 11-15
[11] Po aty faqe 16-18
[12] Po aty faqe 19-21
[13] Po aty faqe 21-27
[14] Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit 2016 – 2019. (Republika e Kosovës 2015)
[15] Po aty, faqe 18

*Strategjitë e Sigurisë Kibernetike të vendeve të tjera të BE-së.*"[16], - shprehen autorët e saj. Është gjithashtu me interes të theksohet, se, në përkufizimin që jepet në këtë strategji për termin "Mbrojtje kibernetike", thuhet: *". . . përbëhet nga këto detyra: mbrojtje, zbulim, reagim dhe rikuperim",*[17] elemente këto, të cilat shprehin në mënyrë të sintetizuar thelbin e kuptimit dhe të realizmit të *sigurisë kibernetike.*

Miratimi i *Dokumentit të Politikave për Sigurinë Kibernetike* nga ana e qeverisë shqiptare, dhe masat ligjore e institucionale të marra në përputhje me rekomandimet e saj, përbëjnë një hap të rëndësishëm për sigurinë shtetërore kibernetike, në kushtet kur përhapja e internetit në vendin tonë, në fazën e përgatitjes së kësaj strategjie, rezultonte me një rritje shumë të shpejtë, nga 0.97 % për vitin 2003 në 60.10 % për vitin 2013[18] (Tabela nr. 1); ndërsa më 31 dhjetor 2017, Shqipëria rezulton me 1 932 024 përdorues të internetit, ose 65.8 % të popullsisë[19].

**Tabela 1**

| VITI | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SHQIPËRIA | 0.97 | 2.42 | 6.04 | 9.61 | 15.04 | 23.86 | 41.20 | 45.00 | 49.00 | 54.66 | 60.10 |

## 3. Krahasimi i ligjit shqiptar me atë ndërkombëtar

Për të realizuar këtë synim të studimit tonë, na duhet fillimisht të bëjmë një përshkrim në terma të përgjithshëm, për aq sa na lejon hapësira e kësaj kumtese, të ligjit ndërkombëtar për sigurinë kibernetike, veçanërisht në fushën penale, me atë shqiptar në këtë fushë.

### *3.1. Ligji ndërkombëtar për sigurinë kibernetike*

Akti themeltar ndërkombëtar, për luftën ndaj krimit kibernetik, mund të konsiderohet Konventa e Këshillit të Evropës mbi Krimin Kibernetik (Convention on Cybercrime)[20], ose e ashtuquajtura, Konventa e Budapestit, e shpallur më 23 nëntor 2001, e cila është ratifikuar deri tani nga 59 shtetet anëtare dhe jo anëtare[21]. Shqipëria është nga të parat shtete që ka ratifikuar këtë konventë, me ligjin nr. 8888, dt. 25.4.2002, "Për miratimin e 'Konventës për krimin në fushën e kibernetikës'".

Dalja e kësaj konvente, u konsiderua si shumë e nevojshme, kur në shumë shtete anëtare dhe jo anëtare të KE-së, nuk kishte një legjislacion të përshtatshëm për dënimin e krimit kibernetik. Sipas parimit të gjithëpranuar ndërkombëtarisht, *"Nullum crimen nulla poena sine lege certa"*,[22] këto krime nuk mund të dënoheshin penalisht, pavarësisht se ato ishin përhapur shumë, dhe ishin shpesh me rrezikshmëri të lartë.

Prandaj, konventa e ka të shprehur qartë në preambulë, qëllimin e saj: "Të ndërgjegjshëm për ndryshimet e thella të sjella nga digjitalizimi, konvergjenca dhe globalizimi i vazhdueshëm i rrjeteve kompjuterike. . . Të shqetësuar nga rreziku, që

[16] Po aty, faqe 18.
[17] Po aty, faqe 8.
[18] Po aty, faqe 12.
[19] Internet World Stats (Internet World Stats 2018).
[20] Convention on Cybercrime, ETS No. 185 (Council of Europe 2001).
[21] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=EZZMOGkz (Counsil of Europe 2018).
[22] Klip, André. *Substantive Criminal Law of the European Union*. Maklu (2011), faqe 69. (Klip 2011).

rrjetet kompjuterike dhe informacioni kompjuterik, mund të përdoren gjithashtu për kryerjen e veprave penale. . . Të bindur. . . për të frenuar veprimet e drejtuara kundër konfidencialitetit, integritetit dhe disponueshmërisë së sistemeve kompjuterike, rrjeteve dhe të dhënave kompjuterike, sikurse dhe keqpërdorimit të këtyre sistemeve, rrjeteve dhe të dhënave, nëpërmjet sigurimit që kjo veprimtari e tillë të kriminalizohet. . . dhe nëpërmjet krijimit të forcave të mjaftueshme për luftimin efektiv të këtyre veprave kriminale, duke lehtësuar zbulimin, hetimin dhe ndjekjen penale të këtyre veprave penale, në të dyja nivelet kombëtare dhe ndërkombëtare, dhe duke siguruar marrëveshjet për bashkëpunim ndërkombëtar të shpejtë e të besueshëm. . . " [23]

Përveç preambulës, konventa është e ndarë në 4 kapituj kryesorë, me titujt respektivë: *përdorimi i termave; masat që duhet të merren në nivel kombëtar; bashkëpunimi ndërkombëtar; dispozita përfundimtare*.

Në interes të studimit tonë, vlen të përshkruhen disa nga rekomandimet më të rëndësishme, të përfshira në kapitullin e dytë: *"Masat që duhet të merren në nivel kombëtar*",[24] i cili në vetvete është i ndarë në 3 seksione, 10 tituj dhe 20 nene, që përmbajnë *masa* të detyrueshme që duhet të ndërmerren nga shtete anëtare dhe jo vetëm, për përcaktimin në legjislacionin e brendshëm, si vepra penale të disa formave tipike të krimit kibernetik, dhe caktimin e masave të përshtatshme procedurale në ndjekjen, hetimin dhe gjykimin e tyre.

Konkretisht, duhet të konsiderohen si vepra penale, veprimet e qëllimshme dhe të padrejta në sistemet kompjuterike, si:

- hyrjet e paligjshme (neni 2);
- interceptimi i paligjshëm (neni 3);
- interferenca e të dhënave (neni 4);
- interferenca e sistemeve (neni 5);
- keqpërdorimi i pajisjeve (neni 6);
- falsifikimet e lidhura me kompjuterët (neni 7);
- mashtrimet e lidhura me kompjuterët (neni 8);
- veprat penale të lidhura me pornografinë e fëmijëve (neni 9);
- veprat penale të lidhura me dhunimin e të drejtës së autorit dhe së të drejtave të tjera të lidhura me të (neni 10)[25].

Me hyrjen në fuqi edhe të "*Protokollit shtesë të Konventës për Krimin Kibernetik*", për penalizimin e akteve me natyrë raciste dhe ksenofobe, të kryera nëpërmjet sistemeve kompjuterike",[26] u përfshinë në detyrimin për t'u cilësuar nga shtetet anëtare, si vepra penale në fushën e sigurisë kibernetike, edhe:

- shpërndarja e materialeve raciste dhe ksenofobe në sistemet kompjuterike (neni 3);
- kërcënimi me motive racizmi dhe ksenofobie (neni 4);
- fyerja me motive racizmi dhe ksenofobie (neni 5);
- mohimi, minimizimi i konsiderueshëm, aprovimi ose justifikimi i gjenocidit ose krimeve kundër njerëzimit (neni 6)[27].

Duke marrë në konsideratë natyrën e veçantë të krimit kibernetik, në konventën e

[23] Ligjin nr. 8888, dt 25.04.2002, "*Për miratimin e "Konventës për krimin në fushën e kibernetikës*", faqe 2-3. (QBZ 2002).
[24] Po aty, faqe 4.
[25] Po aty, faqe 5-7.
[26] Ratifikuar në vendin tonë me Ligjin nr. 9262, datë 29.07.2004. (QBZ 2004).
[27] Ligji nr. 9262, datë 29.07.2004, "Për ratifikimin e "Protokollit shtesë të Konventës për Krimin Kibernetik, për penalizimin e akteve me natyrë raciste dhe ksenofobe të kryera nëpërmjet sistemeve kompjuterike"", faqe 2-3.

BE-së, janë përcaktuar edhe *masat* që duhet të ndërmarrin shtetet, në legjislacionin e tyre të brendshëm procedural penal, që janë të lidhura po ashtu me veçoritë e ndjekjes penale, hetimit dhe gjykimit në fazën e gjetjes, fiksimit dhe marrjes së provave për dokumentimin e kësaj veprimtarie kriminale. Disa nga këto masa janë:

- ruajtja e përshpejtuar e të dhënave kompjuterike të memorizuara (neni 16);
- ruajtja e përshpejtuar dhe hapja e pjesshme e të dhënave të trafikut (neni 17);
- porosia e prodhimit (neni 18);
- kërkimi dhe ngrirja e të dhënave kompjuterike të memorizuara Neni 19);
- mbledhja e të dhënave kompjuterike në kohën reale (neni 20);
- interceptimi i të dhënave të përmbajtjes (neni 21)[28].

Nga studimi i ligjit nr. 8888, dt. 25.4.2002, "Për miratimin e 'Konventës për krimin në fushën e kibernetikës'", konstatohen në pamje të parë këto pasaktësi, që ndofta i duhen nënshtruar një analize më të hollësishme, por që nuk na mundësohet në këtë kumtesë, për shkak të objektit të ndryshëm të saj:

- Ndonëse në titull të këtij ligji thuhet "Për ratifikimin e Konventës për krimin në fushën e kibernetikës", në titullin e variantit të konventës të përkthyer në shqip, që i bashkëlidhet këtij ligji, shkruhet: "Projektkonventë për krimin kibernetik".[29] Duke ju referuar aktit origjinal të koventës, rezulton se ajo titullohet "*Konventa mbi krimin kibernetik*"[30]. Kjo lajthitje e natyrës teknike nuk do të ishte e rëndësishme për t'u evidentuar, në rast se nuk do të pasohej edhe nga disa pasaktësi të tjera.

- Në përkthim duket se nuk është përdorur teksti origjinal i konventës, pasi në variantin e përkthyer nuk pasqyrohet koha dhe vendi i shpalljes së saj,[31] siç është e shprehur në origjinal: "në Budapest, më 23 nëntor 2001",[32] prandaj njihet edhe ndryshe, si Konventa e Budapestit.

- Përkthimi i dokumentit të konventës, duket se është bërë në mënyrën fjalë për fjalë, dhe jo i shqipëruar në pajtim me termat dhe teknikat legjislative, të legjislacionit shqiptar.

### *3.2. Ligji shqiptar për sigurinë kibernetike*

Legjislacioni shqiptar për sigurinë kibernetike, i përmbahet përgjithësisht atij ndërkombëtar, ku në fushën e së drejtës penale, ai është në përputhje me adoptimet e kërkuara në Konventën e KE-së për krimin kibernetik dhe protokollin shtesë të saj.

Ndërhyrjet në legjislacionin penal shqiptar, për të përshirë si vepra penale krimet kibernetike, sipas Konventës së KE-së dhe Protokollit shtesë të saj, janë bërë nëpërmjet dy ligjeve të veçanta si: Ligji nr. 9859, datë 21.1.2008,*"Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995, Kodi Penal i Republikës së Shqipërisë"* dhe ligji nr. 10023, datë 27.11.2008, *"Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995, Kodi Penal i Republikës së Shqipërisë",* ndërsa ndryshimet për masa shtesë në Kodin e Procedurës Penale janë bërë nëpërmjet ligjit nr. 10054, datë 29.12.2008, *"Për disa shtesa dhe ndryshime në ligjin nr. 7905, datë 21.3.1995 Kodi i Procedurës Penale i Republikës së Shqipërisë".*

Me ligjin nr. 9859, datë 21.1.2008, në Kodin Penal është shtuar një paragraf tek

[28] Ligjin nr. 8888, dt 25.04.2002, "Për miratimin e "Konventës për krimin në fushën e kibernetikës", faqe 8-12
[29] Po aty, faqe 2.
[30] Convention on Cybercrime, faqe 1.
[31] Ligjin nr. 8888, dt 25.04.2002, "Për miratimin e "Konventës për krimin në fushën e kibernetikës", faqe 22
[32] Convention on Cybercrime, faqe 1 dhe 25.

neni 117, ku dënohet publikimi në internet, ose mënyra të tjera të pornografisë me të mitur[33]. Por shtesat dhe ndryshimet më të rëndësishme në Kodin Penal, në përputhje me adaptimet që duhen bërë sipas Konventës së KE-së dhe Protokollit shtesë të saj, janë bërë me ligjin nr. 10023, dt. 27.11.2008, si:

- në nenin 7 të Kodit Penal, ku parashikohet zbatimi i ligjit për vepra penale të kryera nga shtetasit e huaj, është shtuar shkronja "j" me përmbajtje: "vepra penale në fushën e teknologjisë së informacionit";[34]

- pas nenit 74, shtohet neni 74/a: "Shpërndarja kompjuterike e materialeve pro gjenocidit dhe krimeve kundër njerëzimit";[35]

- pas nenit 84, shtohet neni 84/a: "Kanosja me motive racizmi apo ksenofobie nëpërmjet sistemit kompjuterik";[36]

- pas nenit 119, shtohet neni 119/a dhe 119/b, përkatësisht: "Shpërndarja e materialeve raciste dhe ksenofobie nëpërmjet sistemit kompjuterik" dhe "Fyerja me motive racizmi apo ksenofobie nëpërmjet sistemit kompjuterik";[37]

- pas nenit 143/a, shtohet neni 143/b: "Mashtrimi kompjuterik";[38]

- pas nenit 186, shtohet neni 186/a: "Falsifikimi kompjuterik";[39]

- neni 192/b ndryshohet: "Hyrja e paautorizuar kompjuterike";[40]

- pas nenit 293, shtohen nenet 293/a, 293/b, 293/c dhe 293/ç, përkatësisht: "Përgjimi i paligjshëm i të dhënave kompjuterike", "Ndërhyrja në të dhënat kompjuterike", "Ndërhyrja në sistemet kompjuterike" dhe "Keqpërdorimi i pajisjeve"[41].

Pra, siç shihet që në pamje të parë, adaptimet e bëra në ligjin penal shqiptar i janë përmbajtur si në forma ashtu dhe përmbajtje, rasteve të krimit kibernetik, të përcaktuara nga Konventa e KE-së për krimin kibernetik dhe Protokolli shtesë i saj[42].

E njëjta gjë mund të thuhet edhe sa i përket masave procedurale, të përcaktuara nga konventa si detyrim, për t'u adaptuar në ligjin procedural penal të brendshëm të shteteve palë. Kështu, me ligjin nr. 10054, datë 29.12.2008, "Për disa shtesa dhe ndryshime në ligjin nr. 7905, datë 21.3.1995, Kodi i Procedurës Penale i Republikës së Shqipërisë", janë transplantuar dispozitat procedurale, si:

- pas nenit 191, shtohet neni 119/a: "Detyrimi për paraqitjen e të dhënave kompjuterike";[43]

- pas nenit 208, shtohet neni 208/a: "Sekuestrimi i të dhënave kompjuterike";[44]

- pas nenit 299, shtohen nenet 299/a dhe 299/b, përkatësisht me këto përmbajtje: "Ruajtja e përshpejtuar dhe mirëmbajtja e të dhënave kompjuterike" dhe "Ruajtja e përshpejtuar dhe zbulimi i pjesshëm i të dhënave kompjuterike"[45].

---

[33] Ligji nr. 9859, datë 21.1.2008,*"Për disa shtesa dhe ndryshime në Ligjin nr. 7895, datë 27.1.1995, Kodi Penal i Republikës së Shqipërisë",* neni 1. (QBZ 2008)

[34] Ligji nr. 10023, datë 27.11.2008, *"Për disa shtesa dhe ndryshime në Ligjin nr. 7895, datë 27.1.1995, Kodi Penal i Republikës së Shqipërisë"* neni 1. (QBZ 2008)

[35] Po aty, neni 11.

[36] Po aty, neni 12.

[37] Po aty, neni 13.

[38] Po aty, neni 15.

[39] Po aty, neni 18.

[40] Po aty, neni 19.

[41] Po aty, neni 23.

[42] Shih paragrafët 5 dhe 6 të nëntitullit 2.1. në këtë studim.

[43] Ligjin nr. 10054, datë 29.12.2008, *"Për disa shtesa dhe ndryshime në Ligjin nr. 7905, datë 21.3.1995, Kodi i Procedurës Penale i Republikës së Shqipërisë"*, neni 2. (QBZ 2008).

[44] Po aty, neni 3.

[45] Po aty, neni 4.

## 4. A është i plotë ligji penal shqiptar kundër krimit kibernetik

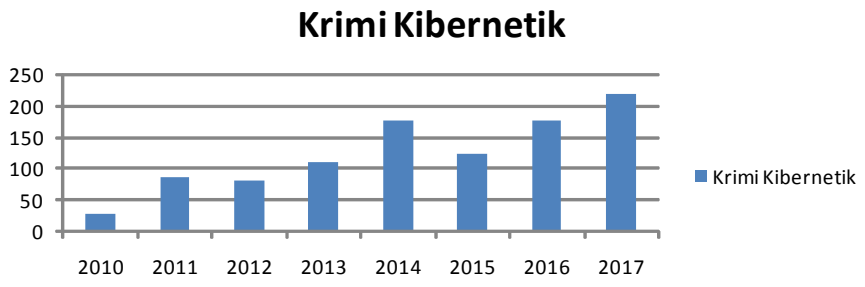
Për të arritur në një konkluzion të saktë, sa i përket ezaurimit të ligjit penal shqiptar, për t'ju kundërvënë në mënyrë të plotë dhe të gjithanshme krimit kibernetik, na duhet të bëjmë shkurtimisht një përshkrim, të dukurive të këtij krimi në vendin tonë dhe kapaciteteve institucionale e logjistike, në përballjen me format e metodat me të cilat ai shfaqet si dhe të mënyrave e mjeteve të përdorura nga autorët.

### *4.1. Situata e krimit kibernetik në Shqipëri*

Ndonëse Shqipëria është ndër të parat vende që ka ratifikuar Konventën e KE-së për krimin kibernetik, në vitin 2002, e kundërta ka ndodhur me situatën ligjore dhe ngritjen e institucioneve përgjegjëse, për të luftuar këtë lloj kriminaliteti. Siç rezulton nga analiza e mësipërme, adaptimet e kërkuara nga konventa për ligjin penal të brendshëm, si në atë material edhe në atë procedural, janë bërë vetëm në vitin 2008. Po kështu ka ndodhur dhe me ngritjen e institucioneve përgjegjëse, siç janë sektori i hetimit të krimit kibernetik, në prokurori, në vitin 2014[46] dhe ai analog, në Policinë e Shtetit, i ngritur më parë; p.sh., regjistrimi i statistikave zyrtare nga Policia për këtë lloj kriminaliteti, rezulton për herë të parë në vitin 2010[47].

Nga shqyrtimi i këtyre statistikave, rezulton se numri i krimeve të ndodhura në fushën e kibernetikës, është gati dhjetëfishuar për periudhën 2010 deri 2017, ku për vitin 2010, rezultojnë 27 raste, ndërsa për vitin 2017, figurojnë 218 të tillë (Figura 1).

**Figura 1**




Për rrjedhojë, vërehet rritje e ndjeshme e volumit të këtyre llojeve krimesh, në krahasim me totalin e krimeve të ndodhura në vendin tonë, që ka ardhur gjithnjë e në rritje, nga 0.2 % në 0.6 % (Figura 2). Kjo, shpjegohet edhe me faktin e rritjes së lartë të penetrimit të internetit në vendin tonë, siç e kemi theksuar më lartë[48].

[46] Po aty, neni 4.
[45] http://www.panorama.com.al/krijohet-sektori-i-hetimit-te-krimit-kibernetik-ne-8-qarqe/ (Gazeta Panorama 2014).
[47] Statistikat e Policisë së Shtetit 2007-2017 (Policia e Shtetit 2018).
[48] Shih Tabela 1 në këtë studim.

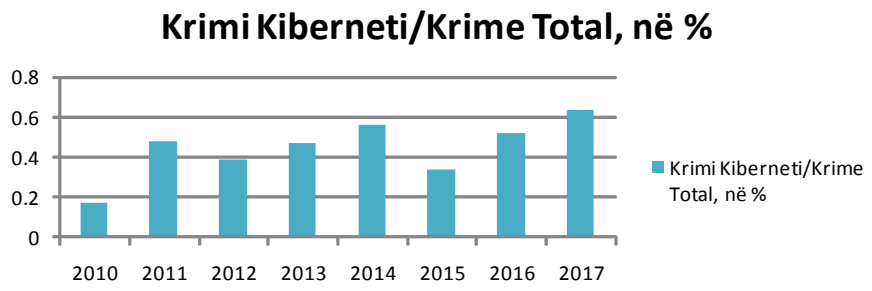



**Figura 2**

### *4.2. A është i plotë ligji penal shqiptar kundër krimit kibernetik*

Nisur nga situata kriminale, aktuale, e krimit kibernetik në vendin tonë, rezulton se ligji penal i adoptuar i është përgjigjur me efektivitet asaj, si në planin e parandalimit të përgjithshëm, ashtu dhe në atë të posaçmin.

Në rast të bërjes së Kodit të ri Penal, siç është diskutuar disa herë publikisht, mendojmë se do të ishte e nevojshme, përfshirja e veprave penale të krimit kibernetik në një ndarje të veçantë (seksion më vete në kreun III, sipas ndarjes në kodin aktual), me argumentet se:

së pari: siç shihet nga përmbajtja e tyre, të gjithë figurat e krimit kibernetik të parashikuara në legjislacionin penal Shqiptar dhe atë ndërkombëtar, kanë si *objekt* të përbashkët, mbrojtjen e marrëdhënieve shoqërore në lidhje me sigurinë kibernetike;

së dyti: nga *ana objektive,* këto figura krimi kanë të përbashkët faktin, se të gjitha kryhen nëpërmjet, ose kundrejt sistemeve kompjuterike;

Së treti: *subjektet* e këtyre figurave të krimit, kanë të përbashkët faktin, se kanë aftësi të veçanta profesionale në fushën e kibernetikës;

Së katërti: nga *ana subjektive,* këto figura krimi gjithmonë kryhen me dashje direkte, ose në raste të veçanta, edhe me dashje indirekte.

## 5. Përfundime

Nga studimi konstatohet se ka një përputhje evidente midis Strategjisë të Sigurisë Kibernetike të BE-së dhe asaj shqiptare, ku kjo e fundit duket se i është përmbajtur nocioneve, parimeve, standardeve, metodologjisë dhe rekomandimeve të së parës. Kjo strategji ka mundësuar kështu, orientimin dhe realizimin e plotë të kuadrit ligjor e institucional, në fushën e sigurisë kibernetike, si në rrafshin administrativ, ashtu dhe në atë penal.

Legjislacioni shqiptar për sigurinë kibernetike, i përmbahet përgjithësisht atij ndërkombëtar, si në frymë ashtu edhe në përmbajtje, ku në fushën e së drejtës penale, është në përputhje me adoptimet e kërkuara në Konventën e KE-së për Krimin Kibernetik dhe Protokollin shtesë të saj.

Adaptimet e bëra në ligjin material penal shqiptar, janë pothuajse identike me rastet e identifikuara në Konventën e KE-së për krimin kibernetik dhe Protokollin shtesë të saj.

E njëjta gjë mund të thuhet edhe sa i përket masave procedurale, të përcaktuara nga

konventa, si detyrim për t'u adaptuar në ligjin procedural penal të brendshëm, të shteteve palë.

Nga studimi i ligjit nr. 8888, dt. 25.04.2002, "Për miratimin e "Konventës për krimin në fushën e kibernetikës", konstatohen disa pasaktësi, që ndofta i duhen nënshtruar një analize më të hollësishme, në një studim të veçantë.

Edhe pse Shqipëria është ndër të parat vende që ka ratifikuar Konventën e KE-së për krimin kibernetik në vitin 2002, e kundërta ka ndodhur me situatën ligjore dhe me ngritjen e institucioneve përgjegjëse, për të luftuar këtë lloj kriminaliteti. Adaptimet e kërkuara nga konventa, për ligjin penal të brendshëm, si në atë material edhe në atë procedural, janë bërë vetëm në vitin 2008.

Numri i krimeve të ndodhura në fushën e kibernetikës është gati dhjetëfishuar për periudhën 2010 deri 2017, si rrjedhojë edhe e rritjes së penetrimit të internetit në vend që ka ecur me ritme impresionuese.

Nisur nga situata kriminale, aktuale, e krimit kibernetik në vendin tonë, rezulton se ligji penal i adoptuar i është përgjigjur me efektivitet asaj, si në planin e parandalimit të përgjithshëm, ashtu dhe në atë të posaçmin.

## 6. Rekomandime

Një studim i veçantë duhet bërë në lidhje me dokumentin e Konventës së KE-së për krimin kibernetik që i është bashkëlidhur ligjit për miratimin e saj, sa i përket përputhshmërisë së këtij dokumenti me origjinalin e Konventës dhe përkthimin e saj.

Në rast të bërjes së Kodit të ri Penal, siç është diskutuar disa herë publikisht, mendojmë se do të ishte e nevojshme përfshirja e veprave penale të krimit kibernetik në një ndarje të veçantë, seksion më vete në kreun III, sipas ndarjes në kodin aktual.

Duke qenë se kemi të bëjmë me institucione të ndjekjes penale dhe hetimit të krimit kibernetik, relativisht të reja, duhet t'i kushtohet vëmendje e veçantë përzgjedhjes dhe trajnimit të personelit të punësuar, si për nga aftësitë e specialitetit në fushën e kibernetikës, por veçanërisht të aftësimit të tyre profesional në drejtim të procedimit penal dhe sigurimit të provave për këto lloje krimesh.

Bashkëpunimi ndërkombëtar në ndjekjen dhe hetimin e këtyre llojeve krimesh është kusht *sine qua non*, pasi është krim që kryhet në largësi, me lehtësi, nga shtetas apo grupe me shtrirje në shtet të ndryshme.

