SIGURIA E INFORMACIONIT NË KOSOVË ME VËSHTRIM TË POSAÇËM TE VEPRAT PENALE TË NDËRLIDHURA ME SIGURINË E INFORMACIONIT

Doktoranti: Ahmet NUREDINI

Dorëzuar më 29.01.2016.
Universitetit Europian të Tiranës
Shkollës Doktorale

Në përmbushje të detyrimeve të studimeve të doktoratës në
Programin: E Drejta Penale me profil E Drejta Publike, për marrjen e gradës shkencore "Doktor".

Udhëheqës shkencor: Prof. Ass. Dr. Lulzim TAFA

Numri i fjalëve: 57893

Tiranë, Janar 2016

DEKLARATA E AUTORËSISË

E drejta e autorit: Ahmet Nuredini

Në përgjegjësinë time deklaroj se ky punim është shkruar prej meje sipas kërkesave të Shkollës Doktorale të Universitetit Europian të Tiranës, nuk është prezantuar para një institucioni tjetër për vlerësim dhe nuk është botuar.

Punimi nuk përmban material të shkruar nga ndonjë person tjetër përveç rasteve të cituara dhe referuara.

Firma: _____

ABSTRAKTI

Informacioni paraqet asetin më të rëndësishëm për të gjitha organizatat dhe agjencionet e sigurisë në përgjithësi dhe për sigurinë nacionale në veçanti.

Me zgjerimin e rrjeteve globale dhe ndërlidhjen e sistemeve të informacionit në botë, metodat e komunikimit dhe teknologjitë informatike kanë rëndësi jetike. Megjithatë, paraqitja e viruseve dhe sulmeve kompjuterike të cilat sulme shpeshherë bëhen në mënyrë të suksesshme nga keqbërësit ka vënë në pah dobësitë në teknologjitë informative aktuale dhe nevojën për të rritur sigurinë për këto sisteme.

Veprat penale të ndërlidhura me sigurinë e informacionit paraqesin sfidat më serioze jo vetëm për institucionet dhe agjencionet e sigurisë dhe sigurinë nacionale të një vendi por edhe për agjencionet ndërkombëtare të sigurisë dhe sigurinë globale. Karakteristika kryesore e veprave penale të ndërlidhura me sigurinë e informacionit është efekti global i tyre dhe për këtë arsye kërkohet një fokus ndërkombëtar, pasi që autorët me rastin e konsumimit të këtyre veprave penale shfrytëzojnë metoda nga më të ndryshmet që nuk kufizohen në njësi të veçanta territoriale. Kërkimet më moderne në lëmin e krimit të organizuar tregojnë se numri i veprave penale kundër sigurisë së informacionit janë në rritje e sipër me zhvillimin e njerëzimit dhe teknologjisë informative.

Në Republikën e Kosovës, në aspektin formal ekzistojnë disa ligje të cilat rregullojnë sigurinë e informacionit dhe veprat penale të ndërlidhura me sigurinë e informacionit por se nuk ekziston një infrastrukturë ligjore e strukturuar.

Në këtë punim doktoral do të gjejmë përgjigje në shumë pyetje ndër të cilat se çka është informacioni dhe siguria e informacionit, si klasifikohen, ruhen dhe përdoren informacionet në mënyrë që ato të jenë në disponimin tonë dhe njëkohësisht të jenë të sigurta nga qasja e paautorizuar në to nga të tjerët dhe se cilat janë sfidat e Institucioneve të Sigurisë për sigurinë e informacioneve.

Fjalët Kyçe : informacion, siguri, klasifikim, krim, inteligjencë.

ABSTRACT

The information represents the most important asset for all security organizations and agencies in general, and the national security in particular. Presently, there is a widespread global network and an interaction of information systems worldwide, therefore the means of communication and information technology play a crucial role in security of information.

However, there is a need for an increased security of systems, due to various attacks on computer systems and networks, this as a result of identified weaknesses on current information technologies by the perpetrators.

The criminal offences related to the security of the information, represent the most serious challenges not only for the national security and its institutions and agencies, but also for international security agencies and global security. The main characteristic of criminal offences related to security of information is their global effect. Being so, an international focus is required, considering that the perpetrators while committing the criminal offences use various means that have no specific territorial boundary. The recent researches on organized crime provide that, as the society develops along with information technology, the number of criminal offences against security of information increases.

Formally, there are several laws that regulate the security of information in Republic of Kosovo, including the sanctioning of criminal offences related to security of information, though a lack of a proper legal infrastructure is noted.

In this PhD thesis, we shall find answers on many questions such as: the concept of information and security of information; its classification; storage and use; means of keeping

the information secure against any unauthorized access, and the challenges of national institutions towards the security of information.

Key words: information, security, classification, crime, intelligence.

FALËNDERIME

Falënderoj në radhë të parë Zotin për të gjitha mirësitë e dhuruara.

Falënderojë familjen time të ngushtë, në radhë të parë prindërit e mi, gruan time,vajzën Edonën dhe dy djemtë e mi Shkëlqimin dhe Urimin, familjen time të gjerë, shokët dhe të gjithë ata të cilët më kanë ofruar ndihmë akademike, kërkimore, logjistike e personale, e cila ndihmë, më ka lehtësuar punën time gjatë procesit të shkrimit dhe të punimit të këtij disertacioni.

Në mënyrë të veçantë falënderojë udhëheqësin doktoral, prof. dr. Lulzim Tafa, i cili më ka përkrahur pa rezervë, dhe udhëzimet e tij ma kanë lehtësuar jashtëzakonisht punën time në finalizimin e punimit tim doktoral.