# Bibliografi


1. Begeja, Prof. Dr. Skënder. *Kriminalistika.* Tiranë: SHBLU, 2004.
2. Council of Europe. "Council of Europe-Convention on Cybercrime." *Council of Europe.* November 23, 2001. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (accessed July 20, 2018).
3. *Counsil of Europe.* July 23, 2018. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=EZZMOGkz (accessed July 23, 2018).
4. European Commission. "Cybersecurity Strategy of the European Union." *eeas.europa.eu.* 7 2, 2013. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed June 14, 2018).
5. Gazeta Panorama. *Krijohet sektori i hetimit te krimit kibernetik.* Qershor 11, 2014. http://www.panorama.com.al/krijohet-sektori-i-hetimit-te-krimit-kibernetik-ne-8-qarqe/ (accessed July 25, 2018).
6. Herring, Jonathan. *E drejta penale.* Tiranë: UETPRESS, 2013.
7. IC3 - Internet Crime Complaint Center . *2017 Internet Crime Report.* Annually Official Report, Washington D.C.: IC3, 2018.
8. Internet World Stats. *Europe Internet Usage Stats.* June 2, 2018. https://www.internetworldstats.com/stats4.htm (accessed July 19, 2018).
9. Jean Pradel, Geert Corstens, Gert Vermeulen. *E drejta penale Evropiane.* Tiranë: Papirus, 2010.
10. Këshilli i Ministrave. "Dokument i Politikave per Sigurine Kibernetike 2015-2017." *http://www.akce.gov.al.* December 2, 2015. http://www.akce.gov.al/wp-content/uploads/2016/04/Dokumenti%20i%20Politikave%20per% 20Sigurine%20 Kibernetike% 202015-2017.pdf (accessed June 12, 2018).
11. Klip, André. *Substantive Criminal Law of the European Union.* Antwerpen, Belgium: Maklu, 2011.
12. Kuvendi. "Fletore Zyrtare nr. 10-2008." *www.qbz.gov.al.* February 13, 2008. http://www.qbz.gov.al/botime/fletore_zyrtare/2008/PDF-2008/10-2008.pdf (accessed July 2, 2018).
13. —. "Fletore Zyrtare nr. 190-2008." *www.qbz.gov.al.* Decembre 31, 2008. http://www.qbz.gov.al/botime/fletore_zyrtare/2008/PDF-2008/190-2008.pdf (accessed July 2, 2018).
14. —. "Fletore Zyrtare nr. 205-2008." *www.qbz.gov.al.* Decembre 2008. http://www.qbz.gov.al/botime/fletore_zyrtare/2008/PDF-2008/205-2008.pdf (accessed July 2, 2018).
15. Kuvendi i Republikës së Kosoves. "Ligji nr. 03/l-166, për parandalimin dhe luftimin e krimit kibernetikë". *Gazeta Zyrtare e Republikës së Kosovës, nr. 74, 20 Korrik 2010.*
16. Kuvendi. "Ligji nr. 8888. datë 25.04.2002 Për ratifikimin e "Konventa për krimin në fushën e kibernetikës"." *Fletore Zyrtare nr.18*, 2002: 553 - 575.
17. Mandro, Prof. As. Dr. Arta. *E drejta Romake (Ribotim i tretë).* Tiranë: Aferdita, 2006 .
18. Ministria e Mbrojtjes. "Strategjia për Mbrojtjen Kibernetike." *http://www.mod.gov.al.* November 2014. http://www.mod.gov.al/images/PDF/Strategjia_per_Mbrojtjen_Kibernetike.pdf (accessed June 12, 2018).
19. OSBE. *Reforma Policore në kuadër të reformës së sistemit të drejtësisë penale.* Vjenë: OSBE, 2013.
20. Policia e Shtetit. *Statistikat e Krimeve 2007-2017.* Statistika, Tiranë: PSH, 2018.
21. QBZ. "Fletore Zyrtare nr. 10-2008." *www.qbz.gov.al.* February 13, 2008. http://www.qbz.gov.al/botime/fletore_zyrtare/2008/PDF-2008/10-2008.pdf (accessed July 2, 2018).
22. —. "Fletore Zyrtare nr. 190-2008." *www.qbz.gov.al.* Decembre 31, 2008. http://www.qbz.gov.al/botime/fletore_zyrtare/2008/PDF-2008/190-2008.pdf (accessed July 2, 2018).
23. —. "Fletore Zyrtare nr. 205-2008." *www.qbz.gov.al.* Decembre 2008. http://www.qbz.gov.al/botime/fletore_zyrtare/2008/PDF-2008/205-2008.pdf (accessed July 2, 2018).
24. —. "Fletorja zyrtare 18-2002." *www.qbz.gov.al.* Maj 2002. http://www.qbz.gov.al/botime/fletore_zyrtare/2002/PDF-2002/18-2002.pdf (accessed July 25, 2018).
25. —. "Fletorja zyrtare 56-2004." *www.qbz.gov.al.* Gusht 16, 2004. http://www.qbz.gov.al/doc.jsp?doc=docs/Ligj%20Nr%209262%20Dat%C3%AB%2029-07-2004.htm (accessed July 23, 2018).
26. —. "Fletorja zyrtare nr.212-2015." *www.qbz.gov.al.* Dhjetor 11, 2015. http://www.qbz.gov.al/botime/fletore_zyrtare/2015/PDF-2015/212-2015.pdf (accessed June 12, 2018).
27. Republika e Kosovës. "Strategjia Shtetërore për Sigurinë Kibernetike." *http://www.kryeministri-ks.net.* December 2015. http://www.kryeministri-ks.net/repository/docs/Strategjia_Shteterore_per_Sigurine_Kibernetike_dhe_Plani_i_ Veprimit_2016-2019_per_publikim_1202.pdf (accessed June 13, 2018).
28. —. "Strategjia Shtetërore për Sigurinë Kibernetike." *http://www.kryeministri-ks.net.* Djetor 2015. http://www.kryeministri-ks.net/repository/docs/Strategjia_Shteterore_ per_Sigurine_Kibernetike_dhe_Plani_i_Veprimit_2016-2019_per_publikim_1202.pdf (accessed June 13, 2018).
29. Reuters. "Cyber crime costs global economy costs $ 445 billion a year." *https://www.reuters.com.* June 9, 2014. https://www.reuters.com/article/us-cybersecurity-mcafee-csis/cyber-crime-costs-global-economy-445-billion-a-year-report-idUSKBN0EK0SV20140609 (accessed June 6, 2018).
30. Shegani, Altin. *E drejta penale e krahasuar.* Tiranë: Darmisa, Fier, 2008.
31. top-channel.tv. *Krimi kibernetik, 130 miliardë dollarë u vodhën në 2017.* January 23, 2018. http://top-channel.tv/2018/01/23/krimi-kibernetik-130-miliarde-dollare-u-vodhen-ne-2017/ (accessed June 11, 2018).
32. Universiteti i Tiranës. *E drejta penale - pjesa e posaçme.* Tiranë: Shtëpia Botuese e Librit Universitar, 1989.
33. Vula, Dr. Veton G. *Kriminaliteti kopjuterik.* Prishtinë: Koha, 2010.

# Trajtimi i krimit kibernetik, sipas legjislacionit të Kosovës, dhe roli i policisë, në luftën kundër krimit kibernetik

■**MSc. Fadil ABDYLI**
*Shef i Sektorit për Hetim të Krimeve Kibernetike,*
*Policia e Kosovës*
*fadil.abdyli@kosovopolice.com*

**Abstrakt**

*Interneti sot është pjesë e përditshmërisë pothuajse e të gjitha shtresave të shoqërisë. Sa i përket përdorimit të internetit në Kosovë, numri i përdoruesve në raport me numrin e popullsisë është mjaft i lartë. Republika e Kosovës ka trajtuar çështjen e krimit kibernetik përmes legjislacionit, përveç sanksionimit të veprave penale,që bien në fushën e krimeve kibernetike, në Kodin Penal të Republikës së Kosovës, është miratuar edhe Ligji për Parandalimin dhe Luftimin e Krimit Kibernetik, edhe në këtë ligj janë paraparë disa vepra penale. Meqenëse Republika e Kosovës nuk është nënshkruese e Konventës së Budapestit ose Konventës së Krimit Kibernetik, Ligji për Parandalimin dhe Luftimin e Krimit Kibernetik është punuar duke u bazuar edhe në këtë Konventë. Gjithashtu, ekzistojnë edhe ligje tjera që në mënyrë indirekte mbështesin parandalimin dhe luftimin e krimit kibernetik. Rastet më të zakonshme që kanë pësuar viktimat nga krimi kibernetik janë: vjedhja e të dhënave të ndryshme, shkatërrimi i të dhënave, ngacmimi në internet (cyber-bullying), materialet abuzive seksuale me fëmijë në internet, vjedhja e identitetit, kanosjet, shantazhet etj. Dëmet që shkaktohen nga krimi kibernetik shpeshherë janë të parikuperueshme. Trendi i rasteve që bien në fushën e krimeve kibernetike ka rritje të hovshme, gjithashtu edhe rastet (kanosjet, mashtrimet, shantazhet, keqpërdorimet e të dhënave personale) që mundësohen të kryhen përmes kompjuterit apo internetit janë në rritje. Referuar statistikave, krahasuar vitin 2012 me vitin 2017, rritja e numrit të rasteve është trefishuar. Policia e Kosovës ka ndërmarrë hapa konkretë në ndërtimin e mekanizmit për parandalimin dhe luftimin e të gjitha formave të krimit kibernetik. Në Shtator të vitit 2011 është funksionalizuar sektori për hetim të krimeve kibernetike, me qëllim të ngritjes së efikasitetit, është bërë ristrukturimi respektivisht profilizimi ku në kuadër të sektorit janë formuar njësi specifike. Freskimi dhe mirëmbajtja e infrastrukturës ligjore si dhe avancimi dhe fuqizimi i mekanizmave për parandalimin dhe luftimin e krimeve kibernetike duhet të bëhet në mënyrë të vazhdueshme dhe bazuar në trendët e rreziqeve kibernetike dhe të krimit kibernetik.*

**Fjalëkyçe:**
**shoqëria, krimi, dëmi, legjislacioni, mekanizëm.**

## 1. Hyrje

Natyrisht se zbulimi i internetit është menduar për qëllime të mira, për të lehtësuar jetën e njerëzve në të gjitha fushat. Por, fatkeqësisht interneti ofron një terren të përshtatshëm edhe për keqbërësit të cilët mundohen të gjejnë anët e dobëta të internetit dhe t'i përdorin ato për qëllime të këqija, qoftë për përfitime materiale apo edhe me qëllim dëmtimin e tjerëve. Interneti ka ndikuar që edhe krimi të marrë një formë tjetër nga, siç njihen, krimet tradicionale. Kemi të bëjmë me një formë krimi mjaft të sofistikuar dhe kompleks që quhet apo njihet si krim kibernetik, krim kompjuterik apo edhe krim i teknologjisë së lartë. Sot, pothuajse çdo vepër penale, qoftë në mënyrë direkte apo indirekte, preket respektivisht mundësohet të kryhet përmes sistemeve kompjuterike.

Ligjvënësit kanë nxjerrë ligje dhe dokumente relevante për parandalimin dhe luftimin e veprimeve kriminale që kryhen përmes internetit. Ndër dokumentet kryesore vlen të përmendet Konventa e Krimit Kibernetik[1] ose siç njihet edhe Konventa e Budapestit (2001), kjo konventë është traktati i parë ndërkombëtar i cili kishte synim adresimin e Internetit dhe Krimeve Kompjuterike duke harmonizuar ligjet kombëtare, përmirësimin e teknikave hetuese si dhe rritjen e bashkëpunimit mes shteteve.

Edhe pse ka kaluar kohë e gjatë që nga nxjerrja e konventës, ajo vazhdon të jetë mjaft e qëndrueshme dhe e dobishme. Plotësimi i saj me dokumente shtesë, siç janë Protokolli Shtesë i Konventës së Krimit Kibernetik[2] që adreson kriminalizimin e veprimeve të natyrës raciste dhe ksenofobe që kryhen përmes sistemeve kompjuterike, pastaj Shënimet Udhëzuese[3] të cilat janë nxjerrë me qëllim lehtësimin e përdorimit dhe zbatimit efektiv të Konventës së Budapestit për krimin kibernetik, e ka forcuar edhe më shumë këtë dokument. Shumë shtete kanë ratifikuar Konventën e Krimit Kibernetik

ose janë në proces të ratifikimit si dhe shumë të tjera, e kanë rregulluar legjislacionin e brendshëm duke marrë për bazë Konventën e Krimit Kibernetik.

Referuar ueb-faqes zyrtare të Këshillit të Evropës, vendet e rajonit janë pjesë e konventës, e kanë nënshkruar dhe ratifikuar atë. Në tabelën 1 janë të dhënat për disa nga shtetet:

**Tabela 1:**

| Shteti | Nënshkruar | Ratifikuar |
|---|---|---|
| **Shqipëria** | 23/11/2001 | 20/06/2002 |
| **Mali i Zi** | 23/11/2001 | 15/09/2004 |
| **Maqedonia** | 07/04/2005 | 03/03/2010 |
| **Bosnja dhe Hercegovina** | 23/11/2001 | 25/03/2006 |
| **Kroacia** | 23/11/2001 | 17/10/2002 |
| **Serbia** | 07/04/2005 | 14/04/2009 |

Vlen të theksohet se asnjëra nga këto shtete nuk kanë ligj të veçantë për luftimin e krimit kibernetik, të gjitha kanë përfshirë veprat penale të parapara në Konventë në Kodin Penal dhe Kodin e Procedurës Penale.

## 2. Infrastruktura ligjore në Republikën e Kosovës

Infrastruktura ligjore në Republikën e Kosovës është e rregulluar mjaft mirë dhe i plotëson nevojat për trajtimin e krimeve kibernetike.

Në kuadër të legjislacionit, i cili qoftë në mënyrë direkte apo indirekte ndikon në trajtimin e krimeve kibernetike, por që nuk kufizohet, hyjnë:

- Kodi Penal i Republikës së Kosovës;
- Kodi i Procedurës Penale i Republikës së Kosovës;
- Ligji për parandalimin dhe luftimin e krimit kibernetik;
- Ligji për komunikimet elektronike;
- Ligji për shërbimet e shoqërisë së informacionit.

Përkundër kësaj, zhvillimi i hovshëm i teknologjisë dhe rritja e rasteve të krimeve kibernetike ka ndikuar që të rishikohet legjislacioni aktual me qëllim plotësimin dhe ndryshimin e tij. Në vitin 2016 Republika e Kosovës ka nxjerrë S*trategjinë shtetërore për siguri kibernetike*[4] dhe *Planin e veprimit*. Një ndër objektivat ka qenë edhe rishikimi i ligjit "Për parandalimin dhe luftimin e krimit kibernetik"[5]. Gjithashtu, është bërë plotësim ndryshimi i Kodit Penal dhe në fillim të vitit 2018 ka përfunduar Projektkodi Penal i Republikës së Kosovës; pritet procedimi i tij për ratifikim. Edhe në projektkodin penal

[1] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[2] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189
[3] https://www.coe.int/en/web/cybercrime/guidance-notes
[4] Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit https://mpb.rks-gov.net/Documents/Strategjia_Shteterore_per_Sigurine_Kibernetike_dhe_Plani_i_Veprimit_2016-2019_per_publikim_1202.pdf
[5] Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit , faqe 34 - https://mpb.rks-gov.net/Documents/Strategjia_Shteterore_per_Sigurine_Kibernetike_dhe_Plani_i_Veprimit_2016-2019_per_publikim_1202.pdf

janë paraparë vepra penale që bien në fushën e krimit kibernetik.

Vlen të theksohet se, si Kodi Penal i Republikës së Kosovës e po ashtu edhe ligji "Për parandalimin dhe luftimin e krimeve kibernetike" nuk e njohin krimin kibernetik si një vepër penale të vetme, por, janë disa vepra që hyjnë në krimet kibernetike.

*- Kodi Penal i Republikës së Kosovës*

Kodi Penal është ligji bazë i cili aplikohet kur kemi të bëjmë me rastet e krimit kibernetik, si nga policia ashtu edhe prokuroria dhe gjykata. Në Kodin Penal të Republikës së Kosovës ekzistojnë disa vepra penale që bien në fushën e krimeve kibernetike, siç janë:

1. neni 238, "Keqpërdorimi i fëmijëve në pornografi";
2. neni 307, "Lëshimi i çeqeve pa mbulesë ose të rremë dhe keqpërdorimi i kartelave të bankës apo të kreditit";
3. neni 339, "Hyrja në sistemet kompjuterike".

Këto vepra penale janë paraparë qysh në Kodin e Përkohshëm Penal të vitit 2003, me të njëjtin titull dhe pothuajse me të njëjtin përshkrim të veprës penale që ekzistojnë në Kodin Penal aktual, i cili është ratifikuar në vitin 2012, si dhe, në Projektkodin Penal të vitit 2018.

Nëse i krahasojmë veç e veç veprat penale që bien në fushën e krimeve kibernetike në tri ligjet, vërejmë se përshkrimi kryesisht është i njëjtë, kurse ndryshon sanksionimi dhe shuma e dëmit pasuror.

*- Ligji për parandalimin dhe luftimin kibernetik* [6]

Ky ligj ka për qëllim parandalimin dhe luftimin e krimit kibernetik 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.

Konventa e Krimit Kibernetik apo siç njihet ndryshe Konventa e Budapestit ka qenë bazë për përgatitjen e këtij ligji. Është dekretuar në korrik të vitit 2010.

Ligji në masë të madhe rregullon fushë-veprimtarinë e mekanizmave relevantë. Por, specifikat e fushës të cilën e rregullon ky ligj e bëjnë sfidues implementimin e tij. Gjithashtu sfiduese janë edhe fushat ku ligji parasheh angazhimin e aktorëve të ndryshëm për parandalimin dhe luftimin e krimit kibernetik. Disa nga pjesët kryesore të këtij ligji janë:

- *Përkufizimet*: Në këtë kategori specifikohet se ç'është krimi kibernetik, sistemi kompjuterik, të dhënat kompjuterike, ofrues i shërbimeve, të dhënat mbi trafikun e të dhënave, të dhënat mbi shfrytëzuesit.

- *Sanksionimi i veprave penale*. Janë 8 (tetë) vepra penale të parapara në këtë ligj; ato janë:

- veprat penale kundër konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave të sistemeve kompjuterike;
- interceptimi pa autorizim;
- transferta e paautorizuar;
- pengimi i funksionimit të sistemeve kompjuterike;
- prodhimi, posedimi dhe tentativa e paautorizuar;
- veprat penale lidhur me kompjuterë;
- shkaktimi i humbjes së pronës;

[6] Ligji "Për parandalimin dhe luftimin Kibernetik", http://kuvendikosoves.org/common/docs/ligjet/2010-166-alb.pdf

- pornografia me fëmijë përmes sistemeve kompjuterike.

*- Obligimet për institucionet relevante*

Me qëllim që të parandalohet dhe luftohet në mënyrë efikase krimi kibernetik, ligjvënësi ka paraparë se institucionet relevante duhet të marrin veprime konkrete për ndërtimin e kapaciteteve dhe rregullimin e infrastrukturës.

Referuar nenit 5 (pesë) të këtij ligji, 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 kibernetik.

Pastaj, 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. Gjithashtu, 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.

Sipas nenit 7 (shtatë) institucionet relevante zhvillojnë programe speciale trajnuese për personelin me qëllim të parandalimit dhe luftimit të krimit kibernetikë në përputhje me kompetencat që ushtrojnë.

Ndër tjera, ligji përmban edhe procedurën e ndjekjes, se si duhet të veprohet nga zbatuesit e ligjit në rastet e sekuestrimit, kopjimit dhe ruajtjen e të dhënave, bashkëpunimin ndërkombëtar, ruajtja e përshpejtuar e të dhënave etj.

*- Ligji për komunikimet elektronike*[7]

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.

Fushëveprim i këtij ligji, ndër tjera, është rregullimi i marrëdhënieve shoqërore që kanë të bëjnë me rrjetet dhe shërbimet e komunikimeve elektronike. Janë disa nene që rregullojnë çështje të caktuara kur kemi të bëjmë me hetime që kryhen nga organet hetuese. Ndër këto nene, janë edhe neni 68, "Ruajtja dhe administrimi i të dhënave personale për qëllime të ndjekjes penale", edhe neni 104: "Mbikëqyrja dhe monitorimi".

*- Neni 68, "Ruajtja dhe administrimi i të dhënave personale për qëllime të ndjekjes penale"*

Ky nen rregullon ruajtjen dhe administrimin e të dhënave personale për qëllime të ndjekjes penale, kjo nënkupton obligimin e ndërmarrësve të rrjetave dhe shërbimeve të komunikimeve elektronike publike që të ruajnë dhe të administrojnë për një periudhë jo më gjatë se një (1) vit skedarët e të dhënave për parapaguesit e vet.

[7] Ligji për komunikime elektronike: http://kuvendikosoves.org/common/docs/ligjet/109%20 Ligji%20per %20komunikimet %20elektronike.pdf

Gjithashtu, ky nen rregullon edhe kategoritë e të dhënave që duhet të ruhen, siç janë:

- të dhënat që kanë të bëjnë me qasjen nga interneti, me adresën *email* të internetit dhe me telefoninë përmes internetit;
- ID e ndarë e përdoruesit;
- emrin dhe adresën e parapaguesit, apo përdoruesit të regjistruar për të cilin është ndarë një adresë e Protokollit të Internetit (IP), një ID e përdoruesit apo numër i telefonit që i është ndarë atij në kohën e komunikimit;
- data dhe koha e kyçjes dhe ç'kyçjes së shërbimit të qasjes së Internetit, duke u bazuar në zonën e saktë kohore, bashkë me adresën IP, qoftë dinamike apo statike, e ndarë nga ofruesi i shërbimit të qasjes së internetit, si dhe ID e përdoruesit të parapaguesit ose përdoruesit të regjistruar;
- të dhënat e domosdoshme për të identifikuar pajisjen komunikuese të përdoruesit ose për çfarë pretendon të jetë pajisja;
- si dhe të dhëna tjera.

*- Neni 104, "Mbikëqyrja dhe monitorimi"*

Ky nen në përgjithësi rregullon ofrimin apo sigurimin e të dhënave nga ndërmarrësit që ofrojnë rrjeta dhe/ose shërbime të komunikimeve elektronike për institucionet kryesore që kryejnë hetime, me qëllim parandalimin, hetimin dhe zbulimin e veprave penale.

## 3. Rishikimi i legjislacionit

Rregullimi i fushës së parandalimit dhe luftimit të krimit kibernetik ndërlidhet me Programin e Qeverisë 2015-2018, më saktësisht me prioritetin strategjik nr. 2, të qeverisë: *Qeverisja e mirë dhe fuqizimi i sundimit të ligjit.* Kjo fushë ndërlidhet edhe me Programin Kombëtar për Zbatimin e Marrëveshjes së Stabilizim-Asocimit, më saktësisht me 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, i ka paraparë aktivitete përkatëse në fushën e parandalimit dhe luftimit të krimit kibernetik.

Qeveria e Kosovës ka ngarkuar Ministrinë e Punëve të Brendshme që të formojë ekipin[8] për zhvillimin e politikave për hartimin e koncept-dokumentit për parandalimin dhe luftimin e krimit kibernetik.

Koncept-dokumenti[9] për parandalimin dhe luftimin e krimit kibernetik 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 kibernetik 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 kibernetik".

[8] Vendimi i Sekretarit të Përgjithsëm të MPB-së.
[9] http://konsultimet.rks-gov.net/viewConsult.php?ConsultationID=40301

Kuvendi i Republikës së Kosovës më 10 qershor 2010 ka aprovuar ligjin Nr. 03/L-166, "Për parandalimin dhe luftimin e krimit kibernetik".

Ky ligj ka për qëllim parandalimin dhe luftimin e krimit kibernetik 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 kibernetik 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 kibernetik.

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.

Edhe në Raportin e Vendit është evidentuar se legjislacioni për krimin kibernetik është në një vijë me parimet dhe politikat e BE-së (EU *acquis*). Gjithashtu, në këtë raport përmendet se rishikimi i ligjit "Për parandalimin dhe luftimin e krimit kibernetik" duhet të merret parasysh nga autoritetet gjatë ndryshimeve të planifikuara në Kodin Penal, duke llogaritur në ekspertizën e komunitetit ndërkombëtar. Kjo do t'u mundësojë autoriteteve, që të kundërpërgjigjen më mirë ndaj ndryshimeve të shpejta të krimit kibernetik. Fillimisht, është bërë vlerësim i situatës në terren, si dhe janë identifikuar pikat se ku duhet të plotësohet dhe ndryshohet ligji. Përmes rishikimit, është gjetur se pothuajse të gjitha nenet, duhet të plotësohen apo ndryshohen, si dhe të shtohen nene të reja.

Gjatë procesit të hartimit të koncept-dokumentit janë zhvilluar konsultime në mënyrë aktive me përfaqësues të organizatave ndërkombëtare të akredituara në Kosovë dhe pas kompletimit të tij, i njëjti është vënë në dispozicion të publikut në mënyrë që të japin vërejtjet dhe sugjerimet e tyre.

## 4. Mekanizmi për parandalimin dhe luftimin e krimeve kibernetike në kuadër të Policisë së Kosovës

Policia e Kosovës në kuadër të ndërtimit të kapaciteteve të saja për parandalimin dhe luftimin e krimit kibernetik, ka themeluar Sektorin për Hetim të Krimeve Kibernetike. Themelimi i këtij mekanizimi ka qenë mëse i nevojshëm, përveç tjerash, edhe për faktin se kriminaliteti po merr formë të re si dhe rrethanat e reja të krijuara.

"Sektori për hetim të krimeve kibernetike", është funksionalizuar në shtator 2011, është i strukturuar në kuadër të Drejtorisë për Hetimin e Krimit të Organizuar. Me qëllim të ngritjes së efikasitetit, është bërë ristrukturimi, respektivisht profilizimi, ku në kuadër të sektorit janë formuar katër njësi: njësia për hetimin e ndërhyrjeve në sistemet kompjuterike; njësia për hetimin e keqpërdorimit të kartelave bankare; njësia për hetimin e pornografisë së fëmijëve në internet; njësia për kontrolle dhe forenzikë të teknologjisë informative.

- *Njësia për hetimin e ndërhyrjeve në sistemet kompjuterike.*

Kjo njësi merret me hetimin e të gjitha rasteve që kanë të bëjnë me veprën penale të kryer nga sistemet kompjuterike, siç janë: sulmet përmes kompjuterit; hyrjet e paautorizuara në sistemet kompjuterike etj.

- *Njësia për hetimin e keqpërdorimit të kartelave bankare.*

Kjo njësi merret me hetimin e rasteve që kanë të bëjnë me veprën penale të keqpërdorimit të kartelave bankare dhe të kreditit, siç janë: vjedhja e të dhënave të kartelave bankare dhe të kreditit; blerja *online* me kartela të vjedhura apo klonuara etj.

- *Njësia për hetimin e pornografisë së fëmijëve në internet.*

Kjo njësi merret me hetimin e rasteve që kanë të bëjnë me veprën penale të keqpërdorimit të fëmijëve në pornografi përmes internetit.

- *Njësia për kontrolle dhe forenzikë të teknologjisë informative.*

Kjo njësi merret me kontrollin e pajisjeve elektronike që sekuestrohen në rastet kur është kryer ndonjëra nga veprat penale që hetohen nga njësitë e përmendura më herët. Gjithashtu, bën edhe analizimin e të dhënave të gjetura në pajisjet e sekuestruara, përgatit raport dhe e përcjell atë tek hetuesit e rasteve. Provat digjitale janë mjaft të ndjeshme dhe të paqëndrueshme, shpeshherë ndodh që ato duhet të merren në vendin e ngjarjes sepse përcaktojnë veprimet hetimore të mëtutjeshme.

- *Veprat penale që hetohen nga sektori për hetim të krimeve kibernetike.*

Policia e Kosovës duke iu referuar Kodit Penal ka nxjerrë një dokument i cili udhëzon dhe përcakton mekanizmat përkatës për trajtimin e rasteve, ndryshe njihet si dokument për kompetencat lëndore. Bazuar në këtë dokument, sektori për hetim të krimeve kibernetike heton veprat penale si në vijim:

- cenimi i fshehtësisë së korrespondencës dhe i bazave së të dhënave kompjuterike;
- zbulimi i paautorizuar i informacionit konfidencial;
- ofrimi i materialit pornografik personave nën moshën gjashtëmbëdhjetë vjet;
- keqpërdorimi i fëmijëve në pornografi;
- lëshimi i çeqeve pa mbulesë ose të rremë dhe keqpërdorimi i kartelave të bankës apo të kreditit;
- hyrja në sistemet kompjuterike.

Në shumë pak raste është aplikuar apo janë zhvilluar hetime sipas ligjit "Për parandalimin dhe luftimin e krimit kibernetik", kjo për arsye se ligji ka disa mangësi dhe nuk ka arritur të promovohet tek zbatuesit. Edhe mungesa e njohurive për krimet kibernetike ka ndikuar në rezistim për aplikim.

- *Format e rasteve*

Për nga natyra, rastet që hetohen janë pothuajse raste të "zakonshme" me të cilat ballafaqohen mekanizmat për luftimin e krimeve kibernetike, ato janë:

• Keqpërdorimi i fëmijëve përmes internetit (pornografia e fëmijëve në internet) – këtu hyn shkarkimi, posedimi dhe shpërndarja e materialeve me përmbajtje pornografike të fëmijëve.

• Kanosje dhe shantazhe përmes *email*-it dhe llogarive në rrjete sociale (përfshirë edhe ndaj personaliteteve të rëndësishme publike dhe institucioneve).

• Cenim i të drejtave të autorit – publikime në internet të punës së tjetrit pa autorizim.

• Hyrje e paautorizuar në sistem kompjuterik (sulme DDoS apo pengim i funksionimit normal dhe ofrimit të shërbimeve në internet ndaj ueb-faqeve të institucioneve të ndryshme publike dhe kompani biznesi, vjedhje e fjalëkalimeve përmes infektimit me viruse kompjuterike etj.);

• Klonimi i kartelave – blerjet *online* dhe në POS (markete) – vjedhja e të dhënave bankare dhe furnizimi me të dhëna bankare të vjedhura, përdorimi i këtyre të dhënave

për klonim të kartelave bankare dhe më pas blerja e gjësendeve të ndryshme nëpër markete përmes POS terminaleve por edhe blerje të gjësendeve përmes internetit;

• Vjedhja e të dhënave të kartelave bankare dhe të kreditit si dhe vjedhja e parave nga bankomatët (vendosja e SKIMMING pajisjeve dhe pajisjeve tjera të modifikuara);

• Mashtrim përmes falsifikimit të email-ve (modifikim i faturave dhe ndryshim i xhirollogarive bankare);

*- Trendi i krimit*

Nëse i referohemi statistikave ndër vite, vërehet qartë se ka rritje të hovshme të numrit të rasteve që bien në fushën e krimeve kibernetike. Kjo mund të shihet nga dy këndvështrime: vetëdijesimi i qytetarëve për ekzistimin e një mekanizmi që lufton krimet kibernetike dhe raportimi i rasteve, si dhe, angazhimi i shtuar i hetuesve policor në luftimin e krimeve kibernetike. Kjo nënkupton edhe avancimin e njohurive në këtë fushë përmes trajnimeve.