PËRMBAJTJA E LËNDËS

LISTA E TABELAVE DHE DIAGRAMEVE

LISTA E SHKURTIMEVE

AKI (Agjencia e Kosovës për Inteligjencë)

ARPA (Agjencia për Mbrojtjen e Projektit Kërkimor)

DCAF (Qendra e Gjenevës për Kontrollin Demokratik të Forcave të Armatosura)

TI (Teknologjia Informatike)

OKB (Organizata e Kombeve të Bashkuara)

OSBE (Organizata për Siguri dhe Bashkëpunim Europian)

NATO (Organizata e Traktatit të Atlantikut Verior)

NJIF (Njësia e Inteligjencës Financiare)

EUROPOL (Organizata Evropiane e Policisë)

INTERPOL (Organizata Ndërkombëtare e Policisë)

ISO (Organizata Ndërkombëtare për Standardizim)

IEC (Komisioni Ndërkombëtar Elektroteknik)

ITU (Unioni Ndërkombëtar i Telekomunikacionit)

ISC (Instituti i Sigurisë Kompjuterike)

MPB (Ministria e Punëve të Brendshme)

MF (Ministria e Financave)

PK (Policia e Kosovës)

IPK (Inspektorati Policor i Kosovës)

SIPK (Sistemi Informativ i Policisë së Kosovës)

KGJK (Këshilli Gjyqësor i Kosovës)

SOA (Agjencia e Sigurisë dhe e Inteligjencës e Kroacisë)

VSOA (Agjencia Ushtarake e Sigurisë dhe e Inteligjencës e Kroacisë)

SSK (Strategjia e Sigurisë Kombëtare)

KPK (Kodi Penal i Republikës së Kosovës)

KPS (Kodi Penal i Republikës së Sllovenisë)

KPKr (Kodi Penal i Republikës së Kroacisë)

KAPITULLI 1: HYRJE

1.1. Shtrimi i problemit

Që nga krijimi i shoqërisë njerëzore ka lindur edhe nevoja për informacionin, fillimisht, për ta përdorur atë me qëllim mbijetese dhe, më pas, për ta përdorur për doktrina të caktuara. Njëkohësisht me marrjen, grumbullimin dhe dhënien e informacionit, natyrshëm, ka dalë edhe problemi i sigurisë së tij, i ruajtjes dhe i fshehtësisë së informacionit. Madje, ky problem, pra, siguria e informacionit, në të gjitha kohët, në të gjitha vendet, vazhdimisht, por sidomos në rrethana dhe në situata të caktuara ka marrë një rëndësi të dorës së parë dhe ka luajtur rol jashtëzakonisht të madh për ekzistencën dhe për zhvillimin e secilit vend, në veçanti, ashtu edhe të njerëzimit në tërësi.

Sigurisht, me kalimin e kohës, format dhe metodat për mbledhjen e informacionit kanë evoluar dhe, me përparimin e shkencës dhe zhvillimin e teknologjisë, ato kanë ardhur vazhdimisht duke u sofistikuar. Por, krahas kësaj, është vënë re se vazhdimisht ka ardhur në rritje edhe rreziku i kërcënimeve ndaj sigurisë së informacionit. Sidomos në stadin e globalizimit të shoqërisë ky rrezik është bërë gjithnjë e më i mprehtë dhe më evident. Globalizimi i komunikimit të të dhënave bën që shpeshherë këto të fundit të jenë të kërcënuara dhe i ekspozon ato ndaj palëve të interesuara për t'i përvetësuar ato në mënyra të paligjshme dhe të palejueshme. Praktika tregon se shumë herë ruajtja dhe përcjellja e informacionit nuk ka garanci maksimale, se

ka dekonspirim dhe rrjedhje informacioni, si dhe raste kur informacioni, për shkak të ndërhyrjeve, nuk përcillet në destinacionin e duhur, por përfundon në duar të tjera.

Është e njohur nga të gjithë që sot, lidhur me informacionin shoqëria po kalon në një etapë më të zhvilluar, madje, mund të thuhet se tani jetojmë në shoqërinë e informacionit. Siç vë në dukje Rifkin, "Ne jetojmë në epokën e aksesit ku qasja në shërbime dhe në rrjete dhe pjesëmarrja në një seri aktivitetesh transferohet në hapësira kibernetike dhe në rrjete kompjuterike" (Rifkin, 2001:221). Dhe, vërtet, sot, në çdo vend, institucionet shtetërore dhe ato private, agjenci të ndryshme, por edhe individë, përdorin teknologji të përparuara të komunikimit dhe të informacionit, duke krijuar një varësi ndaj këtyre teknologjive për funksionimin sa më të mirë për mbarëvajtjen e detyrave dhe të funksioneve të secilit institucion. Tani shohim që zhvillimi ekonomik, juridik dhe social i një shteti varet dhe mbështetet shumë në teknologjinë e informacionit dhe në rrjetet e komunikimit. Duhet thënë se, krahas shumë të mirave dhe avantazheve që ka sistemi i informacionit dhe i komunikimit sot, ai gjendet para disa sfidave të mëdha lidhur me sigurinë e të dhënave dhe të proceseve që kryhen në këtë fushë. Cilat janë këto sfida? Autorët Mark Stamp dhe Jon Willey arrijnë në përfundimin se "Sfidat themelore të sigurisë së informacionit janë: konfidencialiteti, integriteti dhe disponueshmëria e të dhënave" (Mark Stamp & Jon Willey, 2011:11).