Në tabelën 2, jepen statistikat për rastet e krimeve kibernetike në Kosovë**.** Rastet kanë të bëjnë me hyrje në sisteme kompjuterike (sulme ndaj ueb-faqeve të ndryshme), keqpërdorim i kartelave bankare dhe të kreditit (vjedhja e të dhënave bankare të klientëve të bankave përmes vendosjes së pajisjeve të modifikuara si dhe klonimi dhe përdorimi i kartelave bankare apo të kreditit) si dhe pornografi e fëmijëve përmes internetit. Asistimet i referohen kërkesave për asistim nga njësitet e ndryshme brenda Policisë së Kosovës por edhe jashtë saj drejtuar sektorit për hetimin e krimeve kibernetike. Kjo nënkupton kryerjen e veprave penale të mundësuara nga sistemet kompjuterike.

**Tabela 2**

| Vitet | Viti 2012 | Viti 2013 | Viti 2014 | Viti 2015 | Viti 2016 | Viti 2017 |
|---|---|---|---|---|---|---|
| Rastet | 11 | 18 | 24 | 34 | 40 | 42 |
| Asistime | 16 | 55 | 80 | 118 | 152 | 199 |

*- Bashkëpunimi ndërinstitucional dhe ndërkombëtar*

Ndër institucionet vendore me të cilat sektori për hetim të krimeve kibernetike bashkëpunon ngushtë janë, prokuroritë e shtetit, gjykatat, ofruesit e shërbimeve të internetit (ISP), institucionet financiare, dogana si dhe institucione tjera varësisht prej nevojave që paraqiten. Me këtë bashkëpunim, është arritur edhe sukses, në shumë raste që kanë rezultuar me arrestime, konfiskime të pasurisë së fituar nga vepra penale, dënime etj. Por, ka hapësirë të bëhet edhe më shumë për të forcuar këtë bashkëpunim. Kjo ndikon drejtpërdrejt në shkurtimin e kohës së veprimit dhe duke rritur njëkohësisht edhe efikasitetin në trajtimin e krimit kibernetik.

Sektori për hetim të krimeve kibernetike ka arritur të krijojë bashkëpunim me disa agjenci të zbatimit të ligjit; ky bashkëpunim ka rrjedhur si pasojë e rasteve ku dëmi është shkaktuar në vendin tonë, kurse personat e dyshuar, veprën e kanë kryer nga shteti tjetër, apo edhe anasjelltas. Ka pasur raste kur në mungesë të themelimit të komunikimit me shtete përkatëse, nuk është arritur të identifikohen personat e dyshuar apo të sigurohen provat elektronike. Mosanëtarësimi në Interpol gjithashtu është pikë e dobët dhe ndikon

në zhvillim efikas të hetim dhe sigurimit të provave.

*- Parandalimi i krimeve kibernetike*

Me qëllim që të jemi sa më efikas dhe efektiv në parandalimin dhe luftimin e krimeve kibernetike, janë marrë masa konkrete në këtë drejtim.

- është bërë profilizimi i sektorit duke e ndarë në njësi specifike;
- rritja e numrit të hetuesve policor;
- identifikimi i nevojave të trajnimit dhe ndjekja e trajnimeve;
- identifikimi i mjeteve të punës dhe pajisja me to;
- përgatitja e materialit për krimet kibernetike dhe ligjërimi drejtuar kadetëve, hetuesve policor të stacioneve, rajoneve dhe drejtorive;
- ligjërata nëpër shkolla të mesme të ulëta me qëllim vetëdijesimin e nxënësve për rreziqet që vijnë nga përdorimi jo i drejtë i internetit;
- ligjërata nëpër institucione të ndryshme.

## 5. Përfundim

Qëllimi i këtij punimi është trajtimi i një teme mjaft të rëndësishme siç është legjislacioni për krimin kibernetik dhe ballafaqimi i Policisë me krimin kibernetik. Sipas statistikave të fundit, depërtimi i internetit në vendin tonë është mjaft i lartë, kjo nënkupton se qytetarët e të gjitha shtresave janë përdorues mjaft aktivë të internetit. Gjithashtu, ofrimi i shërbimeve të ndryshme *online* është në rritje ku institucione publike dhe private, për çdo ditë e më shumë, orientojnë qasjen apo komunikimin me qytetarin përmes internetit. Shërbimet që ofrohen kanë të bëjnë me nevoja të përditshme të qytetarit, siç janë, shërbimet financiare, shitblerja e gjësendeve, aplikimet e ndryshme (punë, rezervime) etj.

Për këtë arsye, hapësira kibernetike vazhdon të jetë ambient i përshtatshëm për keqbërësit, për kryerjen e veprave të ndryshme penale, duke përdorur mjete dhe programe kompjuterike të sofistikuara. Referuar rasteve të hetuara, qëllimi kryesor i keqbërësve mbetet përfitimi material.

Vërehet se qytetarët që bien viktima të keqbërësve në internet, nuk kanë njohuri të mjaftueshme për rreziqet gjatë përdorimit të internetit. Njëkohësisht, marrë parasysh kërkesat për asistim nga njësitet e ndryshme policore, vijmë në përfundimin, se edhe zyrtarët policorë nëpër njësite të ndryshme, nuk kanë njohuri të mjaftueshme kur kemi të bëjmë me rastet që kryhen përmes kompjuterit apo internetit.

Marrë parasysh gjetjet gjatë trajtimit të temës, lindin natyrshëm edhe rekomandimet se si mund të përballemi më mirë me fenomenin e krimit kibernetik. Në vijim janë disa rekomandime, të cilat janë të përgjithësuara dhe duhet të shtjellohen më tutje e të konsiderohen kyçe, për trajtim adekuat, respektivisht ndërtim të kapaciteteve në kuptimin e plotë të fjalës.

- Identifikimi në vazhdimësi i nevojave për ndërtim të kapaciteteve duke marrë për bazë trendin dhe format e krimit kibernetik, punimi i programeve të trajnimit dhe ndjekja e trajnimeve. Meqenëse se përgatitja profesionale dhe e specializuar merr kohë të gjatë, duhet të bëhet kategorizimi i trajnimit i cili mund të ndahet në bazik dhe të specializuar. Në trajnimin bazik duhet të trajnohen zyrtarët policor të cilët nuk merren drejtpërdrejt me hetimin e krimit kibernetik ose merren me ato vepra që mund të trajtohen edhe në nivele më të ulëta kurse në trajnimin e specializuar duhet të trajnohen

zyrtarët policor të cilët merren drejtpërdrejt me hetimin e krimit kibernetik. Të bëhet analizë periodike e gjendjes së përgjithshme për krimet kibernetike dhe të nxirren rekomandime për parandalim dhe luftim të krimit kibernetik. Objektiv kryesor të jetë ndërtimi i një mekanizmi të qëndrueshëm që merret me hetimin e krimit kibernetik.

- Të ndërtohet qasje strategjike sa i përket bashkëpunimit ndërinstitucional, me sektorin privat, ndërkombëtar dhe me akademinë. Ky bashkëpunim nënkupton shkëmbimin e informatave në kohë reale të cilat përmbajnë të dhëna potenciale që mund të çojnë në identifikimin e veprave penale dhe të dyshuarve. Pikë e fortë janë edhe aktivitetet dhe angazhimet e përbashkëta, siç janë takimet e ndryshme, trajnimet e përbashkëta etj.

- Anëtarësimi në organizata të ndryshme ndërkombëtare të cilat trajtojnë krimin kibernetik është i domosdoshëm. Ekzistojnë platforma online të dedikuara vetëm për zbatuesit e ligjit dhe anëtarësimi në to sjell lehtësime në hetimin e rasteve me element ndërkombëtar.

- Të themelohet një bazë e të dhënave e veçantë e cila do të plotësohej me të dhënat nga rastet aktuale si dhe rastet në të ardhmen. Kjo bazë e të dhënave do të lehtësonte qasjen më profesionale dhe njëkohësisht do të shërbente edhe për vlerësim strategjik për nxjerrjen e rekomandimeve dhe zhvillimin e udhëzimeve për parandalimin dhe luftimin e krimit kibernetik.

- Statistikat tregojnë se numri i përdoruesve të internetit në Kosovë është shumë i lartë. Ky është një tregues se është mëse i nevojshëm, për kryerje e vetëdijesimit të qytetarëve apo të përdoruesve të internetit. Kjo mund të arrihet përmes fushatave të ndryshme, konferencave, broshurave, shfaqjes së videove nëpër televizione, bisedave me fëmijë nëpër shkolla etj. Vetëdijesimi nënkupton apo duhet të përfshijë edhe zyrtarët e institucioneve qeveritare.

## Bibliografi


1. *Konventa e Krimit Kibernetik apo Konventa e Budapestit*, 2001;
2. *Kodi i Përkohshëm Penal*, 2003.
3. *Kodi Penal i Republikës së Kosovës*, 2012.
4. *Projektkodi Penal i Republikës së Kosovës*, 2018.
5. *Ligji për Parandalimin dhe Luftimin e krimit Kibernetik*, 2010.
6. *Ligji për Komunikimet Elektronike*, 2012.
7. *Koncept-dokumenti për parandalimin dhe luftimin e krimit kibernetik*, 2018.
8. *Raporti i Vlerësimeve të Kërcënimeve nga Krimi i Organizuar dhe Krimet e Rënda* (SOCTA), 2016.
9. *Raporte policore*, 2012, 2013, 2014, 2015, 2016, 2017.

# Legjislacioni kombëtar dhe ndërkombëtar mbi krimin kibernetik

■**MSc. Ermira ÇOBAJ**
*Universiteti i Shkodrës "Luigj Gurakuqi"*
*ecobaj@unishk.edu.al*

**Abstrakt**

*Në këtë kohë kur sfida e shumicës së njerëzve është të fitojnë sa më shumë para dhe të arrijnë majat më të larta të suksesit, ka persona që këtë gjë e arrijnë me pandershmëri të plotë. Janë të shumte ata që marrin pa të drejtë identitetin on line të së tjerëve dhe që manipulojnë me të dhënat e tyre. Hapësira kibernetike sot është një nga sfidat më të mëdha ligjore, e cila ka nxitur një formë tjetër të krimit, duke krijuar një mjedis për metodat e reja të krimit. Ky fenomen ka një rëndësi shumë të madhe në shkallë kombëtare dhe globale dhe ka pësuar një rritje të shpejtë në Shqipëri pavarësisht se mungojnë studimet e mirëfillta në këtë fushë. Qëllimi i këtij studimi është paraqitja e situatës së krimit kibernetik në Shqipëri, duke analizuar legjislacionin ekzistues dhe shkallën e zbatueshmërisë së tij në praktikë dhe kuadri ligjor ndërkombëtar mbi krimin kibernetik, mekanizmat për zbatimin e tij. Pyetjet kryesore që ngrihen dhe që synohet t'u jepet një përgjigje nëpërmjet këtij punimi janë: Cila është situata aktuale e krimit kibernetik në Shqipëri, sa i plotësuar është legjislacioni shqiptar mbi krimin kibernetik për t'iu përgjigjur sfidave aktuale? Cilat janë mekanizmat ligjore për mbrojtjen ndaj krimit kibernetik në arenën ndërkombëtare? Ky punim synon të rrisë ndërgjegjësimin e shtetit shqiptar mbi rëndësinë e mbrojtjes së sigurisë kombëtare të shtetit dhe shtetasve shqiptarë nga rreziqet që shfaq krimi kibernetik. Në fund të këtij punimi janë paraqitur konkluzionet e nxjerra nga artikulli për krimin kibernetik në Shqipëri, të arritura si rezultat i konstatimeve të nxjerra gjatë përgatitjes së këtij artikulli.*

**Fjalëkyçe:**

**krimi kompjuterik, hapësirë kibernetike, legjislacion kombëtar, legjislacion ndërkombëtar.**

## 1. Hyrje

Kompjuteri është një nga shpikjet më të rëndësishme në fushën e industrisë në botë. Aplikimi i kompjuterit dhe mundësitë e mëdha që ai ofron, fatkeqësisht po keqpërdoren dhe po shfrytëzohen për kryerjen e një numri te krimeve dhe sjelljeve kriminale. Teknologjia dhe mundësitë që ofron i ka nxitur personat që të përdorin këtë si mjet dhe metodë të fuqishme dhe shumë të sofistikuar, për kryerjen e një vargu krimesh duke iu ofruar mundësi që ata t'i fshehin gjurmët dhe me vështirësi të zbulohen.

Krimi kibernetik është në rritje në shumë vende ku ka depërtuar aplikimi i kompjuterit por edhe në vendet më pak të zhvilluara ngaqë tek këto të fundit mungon një rregullore e mirëfilltë juridike lidhur me pengimin e keqpërdorimit të kompjuterit për qëllime kriminale. Shumë autorë, krimin kibernetik e cilësojnë si formë të veçantë të krimit te organizuar, përkatësisht si krim i jakave te bardha dhe në rend të parë përdoret për krime në fushën ekonomike. Zakonisht kryerësit e veprimeve kriminale me kompjuter janë persona të rinj, shpesh të pushtuar nga pasioni i teknikës dhe ndjenja se duke manipuluar me kompjuter janë duke bërë çudira të ndryshme.

Për ta thuhet se në fillim të karrierës së tyre të manipulimit me kompjuter, nuk nisen nga motivet dhe qëllimet kriminale, por më vonë këta i pushton një ndjenjë e veçantë e sidomos kur fillojnë nga manipulimet e ndryshme te përfitojnë edhe shuma të mëdha, atëherë shndërrohen në tipa të kriminelëve profesionistë. Krimi kibernetik është një aktivitet kriminal që përfshin: infrastrukturën e teknologjisë së informacionit, aksesin e paligjshëm, përgjimin e paligjshëm, ndërhyrjen e të dhënave, falsifikimin dhe mashtrimin elektronik. Duke parë rëndësinë e këtij fenomeni në shkallë kombëtare dhe në shkallë ndërkombëtare, duke pasur parasysh rritjen e shpejtë të krimit kibernetik në Shqipëri

vitet e fundit dhe mungesën e studimeve të mirëfillta në këtë fushë në vendin tonë, vendosa të bëj këtë punim mbi krimin kibernetik, duke marrë si rast studimor vendin tonë, Shqipërinë. Qëllimi i këtij studimi është analizimi i situatës aktuale në Shqipëri, në lidhje me standardet ligjore, evidentimin e problematikave dhe sfidave kryesore me të cilat hasen gjyqtarët, prokurorët, policia, në parandalimin dhe luftimin e krimit kibernetik në Shqipëri. Ky punim është ndarë në disa çështje, sipas tematikave të prekura.

Është bërë një përshkrim i përgjithshëm i krimit kibernetik, duke filluar me përkufizimet kryesore të përdorura përgjatë punimit. Analizimin e fenomenit të krimit kibernetik duke kaluar ne rendin kombëtar të krimit kibernetik, duke paraqitur aktualitetin e këtij lloj krimi në Republikën e Shqipërisë ku paraqiten standardet ligjore kombëtare kundër krimit kibernetik. Çështja e arenës ndërkombëtare të krimit kibernetik ku është paraqitur korniza ligjore ndërkombëtare kundër krimit kibernetik që përfshin: Konventën Kundër Krimit Kibernetik të Këshillit të Europës si dhe standardet ligjore të bashkëpunimit ndërkombëtar në hetimin e krimit. Gjithashtu janë paraqitur mekanizmat ligjore ndërkombëtare në luftën kundër këtij fenomeni për luftimin e krimit kibernetik.

Çështja tjetër trajton një aspekt tjetër mjaft të rëndësishëm të krimit kibernetik, aspekti i sigurisë kombëtare dhe rreziku që i shkaktohet asaj nga sulmet kibernetike. Konkretisht flitet nevojën e një bashkëpunimi dhe mirëkoordinimi global, me qëllim arritjen e rezultateve sa më të larta. Kërkimet e kryera janë bazuar tek metoda vëzhguese duke nxjerrë rezultate në lidhje me situatën e krimit kibernetik në të drejtën shqiptare dhe me qëllim për të përcaktuar nëse shteti shqiptar është mjaftueshmërisht i përgatitur për të luftuar krimin kibernetik dhe sfidat që ai përbën për sigurinë kombëtare. Studimi i krimit kibernetik në të drejtën shqiptare sjell nevojën e përdorimit të një metode krahasuese duke krahasuar legjislacionin shqiptar me atë të Bashkimit Europian për të parë se sa përputhen ata pasi kuptimi dhe përmbajtja e një fenomeni juridik rezultojnë gjithmonë më të plotë nga një qasje e bazuar në të drejtën e krahasuar.

Duke qenë se studimi ka si qëllim përshkrimin dhe analizimin e situatës aktuale të legjislacionit shqiptar dhe të huaj, kërkimi është i bazuar në metoda cilësore të studimit, të cilat mbështeten në literaturën e huaj dhe atë shqiptare, ku përfshihen akte ligje në fushën kibernetike, por jo vetëm, konventa, strategji, libra, monografi, artikuj etj Në fund të këtij punimi janë paraqitur konkluzionet e nxjerra nga studimi kërkimor i zhvilluar.

## 2. Legjislacioni kombëtar lidhur me krimin kibernetik në Shqipëri

Në vitet e fundit, shoqëritë në të gjithë botën kanë bërë përparime të mëdha drejt kalimit në një shoqëri të informacionit. Teknologjia e informacionit dhe komunikimit (ICT) tani përshkon pothuajse çdo aspekt të jetës së njerëzve. Fakti që shoqëria po mbështetet gjithmonë e më shumë, e si rrjedhojë, po varet gjithmonë e më shumë nga teknologjia e informacionit dhe komunikimit e bën atë të ekspozuar ndaj kërcënimeve të tilla si krimi kibernetik, domethënë krimi i kryer kundër të dhënave dhe sistemeve kompjuterike ose nëpërmjet tyre[1]. Çdo ditë, miliona njerëz identifikohen në botën virtuale nëpërmjet përdorimit të pafundësisë së aplikacioneve të ndryshme që ofron

[1] https://rm.coe.int/16802fa3d3

hapësira kibernetike virtuale. Disa janë pjesë e një videoloje, të tjerët janë pjesë e ndërveprimeve sociale, dhe shumë të tjerë përfshijnë elementet personal në kryerjen e veprimeve tregtare si blerje online, shkëmbim informacioni porosi etj. Çfarëdo qëllimi, çdo mjedis në të cilin njerëzit ndër veprojnë mund të çojë në përplasje dhe në mosmarrëveshjeve të llojeve të ndryshme. Dhe më të drejtë lind pyetja nëse ligjet e botës reale mund ose duhet të zbatohen për problemet virtuale botërore.

Kodi Penal i Republikës së Shqipërisë, neni 7: "Shtetasi i huaj, që kryen vepër penale në territorin e Republikës së Shqipërisë, përgjigjet në bazë të ligjit penal të Republikës së Shqipërisë. Ligji penal i Republikës së Shqipërisë është i zbatueshëm edhe për shtetasin e huaj që jashtë territorit të Republikës së Shqipërisë kryen në dëm të interesave të shtetit ose të shtetasit shqiptar një nga krimet e mëposhtme:

a) krime kundër njerëzimit;

b) krime kundër pavarësisë dhe rendit kushtetues;

c) akte terroriste;

d) organizimi i prostitucionit, prodhimi dhe trafiku i jashtëligjshëm i drogës dhe substancave të tjera narkotike, i armëve dhe substancave nukleare, si dhe materialeve pornografike;

e) falsifikimi i vulës së shtetit shqiptar, parave dhe letrave me vlerë shqiptare;

f) krime që cenojnë jetën dhe shëndetin e shtetasit shqiptar, për të cilat ligji parashikon dënim mbi pesë vjet burgim ose çdo lloj dënimi më të rëndë.

g) vepra penale në fushën e teknologjisë së informacionit".[2]

Prova kompjuterike është e pashfaqur, njësoj si gjurmët e gishtave apo ADN-ja. I kapërcen kufijtë juridike shpejt dhe me lehtësi. Ndryshohet, dëmtohet apo prishet me lehtësi. Është e ndjeshme nga faktori kohë. Oficerët e policisë gjyqësore në vendngjarje duhet të mbajnë mend që prova kompjuterike mund të përmbajë dhe prova të tjera fizike si ADN, gjurmë gishtash, lëngje, etj. Provat fizike duhet të trajtohen sipas ekzaminimit përkatës. Me ligjin nr. 10054 date 29.12.2008[3] "Për disa shtesa dhe ndryshime në kodin e procedurës penale" në nenin 191 të kodit të procedurës penale u shtua neni 191/a me këtë përmbajtje:

*"Neni 191/a*

*Detyrimi për paraqitjen e të dhënave kompjuterike.*

1. Gjykata, në rastin e procedimeve për vepra penale në fushën e teknologjisë së informacionit, me kërkesë të prokurorit ose të të dëmtuarit akuzues, urdhëron, mbajtësin ose kontrolluesin të dorëzojnë të dhënat kompjuterike të memorizuara në një sistem kompjuterik apo në një mjet tjetër memorizimi.

2. Gjykata, në këto procedime, urdhëron edhe dhënësin e shërbimit, për dorëzimin e çdo informacioni për abonentët e pajtuar, për shërbimet e ofruara nga dhënësi.

3. Kur ka arsye për të menduar se nga vonesa mund t'u vije një dëm i rëndë hetimeve, prokurori vendos, me akt të motivuar, detyrimin për paraqitjen e të dhënave kompjuterike, të përcaktuara në pikat 1 dhe 2 të këtij neni dhe njofton menjëherë gjykatën. Gjykata vlerëson vendimin e prokurorit brenda 48 orëve nga njoftimi."[4]

Për kriminalitetin kompjuterik, si formë e re e krimit të organizuar në botën bashkëkohore, nga ana shkencore deri me tani nuk ka pasur ndonjë qëndrim të

[2] Ligji nr. 7895, datë 17.1.1995, Kodi Penal i Republikës së Shqipërisë, i ndryshuar, neni 7.
[3] Ligji nr. 10054 datë 29.12.2008.
[4] Kodi i Procedurës Penale i Republikës së Shqipërisë. Tiranë: Botim i Qendrës së Publikimeve Zyrtare, 2011, neni 191/a.

përbashkët në lidhje me definicionin apo për origjinën e paraqitjes së kësaj forme të kriminalitetit.

Disa mendojnë se kjo është një kategori e re, origjina e së cilës lidhet me paraqitjen e kompjuterëve të parë digjitalë elektronikë, nga mesi i shekullit të kaluar, por ka edhe mendime ku thuhet se te keqpërdorimet e para ka ardhur edhe më herët, që në fillim të shekullit dymbëdhjetë, kur janë paraqitur llogaritësit e parë mekanikë.[5] Sot, teknologjia informative, në fakt kompjuterët me komponentët e tyre, janë në funksion të aktiviteteve ditore të secilit njeri. Përdorimi i kompjuterit në kryerjen e shumë funksioneve në fushën ekonomike, juridike, ushtarake, industriale, mjekësore, shkencore e fusha të tjera, kanë zhvilluar një progres aq të shpejtë, sa që mënyra e jetesës ka ndryshuar në mënyrë të pakthyeshme[6].

*Neni 208/a i Kodit të Procedurës Penale:*

"Sekuestrimi i të dhënave kompjuterike"

1. Në rastin e procedimeve për vepra penale në fushën e teknologjisë së informacionit, gjykata, me kërkesë të prokurorit, vendos sekuestrimin e të dhënave dhe sistemeve kompjuterike. Në këtë vendim, gjykata përcakton të drejtën për të hyre, kërkuar dhe marrë të dhënat kompjuterike në sistemin kompjuterik, si dhe ndalimin për kryerjen e veprimeve të mëtejshme apo sigurimin e të dhënave ose të sistemit kompjuterik.

2. Kur ekzistojnë shkaqe të arsyeshme për të menduar se të dhënat e kërkuara kompjuterike janë memorizuar në një sistem kompjuterik apo në një pjesë të tij dhe këto të dhëna janë në mënyrë të ligjshme të kapshme prej ose janë të disponueshme nga sistemi kompjuterik fillestar, që kontrollohet, gjykata, me kërkesë të prokurorit, kërkimin ose hyrjen edhe në këtë sistem kompjuterik.

3. Në zbatim të vendimit të gjykatës, prokurori ose oficeri i policisë gjyqësore,i deleguar nga prokurori, merr masa:

a) për të ndaluar kryerjen e veprimeve të mëtejshme ose për të siguruar sistemin kompjuterik, vetëm të një pjese të tij ose të një mjeti tjetër memorizimi të dhënash

b) për të nxjerrë dhe marrë kopje së të dhënave kompjuterike

c) për të penguar hyrjen në të dhënat kompjuterike ose për t'i hequr këto të dhëna nga sistemet kompjuterike me të drejtë hyrje

ç) për të siguruar paprekshmërinë e të dhënave përkatëse të memorizuara.

4. Për zbatimin e këtyre veprimeve, prokurori mund të urdhërojë thirrjen e një eksperti, i cili ka njohuri rreth funksionimit të sistemeve kompjuterike apo masave të zbatuara për mbrojtjen e të dhënave kompjuterike në të. Eksperti i thirrur nuk mund të refuzojë detyrën pa shkaqe të arsyeshme[7].

Personat që kryejnë vepra penale të kriminalitetit kompjuterik, posedojnë fond përkatës të njohurive dhe shkathtësive nga fusha e teknikës kompjuterike dhe informatikës kriminalistike. Këtu bëhet fjalë kryesisht për personat që bëjnë pjesë në inteligjencën teknike, veprimtaria kriminale e të cilëve nuk është e lehtë të zbulohet dhe të provohet[8].

[5] Drazen Dragiçeviq: Kompjuterski kriminalitet i informacijski sustavi, Zagreb, 1999, f. 114.
[6] Doracaku: International review of criminal policy. UN Manual on the prevencion and control of computer related crime, fq.43-44. marrë nga interneti http://www.ifs.univie. ac.at/~pr2gq1/rev4344.html
[7] Kodi i Procedurës Penale i Republikës së Shqipërisë, neni 208/a.
[8] Wiliam S. Sessions,"Kompjuterski kriminal trend koji eskalira", Prirucnik, nr.3/91, Zagreb, f. 220, cit sipas V. Latifit, Kriminalistika, 2000, f. 249.

## 2. Dimensioni ndërkombëtar i krimit kibernetik

Çështja ka të bëjë me përmasën ndërkombëtare të krimit kibernetik. Duke qenë një krim që i kapërcen kufijtë kombëtarë, kur flitet për krimin kibernetik, është e nevojshme të dihen arritjet e deritanishme kundër këtij fenomeni në arenën ndërkombëtare. Kështu është paraqitur korniza ligjore ndërkombëtare aktuale kundër krimit kibernetik, duke përfshirë: Konventën Kundër Krimit Kibernetik të Këshillit të Europës, legjislacionin specifik kundër krimit kibernetik, si edhe standardet ligjore të bashkëpunimit ndërkombëtar në hetimin e krimit. Përkufizimi i të dhënave kompjuterike dhe sistemeve kompjuterike është dhënë në Konventën "Për krimin në fushën e kibernetikës"[9] ratifikuar nga Parlamenti Shqiptar, me ligjin 8888, datë 25.04.2002 Për ratifikimin e "Konventës për krimin në fushën e kibernetikës":

- *Neni 1 i Konventës:*

"Përkufizimet".

a*) "Sistem kompjuterik" do të thotë çdolloj pajisje apo grup i ndërlidhur, ose pajisje të lidhura, një ose më shumë prej të cilave, vazhduese të një programi kryejnë procesime automatike së të dhënave.*

b) "Të dhëna kompjuterike" do të thotë çfarëdolloj përfaqësimi të fakteve, informacioni apo konceptesh në një formë të përshtatshme për procesim në një sistem kompjuterik, që përfshijnë një program të përshtatshëm për punën e një sistemi kompjuterik për të kryer një funksion.

c) "Dhënës shërbimesh" do të thotë: (i) çfarëdo entiteti publik apo privat, që i siguron shërbimin e tij përdoruesve, me mundësinë për të komunikuar nëpërmjet një sistemi kompjuterik; dhe (ii) çfarëdo entiteti tjetër, që proceson apo memorizon të dhëna kompjuterike në të mirë të një shërbimi të këtillë komunikimi apo të përdoruesve për këtë shërbim[10].

*Neni 18 pika 3 jep* përkufizimin e informacionit të abonentit:

*"Informacion abonenti" do të thotë çfarëdo informacion i futur në formën e të dhënave kompjuterike apo çfarëdo forme tjetër, që mbahen nga dhënësi i shërbimit, që kanë të bëjnë me abonuesit e shërbimeve të tij, të ndryshme nga të dhënat e trafikut ose të përmbajtjes, nëpërmjet të cilave ai mund të tregojë:*

*a) tipin e shërbimit të komunikimit të përdorur, kushtet teknike dhe periudhën e shërbimit;*

*b) identitetin e abonentit(ave), adresën gjeografike apo postare, numrin e telefonit apo numrat e tjerë hyrës, informacion mbi faturat dhe pagesën, të siguruara në bazë të marrëveshjes apo të marrëveshjeve të shërbimit;*

c) çdo informacion tjetër në ambientin e instalimit të pajisjeve të komunikimit, të disponueshme në bazën e marrëveshjes apo të marrëveshjeve të shërbimit[11].

Kemi dhe mekanizmat ndërkombëtarë të bashkëpunimit rajonal dhe global në luftën kundër këtij fenomeni, projekte dhe aktivitete te organizmave rajonalë e ndërkombëtarë, të tilla si Kombet e Bashkuara, Bashkimi Europian, Interpoli, ENISA etj., për luftimin e krimit kibernetikë. Legjislacioni i Bashkimit Evropian përcakton direktivat minimum, nëpërmjet të cilave shtetet anëtare mund të zbatojnë, me anë të ligjit kombëtar, sanksione shtesë kundër sulmeve kibernetike. Instrumenti i parë ligjor

[9] Konventa "Për krimin në fushën e kibernetikës", ratifikuar me ligjin nr. 8888, datë 25.4.2002, f. 553.
[10] Konventa "Për krimin në fushën e kibernetikës", neni 1.

evropian që përfshin krimet kundër sistemeve kompjuterike është Konventa e Këshillit të Evropës mbi "Krimet kibernetike" (2001).

Instrumenti i dytë është paketa ligjore e BE, e cila rregullon çështjet në lidhje me krimet kibernetike. Në këtë paketë përfshihen Vendimi Kornizë i Këshillit (shkurt 2005) mbi sulmet kundër sistemeve të informacionit dhe Direktivat e BE, që mbulojnë fushat e ligjit për mbrojtjen e të dhënave personale (95/46/EC dhe 2002/58/EC); për komunikimet elektronike (2002/58/EC); për ruajtjen e të dhënave (2006/24/EC); për ripërdorimin e informacionit të sektorit publik (2003/98/EC); për shërbimet e shoqërisë së informacionit (2000/31/EC), etj. BE ka ndërtuar një strukturë të posaçme të mbrojtjes kibernetike; "The European Cybercrime Centre[12] e cila u lëshua për herë të parë në janar të vitit 2013. Qendra Europiane e Krimit Kibernetik (EC3). Kjo qendër është vendosur pranë Europol dhe është pika qendrore e BE-së në luftën kundër krimit kibernetik. Strukturat e posaçme të kësaj qendre, kanë për detyrë të kontribuojnë nëpërmjet reagimeve të shpejta në rast të ndodhjes së krimeve *online*. Ajo mbështet shtetet anëtare dhe institucionet e BE-së në ndërtimin e kapaciteteve operacionale dhe analitike për hetime dhe bashkëpunim me partnerët ndërkombëtarë, me qëllim forcimin e ligjit kundër krimit kibernetik në vendet anëtare të EU dhe marrjen e masave për garantimin e sigurisë për të mbrojtur qytetarët evropianë dhe bizneset e tyre nga sulmet kibernetike.

Nisur nga rëndësia që ka mbrojtja *cyber* në sigurinë e NATO-s, në deklaratën e kryetarëve të shteteve dhe të qeverive, pjesëmarrës në Samitin e NATO-s, në Strasburg në 4 prill 2009, krahas të tjerash u theksua se: "Ne mbetemi të angazhuar të fuqizojmë sistemet e komunikimit dhe të informacionit që janë të rëndësisë vendimtare për Aleancën, kundër sulmeve *cyber*, duke qenë se aktorë shtetërorë dhe jo shtetërorë mund të përpiqen të shfrytëzojnë padrejtësisht besimin në rritje të Aleancës dhe aleatëve në këto sisteme[13].

## 3. Siguria kombëtare dhe strategjia kombëtare kundër krimit kibernetik

Krimi kibernetik duke qenë një çështje shumë e rëndësishme duhet të flitet për rëndësinë e mbrojtjes së infrastrukturës kritike të shteteve dhe nevojën e një bashkëpunimi dhe mirëkoordinimi global, me qëllim arritjen e rezultateve sa më të larta. Mekanizmi kryesor që organizatat ndërkombëtare dhe shtetet kanë përcaktuar për mbrojtjen e sigurisë kombëtare kundër sulmeve kibernetike janë strategjitë kombëtare, rajonale dhe ndërkombëtare[14] kundër krimit kibernetik. Kemi strategjinë kundër krimit kibernetik e BE-së[15], draftstrategjia[16] kundër krimit kibernetik e Shqipërisë dhe mekanizma të tjerë të shtetit shqiptar për luftimin e krimit kibernetik dhe mbrojtjen e sigurisë kombëtare[17].

[11] Konventa "Për krimin në fushën e kibernetikës", neni 18 pika 3.
[12] https://www.europol.europa.eu/content/megamenu/european-cybercrime-centre-ec3-1837
[13] Deklarata e Kryetarëve të shteteve dhe të qeverive, pjesëmarrës në Samitin e NATO-s në Strasburg, 4 prill 2009.
[14] http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com
[15] Strategjia kunder krimit kibernetik e BE-se.
[16] *Draft Dokumenti i Politikave për Sigurinë Kibernetike,* Tiranë, ALCIRT, Korrik 2014
[17] Raport shpjegues i Konventës së Këshillit të Europës "Mbi krimin kompjuterik", http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

Por, vetëm ekzistenca e një kuadri ligjor të përshtatshëm nuk është e mjaftueshme për luftimin e kriminalitetit, në rastin konkret të krimit kibernetik. Nevojitet gjithashtu edhe zbatimi efektiv në praktikë i këtij kuadri ligjor. Për arritjen e këtij qëllimi, është i nevojshëm krijimi apo përmirësimi i mekanizmave kundër krimit kibernetik, aktivizimi i të gjithë aktorëve të prekur nga fenomeni i krimit kibernetik në luftimin e këtij fenomeni, rritja e ndërgjegjësimit të popullsisë dhe qeverisë së vendit mbi rreziqet nga të cilat cenohet, si dhe rritja e bashkëpunimit rajonal dhe global në fushën e luftimit kundër krimit kibernetik.

Qeveria duhet të rrisë bashkëpunimin me ISP-ve dhe duhet të rrisë numrin e fushatave për rritjen e ndërgjegjësimit, në lidhje me rreziqet e internetit dhe të sigurisë në internet. Shqipëria ka qenë gjithmonë më e preokupuar me çështje urgjente të tilla, si: varfëria, paqëndrueshmëria politike dhe krimet tradicionale të tilla, si vrasjet dhe vjedhjet dhe lufta kundër krimit kompjuterik është lënë pas dore. Por, kohët e fundit qeveria shqiptare ka bërë një pikë kthese dhe i ka kushtuar më shumë vëmendje veprimtarisë kriminale në hapësirën kibernetike, duke implementuar dispozita të reja ligjore dhe duke marrë masa të reja të mbrojtëse. Gjykatësi norvegjez, Stein Schjolberg, në konferencën e organizuar nga Interpol, mbi krimin kibernetik, hedh idenë e ngritjes së një Gjykate Penale Ndërkombëtare për krimet kibernetike si një domosdoshmëri për luftën kundër këtij krimi[18]:

"*Në mungesën e tanishme të bashkëpunimit gjyqësor mes vendeve botërore, është e nevojshme të krijohet një gjykatë e për Cyberspace, për të mundësuar drejtësi globale për të marrë masa për sulme globale kibernetike. Paqja dhe drejtësia në hapësirën kibernetike duhet të mbrohen nga e drejta ndërkombëtare përmes një traktati ose një grupi traktatesh nën Kombet e Bashkuara. Kjo mund të sigurohet duke zgjeruar juridiksionin e Gjykatës Ndërkombëtare Penale. Por, duke pasur parasysh pozicionet e ratifikimit për Gjykatën Ndërkombëtare Penale, çdo zgjidhje që mund të përfshijnë pranimin nga Kina, Rusia dhe Shtetet e Bashkuara, duhet sot të jetë i kufizuar në një Tribunal ndërkombëtar*".

Në referencë të sa më sipër shumë akademik mendojnë se domosdoshmëria e një traktati ndërkombëtar në luftën kundër krimit kibernetik është një thirrje në emër të mbrojtjes së sigurisë globale. Kjo thirrje është një legjitimim i faktit se të njëjtat të drejta që njerëzit kanë në botën reale ose siç mund ta quajmë në kontekst të këtij punimi *offline* ata duhet të kenë edhe në botën virtuale kur gjenden *online*, dhe kjo thirrje është në përputhje me nenin 19 të Deklaratës Universale të së Drejtave të Njeriut dhe Konventën Ndërkombëtare mbi të Drejtat Civile dhe Politike[19].

## 4. Konkluzione

*1. Krimi informatik (Cybercrime)* , është një e keqe e vazhdueshme ndërkombëtare që kapërcen kufijtë kombëtarë, në një mënyrë që e bën këtë formë të krimit të organizuar një shqetësim global.

*2. Krimi informatik* mund të shfaqet në forma të ndryshme, përfshi mashtrimin *online*, vjedhjen dhe terrorizmin kompjuterik. Tashmë një nga arsyet kryesore që lehtësojnë kryerjen e këtij krimi të tillë është globalizimi i teknologjisë dhe përparimet revolucionare të Teknologjisë së Komunikimit dhe Informacionit dhe (TKI), duke

[19] Deklarata Universale e së Drejtave të Njeriut, neni 9.

ndikuar kështu mbi aktivitetin kriminal. Mjetet dhe pajisjet elektronike dhe kompjuterike po përdoren gjithnjë e më shumë për kryerjen e krimeve. Përhapja e shpejtë dhe në rritje e përdorimit të teknologjisë. si ndihmë në kryerjen e aktivitetit kriminal dhe krimit kompjuterik. Meritojnë më tepër vëmendje duke i dhënë prioritet miratimit dhe marrjes së masave të përshtatshme ligjore dhe implementimit të mjeteve efektive teknologjike dhe shtërnguese, që reduktojnë aktivitetin kriminal kompjuterik.

*3. Tendencat aktuale tregojnë se në të ardhmen, krimi kompjuterik* do të zërë vend si objekt kryesor në zbatimin e politikave globale për luftimin dhe parandalimin e kësaj forme të organizuar krimi, përmes shkëmbimit të informacionit, rritjes së shkallës së intelektit human, koordinimit të përpjekjeve ligjore në nivele kombëtare, rajonale dhe ndërkombëtare, si dhe krijimit të një rrjeti botëror në nivel të lartë të bashkëpunimit mes agjencive dhe institucioneve të zbatimit të ligjit.

## Bibliografia


1. Kushtetuta e Republikës së Shqipërisë.
2. Ligji nr. 7895, dt. 27.1.1995 "Kodi Penal i Republikës së Shqipërisë", i ndryshuar.
3. Ligji nr. 8888, dt. 25.4.2002 "Për ratifikimin e Konventës për Krimin në fushën e Kibernetikës".
4. Ligji nr. 7905, datë 21.3.1995 "Kodi i Procedurës Penale i Republikës së Shqipërisë", i ndryshuar.
5. Elezi. I, *E drejta penale* (Pjesa e posaçme), Botimet Erik, Tiranë 2013.
6. Elezi. I, Kaçupi. S, Haxhia. M, *Komentari i Kodit Penal të RSH* (Pjesa e përgjithshme), Tiranë 2013.
7. Drazen Dragiçeviq: *Kompjuterski kriminalitet i informacijski sustavi*, Zagreb, 1999.
8. Wiliam S. Sessions, *Kompjuterski kriminal trend koji eskalira*, Prirucnik, nr.3/91, Zagreb, cituar në: V. Latifit, *Kriminalistika*, 2000.
9. UN, *Doracaku: International review of criminal policy*, *UN Manual on the prevencion and control of computer related crime*.
10. *Draft Dokumenti i Politikave për Sigurinë Kibernetike,* Tiranë, ALCIRT, 2014.
11. EU, Raport shpjegues i Konventës së Këshillit të Europës, "Mbi krimin kompjuterik", http://conventions.coe.int/Treaty/en/Reports/Html/185.htm
12. Deklarata e Kryetarëve të shteteve dhe të qeverive, pjesëmarrës në Samitin e NATO-s në Strasburg.


AKADEMIA E SIGURISË
AS
1971

# Biznesi shqiptar dhe menaxhimi i rrezikut të informacionit financiar të kompjuterizuar.

## Rasti i programit financiar kompjuterik, "Financa 5"

■**Dr. Petrit PERHATI**
*Kolegji ISPE, Prishtinë*
*pperhati@hotmail.com*

**Abstrakt**

*Bota po përjeton një zhvillim të vrullshëm te komunikimit masiv, në një hapësire kibernetike virtuale, e cila po i përball gjithnjë e më shumë në mënyrë progresive, agjencitë e specializuara, ligjzbatuese dhe strukturat e luftës ndaj krimit me një problematikë të re te krimit kompjuterik dhe kërcënimit kibernetik. Sigurisht që sulmeve të këtij lloj krimi të sofistikuar nuk mund ti shpëtoje as informacioni financiar apo kontabël i kompjuterizuar, që qarkullon në hapësirën ekonomike shqiptare. Informacioni financiar i kompjuterizuar është bërë elementi i pashmangshëm dhe vendimtar në procesin e analizës dhe të vendimmarrjes së bizneseve. Organizatat e sotme të biznesit zotërojnë informacione të shumta, të cilat qarkullojnë në mënyrë të kompjuterizuar, pra janë gjithmonë e më tepër nën kërcënimin kibernetik. Studimi im do të përqendrohet në një vrojtim pilot në studimin e qëndrimit të organizatave të biznesit shqiptar në aspektin e menaxhimit të riskut të informacionit financiar të kompjuterizuar, duke marrë si rast vrojtimin e përdorimit dhe administrimin nga operatoret ekonomike në Tirane, të programit financiar kompjuterik Financa 5. Ky studim, në formën e një vrojtimi të thjeshtë synon të zbulojë ndërvarësinë e rrezikut kompjuterik të informacionit financiar-kontabël, dhe të faktorëve kryesorë që ndikojnë ne cilësinë e mbrojtjes së këtij informacioni, nga krimi i sofistikuar kompjuterik dhe kërcënimi kibernetik, duke marrë si rast një grup operatorësh ekonomikë, në Tiranë, përdorues të programit financiar kompjuterik Financa 5. Do të merren në konsideratë faktorë të tillë si: siguria e programit të ofruar, mjedisi i brendshëm, niveli arsimor dhe profesional i personelit që administron informacionin financiar të kompjuterizuar, dhe të personelit të IT-së. Objektivi i këtij studimi është të sjellë fakte lidhur me perceptimet e ndërlidhura me faktorët që ndikojnë në rritjen e cilësisë së mbrojtjes kibernetike të informacionit. Hulumtimi do jetë përshkrues dhe shpjegues në lidhje me variabëlit me qëllimin që të ndërtojë një tablo të thjeshtë të sistemit të mbrojtjes së informacionit financiar të kompjuterizuar, që aplikon organizata e biznesit. Ky studim synon të japë edhe rekomandime praktike që lindin bazuar në gjetjet e studimit.*

**Fjalëkyçe:**
**krim kompjuterik, informacion financiar i kompjuterizuar, terrorizëm kibernetik, Financa 5, operator kontabël, personel IT.**

## 1. Hyrja

Zhvillimet e fundit në hapësirën ekonomike globale, rritja dhe përdorimi i teknologjive të komunikimit dhe informacionit, po shoqërohen paralelisht nga rritja e gjithnjë e më tepër e aktiviteteve kriminale-kibernetike. Interneti gjithnjë e më shumë po përdoret si mjet në duart e krimit të organizuar dhe terrorizmit. Për shkak të fenomenit të pashmangshëm të globalizimit, sigurisht edhe ekonomia shqiptare është bërë pjesë e këtij zinxhiri ekonomik global, e për rrjedhojë është vënë edhe përballë rrezikut të krimit kompjuterik Papërshtatshmëria e ligjeve aktuale apo mungesa e tyre, për të vepruar mbi format e reja të aktiviteteve antishoqërore, si krimet kompjuterike, si dhe mangësitë e ligjeve ekzistuese penale në këtë drejtim, krijojnë një sfidë permanente për të gjithë ligjvënësit e botës. Nga ana tjetër, shkelësit kanë aftësinë për të shfrytëzuar boshllëqet e ligjeve të vendeve të tyre, por edhe të tjera, për të viktimizuar qytetarët, duke mbetur kështu pa u ndëshkuar. Në këtë kuptim, krimi kompjuterik është një krim global. Duke e parë situatën e krimit kompjuterik në kontekstin dhe në optikën e zhvillimeve në Shqipëri, lind nevoja e ndërgjegjësimit të organeve ligjzbatuese dhe theksimit të marrjes së masave permanente, për mbrojtjen nga ky lloj krimi, i cili për vetë natyrën e sofistikuar që ka, kërkon një rritje të kualifikimit dhe të cilësisë së mjeteve dhe të aktorëve që luftojnë këto lloj krimesh.

### *1.1 Metodologjia*

Megjithëse treguesit e përftuar nëpërmjet perceptimeve mund të na shërbejnë ne funksion të qëllimit të këtij studimi, për të rritur ndjeshmërinë dhe ndërgjegjësimin për

rrezikun eventual dhe permanent të krimit kompjuterik, për hartimin, mobilizimin dhe mbështetjen e politikave të mbrojtjes dhe sigurisë kibernetike, nëpërmjet këtij studimi nuk mund të sigurojmë të dhëna të mjaftueshme dhe të nevojshme që të na japin përmasat e përhapjes së këtij lloj krimi në ekonominë e vendit tonë. Por, për të tentuar në një vlerësim në lidhje me përmasat e përhapjes së këtyre lloj krimesh kompjuterike, në veçanti në fushën e të dhënave financiare dhe kontabël të kompjuterizuara, që prek sektorin e biznesit, duke u fokusuar te treguesit e bazuar tek perceptimi, kemi organizuar një vrojtim i cili ka tentuar të mase këtë fenomen dhe ndikimin e faktorëve kryesorë ndaj përhapjes së krimit kompjuterik në sektorin e biznesit, ku si mostër është marrë një grup operatorësh ekonomikë në Tiranë, që janë përdorues të programit financiar kompjuterik *Financa 5*.

Për të finalizuar këtë studim, ne jemi mbështetur në anketime nëpërmjet pyetësorëve të shpërndarë më parë, në intervista të drejtpërdrejta me specialistë të IT, si dhe, në sondazhet e bëra më përpara. Pra, objektivi i këtij studimi, ka qenë që nëpërmjet organizimit të këtij lloj vrojtimi, të mblidhen të dhënat të cilat janë analizuar dhe përpunuar për të prodhuar vlerësime sa me reale, të bazuara në të dhenë faktike, me qëllim që të vlerësohet marrëdhënia që ekziston, ndërmjet sigurisë së informacionit financiar të kompjuterizuar, dhe rolit që ka cilësia e programit kompjuterik të ofruar, mjedisi i brendshëm dhe niveli profesional i stafit të financiereve dhe specialistëve të IT-së, që operojnë me programin *Financa 5*.

Ndikimi i këtyre faktorëve në rrezikun e informacionit financiar të kompjuterizuar, është vlerësuar, duke i konsideruar ata si të pandryshueshëm. Të dhënat e përftuara nga vrojtimi janë analizuar dhe përpunuar me kujdes, dhe mbi bazën e rezultateve të nxjerra, është arritur në përfundime dhe rekomandime. Mendojmë që ky studim është një material modest, për tu përdorur nga organizatat e biznesit dhe nga institucionet financiare, në lidhje me ndërgjegjësimin për rrezikun e krimit kompjuterik, më qëllim që të dhënat financiare që qarkullojnë në sistemin elektronik, të jenë sa më të sigurta.

### *1.2 Kufizimet e studimit*

Për vetë natyrën e këtij lloj krimi, format e përshfaqjes dhe aktorët që i kryejnë, është shumë i vështirë identifikimi i rasteve dhe përpilimi i statistikave të këtij lloji, për efekte njohje apo krahasimi, të fenomenit. Kështu që në të vërtetë, nuk ka statistika të sakta mbi frekuencën e krimit kompjuterik, apo përmasave të humbjeve. Vetëm nëse do të ketë statistika të sakta mbi krimin kompjuterik, duke shtuar dhe ndihmën nga ekspertët financiarë dhe ato në fushën e ligjit, mund të flasim për një vlerësim real të rrezikut. Fatkeqësisht, sondazhet e pakta të kryera në këtë fushë janë bërë nga individë që nuk e njohin mirë fenomenin e krimit kompjuterik.

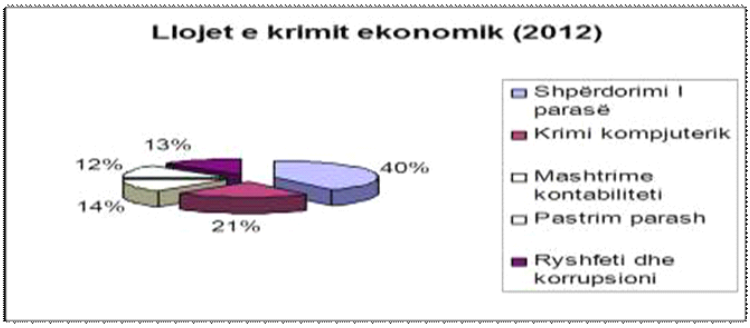
Çdo pjesëtar i sondazhit ka një përkufizim të ndryshëm për këtë lloj krimi dhe mund të mos kenë njohuritë e duhura, për atë që ndodh aktualisht, si ndodh, apo se cilat janë humbjet reale. Një nga faktorët që vështirëson mbledhjen dhe krahasimin e statistikave të këtyre krimeve, ka të bëjë me faktin e natyrës ndërkombëtare të këtyre krimeve, nga vendi kryerës, apo në të cilin ka efekte, ku të paktën, dy shtete rrezikojnë të dublojnë raportimin ose mos të raportojnë si duhet.

## 2. Krimi kompjuterik në kontekstin shqiptar

Nuk ka shumë studime apo statistika në lidhje me krimin kompjuterik në përgjithësi,

në Shqipëri, si dhe të dhëna apo statistika në lidhje me krimin kompjuterik, në ekonominë shqiptare, por nga një studim i kryer në vitet e fundit, për krimin ekonomik dhe korrupsionin, rezulton se në sektorin financiar në Shqipëri, krimet më të përhapura ekonomike janë: krimi kompjuterik, pastrimi i parave, mashtrimet nëpërmjet kontabilitetit, ryshfeti dhe korrupsioni, si dhe, shpërdorimi i parasë.

**Fig.1.**




**Burimi: http://www.kolegjiglobus.com/wp-content/uploads/2017/10/Conferevce-VII-15.pdf**

Nga këto, krimi kompjuterik përfshin rreth 21% të sektorit financiar. Institucionet financiare e kanë nën kontroll informacionin për klientët e tyre por përsëri ka hapësira për abuzime. Nga studimi, kompanitë e shohin këtë krim si një kërcënim të jashtëm. Pra siç shihet nga studimi, rastet e llojeve të krimeve kompjuterike, në strukturën e krimit ekonomik janë të konsiderueshme dhe për këtë duhet te rritet vëmendja për të marrë masa për mbrojtjen nga ky rrezik.

Gjithashtu, është vërejtur nga organizmat ndërkombëtare dhe specialiste të ligjeve se aktualisht, në Shqipëri, ka një mungesë serioze të kornizës ligjore mbi këto lloj krimesh. Herën e fundit që krimet kompjuterike u futën në legjislacionin shqiptar ishte viti 2001. Që prej asaj kohe, me dhjetëra vepra, të cilat ligji ynë nuk i parashikon, konsumohen në Shqipëri. Në Kodin Penal shqiptar, nuk parashikohen disa dhjetëra vepra penale të Konventës Europiane, e cila veç të gjitha llojeve të krimit kompjuterik, lejon edhe ekstradimin për disa nga shkeljet.

Po kështu sipas raportit të Prokurorit të Përgjithshëm, për vitin 2017, kemi të dhënat e mëposhtme në lidhje me rastet e evidentimit të krimit kompjuterik:

*Mashtrimi kompjuterik*: pesha specifike që zë kjo vepër penale në grupin e veprave penale "Kundër krimit kompjuterik" për vitin 2017 është 52 %, ndërsa për vitin 2016 ka qenë 35%. Nga të dhënat statistikore vërehet tendenca në rritje e procedimeve të regjistruara për veprën penale të parashikuar nga neni 143/b i Kodit Penal "Mashtrimi kompjuterik" në vitin 2017, prej 43% në krahasim me vitin 2016. Nga të dhënat vërehet se Prokuroria e Shkallës së Parë, Tiranë, ka regjistruar numrin më të madh të procedimeve për këtë vepër penale, 46 procedime duke përbërë 63 % të totalit të procedimeve të regjistruara në shkallë vendi.

*Falsifikimi kompjuterik*: pesha specifike që zë kjo vepër penale në grupin e veprave penale "Kundër krimit kompjuterik" është 11,4% për vitin 2017, ndërkohë që në vitin 2016 ka qenë 15,8%. Nga të dhënat statistikore në vitin 2017 vërehet tendenca në ulje e procedimeve të regjistruara për veprën penale të parashikuar nga neni 186/a i Kodit Penal "Falsifikimi kompjuterik", me 30,4% krahasuar me procedimet penale të

regjistruara në vitin 2016.

*Ndërhyrja në të dhënat kompjuterike*: pesha specifike që zë kjo vepër penale në grupin e veprave penale "Kundër krimit kompjuterik" është 23,6% për vitin 2017, ndërkohë që në vitin 2016 ka qenë 43,8%. Nga të dhënat statistikore vërehet tendenca në ulje e procedimeve të regjistruara në vitin 2017 për veprën penale të parashikuar nga neni 293/b i Kodit Penal "Ndërhyrja në të dhënat kompjuterike", me 48,4% krahasuar me procedimet penale të regjistruara në vitin 2016[1].

## 3. Disa koncepte bazë

Meqenëse ky studim fokusohet në vlerësimin e qëndrimit të organizatave të biznesit shqiptar në aspektin e menaxhimit të riskut të informacionit financiar të kompjuterizuar, duke marrë si rast vrojtimin e përdorimit dhe administrimin nga operatorët ekonomikë në Tiranë, të programit financiar kompjuterik *Financa 5*, është e nevojshme të qartësojmë në mënyrë të përmbledhur kuptimin e disa nocioneve bazë që do të përdoren në këtë punim.

### *3.1 Informacioni financiar i kompjuterizuar*

Për kuptimin e nocionit "informacioni financiar i kompjuterizuar ose i informatizuar", paraprakisht duhet të kemi një qasje të qartë se çfarë kuptojmë me informacion financiar (kontabël), duke nënkuptuar një tërësi të dhënash kontabël dhe financiare, që formojnë atë që quhet sistem i informacionit financiar (kontabël). Ka shume autorë të huaj dhe vendas që kanë dhënë përkufizime në lidhje me sistemin e informacionit financiar (kontabël), por në përgjithësi pjesa më e madhe e tyre e vënë theksin tek roli që luan sistemi i informacionit financiar (kontabël) në procesin e vendimmarrjes. Disa autorë të tjerë e vënë theksin tek qëllimi i këtij sistemi, të tjerë tek elementet përbërës, por për efekt të kontekstit dhe llojit të studimit, do të japim disa nga përkufizimet me kryesore. Sipas (Simkin M, Bagranoff N, Norman C, 2005, f. 45) " Sistemi i informacionit kontabël është një mbledhje e të dhënave dhe procedurave të përpunimit, që krijon informacion të nevojshëm për përdoruesit e tij".

"Sistemi i informacionit kontabël (sipas Konferencës së Romës, shtator 2012), është një sistem kompleks, i përbërë nga elemente të ndërlidhura në mënyrë rigoroze të tilla, si të dhëna informacioni, burimet njerëzore, mjete IT, modele dhe procedura kontabël, që përfshijnë në thelb mbledhjen, klasifikimin, përpunimin, regjistrimin dhe ruajtjen e të dhënave te kontabilitetit".

Sistemi i informacionit kontabël është quajtur një sistem informacioni që shërben për mbledhjen, përpunimin dhe komunikimin e të dhënave, me qëllim raportimin dhe realizimin e proceseve të marrjes së vendimeve sa me optimale, në përputhje me qëllimet dhe objektivat kryesore të njësisë ekonomike (Lati-Naco, 2010, f. 43). Sipas (Binaj A., 2012), "një sistem i informacionit kontabël është një sistem që mbledh, regjistron, ruan dhe proceson të dhëna për të prodhuar informacion për vendimmarrësit". Po ky autor, thotë që: "Një sistemi i informacionit kontabël është një grup komponentësh të ndërlidhur, që bashkëpunojnë për të arritur një qëllim" (Binaj A., 2012).

Në të gjitha përkufizimet e dhëna nga autorë të ndryshëm vendas dhe të huaj, në lidhje me sistemin e informacionit financiar, ajo që i bashkon është rëndësia dhe roli

[1] https://www.vizionplus.tv/kujdes-nga-krimi-kompjuterik/

determinant që ka ky informacion për marrjen e vendimeve nga udhëheqja e organizatave të biznesit, që në kushtet kur ky informacion administrohet në mënyrë të kompjuterizuar, nënkupton në të njëjtën kohë kujdesin dhe vëmendjen e vazhdueshme që duhet të kenë në mënyrë permanente, subjektet e ngarkuara për ruajtjen mirë, administrimin dhe mbrojtjen e këtij informacioni nga sulmet kibernetike, që po bëhen gjithnjë e më tepër evidente, në kushtet e një ekonomie që po bëhet gjithnjë e më shumë globale.