Konkretisht, siguria e informacionit është e ekspozuar ndaj kërcënimeve të veprave penale të ndërlidhura me të, të cilat vepra, kryhen nga subjekte të ndryshme dhe në format e rrugët më të ndryshme të cilët, përveç të tjerash shfrytëzojnë dhe përdorin në rrugë të paligjshme teknologjinë dhe rrjetet e të komunikimit. Këto veprime njihen si vepra penale, ngaqë rrezikojnë sigurinë e informacionit apo edhe si krime kompjuterike. Kjo dukuri negative përbën një realitet të ri, i cili jo vetëm që konsiderohet si kërcënim i

përhershëm ndaj sigurisë kombëtare të shteteve, por edhe si kërcënim i të drejtës së privatësisë së qytetarëve.

Këto lloj veprash penale janë bërë aq prezente, sa sot i ndeshim shpesh dhe rëndom edhe në shtypin e përditshëm dhe në lajmet apo emisionet e mediave elektronike. Ajo që ka rëndësi të theksohet është se veprat penale kundër sigurisë së informacionit, në të cilat përfshihet edhe kriminaliteti kompjuterik, cilësohen si një formë e veçantë e krimit të organizuar. "Kriminaliteti kompjuterik është një formë e re e krimit të organizuar dhe në radhë të parë përdoret në lëmin e ekonomisë" (Glick, 1995:212). Kjo pjesë e krimit të organizuar, si hyrja e paautorizuar në sisteme kompjuterike për të marrë të dhëna dhe informacione të rëndësishme dhe sekrete të institucioneve, organizatave, agjencive shtetërore ose private, vjedhjet e identitetit të personave të rëndësishëm apo qytetarëve të thjeshtë, zbulimi i paautorizuar i informacioneve të besueshme, spiunazhi kibernetikë etj. janë një kërcënim i madh për sigurinë e informacionit, ndaj përbëjnë vepra të mirëfillta penale, që, rrjedhimisht, kërcënojnë edhe sigurinë kombëtare të një vendi. Por duhet thënë se shqetësim për sigurinë nacionale paraqesin edhe kërcënimet jo konvencionale dhe transnacionale. Këto të fundit janë të pranishme edhe në vendet e rajonit tonë dhe përbëjnë një problem të madh, sepse nga konstatimet e bëra del që vlerësimet e tyre mbizotërohen nga terrorizmi, nga grupe dhe lëvizje ekstremiste, nga krimi i organizuar, nga autorë të trafiqeve ilegale dhe të krimeve kibernetike ("Kosova në kontekstin e sigurisë dhe të mbrojtjes të Ballkanit Perëndimor, KIPRED, 2014: 11).

Për dëmet e mëdha që sjellin dhe për rrezikshmërinë që paraqesin për sigurinë kombëtare të vendeve të ndryshme, këto vepra kriminale janë bërë objekt hetimi dhe

zbulimi nga agjenci dhe organizata të specializuara të zbatimit të ligjit në çdo vend. Por për hetimin dhe zbulimin e krimeve kompjuterike angazhohen edhe administratorë rrjetesh kompjuterike, specialistë të personelit mbështetës-teknik dhe avokatët. (Eastom &. Taylor, 2011: xvi).

Ndonëse veprat penale kundër sigurisë së informacionit nuk kategorizohen si pjesë e veprave tradicionale penale, ato janë të pranishme edhe në shoqërinë tonë. Më shqetësues në këtë mes është fakti se elementet e veprave penale të ndërlidhura me sigurinë e informacionit shprehen dhe ndërlidhen edhe me vepra të tjera penale të rënda siç janë: krimet kibernetike, terrorizmi, krimi i organizuar, mashtrimet, kërcënimet dhe vepra të tjera penale, që janë të ndëshkueshme edhe në Kosovë.

Duke qenë se jemi dëshmitarë të një përdorimi të hovshëm të teknologjisë informative nga e gjithë shoqëria, studimet për fenomenin e veprave penale të ndërlidhura me sigurinë e informacionit në këtë kohë janë më se të domosdoshme, në radhë të parë për një mbrojtje adekuate dhe vetëdijesim kundrejt sulmeve të tilla.

Zhvillimi i vendeve në fushën e teknologjisë së informacionit dhe komunikimit, sjell si rrjedhojë krijimin e organizatave të ekspertëve të sigurisë së informacionit, të cilët do të koordinojnë punën për t'u përgjigjur në çdo lloj sulmi në këtë fushë për të mbrojtur sigurinë kombëtare.

Bazuar në rrezikshmërinë e lartë të cilin e përmbajnë veprat penale kundër sigurisë së informacionit, të gjithë mekanizmat shtetërorë në përgjithësi dhe organizatat e sigurisë në veçanti duhet të ndërtojnë një arkitekturë mbrojtëse të informacionit dhe të sigurisë së tij. Në këtë kontekst, qëllimi i sigurisë së informacionit është për të siguruar disponueshmërinë e sistemeve dhe të dhënave, për të siguruar konfidencialitetin në mënyrë që asnjë person i paautorizuar të mos ketë qasje në informacione, që çdo

informacion të mbetet konfidencial gjatë transmetimit, duke siguruar autentifikimin dhe integritetin e të dhënave.

Në lidhje me sigurinë e informacionit, gjenerali kinez, Sun Tzu Wu, 2400 vjet më parë, ka theksuar:

"*Nëse ju e njihni armikun dhe e njihni veten tuaj, ju nuk duhet të keni frikë nga rezultati i njëqind betejave. Nëse ju e njihni veten, por jo armikun, për çdo betejë të fituar ju do të vuani një humbje. Nëse ju nuk e njihni as armikun e as veten, ju do të dorëzoheni në çdo betejë"* (Sun Tzu, 1988: 84).

Siguria e informacionit, ka qenë dhe mbetet një ndër prioritetet më të mëdha në çdo organizatë, qoftë ajo shtetërore apo jo-shtetërore. Ajo sot gjen zbatim në fushat të tilla si: teknologjia e informacionit dhe softuerët, sistemet kombëtare të vëzhgimit ajror, detar, tokësor, transportit dhe trafikut rrugor, sistemet e strukturave shtetërore të sigurisë kombëtare; sistemet e arkivave, sistemet e energjisë elektrike; sistemi bankar; siguria shëndetësore; sistemi i doganave, etj. Institucionet e ndryshme publike që mbulojnë dhe operojnë në këto fusha, janë përgjegjëse për të analizuar rrezikun dhe për të zbatuar masat mbrojtëse për parandalimin e sulmeve. Marrja e informacioneve me kohë për sulmet e mundshme ndaj këtyre sistemeve dhe analizimi i këtyre informacioneve mund të parandalojë me sukses sulmet e mundshme.

Nëse bëhet një vështrim i thjeshtë në infrastrukturën e sotme të informacionit dhe të komunikimit, është e mjaftueshme që të vlerësojmë arkitekturën e informacionit (Bloch & Barrosh, 2011: 3). Besimi i tepërt në sistemet komunikuese dhe informative i ka bërë shtetet të cenueshme ndaj veprave penale kundër sigurisë së informacionit, të cilat mund të shkaktojnë dëme të mëdha në sistemet kombëtare, në rrjetet dhe në

infrastrukturën e informimit, ekonomisë, bankave, bizneseve, trafikut ajror dhe tokësor. Sot në botë ndodhin qindra-mijëra sulme kibernetike në baza ditore dhe këto sulme po bëhen më të ashpra çdo ditë e më tepër. Pritet që kërcënimet nga veprat penale kundër sigurisë së informacionit dhe në veçanti nga sulmet kibernetike do të shtohen gjatë viteve në vijim. Si i tillë, ky lloj kërcënimi dhe sulmi mund të shkaktojë dëme ekstreme në administratën publike, në ekonominë dhe infrastrukturën e Kosovës.

Këto krime shkaktohen nga një agjendë politike dhe me aktivitete kriminale. Në këtë mënyrë, krimet kibernetike paraqesin një rrezik ndaj sigurisë, stabilitetit dhe funksionimit të shtetit. (Analizë e rishikimit strategjik të Sektorit të Sigurisë, 2014: 19-20).

Për shkak të shpejtësisë dhe avantazheve që ofron interneti, si pjesë e hapësirës së informacionit, zë një vend më të madh si një teknologji e re e komunikimit. Ekzistojnë edhe rrjete të tjera përveç atyre të përmendura më lart, siç janë rrjetet LANs (Local Area Networks) dhe WANs (Wide Area Networks). Këto rrjete quhen ndryshe si intranet, për shkak se janë rrjete brenda një sistemi të mbyllur. Një rrjet i tillë i mbyllur gjendet në institucionet që përfshijnë fushën e sigurisë, ushtarake dhe financiare. Këto sisteme përdoren për qëllimin e mbrojtjes ndaj sulmeve dhe kërcënimeve ndaj informacioneve, të cilat shpeshherë në këto institucione janë edhe sekrete. Çdo shpërndarje e informacionit dhe keqpërdorim i tij në këtë sistem të mbyllur të quajtur intranet, i cili hyn në hapësirën e informacionit dhe të komunikimit, përbën shkelje dhe klasifikohet si krim kibernetik. Nuk duhet të jeni një oficer i zbatimit të ligjit ose një ekspert i sigurisë kompjuterike për të kuptuar se veprat penale kundër sigurisë së informacionit e në këtë kontekst edhe krimet kompjuterike janë në rritje. Rritja e krimit

kompjuterik duhet të jetë shqetësim i rëndësishëm për çdo agjenci të zbatimit të ligjit ose për të gjithë përgjegjësit për sigurinë e çdo rrjeti. (Eastom &. Taylor, 2011: xvi).

1.2. Struktura e punimit

Punimi i kësaj doktorature përbëhet prej tetë kapitujve.

Në kapitullin *e parë* shtjellohet aspekti hyrës në sigurinë e informacionit dhe të veprave penale të ndërlidhura me sigurinë e informacionit.

Në kapitullin e *dytë* shtjellohen aspekte teorike dhe historike të sigurisë së informacionit.

Në kapitullin *e tretë* shtjellohet aspekti juridiko-penal i veprave penale të ndërlidhura me sigurinë e informacionit. Në pjesën e parë të këtij kapitulli shtjellohet aspekti juridiko-penal i veprave penale të ndërlidhura me sigurinë e informacionit të parashikuara në Kodin Penal të Kosovës, ndërsa në pjesën e dytë trajtohen veprat penale të ndërlidhura me sigurinë e informacionit të kryera me anë të mjeteve të teknologjisë informative dhe veprat penale të ndërlidhura me sigurinë e informacionit të parapara me ligjin për parandalimin dhe luftimin e krimeve kibernetike.

Në kapitullin *e katërt* shtjellohet analiza krahasuese e legjislacionit të Sllovenisë dhe të Kroacisë në fushën e veprave penale të ndërlidhura me sigurinë e informacionit.