### *3.2. Aplikimet në "hardware" dhe "software"*

- *Softueri* (anglisht: *software*) quhet bashkësia e programeve kompjuterike dhe të dhënat e tjera që përmbajnë instruksione që i thonë kompjuterit se çfarë duhet të bëjë. Gjithashtu mund të themi se softueri i referohet një apo më shumë programeve kompjuterike dhe të dhënave të ruajtura në memorien e kompjuterit për arsye të caktuara. Programet softuer kryejnë funksionin e programit, ose duke i dhënë instruksione të drejtpërdrejta harduerit të kompjuterit, ose duke shërbyer si *input* për programe të tjera. Termi *softuer* ka lindur si kontrast i termit të vjetër *harduer* (që do të thotë pajisje fizike). Ndryshe nga hardueri, softueri nuk preket ose të shikohet fizikisht. Softueri në përgjithësi, ndahet në dy grupe:

*Softueri sistemor (sistemi operativ).* Një sistem operativ mund të ndahet në dy shtresa:

1. Shtresa e kontrollit, e cila është e padukshme për shfrytëzuesin.

2. Shtresa bashkëvepruese: paraqet një bashkësi së të gjithë programeve që bashkëveprojnë me shfrytëzuesin dhe është e ndërtuar në shtresën e parë. Kompjuterët personalë mund të punojnë me disa sisteme operative, siç janë:

MS-DOS (*Microsoft Disk Operating System*), Windows 95 dhe 98, S\2 (Sistemi operativ 2), *Windows* XP, Windows 7, *Windows* 8 dhe 8.1, *Windows* 10 (i fundit)[2].

- *Hardueri* (anglisht: *hardware)*: përfshin çdo pajisje që është e lidhur në kompjuterin dhe që kontrollohet nga mikroprocesori. Ky, përfshin pajisjen që është lidhur në kompjuter kur ai u prodhua, si edhe pajisjen periferike e cila i shtohet pastaj. Pajisjet mund të lidhen me kompjuterin në disa mënyra të ndryshme. Disa pajisje, si përshtatësit e rrjetit dhe kartat e zërit, janë lidhur në çarjet e zgjerimit, brenda kompjuterit. Pajisjet e tjera, si printerët dhe skanerët, janë lidhur në porta jashtë kompjuterit. Që një pajisje të punojë si duhet me *Windows*, në kompjuter duhet të instalohet softueri i njohur si drejtues i pajisjes. Çdo pajisje mbështetet nga një ose më shumë drejtues pajisjesh, të cilat janë furnizuar në mënyrë tipike nga prodhuesi i pajisjes. Disa drejtues pajisjesh përfshihen me *Windows*-in. Kjo do të thotë që *Windows*-i mund ta zbulojë atë automatikisht dhe të instalojë drejtuesit e duhur të pajisjeve. Nëse pajisja nuk është instaluar nga *Windows*-i, eksperti për gjetjen e harduerit të ri do të shfaqet dhe do të pyesë për të ndërfutur ndonjë disk kompakt ose ndonjë disketë të siguruar bashkë me pajisjen[3].

### *3.3 Inteligjenca artificiale*

Inteligjenca artificiale (IA) i referohet aftësisë së një kompjuteri për të kryer funksione dhe arsyetime që aktualisht janë tipike vetëm të mendjes njerëzore. Shpesh termi i

[2] https://sq.wikipedia.org/wiki/Software
[3] https://sq.wikipedia.org/wiki/Harduer_kompjuterik

referohet edhe degës së shkencës kompjuterike që ka për qëllim krijimin e saj. Tekstet e librave e përkufizojnë këtë fushë si: "studimi dhe krijimi i agjentëve inteligjent", ku një agjent inteligjent, është një sistem që e percepton mjedisin e tij dhe merr masa për të maksimizuar shanset e tij për sukses. John McCarthy, i cili solli termin më 1956, e përkufizon si "shkenca dhe inxhinieria e bërjes së makinave inteligjente".

Fusha u themelua mbi pohimin se një veti qendrore e njerëzve, inteligjenca (urtësia e njeriut) mund të përshkruhet me hollësi të mjaftueshme sa të mund të simulohet nga një makinë. Kjo ngre çështje filozofike për natyrën e mendjes dhe etikën e krijimit të qenieve artificiale, çështje të cilat janë trajtuar nga miti, trillimi dhe filozofia që në lashtësi. Kërkuesit e hershëm të inteligjencës artificiale kanë zhvilluar algoritme që imitojnë hap-pas-hapi arsyeshmërinë që njerëzit e përdorin kur duan të zgjidhin mistere ose të japin përfundime logjike.

Për probleme të vështira, shumica e algoritmeve mund të kërkojnë burime të panumërta kompjuterike – përvoja me një "eksplodim kombinatorik": një sasi e memories ose kohës së kërkuar të kompjuterit bëhet astronomike kur problemet shkojnë pas madhësisë së paracaktuar. Kërkimi për më shumë algoritme për zgjidhjen e problemeve është një prioritet i lartë për hulumtuesit e IA-ve.

Qeniet njerëzore zgjidhin shumicën e problemeve të tyre duke përdorur gjykime të shpejta, intuitive më shumë se me ndërgjegje, përfundim hap-pas-hapi që hulumtuesit e hershëm të IA-ve ishin të gjendje të modelonin. IA-të kanë shënuar progres në imitimin e këtij lloji të zgjidhjes së problemeve: agjentët e mishëruar theksojnë rëndësinë e aftësive sensorimotorike të arsyetimit të lartë; rrjeti nervor kërkon përpjekje për të simuluar strukturën brenda trurit që i jep rritje kësaj aftësia; qasjet statistikore të IA-ve imitojnë natyrën probabilistike të aftësive njerëzore për të menduar[4].

### *3.4 Kuptimi i konceptit të "Cybercrime" (krimi kompjuterik)*

Përgjithësisht, kompjuterët, në krime mund të shërbejnë si objekte, subjekte, dhe mjete. Janë objekte të krimeve, kur ata sabotohen ose vidhen. Në shumë raste, kompjuterët janë goditur, djegur, janë nxjerrë jashtë përdorimit me instrumente të caktuar. Dëmet, në kësi rastesh, mund të jenë ndërkombëtare dhe të rënda, si p.sh. dëmtimi i qëllimshëm i një infrastrukture financiare ose, padashur.

Janë në rolin e subjekteve, kur ata janë mjediset në të cilat zbatimet teknologjike kryejnë krime. Në këtë kategori përfshihen p.sh., sulmet me viruse kompjuterike. Kur ndodhin krime kompjuterike, kompjuterët mund të jenë dhe subjekt i sulmeve. Roli i tretë i kompjuterëve në krime është përdorimi i tyre si mjet për të prodhuar informacion të rremë, apo që planifikojnë dhe kontrollojnë krime, të cilat mund të kryhen në një ardhme. Sipas disa përcaktimeve ndërkombëtare, termi krim kompjuterik, është i ndarë në dy kategori:

a) në një kuptim të ngushtë, me krim kompjuterik, do të kuptohet çdo sjellje e kryer nëpërmjet veprimeve elektronike, të cilat drejtohen ndaj sigurisë së sistemeve kompjuterike dhe të dhënave të përpunuara prej tyre;

b) në një kuptim më të gjerë, me krim kompjuterik, do të kuptohet çdo sjellje e paligjshme, e kryer nga mënyra apo nëpërmjet një kompjuteri apo sistem kompjuterik, përfshirë krime të tilla si, përpunimi i paligjshëm, ofrimi apo shpërndarja e informacionit nga një kompjuter apo rrjet, për të abuzuar dhe tërhequr vëmendjen me forma të tilla

[4] https://sq.wikipedia.org/wiki/Inteligjenca_artificiale

si ato për përkrahje të grupeve p.sh terroriste, neonaziste, pornografia dhe pedofilia. Këtu do të përfshihen edhe llojet e krimeve të mashtrimeve, duke shkelur sigurinë e rrjeteve si, bixhozi i paligjshëm, skemat piramidale, mashtrimi me karta krediti dhe lloje të tjera të aktiviteteve të paligjshme. Në *cybercrime*, komponenti "cyber", zakonisht i referohet për të kualifikuar shkeljet e reja, të mundësuara nga teknologjia e informacionit, apo ndërveprimi të hapësirës kompjuterike, në shumë aktivitete tradicionale[5].

### *3.5 Siguria e informacionit (*InfoSec - Information security*)*

Dy aspektet më të mëdha të sigurisë së informacionit janë:

- *Siguria e IT*: Ndonjëherë i referohemi si siguria kompjuterike, siguria e teknologjisë së informacionit është siguria e informacionit e aplikuar në teknologji (shpeshherë si formë e sistemit të kompjuterit). Është e vlefshme të shënohet se me kompjuterët nuk do të thotë domosdoshmërish një *Desktop* shtëpie. Një kompjuter është çdo pajisje me *një njësi qendrore procesuese* dhe disa memorie (madje dhe një llogaritës). Specialistet e sigurisë së IT janë pothuajse gjithmonë të gjendura, në çdo ndërmarrje të madhe, për shkak të natyrës dhe vlerës së të dhënave brenda bizneseve të mëdha. Ata janë përgjegjës për mbajtjen e të gjithë teknologjinë brenda sigurisë së kompanisë nga sulmet kibernetike dashakeqe që shpesh përpiqen të shkelin informacion privat kritik apo për të fituar kontroll në sistemet e brendshme.

- *Siguria e informacionit*: akti i sigurimit, së të dhënave që nuk kanë humbur, kur lindin çështjet kritike. Këto çështje përfshijnë, por nuk kufizohen vetëm në: fatkeqësitë natyrore, mosfunksionim i kompjuterit/serverit,vjedhja fizike, ose ndonjë shembull tjetër, ku të dhënat kanë potencialin për të qenë të humbura. Meqenëse informacioni në epokën tonë moderne, është i ruajtur në shumicën e kompjuterëve të sigurimit të informacionit është trajtuar në mënyrë tipike me nga specialistët e sigurisë (IT). Një nga metodat më të zakonshme për të pasur siguri të informacionit është që të kemi një *backup off-site* së të dhënave, në rast se lindin një nga çështjet e përmendura me lart[6].

## 4. Biznesi shqiptar përballë rrezikut të krimit kompjuterik

Edhe në Shqipëri, me futjen në përdorim të programeve financiare të kompjuterizuara, të dhënat financiare dhe kontabël të bizneseve administrohen nëpërmjet programeve të caktuara kompjuterike, programe të cilat janë të ekspozuara ndaj krimit kompjuterik Në këtë kuptim edhe ky studim është fokusuar në menaxhimin e riskut nga bizneset shqiptare së të dhënave financiare të kompjuterizuara. Aktualisht në Shqipëri, programet kryesore financiare kompjuterike që përdoren nga operatorët ekonomikë, publikë ose jopublikë, janë tre: programi *Financa 5*, programet *Alfa* dhe programi *Bilanc*.

Për të vlerësuar sesi biznesi shqiptar reagon përballë rrezikut kompjuterik, në aspektin e ruajtjes së të dhënave financiare-kontabël të kompjuterizuara, unë kam bërë një studim në formën e një vrojtimi pilot, në një fashë operatoresh ekonomikë që operojnë në Tiranë, që janë përdorues të programit financiar të kompjuterizuar të quajtur *Financa 5,* program i cili ofron shërbim të kompjuterizuar për menaxhimin

[5] https://sq.wikipedia.org/wiki/Krimi_kompjuterik
[6] https://sq.wikipedia.org/wiki/Siguria_e_informacionit

financiar dhe mbajtjen e kontabilitetit. *Financa 5* është një zgjedhje cilësore. Programi u shërben të gjithë operatorëve të biznesit sipas funksioneve që ata kryejnë në kompani si: magazina, blerje, shitje, arka, banka deri tek nivelet më të larta të vendimmarrjes. Organizimi i punës me programin funksionon me module. Në çdo modul të drejtat e përdorimit të sistemit kufizohen ose lejohen sipas funksionit që kryen çdo operator në program.

Në versionin e fundit të *Financa 5*, administrimi i të drejtave të përdoruesve vjen në nivel më të avancuar. Kompania që ofron këtë program është *Infosoft Software Developer* (ISD), e cila është themeluar në 1991, si kompania e parë private që operon në fushën e informatikës financiare dhe shërbimeve IT. ISD ka më shumë se 25 vite përvojë dhe ekspertizë në ofrimin e shërbimeve IT të integruara për financë, kontabilitet, buxhet dhe organizim të burimeve njerëzore për biznese dhe institucione publike. Standardet e kompanisë konfirmohen nga certifikimet ISO / IT Mark / CMMI dhe nga më shumë se 5000 klientë besnikë. Të gjitha bizneset e anketuara, kishin mbi pesë vite që ishin përdorues të programit *Financa 5*.

## 5. Përfundime

- Vrojtimi ynë i organizuar në rajonin e Tiranës, në operatorët ekonomikë që përdorin programin kompjuterik *Financa 5*, evidenton faktin se ka një ndjeshmëri të lartë perceptimi për sa i përket fenomenit të krimit kompjuterik në fushën e të dhënave financiare dhe kontabël dhe përhapjes së tij, në ambientin e biznesit shqiptar.

-Megjithëse rastet e konstatuara të këtij fenomeni konsiderohen të pakta, vrojtimi ynë zbulon se përfaqësuesit e biznesit e konsiderojnë rrezikun e informacionit kontabël dhe financiar, të kompjuterizuar, si rrezik serioz eventual.

- Nga analizimi i të dhënave, të përfituara nga anketimi, rezulton se shumica e specialistëve të financës dhe të kontabilitetit, u shprehen për njohuri jo të mjaftueshme për llojet e krimeve kompjuterike në ekonomi, dhe për specifikat e tyre, ndërsa specialistët e sektorit të IT-së, u shprehën për njohuri të mjaftueshme për krimin kompjuterik.

- Në realitetin e sotëm ekonomik, ku organizatat e biznesit po kthehen gjithnjë e më tepër në firma digjitale, për shkak të përhapjes gjithnjë e më tepër të fenomenit të globalizimit të ekonomisë, suksesi i organizatave të biznesit po krijon ndërvarësi gjithnjë e më shumë nga administrimi dhe ruajtja e informacionit financiar të tyre.

- Miradministrimi dhe sigurimi i informacionit financiar dhe kontabël, të kompjuterizuar, kërkon një kuptim të drejtë të menaxhimit, mirëmbajtjes dhe sigurisë sistemit të teknologjisë së informacionit.

- Në suksesin e përdorimit me efikasitet dhe të sigurt të informacionit financiar të kompjuterizuar, të organizatës së biznesit, merr një rëndësi të dorës së parë përzgjedhja e softuerëve dhe harduerëve, që të sigurojnë një përdorim të sigurt dhe afatgjatë të informacionit financiar të kompjuterizuar.

- Siguria e informacionit financiar të kompjuterizuar është shumë e rëndësishme për vlerësimin e organizatës së biznesit dhe e ndërvarur me performancën financiare të saj.

- Cilësia e internetit dhe shkalla e informatizimit ndikojnë në cilësinë e sigurisë së informacionit financiar të kompjuterizuar.

- Madhësia dhe shtrirja gjeografike e organizatës së biznesit ndikon në rrezikun e

informacionit kontabël dhe financiar të kompjuterizuar.

- Niveli dhe profili profesional i specialistëve të IT-së, ndikon drejtpërdrejtë në menaxhimin e sigurisë kompjuterike të informacionit kontabël dhe financiar.

- Në rrezikun e informacionit kontabël dhe financiar të kompjuterizuar, ka ndikim të rëndësishëm profili profesional dhe arsimor i specialistëve të financë-kontabilitetit, që administrojnë informacionin kontabël dhe financiar, të kompjuterizuar, të organizatës.

- Konsiderohet që sektori financiar, me zhvillimet e shpejta, të shtimit të llojit të shërbimeve të reja bankare dhe financiare, është sektori më i ekspozuar ndaj krimit kompjuterik, i cili mund të shfaqet në të gjitha format e tij, prandaj krimi kompjuterik dhe siguria kompjuterike janë rreziqe që nuk duhen injoruar kurrsesi. Aq më tepër që në dallim nga krimet tradicionale, llojet e krimeve kompjuterike realizohen përmes hapësirave dhe mjeteve kompjuterike, të padukshme, të cilat nuk njohin kufij konvencionalë shtetërorë, pra duke i dhënë përmasa globale.

## 6. Rekomandime

- Drejtuesit e organizatave të biznesit duhet t'i kushtojnë rëndësinë e duhur ruajtjes dhe miradministrimit të informacionit financiar dhe kontabël, të kompjuterizuar, sepse gjithnjë ka nevojë për përmirësim të marrjes së masave efektive dhe të nevojshme, në funksion të mirëmenaxhimit të organizatës.

- Në planet strategjike të drejtuesve të bizneseve, duhet të jenë në plan të parë edhe masat për mbrojtjen dhe sigurinë e informacionit financiar të kompjuterizuar, krijimi i sistemeve mbrojtëse, auditimi i vazhdueshëm i sigurisë kompjuterike.

- Drejtuesit e bizneseve duhet të ndërgjegjësohen për rrezikun gjithnjë më të ndjeshëm të krimit kompjuterik dhe në planet e tyre të drejtimit, duhet të vlerësojnë këtë rrezik, duke parë pse jo edhe mundësinë e ndërgjegjësimit, për një kompromis në radhët e drejtuesve të bizneseve, për nxitjen dhe zhvillimin e nismave të përbashkëta për të kuptuarit e pasojave të dëmshme nga ky lloj krimi, dhe me qellim, kompromisin për një shpërndarje efikase të burimeve njerëzore, financiare dhe teknike, për luftën ndaj krimit të sofistikuar kompjuterik.

- Fokusi i politikave shtetërore, në drejtim të luftës kundër krimit në ekonomi, duhet të përqendrohet në pikat kyçe, të cilat sjellin edhe problemet dhe pengesat për suksesin ndaj këtij fenomeni, që mund të jenë hartimi dhe konsolidimi i politikave të forta kundër krimit kompjuterik, nëpërmjet krijimit të një baze të fortë ligjore të harmonizuar me BE-në, ndërmarrja e reformave te thella në organet ligjzbatuese dhe sektorët që janë të ndjeshëm ndaj këtij lloj krimi, mbështetjes të vazhdueshme teknike, financiare dhe me burime njerëzore të kualifikuara dhe të specializuara ndaj këtyre sektorëve.

## Bibliografi


1. Collis, J., Hussey, R., *Research Methodology*, 2003.
2. Bagranoff, N, A., Simkin, M, G., Norman, C, S., *Core Concept of Accounting Information System*, 2005.
3. Montgomery M., 1992.
4. Georghiou, L., Rossner, D., *Evaluating technology programs: tools and methods*, 2000.
5. Lati, L., Naço, M., *Kontabiliteti i kostos*, Tiranë: 2010.
6. Binaj, A., Limaj, I. (red.), Mero, L. (red.), *Sistemet e teknologjisë së informacionit kontabël : cikël leksionesh*, Tiranë: Ilar, 2012.
7. Konferenca e Romës, shtator 2012.

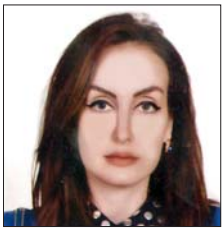
**Burime nga interneti:**

1. http://www.pp.gov.al/web/Raporte_te_Prokurorit_te_Pergjithshem_353_1.php#.W64Q2nszaUl
2. https://sq.wikipedia.org/wiki/Software
3. https://sq.wikipedia.org/wiki/Harduer_kompjuterik
4. https://sq.wikipedia.org/wiki/Inteligjenca_artificiale
5. http://www.isd.com.al
6. http://www.imb.al
7. https://bilanc.com/
8. https://sq.wikipedia.org/wiki/Programi_kompjuterik
9. https://sq.wikipedia.org/wiki/Siguria_e_informacionit
10. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2007_004_001_14837.pdf
11. http://www.kolegjiglobus.com/wp-content/uploads/2017/10/Conferevce-VII-15.pdf
12. http://www.pp.gov.al/web/Raporte_te_Prokurorit_te_Pergjithshem_353_1.php#.W64Q2nszaUl


AKADEMIA E SIGURISË
AS
1971

# Mbrojtja dhe siguria nga krimi kibernetik, në organizata publike dhe private:

## motivet që shtyjnë *hacker*-at, në cenimin e arkivave digjitalë



**MSc. Sheldiana JANO**
*Juriste*
*sheldaagaraj@yahoo.com*

**Abstrakt**

*Ndërsa bota gjithnjë e më shumë bëhet më e varur nga teknologjia dhe rrjetet e ndërlidhura, ato ndryshojnë dinamikën se si funksionon bota. Sektorët publikë përdorin teknologjinë me nivele bashkëkohore të larta, dhe ndoshta më të rëndësishme, në krahasim me ato private. Bazat e të dhënave shtetërore që përmbajnë informacion mbi ADN, shenjat e gishtërinjve, rastet e hapura për këqyrje me teknologjinë e kriminalistikës në terren, digjitalizimi i tyre u lejojnë organeve hetimore të përdorin mjete dhe metoda në mënyrë që informacioni të përthithet shpejt dhe me efikasitet që të zgjidhin rastet sa më shpejt. Ky ndryshim ka krijuar bazën e të dhënave jashtëzakonisht të mëdha dhe të rëndësishme në rrjetet e hapësirës së magazinimit ose arkivat digjitale. Këto informacione nga organizata private dhe publike janë një objektiv shumë tërheqës për sulmuesit e rrjetit kibernetik. Për shkak të sasisë mbresëlënëse të informacionit që mund të merret, edhe duke mos qenë fizikisht në vendin e ngjarjes, këto informacione bëhen prè e një objektivi që është shumë joshës për t'u injoruar. Kjo tezë nuk propozon një teknologji të re për luftimin e përdoruesit keqdashës, por jep një vështrim se kush është në të vërtetë problemi që ka ndërhyrë në prishjen e sistemit dhe çfarë mund të motivojë një hacker për t'i sulmuar këto organizata. Një citim i famshëm është: "Nëse e njihni armikun dhe e njihni veten, nuk duhet të keni frikë rezultatin e një beteje. Nëse e njihni veten, por jo armikun, pas çdo fitoreje bëni që armiku ta vuajë humbjen". Kjo tezë ka për qëllim të ofrojë hulumtime mbi motivet e sulmuesit. Sepse në krimin kompjuterik dhe të sigurisë, prapa sulmuesve elektronikë janë arsyet financiare, mungesa relative e njohjes së ndëshkimit nga ligji.*

**Fjalëkyçe:**
**krimi kibernetik, siguria kombëtare, legjislacioni, hacker, kërcënim kibernetik.**

## 1. Hyrje

Krimi kibernetik është një nga sfidat më të mëdha ligjore. Që nga viti 2000 deri në vitin 2014 interneti është zgjeruar me një normë mesatare prej 741.0% në nivel global, dhe aktualisht rreth 3 miliard njerëz janë *online*[1]. Krimi kibernetik është një aktivitet kriminal që përfshin: infrastrukturën e teknologjisë së informacionit, aksesin e paligjshëm, përgjimin e paligjshëm, ndërhyrjen në të dhëna, falsifikimin dhe mashtrimin elektronik. Hapësira kibernetike sot është një nga sfidat më të mëdha ligjore, e cila ka nxitur një formë tjetër të krimit, duke krijuar një mjedis për metodat e reja të krimit. Tani, pothuajse, të gjitha krimet mund të kryhen me përdorimin e kompjuterëve.

Duke parë rëndësinë aktuale të këtij fenomeni në shkallë globale dhe në shkallë kombëtare, duke pasur parasysh rritjen e shpejtë të krimit kibernetik në Shqipëri, vitet e fundit dhe mungesën e studimeve të mirëfillta në këtë fushë në vendin tonë, vendosa të bëj një kërkim shkencor mbi krimin kibernetik, duke marrë si rast studimor vendin tonë, Shqipërinë. Vendosa ta bëj këtë hulumtim, e nisur edhe nga synimi për të pasuruar literaturën shqiptare mbi këtë fushë, e cila duke qenë shumë e pakët, bën që vendi ynë të vuajë nga mangësia e njohurive të nevojshme mbi krimin kibernetik, duke i zënë kështu qytetarët të papërgatitur e të pambrojtur ndaj këtij fenomeni të ri.

Qëllimi i këtij studimi është analizimi i situatës aktuale në Shqipëri, në lidhje me standardet ligjore, mekanizmat për hetimin dhe ndjekjen penale të krimit kibernetik dhe evidentimin e problematikave dhe sfidave kryesore me të cilat hasen gjyqtarët, prokurorët, policia dhe shteti shqiptar, në parandalimin dhe luftimin e krimit

[1] Shih: Internet Society, Global Internet Report 2015, Mobile evolution and development of the Internet, 2015, f. 9; dhe, Internet Live Stats, e aksesueshme në faqen web, http://www.internetlivestats.com/internet-users/ aksesuar me 22 korrik 2015

kibernetik në Shqipëri.

## 2. Metodologjia

Së pari, kërkimet e kryera janë bazuar në një qasje induktive të temës, pra duke observuar dhe studiuar faktet, të nxirren rezultate në lidhje me situatën e krimit kibernetik në të drejtën shqiptare, dhe me qëllimin për të përcaktuar nëse shteti shqiptar është mjaftueshëm i përgatitur, për të luftuar krimin kibernetik dhe sfidat që ai përbën për sigurinë kombëtare.

Së dyti, studimi i krimit kibernetik, sjell nevojën e përdorimit të një qasjeje krahasuese për organizatat private dhe ato publike. Për të studiuar krimin kibernetik, sidomos për të identifikuar sfidat dhe problematikat që ka shteti shqiptar në këtë drejtim, për të kuptuar nocionin e krimit kibernetik, është parë e nevojshme që t'i drejtohet literaturës së huaj dhe legjislacionit ndërkombëtar.

Së treti, trajtimi i krimit kibernetik në të drejtën shqiptare është interesant, për vetë faktin e mungesës së thellë të studimeve në këtë fushë. Në fakt, duke marrë në konsideratë faktin, që krimi kibernetik në Shqipëri, është një fenomen i ri dhe jashtëzakonisht dinamik.

## 3. Vështrim i përgjithshëm mbi kuptimin e krimit kibernetik dhe shembuj të ndikimit të tij në organizata publike dhe private

Asete të paprekshme, të paraqitura në formate të dhënash, si depozitat e parave, apo orët e punës, janë shënjestrat më të kërkuara për mashtrimet kompjuterike. Bizneset moderne po transferojnë dhënien kesh të parave me depozitat me transaksione, nëpërmjet sistemeve kompjuterike, duke krijuar një terren të përshtatshëm për mashtrimet kompjuterike. Komuniteti i krimit të organizuar ka në shënjestër të tij, informacionet mbi kartat e kreditit, ashtu si dhe informacione personale financiare të klientëve.

Sipas disa përcaktimeve ndërkombëtare, termi krimi kompjuterik, është i ndarë në dy kategori[2] :

a) në një kuptim të ngushtë, me krim kompjuterik do të kuptohet çdo sjellje e kryer nëpërmjet veprimeve elektronike të cilat drejtohen ndaj sigurisë së sistemeve kompjuterike dhe të dhënave të përpunuara prej tyre;

b) në një kuptim më të gjerë, me krim kompjuterik do të kuptohet çdo sjellje e paligjshme e kryer nga mënyra apo nëpërmjet një kompjuteri apo sistem kompjuterik, përfshirë krime të tilla si përpunimi i paligjshëm, ofrimi apo shpërndarja e informacionit nga një kompjuter apo rrjet, për të abuzuar dhe tërhequr vëmendjen me forma të tilla, si ato për përkrahje të grupeve p.sh. terroriste, neonaziste, pornografia dhe pedofilia. Këtu do të përfshihen edhe llojet e krimeve të mashtrimeve, duke shkelur sigurinë e rrjeteve, si: bixhozi i paligjshëm, skemat piramidale, mashtrimi me karta krediti dhe lloje të tjera të aktiviteteve të paligjshme[3].

[2] Aaron Shull, *Global Cybercrime: The Interplay of Politics and Laë, Internet Governance Papers* Paper No. 8 — Qershor 2014, Canada

[3] Akdeniz, Y. Internet Child Pornography and The Law: National and International Responses. Hampshire: Ashgate Publishing, 2008.