Në kapitullin *e pestë* bëhet një analizë empirike e të dhënave statistikore për veprat penale të ndërlidhura me sigurinë e informacionit në Kosovë në periudhën 2007 – 2015. Në pjesën e parë të këtij kapitulli jepet analiza e të dhënave të Policisë së Kosovës

dhe të Këshillit Gjyqësor të Kosovës, ndërsa në pjesën e dytë bëhet një analizë empirike e të dhënave të fituara përmes instrumentit të pyetësorit.

Në kapitullin *e gjashtë* shtjellohet aspekti fenomenologjik dhe etiologjik i veprave penale të ndërlidhura me sigurinë e informacionit.

Në kapitullin *e shtatë* shtjellohet aspekti krahasues i klasifikimit të informacioneve dhe shërbimeve të inteligjencës dhe i rolit të tyre për sigurinë e informacionit.

Në kapitullin *e tetë* janë evidencuar disa përfundime dhe rekomandime, bazuar në hulumtimin dhe në analizën e materialit të studiuar për këtë temë.

1.3. Qëllimi i studimit

Qëllimi parësor i studimit është që t'i kontribuojë aspektit teorik dhe praktik të parandalimit dhe të luftimit të veprave penale të ndërlidhura me sigurinë e informacionit.

Qëllimi i kësaj mikroteze doktorature është që t'u kontribuojë reformimit të legjislacionit penal në fushën e sigurisë së informacionit, avancimit të njohurive të përgjithshme për informacionin, rëndësinë e sigurisë së informacionit për sigurinë nacionale dhe për studimin e hulumtimin e aspektit juridiko-penal të veprave penale të ndërlidhura me sigurinë e informacioneve.

Qëllim dytësor apo sekondar është hulumtimi i aspektit fenomenologjik dhe etiologjik të veprave penale kundër sigurisë së informacionit.

1.4. Hipotezat e punimit

Hipotezat kërkimore të këtij disertacioni janë ngritur dhe formuluar për të arritur në konstatime dhe në konkluzione finale në funksion të tematikës së kërkimit shkencor.

Me qëllim të studimit sa më përmbajtësor dhe të analizimit të veprave penale të ndërlidhura me sigurinë e informacionit në Kosovë, kam parashtruar katër hipoteza:

- *Hipoteza e parë (kryesore):* Në Republikën e Kosovës nuk ekziston një infrastrukturë ligjore e strukturuar, e cila rregullon sigurinë e informacionit.

- *Hipoteza e dytë*: Në Kosovë, në aspektin formal ekzistojnë disa ligje të cilat rregullojnë sigurinë e informacionit, por sfidë mbetet zbatimi i këtyre ligjeve në praktikë.

- *Hipoteza e tretë:* Në institucionet e sigurisë së Republikës së Kosovës, siguria fizike e informacionit i plotëson të gjitha standardet e parapara me ligjet e aplikueshme.

- *Hipoteza e katërt:* Në Kosovë janë shënuar pak raste të veprave penale të ndërlidhura me sigurinë e informacionit, në të cilat raste autorë të këtyre veprave penale janë kryesisht personat e gjinisë mashkullore.

1.5. Pyetjet kërkimore hulumtuese

Pyetja kërkimore hulumtuese ka funksion të dyfishtë: ajo shpreh qëllimin e projektit të hulumtimit, por edhe na jep drejtimin në procesin e hulumtimit (Matthews B., & Ross L., 2010:57).

Pyetjet kërkimore të aplikuara në këtë punim doktorature kanë rëndësi themelore për projektin dhe i kanë dhënë hulumtimit kahjen e shqyrtimeve, duke mundësuar lehtësimin e analizave dhe arritjen e disa konkluzioneve të punimit.

Në këtë punim janë aplikuar këto pyetje kërkimore:

- Çka janë informacionet? Si duhet t'i klasifikojmë, si t'i ruajmë dhe si t'i përdorim informacionet në mënyrë që ato të jenë në disponimin tonë dhe, njëkohësisht, të jenë të sigurta që të tjerët të mos kenë qasje të paautorizuar në to?

- Cilët janë faktorët që ndikojnë në sigurinë e informacionit? Pse informacioni dhe siguria e tij janë të rëndësishme për shoqërinë, në përgjithësi, dhe për sigurinë kombëtare, në veçanti?

- Si është organizuar mbrojtja kibernetike dhe mbrojtja e sistemeve të informacionit në Kosovë ndaj sistemeve depërtuese të vendeve që janë të interesuara për arsye historike në zotërimin e informacionit të klasifikuar të Republikës së Kosovës?

- Si i rregullon legjislacioni kombëtar veprat penale të ndërlidhura me sigurinë e informacionit në Kosovë? Cilat janë sfidat që vështirësojnë zbatimin në praktikë të këtij legjislacioni?

- Cilat janë sfidat e institucioneve shtetërore të sigurisë për sigurinë e informacionit? Cili është i roli i shërbimeve të inteligjencës për sigurinë e informacionit?

- Si përkufizohen veprat penale të ndërlidhura me sigurinë e informacionit? Cilat janë motivet dhe mënyrat e kryerjes së veprave penale të ndërlidhura me sigurinë e informacionit?

- Cilat janë veçoritë e të dyshuarve dhe të autorëve të veprave penale të ndërlidhura me sigurinë e informacionit sipas gjinisë, moshës, përkatësisë etnike, nivelit arsimor?

1.6. Metodologjia dhe metodat e kërkimit

Metodologjia e kërkimit

Metodologjia në thelb ka të bëjë me epistemologjinë dhe ontologjinë e hulumtimit Matthews B., & Ross L., (2010:57).

Ngaqë në fokus të këtij studimi kanë qenë siguria e informacionit dhe veprat penale kundër sigurisë së informacionit në Republikën e Kosovës, numri më i madh i të dhënave janë grumbulluar nga burime të ndjeshme të informatave - burimet e mbyllura, siç janë baza e të dhënave e sistemit informativ të Policisë së Kosovës, bazat e të dhënave të Këshillit Gjyqësor të Kosovës, raportet statistikore të policisë dhe të gjykatave etj. Pjesa tjetër e të dhënave janë grumbulluar nga burimet e hapura të informacioneve, siç janë uebfaqet e internetit, mediat elektronike dhe ato të shkruara, rrjetet e ndryshme sociale etj.

Me qëllim grumbullimin e të dhënave sa më relevante dhe arritjen e rezultateve sa më të sakta është hartuar një pyetësor i përbërë nga 24 pyetje, kryesisht, nga fusha e informacionit dhe e sigurisë së informacioneve, ku si kampion ishin zgjedhur 400 zyrtarë të institucioneve të ndryshme, të cilët kishin qasje në informacionet e klasifikuara. Institucionet në të cilat janë mbledhur të dhënat janë Policia e Kosovës, Inspektorati i Policisë së Kosovës dhe Dogana e Kosovës. Megjithëse ishte planifikuar mbledhja e të dhënave edhe nga institucione të tjera të sigurisë, disa nga këto

institucione përkundër faktit që i kanë pranuar pyetësorët, nuk i kanë plotësuar ata, me arsyetimin se përgjigjet në disa nga pyetjet që përmbante pyetësori mund të përbënin shkelje të konfidencialitetit të të dhënave.

Në studim janë përfshirë zyrtarë të institucioneve të ndryshme të sigurisë, të cilët kryesisht grumbullojnë, vlerësojnë, analizojnë dhe shpërndajnë të dhëna dhe informacione të klasifikuara. Po ashtu, një numër i konsiderueshëm i këtyre zyrtarëve çdo ditë trajtojnë informacione të klasifikuara dhe hartojnë raporte analitike strategjike, siç janë vlerësime strategjike, vlerësime për kërcënimet nga krimet e rënda dhe nga krimi i organizuar, vlerësime mbi situatën e sigurisë.

Metodat e kërkimit

Në zhvillimin e këtij disertacioni kam aplikuar disa metoda shkencore, të cilat konsistojnë në studimin e informacionit, të sigurisë së informacionit dhe të veprave penale kundër sigurisë së informacionit në dimensionet e evoluimit dhe të shfaqjes së tyre, por duke u fokusuar në shoqërinë bashkëkohore, e parë kjo në perspektivën e kuadrit ligjor kombëtar dhe ndërkombëtar.

Metodat që janë aplikuar në studimin e kësaj teme janë: metoda juridike, metoda e analizës, metoda statistikore, metoda krahasuese dhe metoda tjera studimore, të cilat janë gërshetuar në çështjet e trajtuara në këtë punim. Aplikimi i këtyre metodave arsyetohet me faktin e pasqyrimit të rëndësisë së informacionit, të veprave penale të ndërlidhura me sigurinë e informacionit, por edhe të rrezikut që u kanoset nga këto vepra shoqërisë, shtetit dhe sigurisë kombëtare.

Metoda juridike është zgjedhur dhe zbatuar në mikrotezën time doktorale për të pasqyruar infrastrukturën ligjore në fushën e sigurisë së informacionit. Aplikimi i kësaj metode ka qenë mjaft e përshtatshme për temën, sepse përmes saj janë pasqyruar karakteristikat juridiko-penale të veprave penale të ndërlidhura me sigurinë e informacionit, është paraqitur një analizë krahasuese e legjislacionit të disa vendeve në fushën e klasifikimit të informacioneve dhe të veprave penale të ndërlidhura me sigurinë e informacionit.

Metoda e analizës është aplikuar për të njohur sa më mirë materien e sigurisë së informacionit dhe të veprave penale të ndërlidhura me sigurinë e informacionit. Me aplikimin e kësaj metode kemi mundur të pasqyrojmë analizën e të dhënave për rastet e veprave penale të ndërlidhura me sigurinë e informacionit për periudhën 2007-2015. Me këtë rast, fillimisht janë grumbulluar dhe, më pas, janë analizuar të dhënat e policisë, të dhënat e sistemit gjyqësor dhe të dhënat e fituara me instrumentin e pyetësorit.

Të dhënat e grumbulluara nga policia janë analizuar për secilën vepër penale të ndërlidhur me sigurinë e informacionit, veç e veç, sipas periudhës së raportimit, sipas rajoneve në të cilat kanë ndodhur këto vepra, pastaj janë analizuar të dhënat për gjininë, moshën, përkatësinë etnike dhe arsimimin e personave të dyshuar për veprat penale.

Të dhënat e grumbulluara nga sistemi gjyqësor janë analizuar për secilën vepër penale të ndërlidhur me sigurinë e informacionit, veç e veç, sipas vendimeve për numrin e personave të gjykuar në Kosovë, janë analizuar të dhënat për gjininë, moshën, përkatësinë etnike dhe arsimimin e personave të dënuar dhe të dhënat për rastet e veprave penale të gjykuara sipas rajoneve të Kosovës.