### *3.1 Krimet tradicionale dhe krimet kompjuterike*

Në dallim nga krimet tradicionale, krimi kompjuterik është një krim global. Këto lloj krimesh, kryhen përmes hapësirave dhe rrjeteve kompjuterike dhe nuk ndalojnë në kufijtë konvencionale shtetërorë. Rasti "virusi i dashurisë" e ka vërtetuar këtë. Ekspertët shumë shpejt zbuluan virusin që vinte nga Filipinet. Duke përdorur informacionin e marrë prej një *shërbimi shpërndarës* (*service provider*) të internetit, hetuesit e Agjencisë Kombëtare të Hetimit në Filipine dhe ata të FBI-së, identifikuan personat e dyshuar për shpërndarjen e virusit. Megjithatë, pati disa probleme lidhur me hetimin, për shkak të mungesës së ligjeve specifike, kështu që krijimi dhe përhapja e një virusi nuk ishte një krim. Në këtë rast, hetuesit nuk kishin kohën dhe mundësitë e duhura për të hetuar, gjetur prova dhe dënuar autorin.

### *3.2 Qëllimi i fenomenit*

Duke njohur se sa shumë krime mund të kryhen, mund të jemi në gjendje të dimë se sa duhet të shpenzojmë, në lidhje me sigurinë. Përllogaritjet nga ekspertë të sigurisë së rrjeteve, mbi humbjet e përafërta nga krimet kompjuterike, shkojnë nga 555 milionë $ deri në 13 miliardë $, por aktualisht nuk ka statistika të sakta mbi humbjet nga kjo formë krimi, pasi asnjë nuk di sa raste mund të jenë të paraportuara.

### *3.3 Mashtrimet* online[4]

Llojet me të spikatura të mashtrimeve kompjuterike janë:

a) Mashtrimi nëpërmjet manipulimit kompjuterik. Bizneset moderne po transferojnë dhënien kesh të parave me depozitat me transaksione, nëpërmjet sistemeve kompjuterike, duke krijuar një terren të përshtatshëm për mashtrimet kompjuterike.

b)Falsifikimi kompjuterik i firmës dhe falsifikimi i desktopit. Kur një kriminel ndryshon të dhënat e regjistruara në një sistem kompjuterik, krimi i kryer mund të jetë falsifikim. Në këtë rast, sistemi kompjuterik mund të jetë në shënjestër të aktivitetit kriminal.

### *3.4 Modifikimi i të dhënave apo programeve*

Kjo kategori e aktiviteteve kriminale përfshin ato lloj hyrjesh të paautorizuara në një sistem kompjuterik, nëpërmjet përdorimit të *software*-ve prishës. Modifikimi i paautorizuar i të dhënave kompjuterike apo funksioneve, me qëllimin për të fshirë funksionimin normal të sistemit, është një aktivitet i pastër kriminal dhe shpesh lidhet me një sabotim kompjuterik.

Në një rast, një mbikëqyrës i një operacioni kompjuterik në një bankë të *New Jersey*-t, përdori një program për të rritur balancën e llogarive të disa shokëve të tij. Shokët e tij tërhoqën paratë dhe atëherë ai shkatërroi gjurmën e tërheqjes. Plani i tij ishte të ndalonte vjedhjen para fundit të kohës së auditit, për të shmangur zbulimin. Shoku i tij, sidoqoftë, u tregua shumë lakmitar për të ndalur dhe e detyroi atë të procedonte më tej. Kur auditorët gjetën një transaksion mashtrues në balancën e sistemit kompjuterik, ata hetuan për të parë se kush kishte mundësinë për të shkaktuar mospërputhjet. Mbikëqyrësi ishte i vetmi që kishte mundësinë e futjes së faturave.

[4] Albert J. Marcella, Jr. Doug Menendez, *Cyber Forensics, Second Edition, A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes,*

### *3.5 Terrorizmi kompjuterik*

Terrorizmi kompjuterik është një ndërthurje e terrorizmit dhe hapësirës kompjuterike. Ai është përkufizuar si një sulm i paramenduar, politik, i motivuar kundër informacionit, sistemeve a programeve kompjuterike, dhe të dhënave të cilat pasojnë në dhunë, kundër shënjestrave nga grupeve ndërkombëtare apo agjentë klandestinë. Sulmet që shkaktojnë vdekje, dëmtime trupore, shpërthime, rënie avionësh, kontaminim uji apo humbje të ndryshme ekonomike, mund të jenë shembuj. Sulme të rrezikshme mund të kryhen ndaj infrastrukturës dhe të jenë krime kompjuterike, në varësi të ndikimit të tyre.

Shumë prej sulmeve janë serioze dhe me dëme. Në 1998, protestues spanjollë bombarduan "Institutin për Komunikimin Botëror" (IGC), me qindra *email* fals. Ato ishin të lidhura dhe ishin të padeshifrueshme për ISP-të e përdorueseve, dhe përdornin linja që kishin lidhje me njerëz që nuk mund të gjenin *email*-et e tyre. Po këtë vit, një 12 vjeçar piratoi në mënyrë të suksesshme kontrollin e digave të njohura *Rossvelt Dam*, mbi Lumin Salt në Arizona. Ai mund të hapte portat e digës, të cilat mund të kishin përmbytur pa frikë banorët përreth, duke kërcënuar rreth 1 milion njerëz. Dhe në vitin 2002, faqe të njohura interneti në Indi, u dëmtuan.

### *3.6 Vjedhja kompjuterike* [5]

Ka disa lloje të ndryshme vjedhjesh kompjuterike, apo rrugësh të përdorimit të TKI-ve për të vjedhur informacion, para, apo të tjera gjëra të çmuara. Shkeljet janë:

a) Përvetësimi, i cili përfshin shpërdorimin e parave apo pasurive për përdorim vetjak të shkelësit, të cilit i janë besuar këto nga dikush tjetër. Prishja e fshehtë e mbajtësve së të dhënave, një formë e interceptimit të paautorizuar, në të cilën personat e futur manipulojnë përmbajtjen e fshehtë të mbajtësit së të dhënave të një kompjuteri, duke rivendosur rrjetin e transmetimit në serverët e tyre.

b) Përvetësimi i paligjshëm, i cili dallon nga përvetësimi në të cilin kriminelët nuk janë të interesuar për gjërat e çmuara, por sigurojnë hyrje nga jashtë kompanive dhe transferojnë fonde apo modifikojnë dokumente.

c) Plagjiatura, në të cilën është vjedhja e shkrimeve origjinale të dikujt tjetër, me qëllim konsiderimin e saj si të fituar në mënyrë të ligjshme. Pirateria, kopjimi i paautorizuar i të drejtave të prodhimit të *sofware*-ve, muzikës, filmave, artit, librave dhe të tjerave si këto, pasuar me humbje së të ardhurave nga pronësia e ligjshme dhe autorësia.

d) Vjedhja e identitetit, në të cilën hapësira kompjuterike përdoret për të marrë informacione personale të viktimave, si numrin social, të patentës etj., duke i modifikuar, shtuar apo ndryshuar të dhënat e identitetit të personit, për kryerje veprimesh kriminale apo të marrë të drejta pasurore, ose para apo të përdorë karta krediti apo llogari bankare që i përkasin viktimës.

### *3.7 Spiunazhi kompjuterik* [6]

Spiunazhi kompjuterik ka të bëjë me zbulimin e "informacionit", apo "evidencave". Një spiun industrial mund të kërkojë të zbulojë informacione sekrete mbi një laptop të

[5] *An evaluation Framework for National Cyber Security Strategies,* ENISA, European Union Agency for Network.
[6] Anthony Reyes, Richard Brittson, Kevin OShea, Jim Steel, *Cyber Crime Investigations Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors,* Syngress Publishing, Inc, US.

një menaxheri projektesh të Mikrosoftit, i cili në mënyrë specifike ka të bëjë me të ardhmen e kompanisë duke neutralizuar sistemet operuese. Në varësi të informacionit, ai mund të përpunohet në evidenca të caktuara.

### *3.8 Çfarë është partneritet publiko-privat?*

Duke krijuar sfondin e partneriteteve publike-private, tani është e nevojshme të jetë e qartë çfarë është saktësisht ky partneritet. Ka një gamë të madhe të marrëveshjeve të ndryshme që janë referuar si partneritete publike-private, nga ofrimi i përbashkët i shërbimeve me disa rregullatorë qeveritarë për mbikëqyrjen (sektorin e shëndetësisë), për të kontraktuar nga afër *outsourcing* e infrastrukturës së madhe, projekte (ndërtimi i urave, mbajtja e Lojërave Olimpike etj.). Për sektorin privat vendimet merren brenda një modeli biznesi që i përgjigjet kufijve të fitimit dhe interesave të aksionarëve. Kjo është kryesisht e papërputhshme me promovimin e "të mirës publike". Sektori privat ngre kundërshtime kryesore ndaj rolit që qeveria e percepton atë në strategjitë e sigurisë kibernetike. Ai argumenton se shpenzimet e sigurimit për sigurinë kibernetike për një shtetas do të ishte i rëndësishëm.

Pronarët e sektorit privat pranojnë përgjegjësinë në sigurimin e sistemeve të tyre - deri në atë pikë sa është fitimprurëse; sa i përket kostos. Megjithatë, ata tentojnë të bëjnë një dallim midis mbrojtjes kundër kërcënimeve të nivelit të ulët të brenda biznesit te tyre te tilla si hakerat individualë, dhe jo për një mbrojtje kundër një sulmi ndaj shtetit (siguria kombëtare). Kjo tezë mbështet në idenë se duhet të jetë qeveria të mbrojë nga kërcënimet më të mëdha - krimin e organizuar, terroristët dhe kërcënimet e shtetit kombëtar, - qoftë përmes zbatimit të ligjit ose mbrojtjes kombëtare.

## 4. Krimi kibernetik në Shqipëri: juridiksioni dhe territorialiteti

Me sofistikimin e teknologjisë, "përparojnë" dhe metodat e vjedhjeve e mashtrimeve. Tashmë nuk duhet të ruash vetëm kuletën, apo sende të tjera me vlerë, por edhe të jesh i kujdesshëm me përdorimin e kartave bankave, apo fjalëkalimeve. Mashtrimi, falsifikimi, apo ndërhyrja kompjuterike rezulton se janë shtuar vitin e kaluar. Nga të dhënat statistikore të deklaruara, rezulton se në vitin 2015 ka një rritje prej 8,8% të numrit të procedimeve të regjistruara për vepra penale të krimit kompjuterik, në krahasim me vitin 2014, ndërsa numri i procedimeve të dërguara për gjykim, është në të njëjtin nivel.

Pesha specifike që ky grup veprash penale zë për vitin 2015, është 0,4% ndërsa për vitin 2014, ky grup veprash, përbënte 0,37% të numrit total, të procedimeve penale të regjistruara në shkallë vendi. Pra, vihet re një rritje e këtij treguesi për vitin 2015, në krahasim me vitin 2014.

Treguesit për të pandehurit gjatë vitit 2015, rezultojnë me ulje dhe përkatësisht, kemi ulje prej 71% të numrit së të pandehurve të regjistruar përkundrejt këtij totali në vitin 2014, ulje e numrit së të pandehurve të cilët i janë dërguar gjyqit prej 76% në krahasim me vitin 2014. Nga të pandehurit e regjistruar për këtë grupveprash penale, rezultojnë të rritur (mbi 18 vjeç) 11% femra dhe 89% meshkuj. Ndër to, vetëm një i pandehur, i mitur, mashkull dhe në vitin 2015, është regjistruar një i pandehur i huaj. Në lidhje me arsimin e të pandehurve rezulton se 37.5% e të pandehurve janë me arsim deri 9-vjeçar, 37.5 % me arsim të mesëm dhe 25%, të pandehur me arsim të lartë.

Rezulton se të gjithë të pandehurit kanë vendbanimin në qytet.

Llojet e veprave penale që janë konstatuar:

- *Mashtrimi kompjuterik.*

Pesha specifike që zë kjo vepër penale në grupin e veprave penale "Kundër krimit kompjuterik" për vitin 2015 është 44 %, ndërsa për vitin 2014 ka qenë 40,8 %.Nga të dhënat statistikore vërehet tendenca në rritje e procedimeve të regjistruara për veprën penale të parashikuar nga neni 143/b i Kodit Penal "Mashtrimi kompjuterik" në vitin 2015, prej 17,6 % në krahasim me vitin 2014.

- *Falsifikimi kompjuterik.*

Pesha specifike që zë kjo vepër penale në grupin e veprave penale "Kundër krimit kompjuterik" është 13 % për vitin 2015, ndërkohë që në vitin 2014 ka qenë 21,6 %.

- *Ndërhyrja në të dhënat kompjuterike.*

Pesha specifike që zë kjo vepër penale në grupin e veprave penale "Kundër krimit kompjuterik" është 34 % për vitin 2015, ndërkohë që në vitin 2014 ka qenë 23 %.

### *4.1 Juridiksioni për veprat që kryhen ndaj/nëpërmjet sistemeve kompjuterike*

Natyra e ndërlidhur e mjeteve të teknologjisë së informacionit dhe komunikimit i ka dhënë një shtrirje globale kriminalitetit kompjuterik. Duke qenë se ditët e sotme, njerëzit mund të komunikojnë përtej detit, njësoj sikurse përtej derës së shtëpisë, keqbërësit, mund të jenë prezent dhe të shkaktojnë dëme kudo ku ka një lidhje efektive interneti.

1. Secila palë merr masa të tilla legjislative ose të tjera, që janë të nevojshme për të caktuar juridiksionin për çdo vepër penale të kryer në pajtim me përcaktimet e kësaj Konvente, kur një vepër e tillë kryhet: 117 a) në territorin e tij; ose b) në bordin e një anijeje që mban flamurin e tij shteti; ose c) në bordin e një avioni të regjistruar sipas ligjit të atij shteti; ose d) nga njeri prej shtetasve të saj, nëse vepra penale është e dënueshme sipas ligjit penal ku ajo është kryer ose nëse vepra është kryer jashtë juridiksionit territorial të çdo Shteti.

2. Secili shtet mund të rezervojë të drejtën për të mos zbatuar ose për të zbatuar vetëm në raste të caktuara ose kushte të caktuara rregullat juridiksionale të parashikuara në paragrafët (1)b –(1)d të këtij neni ose të ndonjë pjese të tyre.

3. Secila palë merr masa të tilla që janë të nevojshme për të caktuar juridiksionin mbi të gjitha veprat penale të përmendura në nenin 24, paragrafi (1) i kësaj Konvente[7], në rastet kur kryerësi i prezumuar i veprës penale është prezent në territorin e saj dhe ajo nuk e ekstradon atë tek një palë tjetër, kryesisht mbi bazën e shtetësisë së tij/saj pas kërkesës së bërë për ekstradim.

4. Kjo Konventë nuk përjashton asnjë juridiksion penal të ushtruar në pajtim me ligjin vendas.

5. Nëse më shumë se një palë pretendon juridiksionin mbi një vepër që prezumohet e kryer në pajtim me këtë Konventë, Palët e interesuara, kur është e përshtatshme, bëjnë një konsultë për të përcaktuar juridiksionin më të përshtatshëm për të bërë ndjekjen penale.

Nëse vepra është kryer në një hapësirë ku nuk shtrihet juridiksioni territorial i asnjë shteti (si p.sh. në ujërat ndërkombëtare ose hapësirat ajrore ndërkombëtare), atëherë

[7] Clough, J. (2012). The Council of Europe Convention on Cybercrime: Defining 'Crime' in a Digital World. Criminal Law Forum, Vol 23(4). Heidelberg: Springer, f. 36; Konventa është ratifikuar nga vendi ynë me ligjin nr.8888, datë 25.4.2002 'Për Ratifikimin E "Konventës Për Krimin në Fushën e Kibernetikës"'; Neni 22 i Konventës.

mjafton që vepra penale të jetë e ndëshkueshme sipas ligjit të shtetit, shtetësinë e të cilit mban autori i saj, për t'u ushtruar juridiksioni i këtij shteti.

## 5. Teori dhe hulumtime nga studiues të ndryshëm për metodat mjetet e krimit kibernetik dhe kategoritë në të cilat ndahen hakerat[8]

Edhe pse shumë janë shkruar dhe hulumtuar në lidhje me metodat teknologjike për të siguruar sistemin e informacionit të një ndërmarrjeje, shumë pak është hulumtuar rreth njerëzve prapa këtyre sulmeve. Ndoshta kjo është për shkak të fushës relativisht të re të teknologjisë së informacionit. Ka pasur disa hulumtime në lloje të ndryshme të hakerëve siç tregohet në hulumtim nga Holt dhe Kilger (2008). Në këtë studim ata intervistuan dy kontingjente të hakerëve. Grupi parë janë ata të intervistuar nga një konventë *hacker* dhe u etiketuan si grup i egër dhe posesivë. Grupi i dytë përbëhej nga studentë të regjistruar në një kurs sigurie informacioni. Qëllimi i këtij studimi është të shihet nëse ekzistojnë dallime të rëndësishme midis dy kontrolleve të grupeve dhe çfarë mund të shkaktojë këto dallime.

Përfundimi i parë interesant i këtij studimi kishte të bënte me karakteristikat gjinore. Sipas këtij studimi, grupi i kontrollit dhe hulumtimit zbuloi se kishte një përqindje më të lartë të femrave në kategorinë e të kualifikuarave në kursin e sigurisë, sesa në grupin e dytë të kontrollit të egër, ndërsa përqindja më e lartë e meshkujve ishin në grupin e hakerave të egër dhe posesivë. Tradicionalisht fusha e dominuar nga meshkujt është ajo që ka një fluks të madh të hakerave dashakeqës dhe tejet profesionistë.

Ky studim gjithashtu duket sikur largon mitin se hakerat e shumtë dhe shumë profesionistë janë adoleshentë të shkëlqyeshëm dhe shumë studiues në lidhje me teknologjinë e informacionit. Megjithëse grupmosha 18-24 vjeç, ishte e lartë për të dy grupet, nga hulumtimet del se hakerat superprofesionistë janë mes moshës 25-36 vjeç. Mosha mesatare e kontrollit grupi (33 vjeç).

Gjetjet në lidhje me nivelin e arsimimit së të dy grupeve ndryshojnë disi. Derisa grupi i kontrollit kishte një përqindje më të lartë në "disa kolegje" dhe "disa grada në studime" , grupi i egër kishte një përqindje më të lartë në "shkollën e mesme" dhe "gradë kolegji".

Ky studim supozon se ka grupe të ndryshme hakerash dhe këto grupe të ndryshme janë të motivuara në veprimet e tyre për arsye shumë të ndryshme. Grupi i parë i hakerëve përgjithësisht është i motivuar nga kurioziteti dhe ndjekja intelektuale, ndërsa tjetra është e motivuar nga krimi. Steven Branigan, një anëtar themelues i *task forcës* elektronike për krimet elektronike të New Jorkut, thotë se ata që futen në kompjuterë së pari dhe pastaj fillojnë sulmin, janë të motivuar nga kurioziteti, ndërsa ata që kanë tendenca kriminale e fillojnë me mësimin e teknologjisë kompjuterike.

## 6. Sfidat e sigurisë[9]

Disa nga sfidat që karakterizojnë këtë situatë dhe orientimi i tyre për të ardhmen janë si në vijim[10].

[8] Babak Akhgar, Andreë Staniforth, Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook,* Edited by Elsevier Inc, US 2014.
[9] *Ligji nr.7895, dt. 27.1.1995 "Kodi Penal i Republikës së Shqipërisë", i ndryshuar*
[10] *strategjia për mbrojtjen kibernetike 2018-2020 ministria e mbrojtjes*

- *Rritja e kërcënimeve në hapësirën kibernetike*: hapësira kibernetike, të cilën çdo njeri mund ta përdorë pa kufij kohorë dhe gjeografikë, jep në mënyrë asimetrike avantazhe për sulmuesit keqdashës, jo atyre që mbrohen. Si rezultat i metodave të sofistikuara, abuzimi me identitetin është një sfidë në rritje për çdo individ dhe autoritetet institucional.

- *Anonimati dhe atributet*: hapësira kibernetike nuk ka kufij fizikë. Sulmuesit në fushën kibernetike janë të ndryshëm dhe vështirësia për t'u identifikuar ua bën punën më të lehtë (nga hakerat individual deri në grupet e organizuara kriminale dhe deri në shtete), p.sh. hakerat dhe kriminelët kibernetikë mund të përdorin avantazhin e metodave për të lëshuar sulme të cilat janë të pagjurmueshme dhe të vështira për t'u eliminuar.

- *Objektivat e strategjisë së sigurisë kibernetike*: Strategjia shtetërore për sigurinë kibernetike ka këto objektiva strategjike: mbrojtja e infrastrukturës kritike të informacionit; zhvillimi institucional dhe ngritja e kapaciteteve; ndërtimi i partneritetit publiko-privat; reagimi ndaj incidenteve; bashkëpunimi ndërkombëtar.

## 7. Përfudime

Pavarësisht avantazheve dhe zhvillimit të shpejtë që sjell teknologjia, ajo ka treguar se ka edhe një anë të errët. Hapësira kibernetike sot është një nga sfidat më të mëdha ligjore e cila ka nxitur një formë tjetër të krimit, duke krijuar një mjedis për metodat e reja të krimit. Tani pothuajse të gjitha krimet mund të kryhen me përdorimin e kompjuterëve. Rritja e mundësive për sjellje kriminale përmes internetit ka çuar në rritjen e kriminalitetit dhe të kërcënimeve kombëtare dhe ndërkombëtare. Krimet e kryera në mjediset *online* i tejkalojnë kufijtë kombëtarë, duke u bërë gjithnjë e më e vështirë për t'i hetuar. Si rezultat i kësaj, kërcënimet ndaj sigurisë kombëtare dhe ndërkombëtare janë rritur. Duke parë që ky fenomen sot përbën një nga shqetësimet dhe prioritetet kryesore në arenën ndërkombëtare, si dhe kërcënimet gjithnjë e në rritje që po shfaqen në Shqipëri nga ky lloj kriminaliteti. Qëllimi i këtij studimi është analizimi i situatës aktuale në Shqipëri, në lidhje me standardet ligjore, mekanizmat për hetimin dhe ndjekjen penale të krimit kibernetik dhe evidentimi i problematikave dhe sfidave kryesore në luftimin e krimit kibernetik. Ky punim synon të rrisë ndërgjegjësimin e shtetit shqiptar mbi rëndësinë e mbrojtjes së sigurisë kombëtare të shtetit dhe shtetasve shqiptarë nga rreziqet që shfaq krimi kibernetik, si dhe nxjerrjen e rekomandimeve mbi masat që duhen marrë për një luftim më efikas të kriminalitetit kibernetik në Shqipëri.

## 8. Rekomandime

Në bazë të studimit të zhvilluar në kuadër të këtij punimi, pasi u identifikuan sfidat dhe problematikat kryesore të shtetit shqiptar në luftën kundër krimit kibernetik, duke u bazuar në analizimin e kuadrit ligjor, arritjeve të deritanishme, statistikave dhe rezultateve të përfituara nga intervistat e zhvilluara me specialistët përgjegjës për hetimin, ndjekjen penale dhe luftimin e krimit kibernetik, u arrit të nxirren disa rekomandime që duhen ndjekur nga shteti shqiptar për përmirësimin e situatës aktuale, në lidhje me krimin kibernetik. Këto rekomandime janë si vijon:

- ndërhyrje dhe ndryshime në terminologjinë e përdorur në legjislacion për sa i

përket kuptimit të termave "krim kompjuterik" dhe "krimi kibernetik";

- nevojitet të merren masa për ndarjen dhe qarkullimin e të dhënave dhe informacionit në mënyrë më të sigurt, si brenda institucioneve publike ashtu edhe atyre private, me qëllim parandalimin dhe luftën kundër krimit dhe garantimin e politikave të duhura të sigurisë;

- rritja e ndërgjegjësimit mbi sfidat e sigurisë kibernetike, me qëllim përmirësimin e politikave në këtë fushë.

## Bibliografi


1. Aaron Shull, *Global Cybercrime: The Interplay of Politics and Laë, Internet Governance Papers* Paper No. 8 — Qershor 2014, Canada
2. Akdeniz, Y. Internet Child Pornography and The Law: National and International Responses. Hampshire: Ashgate Publishing, 2008.
3. Al Rees, *Cybercrime Laës Of The United States*, Compilation, Tetor 2006 by, ÇIPS
4. Albert J. Marcella, Jr.Doug Menendez, *Cyber Forensics, Second Edition, A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes,*
5. Auerbach Publications, US 2008
6. *An evaluation Frameëork for National Cyber Security Strategies,* ENISA, European Union Agency for Netëork and Information Security, Nëntor 2014
7. Anthony Reyes, Richard Brittson, Kevin OShea, Jim Steel, *Cyber Crime Investigations Bridging the Gaps Betëeen Security Professionals, Laë Enforcement, and Prosecutors,* Syngress Publishing, Inc, US 2007
8. Autoriteti i Komunikimeve Elektronike dhe Postare, *Raporti Vjetor i Veprimtarisë për vitin 2014*
9. Babak Akhgar, Andreë Staniforth, Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook,* Edited by Elsevier Inc, US 2014
10. Begeja. S, Kriminalistika, Tiranë, 2007

**Akte ligjore**

1. Ligji nr. 7895, dt. 27.1.1995 "Kodi Penal i Republikës së Shqipërisë", i ndryshuar
2. Ligji nr. 10 023, datë 27.11.2008 "Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995 "Kodi Penal i Republikës së Shqipërisë", të ndryshuar
3. Ligji nr. 8737, dt 12.2.2001 "Për organizimin dhe funksionimin e prokurorisë në Republikën e Shqipërisë".
4. Ligjin nr. 8417, datë 21.10.1998 "Kushtetuta e Republikës së Shqipërisë", e ndryshuar
5. Ligji nr. 9749, datë 4.6.2007 "Për Policinë e Shtetit".
6. Ligji nr. 9157, datë 4.12.2003 " Për përgjimin e komunikimeve elektronike", ndryshuar me ligjin nr. 9885, datë 3.3.2008, si dhe me ligjin nr. 116, datë 13.12.2012 .
7. Ligji nr. 8888, dt. 25.04.2002 "Për ratifikimin e Konventës për krimin në fushën e kibernetikës".

# Manipulimet kontabël, evazioni fiskal e pastrimi i parave, dhe efektet e tyre në ekonominë informale

**Dr. Jonada MAMO**
*Universiteti "Aleksandër Moisiu", Durrës*
*jonada.mamo@yahoo.com*

**Prof. Asc. Dr. Gaqo TANKU**
*Universiteti "Aleksandër Moisiu", Durrës*
*gaqotanku@hotmail.com*

**Abstrakt**

*Çdo ditë në kontabilitet, njësia ekonomike regjistron një numër të madh dhe të shumëllojshëm transaksionesh. Është shumë e rëndësishme që paraqitja e tyre në mënyrë të saktë, të reflektojë situatën e vërtetë financiare. Përdoruesit e informacionit financiar janë aksionerët, drejtuesit, bankat, autoriteti tatimor, klientët, furnitorët, punonjësit, etj. Ne do të zgjerojmë kërkimin në një perspektivë makro. Do të studiojmë ekonominë informate në vendet në zhvillim, si Shqipëria. Më pas, do të analizojmë efektet e manipulimeve kontabël, evazionit fiskal dhe pastrimit të parave në ekonominë informale. Të dhënat që do të përdoren në kërkim, janë të dhëna sasiore dhe financiare të njësive ekonomike dhe të dhëna të tjera, mbledhur për tregues si GDP, taksat, korrupsionit, biznesit dhe qeverisë. Në kërkim, do të shohim zhvillimin e ekonomisë informate, në vite të Shqipërisë. Specifikisht, do të merremi me efektet e variabëlve të përmendur më sipër në ekonominë informale përmes shmangies së taksave, menaxhimit së të ardhurave dhe praktika të tjera joligjore si pastrimi parave. Përgjatë punimit, do i japim përgjigje shumë pyetjeve si: cilët janë treguesit financiarë më të prekur nga ekonomia informale? A janë bizneset, duke përdorur mënyra ligjore dhe joligjore, për të shmangur taksat, dhe, duke rrezikuar sigurinë e ekonomisë dhe të gjithë shoqërisë? Për këto dhe pyetje të tjera, do të jepet përgjigje përgjatë konkluzioneve të punimit. Shqipëria ka nevojë të rrisë ekonominë formale, për më shumë taksa dhe shërbime për qytetarët. Gjithashtu, duke aspiruar të bëhet pjesë e Bashkimit Europian, i duhet të plotësojë kriteret e tij.*

**Fjalëkyçe:**
**manipulime kontabël, pastrim parash, mashtrim, evazion fiskal.**

## 1. Zhvillimi i ekonomisë informale në Shqipëri

Ekonomia informate, është një temë aktuale që diskutohet në shumë tavolina, me aktorë të ndryshëm. Edhe pse kohët e fundit, interesi për matjen e ekonomisë informale në vende të ndryshme është rritur, shumë pak interes është treguar për investigimin e pasojave të ekonomisë informale. Diskutohet gjatë nëse ekonomia informale ka pasoja pozitive apo negative, për zhvillimin e një vendi. Një pjesë e shoqërisë ka një mendim pozitiv drejt fenomenit, ndërsa pjesa që nuk përfiton prej saj, ka një qëndrim negativ. Termin "ekonomi informale" mund ta hasim ndryshe dhe me terma si ekonomia në të zezë (*black economy*), ekonomia hije (*shadow economy*) ose e nëndheshme (*underground economy*). Studiuesit e kanë përkufizuar në mënyra të ndryshme.