Nga të dhënat e mbledhura dhe analizuara gjininë, moshën dhe arsimimin janë arritur deri tek analizat konkrete dhe përfundimet për aspektet fenomenologjike të

personave të dyshuar, personave të dënuar dhe viktimave të veprave penale të ndërlidhura me sigurinë e informacionit.

Me metodën e analizës janë analizuar po ashtu edhe të dhënat e fituara përmes pyetësorëve. Si rezultat i aplikimit të kësaj metode kemi arritur deri te faktet dhe rekomandimet shumë të rëndësishme, të cilat do të na shërbejnë për të hulumtuar rreth informacionit, sigurisë së informacionit, por edhe për veprat penale të ndërlidhura me sigurinë e informacionit.

Metoda statistikore ka shërbyer për të evidencuar vëllimin, strukturën dhe dinamikën e veprave penale të ndërlidhura me sigurinë e informacionit. Duke marrë për bazë të gjitha statistikat e mbledhura nga institucione të ndryshme përmes kësaj metode, kemi realizuar zbërthimin e këtyre të dhënave dhe krahasimin e tyre ndërmjet institucioneve të zbatimit të ligjit në Kosovë. Gjithashtu, përmes kësaj metode janë analizuar të dhënat e grumbulluara nga institucione të ndryshme për veprat penale kundër sigurisë së informacionit, për të nxjerrë karakteristika të të dyshuarve, të të dënuarve dhe të viktimave të këtyre veprave penale.

Metoda krahasuese është përdorur për të vënë përballë rregullimin e bërë nga legjislacioni i Kosovës në fushën e klasifikimit të informacionit, të veprave penale të ndërlidhura me sigurinë e informacionit, e parë kjo në raport me rregullimin e bërë nga legjislacioni i dy vendeve të BE-së, që bëjnë pjesë në rajonin tonë: Sllovenisë dhe Kroacisë.

Për të nxjerrë përfundime të sakta, të dhënat e grumbulluara janë krahasuar sipas rasteve të veprave penale të ndërlidhura me sigurinë e informacionit në Kosovë, të evidencuara dhe të trajtuara në Polici dhe në Gjykata.

1.7. Mundësitë dhe kufizimet

Mundësitë

- Njohuritë teorike dhe përvoja praktike në fushën e sigurisë së informacionit.

Njohuritë teorike dhe përvoja praktike në fushën e informacionit dhe të sigurisë së informacionit kanë paraqitur një mundësi të mirë. Përvoja ime 16-vjeçare e punës dhe e e aktivitetit pedagogjik në Polici, përvoja pesëvjeçare teorike dhe praktike në një kolegj universitar si ligjërues i lëndës 'Siguria e Informacionit', në njërën anë, dhe përvoja praktike pesëvjeçare si Drejtor i Drejtorisë së Inteligjencës dhe Analizës, në fushën e grumbullimit, vlerësimit, analizimit dhe shpërndarjes së informacioneve të klasifikuara më kanë lehtësuar shumë punimin e kësaj mikroteze doktorature.

-Mundësia e studimit nga burimet bibliografike

Ekziston një literaturë e bollshme shkencore dhe akademike në fushën e sigurisë së informacionit andaj kjo ishte mundësi tjetër, e cila e ka lehtësuar punën time në finalizimin e kësaj teme.

-Mundësia e studimit nga burimet e hapura të informacioneve

Burimet e hapura të informacioneve më kanë ofruar mundësi të mirë për qasje në literaturë shkencore dhe akademike në fushën e sigurisë së informacionit në veçanti për të studiuar aspektin krahasues të legjislacionit.

- Qasja në të dhënat e Policisë për trendin e veprave penale të ndërlidhura me sigurinë e informacionit.

Policia e Kosovës zotëron një mori bazash të të dhënave, të cilat përmbajnë informacione të mjaftueshme lidhur me ecurinë e të gjitha veprave penale të parapara në Kodin Penal të Kosovës. Kjo ka paraqitur një mundësi mjaft të mirë. Të dhënat e rasteve të evidencuara në sistemin informativ të Policisë së Kosovës më kanë mundësuar trajtimin dhe analizimin hollësishëm të veprave penale të ndërlidhura me sigurinë e informacionit në Kosovë, si edhe analizimin e të dhënave për personat e dyshuar si autorë të këtyre veprave penale dhe të karakteristikave të tyre sipas gjinisë, moshës, arsimimit, përkatësisë etnike.

- ***Qasja në të dhënat e Këshillit Gjyqësor të Kosovës***

Të dhënat e rasteve të evidencuara në bazat e të dhënave të Këshillit Gjyqësor të Kosovës më kanë mundësuar analizimin hollësishëm të vendimeve gjyqësore të shqiptuara ndaj autorëve të veprave penale të ndërlidhura me sigurinë e informacionit, vendime që përmbajnë të dhëna të mjaftueshme për autorët e dënuar e për këto vepra penale, si dhe karakteristikat e tyre sipas gjinisë, moshës, arsimimit, përkatësisë etnike.

Kufizimet

Gjatë punës kërkimore kam hasur dhe jam ballafaquar me shumë kufizime, të cilat ndërlidhen me natyrën specifike të veprave penale të kësaj fushe, kufizime të tilla si:

- Mungesa e të dhënave në praktikën gjyqësore të Kosovës për rastet e veprave penale të ndërlidhura me sigurinë e informacionit

Kjo ishte një pengesë e madhe të cilën jemi ballafaquar ishte mungesa e të dhënave në Praktikën Gjyqësore të Kosovës për raste të veprave penale të ndërlidhura me sigurinë e informacionit.