Schrage (1984) dhe Thomas (1992), e kanë përkufizuar ekonominë informale si: "Një bashkësi aktivitetesh, që në parim ushtrohen legalisht, dhe që duhet t'i nënshtrohet tatimimit, por që nuk deklarohen si aktivitete komerciale legale dhe si të tilla, nuk përfshihen në vlerën e të ardhurës kombëtare, ose që pjesërisht, përfshihen në PBB-në". Në literaturat e viteve të fundit, si dhe nga FMN-ja, është pranuar përkufizimi, sipas së cilit në ekonomitë që janë përfshirë nga ryshfeti dhe korrupsioni, iniciativat ekonomike shtrembërohen pasi zyrtarët, qeveritarët, si dhe individët privatë shtyhen që të paguajnë pjesë më të vogla të shpenzimeve publike nga të cilat ofrohen të mira publike. Si pasojë, qeveria mbledh më pak të ardhura që çojnë në uljen e investimeve publike, dhe në rritjen e varfërisë dhe pabarazisë së qytetarëve. Përkufizimet ndryshojnë nga njëri-tjetri, sipas qasjes dhe specialiteti e qëllimi i punës. Është e vështirë për të dalë me një përkufizim të vetëm e të plotë (Trebicka, 2014)[1].

[1] B. Trebicka, *Ekonomia informale, shkaqet dhe pasojat e saj në Shqipëri, disertacion për gradën Doktor*, Fakulteti i Biznesit, Universiteti "Aleksandër Moisiu", Durrës, 2014.

Në Shqipëri, fenomeni i ekonomisë informale u vu në qendër të diskutimeve pas viteve '90. Në vitin 1991, Shqipëria kaloi nga një vend me ekonomi të centralizuar në një vend me ekonomi tregu. Si rezultat, të gjitha zhvillimet e mëtejshme politike dhe ekonomike ndikuan në krijimin e kushteve të favorshme për rritjen e ekonomisë informale.

Tre aktorët kryesor në treg janë biznesi, qeveria dhe konsumatori. Njësitë ekonomike gjejnë hapësira ligjore ku të mund të shmangin pagesën e taksave. Ka mjaft teknika dhe praktika për të shmangur pagesën e taksave dhe për të demonstruar këtë gjatë punimit do ti jepet një rëndësi manipulimeve kontabël. Informaliteti nga biznesi manifestohet në forma të ndryshme të tilla si biznese të paregjistruara, punëtorë të padeklaruar, evazion fiskal, korrupsion, trafikim etj.

Në mesin e vitit 2015, Qeveria filloi një aksion të madh kundër informalitetit i cili prek kryesisht bizneset e vogla të paregjistruara duke miratuar një rritje të madhe të penaliteteve për bizneset e parregullta. Sipas Organizatës Ndërkombëtare të Punës, 30% e fuqisë së përgjithshme të punës, në sektorin e ndërtimit, është punësuar në mënyrë informale. Gjate këtij punimi do shohim zhvillim e tij në vite dhe përpjekjet për matjen e tij, faktorët që e ndikojnë si dhe përpjekjet për matjen e tij dhe masat për uljen e këtij fenomeni.

## 2. Faktorët që ndikojnë në rritjen e informalitetit

Sipas një studimi të kryer nga Këshilli Investimeve të Shqipërisë[2], realizuar me bizneset, ka mospërputhje në llogaritë kombëtare të Shqipërisë që sugjerojnë se ekonomia informale zë mesatarisht 36.2% të GDP-së për periudhën 1996-2012. Pjesa më e madhe e bizneseve, 60% e tyre, e konsiderojnë informalitetin si kosto e ndërkohë 67% e tyre nuk pranojnë që të ketë informalitet tek biznesi i tyre.

*Problemet kryesore të evazionit fiskal për bizneset shqiptare janë ato që lidhen me:*

- regjistrimin e bizneseve dhe licencimin e aktivitetit,
- numri i taksave dhe barra fiskale,
- punësimi dhe deklarimi i punonjësve,
- problemet me import/eksportet.

Ndërkohë që faktorët që nxisin informalitetin gjatë të bërit biznes janë:

- korrupsioni,
- konkurrenca e pandershme,
- kapacitetet e administratës tatimore dhe doganore,
- cilësia dhe qëndrueshmëria e legjislacionit
- niveli i ulët ekonomik.

Në bazë të analizave të reja, nga Banka Evropiane për Rindërtim dhe Zhvillim (BERZH), konkurrencat që u bëhen bizneseve të ndershme nga ekonomia e informale dhe praktikat korruptive, janë identifikuar si pengesa të larta në mjedisin e biznesit në Shqipëri. Sipas raportit, konkurrenca nga *ekonomia hije* mbetet një pengesë kryesore për ndërmarrjet e vogla dhe të mesme, ndërsa korrupsioni u emërua si problemi më i madh nga ana e ndërmarrjeve të mëdha.

Administrata tatimore, ishte në mesin e pengesave kryesore për ndërmarrjet e reja. Në anketën e BERZH-it, 40.8% e bizneseve raportuan se përballen me konkurrencë

[2] Albanian Investment Counsil. (2015), *Informaliteti: sfida e përbashkët qeveri – biznes,* Tiranë.

nga biznese informale. Aktiviteti informal zë pjesë të rëndësishme në prodhimin dhe punësimin total, të ekonomisë shqiptare. Përllogaritet se për periudhën 1996-2012, ekonomia informale përbën mesatarisht 36.2% të Prodhimit Kombëtar. Ndërkohë, për bizneset e mëdha, problemi kryesor është korrupsioni. Ndërsa për sa i takon bizneseve të reja, problemi kryesor rezultoi marrëdhënia me administratën fiskale. Rreth një e treta e bizneseve të anketuara në Shqipëri, u përgjigjën se pagesat apo dhuratat informate, kërkohen në procesin e aplikimit për marrje autorizimesh, lejesh apo licencash nga administrata shtetërore. Ky tregues është shumë më i lartë, krahasuar me nivelin mesatar prej 18.8% të vendeve të Europës Juglindore, të përfshira në anketim.

Edhe për vitet 2013/2014, BERZH-i dhe Banka Botërore kanë kryer raundin e pestë të performancës së ndërmarrjeve dhe mjedisit të biznesit. Nëpër të gjithë rajonin e tranzicionit, sërish, ankesa e vetme më e madhe nga drejtuesit, ishte rreth konkurrencës së pandershme nga ekonomia informale, ku kompanitë nuk janë regjistruar gjithmonë, ose, kërkojnë shmangien nga taksat, nga të ardhurat, nga numri i të punësuarve apo i pagave që u paguajnë.

## 3. Informaliteti dhe korrupsioni

Indeksi vjetor i korrupsionit botëror, i publikuar nga *Transparency International,* është një indeks, i cili rendit 180 vende dhe territore sipas niveleve të perceptuara të korrupsionit në sektorin publik, sipas ekspertëve dhe biznesmenëve, dhe përdor një shkallë nga 0 deri në 100, ku 0-ja është "shumë e korruptuar" dhe 100-a është "shumë e pastër". Këtë vit, indeksi gjeti, se më shumë se dy të tretat e vendeve, shënojnë nën 50, me një rezultat mesatar prej 43. Për fat të keq, krahasuar me vitet e fundit, kjo performancë e dobët nuk është asgjë e re.

*Transparency International*, vuri në dukje se Shqipëria ka përmirësuar renditjen e saj. Anketa, e cila i rendit shtetet në një shkallë 0 (shumë të korruptuar) deri në 100 (shumë të pastër), i dha Shqipërisë një rezultat prej 39 pikësh, nga 36 pikë, në vitin 2015. Shqipëria renditet në vendin e 83-të, midis vendeve të tjera nga vendi i 88-të 2015. Ndërkohë në vitin 2017, nuk kemi ndryshim nga pozicioni, por bie me një pikë vlerësimi duke perceptuar një nivel më të lartë korrupsioni se një vit më parë. Krahasuar me vendet e rajonit, Shqipëria renditet më mirë se Kosova dhe, Bosnje dhe Hercegovina.

Niveli i perceptuar i korrupsionit. Burimi: Transparency International 2017

| Pozicioni | Vendi | 2017 | 2016 | 2015 | 2014 | 2013 | 2012 |
|---|---|---|---|---|---|---|---|
| **54** | Italy | 50 | 47 | 44 | 43 | 43 | 42 |
| **57** | Croatia | 49 | 49 | 51 | 48 | 48 | 46 |
| **59** | Greece | 48 | 44 | 46 | 43 | 40 | 36 |
| **64** | Montenegro | 46 | 45 | 44 | 42 | 44 | 41 |
| **77** | Serbia | 41 | 42 | 40 | 41 | 42 | 39 |
| **81** | Turkey | 40 | 41 | 42 | 45 | 50 | 49 |
| **83** | **Albania** | **38** | **39** | **36** | **33** | **31** | **33** |
| **85** | Kosovo | 39 | 36 | 33 | 33 | 33 | 34 |
| **91** | Bosnia and Herzegovina | 38 | 39 | 38 | 39 | 42 | 42 |
| **107** | The FYR of Macedonia | 35 | 37 | 42 | 45 | 44 | 43 |

Sipas raportit të *United Nations Office*[3], qytetarët shqiptarë e rendisin korrupsionin si problemin e dytë më të rëndësishëm me të cilin ballafaqohet vendi pas papunësisë.

- 28.3 për qind e shtetasve shqiptarë, kanë qenë ekspozuar qoftë drejtpërdrejt, ose nëpërmjet një anëtari të familjes, në një përvojë ryshfeti me një zyrtar publik. Sipas shkallës së përhapjes së ryshfetit, përqindja e qytetarëve që paguajnë ryshfet midis atyre që kishte kontakt me zyrtarët publikë është 19.3 për qind.

- Ka disa dallime në përhapjen e ryshfetit në zonat urbane (17.7%) dhe në zonat rurale (20.9%).

- Shkalla e përhapjes së ryshfetit, është 21.3 për qind për gratë shqiptare, në krahasim me 17 për qind, për meshkujt shqiptarë.

- Pothuajse të gjitha ryshfetet paguhen me para në dorë (99.6%) dhe ryshfeti mesatar, është 5,710 lekë, ose ekuivalenti i përafërsisht, 43 Euro.

- Qëllimet kryesore të pagesës së ryshfetit në Shqipëri, janë për: trajtim më i mirë (71%), përshpejtimin e një procedure (9%) ose për të shmangur pagesën e një gjobe (9%).

- Më shumë se 70 për qind e të gjithë atyre që paguajnë ryshfet në Shqipëri, i paguajnë ryshfete mjekëve (71%); pothuajse gjysma (47%), ua paguajnë infermierëve dhe 14 për qind, policëve.

- Qytetarët nuk e raportojnë ryshfetin, sepse: e shohin atë si një praktikë të zakonshme (45%); japin ryshfet vullnetarisht si shenjë mirënjohjeje (13%) ose mendojnë se raportimi është i pakuptimtë, pasi askush nuk do të kujdeset (29%).

- Shqetësimet për korrupsionin në sektorin publik, konfirmohen nga përvoja e atyre të cilët, në tre vjet para këtij anketimi, siguruan një punë në administratën publike, dhe 9 % e tyre, u rekrutuan me ndihmën e një ryshfeti.

Ryshfeti ka një shkallë më të lartë të përhapjes sesa krime të tjera si vjedhja, sulmet dhe grabitjet. Në Shqipëri, është regjistruar shkallë e ulët për krime të tilla, duke shpjeguar kështu se pse qytetarët ndjehen të sigurt në shtëpi, pas errësirës, dhe nuk përdorin sisteme të avancuara të sigurisë për të mbrojtur shtëpitë e tyre.

## 4. Informaliteti në punësim

Sipas Rulit (2003), fakti më shqetësues i informalitetit në fushën fiskale qëndron në ndërmarrjet e vogla dhe të mesme si dhe në ato të mëdha, të cilat janë të regjistruar ligjërisht por fshehin përveç të ardhurave të tyre, numrin e të punësuarve dhe nivelin e vërtetë të pagave. Raporti i publikuar në Ditën Ndërkombëtare të Punës, e rendit Shqipërinë si vendin që ka normën më të lartë të punësimit informal në Evropë, në 61% të totalit të punësimit. Ndër to, gra në punë informale janë 63.5 %, prej të cilave 36.4 % konsiderohet ato shtëpiake.

## 5. Informaliteti dhe evazioni fiskal në sistemin tatimor e doganor

Një nga format më thelbësore të aktivitetit të paligjshëm është evazioni fiskal, me efekte më të dukshme në makroekonomi. Një deficit qeveritar është në qendër të

[3] United Nations Office on Drugs and Crime (2011). *Corruption in Albania: Bribery as experienced by the population.* Vienna: United Nations Office on Drugs and Crime.

vëmendjes të vështirësive ekonomike të shumë vendeve dhe masat për rregullimin e tij janë në qendër të programeve stabilizuese ekonomike. FMN-ja ka përqendruar forcat e veta në përmirësimin e kapaciteteve taksambledhëse të vendeve anëtare të saj. Megjithëse biznesi i vogël është një sektor i rëndësishëm për evazion fiskal, ai gjithashtu jep drejtimin e rritjes ekonomike. Pra, ekziston si mundësi që shumë vende në fillimet e zhvillimit ekonomik të jenë viktima të evazionit fiskal dhe shoqërive të pastrimit të parave[4].

Evazioni fiskal është një problem shqetësues, jo vetëm për vendet në tranzicion si Shqipëria, por edhe për vendet që kanë një sistem fiskal të zhvilluar. Një problem për Shqipërinë, është se ende nuk ka statistika të sakta dhe metoda të standardizuara për përcaktimin e evazionit fiskal. Nuk ka raporte të sakta të institucioneve përgjegjëse për këtë fenomen[5].

Evazioni fiskal është një aktivitet joligjor dhe i fshehur. Sipas të dhënave të Bankës Botërore, Shqipëria ka kontributin më të ulët të mbledhjes së të ardhurave publike ndaj PBB-së në rajon, ndërkohë që barra fiskale është në nivelet më të larta, ndërsa procedurat për të qenë korrekt me taksat, janë ndër më të komplikuarat në rajon, pas Serbisë. Anketa e Këshillit të Investimeve mbi Informalitetin tregon se procedurat, numri i taksave dhe barra fiskale, mbeten ndër më problematiket për bërjen e biznesit në vend. Ka reagime të shumta, nga bizneset dhe ekspertët fiskalë, që shikojnë fragmentimin e sistemit tatimor si shtysë për informalitet, kundrejt një administrate tatimore me kapacitete të kufizuara që nuk i përgjigjet intensitetit dhe profesionalizmit, që kërkon reforma kundër informalitetit.

Ndonëse janë ndërmarrë hapa të rëndësishëm kohët e fundit, nga Drejtoria e Përgjithshme e Tatimeve, sikurse është zbatimi i modulit të riskut apo kryerja e trajnimeve intensive, mendojmë se ka vend për përmirësimin e marrëdhënies administratë tatimore-biznes. Krijimi i një klime mirëkuptimi dhe zhvillimi i dykahshëm gjatë kontrollit, është thelbësor, nëse fillimisht synohet një qasje më këshilluese (për shembull, kontrolli i parë nga tatimorët tek biznesi, të ishte konsultativ dhe në rast të moszbatimit të udhëzimeve të lëna nga tatimorët, kontrolli i dytë të vijonte me zbatimin e penaliteteve). Kjo gjë do të shmangte konfuzionin, keqinterpretimet dhe abuzimet nga të dyja palët. Sipas studimit të Këshillit të Investimeve, korrupsioni dhe ndikimi politik në administratë (në rreth 25% të përgjigjeve), krijon premisa për të nxitur informalitetin dhe mospagimin e taksave[6].

*Faktorët kryesorë që çojnë në informalitet nga sistemi tatimor:*

- rivlerësim dhe analizë e sistemit fiskal: fragmentim i zinxhirit të TVSH-së dhe tatim fitimit; vlerësim i favorizimeve, p.sh. për bizneset e reja, subvencionet në bujqësi; kuponi tatimor, etj.; thjeshtim i burokracive administrative, si p.sh. procedurat për SME, pagesat *online*, sistemi bankar;
- rritja e përgjegjshmërisë së administratës, si p.sh., modernizimi i sistemit, specializim i administratës, apelim efektiv;
- analizë e çmimeve të referencës;
- problematika e kasave fiskale.

[4] Peter. J. Quirk, Këshilltar në Departamentin e Marrëdhënieve me Jashtë në FMN.
[5] Fortuzi, S. (2015 ). *Informal economy and money laundering in Albania*. *International Journal of Economics, Commerce and Management, Vol. III, Issue 10, United Kingdom* , 737-748.
[6] Studimi i Këshillit të investimeve të Shqipërisë.

## 6. Informaliteti dhe pastrimi i parave

Pastrimi i parave është një nga problemet më të mëdha që hasin ekonomitë e vendeve në zhvillim. Ekonomitë e vendeve në zhvillim ofrojnë mundësi të pafundme për të injektuar para të paligjshme, të pajustifikuara, duke qenë se sektorët më të rëndësishëm të tyre, si, ndërtimi apo investime të mëdha publike në infrastrukturë, kërkojnë kapitale të mëdha financiare. Gjithashtu, sistemi bankar i pakonsoliduar, si nga pikëpamja financiare, ashtu edhe nga pikëpamja e rregullave të forta ligjore të operimit në treg, krijojnë mundësi dhe hapësira të mëdha për të hyrë në marrëveshje investimi të parave të pista, të fituara nga aktivitetet e paligjshme. Duke qenë se nga aktivitetet kriminale si, prodhimi dhe trafikimi i drogave, trafiku i armëve, etj., gjenerohen shuma shumë të mëdha parash, kryesisht ne kesh, ato nevojiten të injektohen në ekonomi, në formë investimesh, në sipërmarrje apo aksione kompanish. Rreziqet prej saj janë të mëdha, pasi nëpërmjet saj mund të prishet konkurrenca e lirë në treg, të blihet informacion, të porositen politika të caktuara ekonomike, nëpërmjet ndryshimeve ligjore, me qëllim favorizimin në treg të një biznesi të caktuar, etj.

Pastrimi i parave kërcënon sisteme ekonomike dhe financiare, në shumë vende, dhe komuniteti ndërkombëtar, financiar, duhet me domosdo, të mbështesë masat kundër pastrimit të parave. Për të provuar që pastrimi i parave ka ndikim të rëndësishëm për makroekonominë, është e nevojshme të tregojmë se përfshin shuma relativisht të mëdha për të gjithë aktivitetin ekonomik. Janë bërë shumë përpjekje nga makroekonomistët, kryesisht në vitet 1980, për të matur vlerën e tregut të zi. Ata kishin matur në fakt, pastrimin e parave, sepse ata panë zëvendësimet në kohë për kërkesat e monedhave të lidhura me taksat më të larta, si rrjedhim, pra, të analizonin evazionin fiskal.

*Pastrimi parave përfshin:*

- përdorimin e depozitave kesh, më të vogla sesa sasia minimale e kërkuar për një llogari për t'u deklaruar;
- mosfaturimi i eksporteve, falsifikimi i dokumentacionit të importit dhe deklarimet fiktive, mund të vulosin transfertat ndërkufitare, p.sh., të trafikut të drogës;
- shkëmbimet: pronësitë e vjedhura (p.sh., antiket ose makinat luksoze) mund të shkëmbehen, nëpërmjet kufijve kombëtarë, me substanca të paligjshme;
- transaksionet paralele të kreditimit, mund të përdoren për të shmangur ekonominë formale, përveç rasteve të kthimit, nga aktivitet i paligjshëm në blerjen dhe futjen e kapitalit në rrugë të ligjshme.

Për shkak të krimeve, aktivitetit të fshehtë dhe pastrimit të parave, të cilat japin një efekt në shkallë të gjerë, politikëbërësit e makroekonomisë duhet t'i marrin ato në konsideratë. Por, për shkak se këto aktivitete janë të vështira për t'u monitoruar, shpesh shtrembërohen të dhënat ekonomike dhe komplikohen përpjekjet e qeverisë për të menaxhuar politikat ekonomike. Një studim i hershëm, i vitit 1996, zhvilloi teste empirike mbi marrëdhëniet e rritjes së GDP-së me pastrimin e parave, në 18 vende të industrializuara. Ky studim u krye për herë të parë. Në përfundim, u arrit në konkluzionin se ulja e GDP-së vjetore, ishte e shoqëruar me rritje të pastrimit të parave, në periudhën e viteve 1983-1990. Aktiviteti i pastrimit të parave, mund të korruptojë pjesë të sistemit financiar dhe të minojë udhëheqjen bankare. Nëse menaxherët e bankave, korruptohen

nga shumat e përfshira në pastrimin e parave, qëndrimet në tregun e zi mund të shpërndahen më tepër në zona jashtë veprimeve bankare sesa në ato të lidhura direkt me pastrimin e parave, pasi kjo krijon rrezik për sigurinë e bankës.

## 7. Konkluzione dhe rekomandime

Shqipëria ka kontributin më të ulët, të mbledhjes së të ardhurave publike, ndaj PBB-së, në rajon, ndërkohë që barra fiskale është në nivelet më të larta. Njësitë ekonomike gjejnë hapësira ligjore ku të mund të shmangin pagesën e taksave. Ka mjaft teknika dhe praktika për të shmangur pagesën e taksave. Një nga format më thelbësore të aktivitetit të paligjshëm, është evazioni fiskal, me efekte më të dukshme në makroekonomi.

Ryshfeti ka një shkallë më të lartë të përhapjes sesa krime të tjera, si: vjedhja, sulmet dhe grabitjet. Për krime të tilla, është regjistruar shkallë e ulët në Shqipëri, duke shpjeguar kështu, se përse qytetarët ndjehen të sigurt në shtëpi, pas errësirës, dhe nuk përdorin sisteme të avancuara të sigurisë për të mbrojtur shtëpitë e tyre.

Pastrimi i parave kërcënon sisteme ekonomike dhe financiare në shumë vende, dhe komuniteti ndërkombëtar financiar, duhet me domosdo të mbështesë masat kundër pastrimit të parave.

*Disa nga rekomandimet që dalin nga analiza e punimit janë:*

- incentiva/favorizimi dhe përmirësimi i administrimit fiskal, si parakushte për formalizim;
- luftë efektive ndaj informalitetit, jo rritje e mëtejshme të taksave;
- gjoba shumë të ashpra në fushën tatimore;
- ndryshime në legjislacion, pa konsultim paraprak me biznesin; jo! gjobave të paarsyeshme dhe dënimeve për biznesin;
- ulje e barrës fiskale;
- aksioni agresiv dhe masat ndëshkuese joproporcionale;
- lufta kundër informalitetit duhet të jetë e vazhdueshme/kujdes varfërinë;
- shmangie e dy standardeve në pasqyrat financiare dhe bilancet e kompanive;
- koordinim dhe shkëmbim informacioni ndërmjet institucioneve publike në marrëdhëniet me biznesin sidomos ato rregullatore (AKU, Mjedis, Pune, etj);
- konsultimi, transparenca dhe ndërgjegjësimi me qytetarët;
- një nga masat është shpërndarja e kompetencave raportuese dhe monitoruese, për pastrimin e parave, nga ato zyrtare deri tek ato jofitimprurëse;
- një tjetër, është sigurimi i informacionit dhe trajnimit mbi mbikëqyrjen ndaj formave të parave të pista, të cilat tërhiqen nga zyrat e këmbimeve valutore nëpërmjet kanaleve të tilla si, kodi i sjelljes në zyrat e këmbimeve, që zakonisht janë të hartuara nga shoqëritë kombëtare të zyrave të këmbimeve valutore ose institucioneve bankare me ndihmën e FMN-së.
- Shqipëria ka nevojë të rrisë ekonominë formale, për më shumë taksa dhe shërbime për qytetarët; gjithashtu, duke aspiruar të bëhet pjesë e Bashkimit Europian, i duhet të plotësojë kriteret e tij.

## Bibliografi


1. United Nations Office on Drugs and Crime . (2011). *Corruption in Albania: BRIBERY AS EXPERIENCED BY THE POPULATION*. Vienna: United Nations Office on Drugs and Crime.
2. Albanian Investment Counsil. (2015). *INFORMALITETI: SFIDA E PËRBASHKËT QEVERI – BIZNES.* Tirane.
3. Bajada, C., & Schneider, F. (2009). Unemployment and the Shadow Economy in the oecd. *Revue Économique*. doi:10.3917/reco.605.1033
4. Fortuzi, S. (2015 ). INFORMAL ECONOMY AND MONEY LAUNDERING IN ALBANIA. *International Journal of Economics, Commerce and Management, Vol. III, Issue 10, United Kingdom* , 737-748.
5. OECD. (2004). THE INFORMAL ECONOMY IN ALBANIA ANALYSIS AND POLICY RECOMMENDATIONS. Retrieved May 04, 2014, from: http://www.pintoconsulting.de/Images/pdf/9_informal_economy_albania_2004.pdf
7. Olters, J.-P. (2003). ALBANIA'S INFORMAL ECONOMY: AN IMPEDIMENT TO ECONOMIC DEVELOPMENT? In *4th conference of The Bank of Albania*.
9. Schneider, F., & Enste, D. H. (2000). Shadow Economies: Size, Causes, and Consequences. *Journal of Economic Literature*. doi:10.1257/jel.38.1.77
10. Thomas, J. (1992). Informal Economic Activity. *New York: Harvester/Weatsheaf*.
11. Thomas, J. (1999). Quantifying the black economy: "measurement without theory" yet again? *The Economic Journal,*, 381–389.
12. Trebicka, B. (2014). *EKONOMIA INFORMALE, SHKAQET DHE PASOJAT E SAJ NË SHQIPËRI*. Durrës.


AKADEMIA E SIGURISË
1971

Academy of Security

Third International Scientific Conference

# Computer crime, cybercrime and national security

21 November, 2018
Tirana, Albania

ENGLISH

# ABSTRACTS

"POLICIMI DHE SIGURIA", NR. 13, NOVEMBER, 2018

## Cybernetic security in the armed forces

- PhD. Zihni GOXHAJ

ABSTRACT

Cybernetic security in the Armed Forces. This is a work which explains why and how cybernetic technology is used by the Armed Forces; it also determines their function mode and utilization. Cybernetic security is an important element of the information interconnection system security, providing distribution and management of the I.I.S. services in reaction of harmful actions experienced through cybernetic space. Information security is a very important case for I.I.S. because the systems and networks manage critical information of an organization and this information must be reliable, secure and the processes must be in the right place in way to identify and fight the undesirable activity. An interesting point is how the military structures take actions to provide the communication, information and other electronic systems security which is deposited, elaborated or transmitted in this systems according to the confidentiality, integrity, availability, authentication and undeniability. Why is it hard and necessary to assure cybernetic defense....Because this enemy (cybernetic attack), doesn't attack us with an explosive truck, neither a Sarine gas suitcase or dynamite on a fanatic body. This enemy attacks us with 1 and 0 in a place where we are more vulnerable: the point where physical and virtual worlds converge.

*Keyword: IIS, cybernetic defense, information security, cybernetic security, classification, compound, principles, concepts, interoperability.*

## Childrens online pornography: causes, investigation and prevention

- MSc. Luljeta ISMAJLUKAJ

ABSTRACT

The Internet has opened up a new world - a world with endless opportunities. It's an exciting world where anyone who can use the internet can have his word, find information more easily than ever before, and share his private thoughts or preferences with the world. Every day we face the dark opportunities that offer to those who consume online pornography with children. For everyone it is well-known that sexual exploitation has existed long before the information revolution and that everyone, mainly men, were and are capable of abusing in different forms with children of different ages. The difference today is that the availability and access to pornography with children is much easier. In the era of internet abusers can easily find their victims through social networks.

We hear about so many cases who are offenders and victims and how they are connected via the Internet and other technologies. Pornography of children online is a typical global crime that brings with it increasingly familiar problems of police crimes otherwise defined in multiple states and multiple jurisdictions, due to the decentralization of the internet, the ability to transmit images immediately around the world and the availability of smartphones and other mobile devices for children and everyone who would use them. Production and distribution of child pornographic images result from sexual abuse of contact by adults with close family or social relationships with children. But this does not remain in a domestic jurisdiction, because the international distribution and image consumption through the Internet

convert these local crimes to global ones. It is therefore concluded that this global crime is taking giant proportions every day and more. All interested actors in the fight for the prevention and investigation of these crimes bring in it as a moral threat against which to react to neutralize and identify and prosecute these crimes before justice.
Abuse of online children is a problem for the entire community. This requires coordination of business and law enforcement efforts at local and international level. The Internet is already a multi-dimensional part of every individual's life, thus playing an inalienable role in the psychology of humans and thus influencing the addictive problem of him to know too high figures. Of course, born in a world where everything is a click away, children are the target group most sensitive to this phenomenon. So everybody's job is to try to create a safer environment for them.
Key words: pornography, internet, solitude, shame, self-esteem, children, abuse.

## Cyber threats, their impact and distribution in Albanian state institutions

- PhD. candidate Kozeta LIGEJA

ABSTRACT
The hypothesis is: Albania ranks among the countries where telecommunications development, internet access and computerization of the society is progressing very quickly. Increased use of communication is an added value in the country's economic and social development, but at the same time it exposes it to the hazards of the cyber nature with state and non-state actors. Cyber attacks have the potential to severely damage the exchange of information in public institutions, telecommunications and the financial and banking system, causing interruption of vital services.
Purpose of the paper: The purpose of this paper is to prove through evidence, mainly of theoretical analysis, but also of the practicality that Albania as a society experiences problems from cyber attacks. Methodology: The paper will be based on several study methods. Mostly inductive methods will be used, passing from specific facts to general conclusions, but also to the deductive one, passing from general conclusions to draw conclusions on the consequences and special problems. Through the analysis of specific cases in Albania, which have addressed specific issues of importance for the development of the work.
*Key words: Albania - Cyber bullying - State Institutions – Impact.*

## Money loundering through cyber crime

- PhD.sc. Oreta SALIAJ, MSc. Vehbi MORINA

ABSTRACT
Most of the hackers have the passion firstly, or the benefit depending on the type of hacker and their nature of work. When a hacker aims to profit, in the first place, he will find easier ways to perform complex transactions, as a result of money laundering earned by his criminal activity, aided by cybercrime. Knowing that Albania is often found in international reports on organized crime and money laundering, we consider that addressing this topic would be an indication for the Albanian State to be more alert to online transactions, in order to minimize the level of money laundering, while

the latter globally spends several billion euros over the years.
Thus, knowing that there are different criminal groups in Albania, those groups can easily cooperate with hackers to realize a multitude of complex international transactions. Is there a possibility of investigating Albania in relation to cryptovalutat and block-chain technology of money laundering investigation? This paper will analyze and elaborate some forms of money laundering online, helped by cyber crime, as a threat to country's economy, money laundering, fiscal evasion, etc.
*Key words: criminality, internet, money laundering, cryptography, transactions.*

**International access in computer systems and the principle of state supply**

- Magistracy Ylli PJETERNIKAJ, Magistracy candidate Enisa SHAHINI

ABSTRACT
The ability to access computer data, located in other jurisdictions, in a quick way, is an important aspect of modern criminal investigations. However, the fact that prosecuting authorities have the capacity to conduct such searches does not allow it. This will usually be considered as a breach of territorial sovereignty for those from a country conducting investigations in a foreign country without the authorization of that country. The principle of international law provides that no state can enforce its jurisdiction within the territory of another sovereign state. Consequently, a state cannot enforce its laws, conduct investigations or arrest a person in the territory of another state, without the clear legal authority that allows it to do so.
The issue of cross-border access to electronic evidence has been recognized since 1980, although the issue did not appear "very impressive at the time and in embryonic stages." However, technology changes showed that the issue quickly became urgent and was debated, by the European Committee on Crime, the G8 and the Council of Europe. The drafters finally concluded that it was not yet possible to prepare a full, legally binding regime in this area. Problems observed are related to the fact if the courts of the Republic of Albania order entities that are not in the territory of our country to make computer data available. Also, the international character of computer crime raises the issue of the criteria referred to in the convention to determine which state party has jurisdiction, in cases when the action is carried out by a foreign national outside the territory and the consequences come to the territory of another state.

**Cyberdeviance and the Role of Data Protection Officer Sustainable Structures in its Prevention**

- PhD. Silva IBRAHIMI, PhD. Eglantina DERVISHI, Cav.PhD. Ervin IBRAHIMI, Dr. Eleonora LUCIANI

ABSTRACT
Prevention is undoubtly one of the core items of today’s health and social care! Mass media, technology and the information technology system are of the most influential tools in the cognitive and psychological development of a person's social life.
The objective of the present article is to explore some of the basic aspects of the relationship between cyber-deviant behaviors and the role of order security and cyber

security structures such as the Data Protection Officers (DPO) that exist in the cyber-digitalization preventing process.
This article intersects the core aspects of deviant cyber subculture and the role of DPO officers in the screening and prevention of criminal extreme acts.
The implementation of consumer protection and security strategies from dangerous navigation and risky behaviors are more important in developing a psycho-informatics prototype for people with a high incidence of active criminality, focusing them more on antisocial personality development.
*Keywords: cyber deviant behavior, digitalization technology, DPO, national security, prevention.*

**Addressing ways of cyber threats**
- MSc. Tereza MATRAKU

ABSTRACT
This paper tries to reach a contribution in the cyber war theme, by concluding that its real notion has been abused. One of the main contemporary problems in cyber war is the grouping of all kinds of attacks so I have described some main attacks such as ddos, attacks on websites and scada. I've also explained the role of each player in this game, from criminals to hacktivsts and how each of them affects other actors, governmental or not. On the other side, the legal view of the issue is also of crucial importance. If a cyber attack classifies as an act of war the attacked country possesses the right to fight the attacker by war means. Although most of the attacks we discuss here do not fall in this category they are discussed according to the legislature of the time of the attack.
To explore the argument even further I have taken into consideration notorious cases of cyber attacks such as the one in Estonia, Georgia or those committed against Google. I explore these cases in the light of classification terms focusing on the arguments to categorize them as acts of cyber war or not. As a side scenario I have chosen a more delicate example, the attack of Israel and USA via "Stuxnet worm" on nuclear impiants in Iran, already classified as an act of cyber war. Having explored and represented different views and arguments on the cyber war topic I consider that a real cyber war is very difficult to happen if not impossible because the attacks are not easy to execute and maintain making most of them conflict cases. It is my belief after investigating this topic that the cyber war is not an adapt concept to address security threats. Most of the threats appear to be crimes more than acts of war. Thus, the best way to handle them is by civil response. I conclude this thesis by giving some recommendations on how to improve the cyber security. Among them I propose an extensive public discussion on the topic, more strict international measures to fight the attacks, becoming knowledgeable on the attacks and using AI in enhancing the process of identifying and disintegrating the attacks.

**Cibernetic threats - their impact on Kosovo state safety**
- PhD. candidate Riza SHILLOVA

ABSTRACT
The conventional threats that were against the state today have been considerably reduced. Today there is a general trend of increasing non-conventional threats such

as weapons of mass destruction, terrorism and cybercrime.
Based on the data available today in Kosovo, Europe and beyond, cyber attacks occur on a daily basis and are getting tougher every day. Referring to available data in Kosovo it is expected that the threat of cyber attacks will increase over the next few years. Such threats can cause extreme damage to the economy, public administration and critical infrastructure of Kosovo. These attacks are considered to be encouraged not only by criminal activities but also by political agendas. In this way, cybercrime poses a threat to the security, stability and functioning of the state.
The development of digital infrastructure has changed our daily social and economic life, and has also influenced the introduction of new criminal offenses related to cybercrime. The main activity of criminal groups in Kosovo is narcotics, trafficking in human beings, prostitution, terrorism, smuggling with migrants, goods, weapons, gambling, corruption, etc. Cyber space offers greater opportunities for criminal activities mentioned above, but also other forms of criminality that affect state security such as: cyber attacks, cyber-spying or cyber sabotage, cyber-intelligence and cyber terrorism. Based on the analysis of the strategic review of the security sector in the Republic of Kosovo, cybercrime as an unconventional threat has been identified as one of the risks, challenges or global threats that may also affect Kosovo's security. The Government of the Republic of Kosovo has drafted the Cyber Security Strategy 2016-2019 and the Action Plan which is in line with the Guidelines of the European Network and Information Security Agency (ENISA) and in the spirit of the European Integration. In terms of strategic approach, Kosovo institutions have determined that cyber security priority is inter-institutional coordination, protection of critical information infrastructure, capacity building (legal, human and infrastructural), building public-private partnerships, response to incidents and co-operation international.
*Key words: security, nacional, cyber, threat, strategy.*

## Computer systems application in conducting illegal activities and cyber attacks

-MSc. Sabrina QYPI

ABSTRACT
With modern technological developments, using of computer systems, social networks, the internet, applications and various platforms, that are offered in the field of information technology, new ways of committing illegal and criminal activities, have emerged significantly. Cyber attacks, as a new form of hackers interfering in computer systems, exponentially increase the risk of stealing data, information, damaging them, and committing illegal actions in the banking and non-banking systems. The different ways and methods of these attacks are difficult to capture and stop, good specialists are required to build an effective cybersecurity system. Focus and strategies of police structures persist on taking appropriate measures to prevent, disrupt, detect criminal activities and cyber attacks that are being developed. Cyber attacks and computer system exploitation are a concern around the world because they serve as a catalyst forcriminality. The problem lies in the great times, often in the inability to discover, find and capture the authors of these attacks. With Albanian digitalization, day by day we are seeing gaps in the legal provisions that do not foresee these new forms of cybercrime. It is worth mentioning the imperative need of

professional capacity building, well-organized and specialized structures, institutional and international cooperation and interaction, as well as the awareness of the population about the dangers and ways in which they can be protected from cyber attacks without being the victims and minimizing the consequences. The future will be dominated by these crimes and cyber attacks, so the efforts of the State Police should be oriented and intensified in this delicate way.
*Keywords: cyber attacks, computer systems, hackers, information technology, cyber security.*

**Albanian material in the field of cybernetic crime. Approach to the Budapest Convention. Issues**
- Magistracy Elsa MIHA

ABSTRACT
Over the last decades, just like anywhere in the world and in our country, technology has progressed in tremendous rates. In addition to the benefits of this technological development in various areas of life, the criminal activity that is carried out through and against technology has also been improved. These indicators of cybercrime, made the Albanian legislature aware of the need to anticipate these socially dangerous actions, as criminal offenses in our criminal code.
This paper will address the material criminal law legislation in the field of cybercrime in Albania, its compatibility with the provisions of the Budapest Convention and some issues and shortcomings that dictated the practice in this regard. There are also some basic notions regarding technical elements or analyzes not found in almost all computer provisions and which was considered crucial for their well understanding. A detailed analysis will be carried out for each category of cybercrime and specifically for computer-related and content-related crimes referred to in the provisions of the Budapest Convention and the domestic law. At the end of the process, there will be a number of conclusions or suggestions in this paper as well as the need to improve and supplement domestic legislation in the field of cybercrime, and the need for persistent training of law enforcement structures due to the dynamic nature of this crime.

**Business scams, billing bank cards and safe internet usage**
MSc. Visar PACOLLI

ABSTRACT
Technology, the Internet, the use of ATMs and online payments by businesses has taken its place alongside the development of information technology as an important part of people's lives. Customers use ATMs, POS terminals and the internet to buy online, and invest online. Most consumers as well as businesses nowadays use credit or debit cards for withdrawals and make various online payments without anticipating the risks that are posed to you while doing these services. Most of these mechanisms require the involvement of a third party to serve as a mediator in transactions. Depending on the mechanism, the mediator may have a contractual relationship with the buyer, the seller, or both.
The main advantages of online payment methods are comfort and efficiency. For

example, an online payment service may enable a buyer to purchase goods from an individual from a credit card, causing the seller to ship the goods immediately, rather than delaying a few days or weeks. Some of these services have very high tariffs that are comparable, along with some that sometimes cost even cheaper.
Although financial institutions, respectively banking services make it impossible to ensure the use of cards online as well as to make payments, again the rights of the buyer and the seller are generally controlled by the terms of each provider.
This paper will address some of the risks of cash withdrawals from ATM's, personal bank robbery, cloning of cards and ways of cloning, their use, online shopping and new forms of business fraud as well as some ways how to protect ourselves from those dangers.
*Key words: ATM, online, cloning, fraud, payment.*

**Cyber Crime and Consumer Protection**
- Assc. Proffessor Ersida TELITI, MSc. Ketjona KAÇUPI

ABSTRACT
The development of information technology and the Internet world have broken the rules or boundaries of domestic and traditional trade. Nowadays, quick responses, purchases and contacts are made via the Internet.
Recently, it has been invented the concept of the virtual consumer which can make purchases and payments directly via internet. Electronic contracts are typical contracts, with sellers and buyers who do not know each other but perform financial transactions. All these online legal actions have resulted in a number of problems in the field of consumer rights protection. In this legal relationship, the customer is the weakest party, as from the power, as from the information or security point of view. As a consequence cyber crime is directed at him, though the party that is intended to be is the trader. By damaging the consumer through this criminal offense, the image and the security of the trader are violated.
This article will address in the theoretical and practical frame cybercrime and its impact on the consumer, the violation of personal data, their exploitation, and consumer's insecurity in online commerce. Particular attention will be paid to the Albanian legal framework as well as the legal aspect in civil and criminal law.
At the end of the paper, the authors will provide appropriate recommendations for the improvement of the legal and institutional framework to create a safer environment for the virtual consumer in Albania.
*Key words: consumer, cybercrime, personal data, electronic contracts.*

**Computer crime investigation in Albania**
- PhD. candidate Armand GURAKUQI

ABSTRACT
Due to the special features that characterize computer crime its investigation presents issues that differ from the investigation of traditional criminal offenses. Cybercrime can be committed in a fairly fast time, while the constituent elements of criminal offenses in the field of information technology may be widespread in different countries. The international nature of cyber criminality makes it mandatory to conduct

the activity of investigation in several countries. The levels of international cooperation vary depending on the domestic legislation and the will of the states in which the offense is extended. The success or failure of interstate investigation in the field of technology is closely related to timely completion and fulfillment of all investigative actions by each of the participating States.
In addition, the problematic in investigation of computer crimes is related to the fact that investigative bodies, in the framework of legal proceedings, should direct their activities to computer systems in which except traces of criminal offenses can also be found data that are included in the private life of an individual. This moment raises before the prosecutor the obligation to provide all the necessary guarantees in order to respect the private life of a person. This paper will deal with the legal provisions that govern the investigation of cybercrime in Albania, by conducting a comparative analysis of international legal instruments. At the same time, the difficulties and problems that are confronted during the investigation will be presented as part of this analysis.
Key words: investigation, computer, crime, international, cooperation.

## The Importance of Micro-Learning in Organization

- Assc. Proffessor Gaqo TANKU, PhD. Piro TANKU, MSc. Aida DELIU

ABSTRACT
Micro-learning is a holistic approach for skill based learning, education, which deals with relatively small learning units. It involves short – term – focused strategies especially designed for skill based understanding – learning – education. Micro learning refers to micro – perspectives of learning, education, training and skill development. The approaches followed for assessment of micro learning are multidimensional & holistic in nature and need based in particular cases. This is an ideal instructional approach for many situations especially in higher education for skill development, trainability and employability of learners, students. The technique is capable enough to address challenges associated with slow learners. Without taking care of micro – perspectives in the context of learning, education, training and skill development, a skill based education cannot be imparted effectively. In a wide sense, micro learning can be understood as a metaphor, which refers to micro aspects of a variety of micro-learning models, concepts and processes.
This research paper is about microlearnig in organization. We are a country that is developing recently in using technology. The main topic of this project is an approach to the definition of micro learning, how does it help in the organization, for what is used, how can effect our employees or how it can make an impact on increasing the use of technology in the company. Will it cause cost increase for the organization? Will this be negative for companies? Because we know that one of companies' priorities is minimizing costs.
*Keyword: micro learning, company, organization, technology, product.*

## Computer crime in Albania: legal basis approach and relevant chronological statistics

MSc. Artan DASHI

ABSTRACT
From 2009 to 2018 the Internet has expanded 10 times or more, Computer Crime is

now one of the biggest legal challenges. At global level, all-inclusive digitalization, economic-social, social and wider activity in every aspect of human society where, currently, about 4 billion people are online. Computer space today is one of the biggest legal challenges that has stimulated another form of crime by creating an environment for new crime methods. Now almost all crimes can be committed with the use of computers and computer systems. Given the current importance of this phenomenon nationally, given the rapid growth of Computer Crime in Albania in the last 10 years and the lack of statistical analytical interpretations of the criminal and cybercrime offenses affecting the society, the individual, the enterprise and private companies in our country and beyond, I decided to do a research on cybercrime, the legal grounds, the requirements and the need for improvement, the analytical interpretation of the cyber crime statistics in our country in the last 10 years.
The purpose of this study is to analyze the current situation in Albania in relation to legal standards, the need for legal improvements, the mechanisms for investigating and prosecuting computer crime, and the identification of the main issues and challenges facing investigators, prosecutors, police and Albanian State in preventing and combating computer crime in Albania. The following is the statistical situation according to the Criminal Code in the Republic of Albania of Computer Crime, analyzing the existing legislation and the degree of its applicability in practice, accompanied by concrete cases identified in the main urban centers in Albania.
The main questions raised and intended to be answered through this paper are: What is the current situation of Computer Crime in Albania, how is Albanian legislation on Computer Crime Corrected to respond to current challenges? and protection, preventive prophylactic measures against possible cyber attacks and attacks? The last chapter contains an analysis of the results of interviews with prosecutors and investigators of cybercrime in Albania and mainly in the city of Tirana, interviews conducted with the aim of having a more tangible and current approach to the situation and the problems of this phenomenon in Albania. To conclude, at the end of this paper are presented some recommendations for a better access and statistical analysis of cybercrime in Albania.

**Cyber Criminality and Public Safety: The Ludopathic Addictive Syndrome: Psychosocial Aspects and the need for Implementation of policing national intervention strategies!**

- Assc. Proffessor Lindita DURMISHI, PhD. Silva IBRAHIMI

ABSTRACT
Game is a basic and close instrument of learning through which the human being share in a given part with other species that have not developed a high psychic functionality. Gambling and betting sites online are one of the most motivational attitudes of cyber criminality not only to our society. The evolution of forms ranging from different online gambling levels requires at the same time a development of academic, scientific and security structures for screening, profiling and interpreting efficient systemic interventions. The present article aims to present a synthesis of a study work conducted in the period January 2018-June 2018, in a sample population of 1500 younger's on the age group 18-24 years old in Albania.
The methods administered by this study were the "Behavior Assessment Questionnaire Addictive South Oaks "and Case Studies. The obtained results revealed a progressive

increase of about 45% of the positive attitude and tendency for addiction to gambling in the cyberspace among youth. As a result, we could replicate for the development of a Ludopatic Adictive Cybercriminality dimension with specific psychological, social and cognitive characteristics and of cyber profile at the Early Adulthoold which address a specific concern of public Cybersecurity.
*Key words: Cybercriminality, Public Cybersecurity, Ludopathic Addictive Syndrome, psycho-social intervention.*

**Internet banking security**
- PhD. Bitila SHOSHA, PhD. Armela ANAMALI, PhD. Alma ZISI

ABSTRACT
With the economic development of the country, we notice an increase and improvement in the technological development in our country same as in other countries. E-banking as one of the latest trends and innovations in Albania has been best adopted as a service offered by commercial banks. One of the main problems encountered when the customer accepts to pay electronically is security. According to Kima (2010), electronic payment security depends on five factors, the system factor, technical and infrastructure factors, implementation, financial transactions and legal factors.
In protection of the customer from electronic criminality, banks offering E-banking use advanced security systems that encrypt all information between banks and their customers. One of the main reasons for using Internet Banking is to get a practical and convenient service saving time and money.
Internet Banking Technology provides one of the most effective ways to connect banks with customers by providing access to a wide range of products and financial services. E-banking automated services offer opportunities to maximize profits.
Internet Banking has also financial costs associated with investment in technology. Technology develops very fast and there is a specific cost in reaching its pace as well as improving the service.
Based on a thorough review of the literature, as well as relying on published resources regarding the security of transactions in customer protection, we will finalize our study with some important conclusions and recommendations.
*Key words: Internet Banking, e-banking, mobile Banking, security, computer systems, database, commercial bank.*

**Cyber Crime - Comparative review of legislation**
MSc. Besnik SHEHAJ

ABSTRACT
Information Technology (IT) developments and its ever-increasing applications in everyday life have unimaginably improved the quality of life of human beings, as they have made it even more vulnerable from third party interventions on personal information used through TI. This unauthorized activity of third persons has created a new area of criminal activity of persons or groups with greater scope and danger than any other conventional crime activity. This fact is evident when looking at the volume of crimes of this category in relation to criminality as a whole or the consequences of damage caused to financial value. These data may be even more frightening considering the dark part of this kind of criminality. The features of rapid

spread, with large extent and great danger, make cybercrime a mandatory target for many public and private law enforcement agencies that have to contend with specialized structures, which should be completed with professionally trained personnel and special IT knowledge, with high-level equipment and technology, well-funded and well-organized, but above all with the necessary legislation, strategy and specific action plans.
Precisely on these latest instruments of the fight against cybercrime is focused this study, claiming to carry out a comparative look between international and domestic legislation, with the aim of showing: whether it is the latest in compliance with the Acquis Communautaire; whether it is complete to combat all forms of cybercrime; if we have to anticipate with additional penal measures for some forms of emergence of this kind of crime in the world but not yet present in our country, etc.

**Handling computer crime under the Kosovo legislation and the role of police in fighting compulsory crime**
- MSc. Fadil ABDYLI

ABSTRACT
The Internet today is part of the daily life of almost all layers of society. Regarding the use of the Internet in Kosovo, the number of users in relation to the population is quite high. The Republic of Kosovo has addressed the issue of cybercrime through the legislation, in addition to the sanctioning of criminal offenses that fall in the field of cybercrime, in the Criminal Code of the Republic of Kosovo, the Law on Prevention and Combating Cybercrime has also been approved, in this law some criminal acts are foreseen. Since the Republic of Kosovo is not a signatory to the Budapest Convention or the Cybercrime Convention, the Law on Prevention and Combating Cybercrime has been based on this Convention. There are also other laws that indirectly support the prevention and fight against cybercrime.
The most common cases that cybercrime victims have suffered are: theft of different data, data destruction, cyber-bullying, online abusive sex materials with children, identity theft, threats, blackmail, etc. The damage caused by cybercrime is often cannot be compensated. The trend of cases falling in the field of cybercrime has increased rapidly, as well as cases (threats, scams, blackmails, personal data abuses) that are made possible through computer or internet are growing. Referring to statistics, compared to 2012 by 2017, the increase in the number of cases has tripled. The Kosovo Police has taken concrete steps to build a mechanism for preventing and combating all forms of cybercrime. In September 2011, the Sector for Investigation of Cyber Crime has been functional, in order to increase efficiency, it has been re-structured respectively profiling where within the Sector are formed specific units. The updating and maintenance of legal infrastructure as well as the advancement and strengthening of mechanisms for the prevention and combating cybercrime should be done consistently and based on the trends of cybercrime and cybercrime.
*Key words: society, crime, damage, legislation, mechanism.*

**National and international legislation on cybercrime**
- MSc. Ermira ÇOBAJ

ABSTRACT
At this time when the challenge of most people is to win as much money as possible and to reach the highest levels of success, there are people who do this with complete dishonesty. There are many who take unjustly the online identity of others and manipulate with their data. Cyberspace is one of the biggest legal challenges today which has sparked another form of crime, creating an environment for new crime methods. This phenomenon has a great national and global importance and it has grown rapidly in Albania despite the lack of proper studies in this area. The purpose of this study is to present the cybercrime situation in Albania, by analyzing the existence of legislation and the degree of its implementation in practice, accompanied by concrete cases and the international legal framework on cybernetics, mechanisms for its implementation. The main questions raised and intended to be answered through this paper are: What is the current situation of criminal cybernetics in Albania, how is Albanian cybernetic legislation supplemented to cope with current affairs? What are the legal mechanisms for cyber defense in the international arena?
This paper aim is to raise the awareness of the Albanian state on the importance of protecting the national security of the state and Albanian citizens from the dangers of cybernetics and by issuing recommendations on measures to be taken for a more efficient fight of this phenomenon in Albania. At the end of this paper are presented the conclusions drawn from the article and some recommendations for cybercriminals in Albania, achievements as a result of the findings made during the preparation of this article.
*Keywords: cybercrime, cyberspace, national legislation, international law.*

## Albanian business attitude towards risk management of computerized financial information: The case of financial software program 'Finance 5'

- PhD. Petrit PERHATI

ABSTRACT
The world is experiencing a rapid development of mass communication in a virtual cyberspace that is increasingly faced with progressive processes, specialized agencies, law enforcement agencies and crime-fighting structures with a new cybercrime problem and cyber threat. Of course, the attacks of this kind of sophisticated crime can not save even financial information or computerized accounting, circulating in the Albanian economic space. Computerized financial information has become the inevitable and decisive element in the process of business analysis and decision-making. Today's business organizations have a wealth of information that circulates in a computerized manner, so they are increasingly subject to cyber threats.
My study will focus on a pilot survey on the study of the attitude of Albanian business organizations in the aspect of risk management of compiled financial information, taking as a case the survey of use and administration by economic operators in Tirana, of the financial software FINANCA 5. This study, in the form of a simple survey, seeks to detect the dependence of the computer risk of financial and accounting information and of the key factors affecting the quality of this information, sophisticated computer crime and cyber threat, a group of economic operators in Tirana, who are users of the financial software program FINANCE 5. Consider factors

such as: security of the offered program, internal environment, educational and professional level of personnel managing computerized financial information, and of the IT infrastructure. The objective of this study is to bring about perceptions related to the factors that influence the enhancement of the quality of cyber defense information. The research will be descriptive and explanatory about the variables with a view to building a simple picture of the computerized financial information protection system applied by the business organization. This study aims to provide practical recommendations that arise based on the findings of the study.
*Keywords: computer crime, computerized financial information, cyber terrorism, FINANCA5, accounting operator, IT staff.*

**Cyber crime protection and security in public and private organizations, motives that push hackers to compromise digital archives**
- MSc. Sheldjana JANO

ABSTRACT
As the world increasingly becomes more dependent on technology and related networks, they change the dynamics of how the world works. Public sectors use technology with high levels of contemporary, and possibly which are more important, than privates. Fundamentals data of state that contain information on DNA, fingerprints, open cases for scrutiny with field crime technology, their digitalization allow investigative bodies to use tools and methods so that information can be quickly and efficiently absorbed and they will resolve cases as soon as possible. This change has created an extremely large and important database in storage space networks or digital archives. This information from private and public organizations is very attractive target for cyber attackers. Because of the impressive amount of information that can be obtained even by not being physically at the scene, this information becomes a prey to an objective that is very captivating to be ignored. This thesis does not propose a new technology to combat malicious users, but gives a glimpse of what really is the problem that has interfered with system breakdown and what could motivate a hacker to attack these organizations. This thesis aims to provide research on the motives of the attacker. Because in computer and security crime, behind electronic attackers are the financial reasons and the relative lack of recognition of law enforcement.
*Key words: cybercrime, national security, legislation, hacker, cyber threat.*

**Accounting manipulation, tax evasion and money laundering and their effect on informal economy**
- PhD. Jonada MAMO, Associate Proffessor Gaqo TANKU

ABSTRACT
Accounting held in accordance with the rules, principles and standards is vital to the entity. Every day in the accounting entity is recorded a large number and diverse transactions. It is very important that their appearance as accurate as possible reflect the real financial situation at every moment of the entity. Users of financial information are shareholders, directors, banks, tax authorities, customers, suppliers, employees, etc. Financial information is the basis of every decision. All are based on financial data to achieve the proper functioning of their organs, or to achieve an effective decision-making. We would like to extend the research in a macro perspective. We

will study the effects of accounting manipulation, tax evasion or money laundering on informal economy. Then, we will analyze informal economy on developing countries like Albania. Primary sources that will be used in the research are quantitative data collected by the National Registration Center for the entity's financial statements and other data collected for indicators like GDP, Taxes, Individual, Business and Government expenditure, which will be used as variables of research methodology.
We will study the development of informal economy through years in Albania. Specifically, we will stand on the effects of the variables mentioned above on it, through tax avoidance, earning management and other practices like money laundering. During the paper we will give answer to many research questions like:
Which are the indicators that are most effected from informal economy?
Are businesses using legal and illegal ways to avoid taxation and becoming unsafe for the economy and the hole society?
What may we do, to stop it?
For those and other questions we are going to give answers through the conclusions of the paper. Albania need to increase formal economy, for more taxes and more services for citizens. Also, aspirating to be part of European Union, Albania need to achieve EU's criteria.
*Key words: Accounting manipulation, money laundering, fraud.*

ISBN 978-9928-210-09-8
ISSN 2413-1334
AKADEMIA E SIGURISË
ISBN 9789928210098


**AKADEMIA E SIGURISË**
Qendra Kërkimore Shkencore
Rruga e Elbasanit, Sauk, Tiranë

POLICIMI DHE SIGURIA
NËNTOR 2018
NR
13