Megjithëse shfletuam të gjitha botimet e Buletineve të periudhës 2007-2015 të Praktikës Gjyqësore të Gjykatës Themelore, të Gjykatës së Apelit, të Gjykatës Supreme dhe të Gjykatës Kushtetuese, nuk arritëm të gjejmë të dhëna për veprat penale që janë në fokus të studimit tonë.

- Mungesa e studimeve të thelluara hulumtuese dhe shkencore lidhur me këtë temë

Në Republikën e Kosovës mungojnë studimet e thelluara hulumtuese dhe shkencore lidhur me informacionin dhe sigurinë e informacionit. Ky është i pari studim në Kosovë, që trajton sigurinë e informacionit dhe veprat penale të ndërlidhura me sigurinë e informacionit.

- Mangësitë e kuadrit ligjor

Ekzistojnë mangësi të konsiderueshme të legjislacionit në fushën e sigurisë së informacionit. Informacionet dhe veprat penale të ndërlidhura me informacionin rregullohen me pak ligje. Ky fakt ka paraqitur vështirësi të konsiderueshme në trajtimin e kësaj teme.

- Procedurat e ndërlikuara për aprovimin e kërkesave të bëra nga ana jonë për qasje në të dhëna

Një tjetër vështirësi të madhe kanë paraqitur procedurat e ndërlikuara dhe vonesat për aprovimin e kërkesave të bëra nga ana jonë për qasje në të dhëna. Këto kërkesa diktoheshin nga mungesa e të dhënave apo nga refuzime të kërkesave tona për qasje në të dhëna në disa Institucione të Kosovës. Veçanërisht, disa agjenci të Sigurisë kanë hezituar në aprovimin e kërkesës për plotësimin e pyetësorëve, me arsyetimin se disa nga përgjigjet e pyetjeve që i përmbante pyetësori mund të përfshinin të dhëna të klasifikuara.

- Mungesa e të dhënave të Prokurorisë së Shtetit

Prokuroria e Shtetit i është përgjigjur negativisht kërkesës sonë për të dhëna statistikore lidhur me veprat penale të ndërlidhura me sigurinë e informacionit, me arsyetimin se Zyra për Statistika nuk disponon këto lloje të dhënash dhe se Këshilli Prokurorial i Kosovës nuk disponon një sistem elektronik për menaxhimin e rasteve të kësaj natyre, që do të thotë se prokuroritë raportimin statistikor e bëjnë me formularë.

- Mungesa e qasjes në të dhëna të Agjencisë së Kosovës për Inteligjencë

Kufizim tjetër ka paraqitur mungesa e qasjes në të dhëna të Agjencisë së Kosovës për Inteligjencë, bazuar në faktin se kjo agjenci ende nuk e ka të krijuar faqen e saj të internetit.

- Mungesa e qasjes në të dhëna të Forcës së Sigurisë së Kosovës

Ministria e Forcës së Sigurisë nuk iu përgjigj kërkesës sonë për plotësimin e pyetësorëve, që i dërguam me synimin që të realizonim analiza sa më cilësore të problematikës së studimit.

1.8. Rëndësia e studimit

Studimi merr rëndësinë e vet, sepse ai plotëson një boshllëk që ekziston nga fakti se në Republikën e Kosovës një temë e tillë që lidhet me aspektin e sigurisë së informacionit nuk është studiuar deri më tani dhe ngaqë këtu ka mungesë të ndjeshme të literaturës dhe të kuadrove të sigurisë së informacionit dhe veçanërisht në institucionet e sigurisë.

Si një hap i parë në këtë drejtim, ky punim besojmë se do t'u shërbejë të gjithë të interesuarve për t'u njohur me anën teorike të çështjes së informacionit dhe të sigurisë së tij, si edhe me problematikat praktike në këtë fushë kaq të rëndësishme. Po ashtu, mendojmë se ky punim do të jetë një bazë e mirë për hulumtime dhe studime të mëtejshme nga studentë dhe persona të tjerë të interesuar, për ta çuar më tej avancimin e analizave të sigurisë së informacionit, të veprave penale të ndërlidhura me sigurinë e informacionit në funksion të parandalimit dhe luftimit sa më efikas të këtyre veprave, që përbëjnë kërcënim edhe për sigurinë kombëtare.

Njëkohësisht, mendoj se studimi i kryer nga ana jonë do të jetë një shtytje dhe kontribut edhe për reformimin, plotësimin dhe përmirësimin e legjislacionit penal në fushën e sigurisë së informacionit. Në të pushteti legjislativ do të gjejë edhe propozime e sugjerime konkrete në këtë fushë, si, fjala vjen: të hartohet një strategji nacionale për

sigurinë e informacionit; në Kodin Penal të Kosovës, veprat penale kundër sigurisë së informacionit të përfshihen në një kapitull të veçantë të veprave penale etj.

Nga ana tjetër, ky punim doktorature mendojmë se do të jetë një ndihmesë për agjencitë e zbatimit të ligjit, si policia, prokuroria, gjykatat, institucionet e sigurisë kombëtare, të shërbimeve të inteligjencës dhe veçanërisht për grupet hetuese që merren me parandalimin dhe me luftimin e veprave penale kundër sigurisë së informacionit, të cilat do të gjejnë në të analiza, ide, që zgjerojnë horizontin teoriko-profesional të tyre, por edhe rekomandime dhe sugjerime që lidhen me veprimtarinë praktike të tyre. Në këtë punim janë bërë përpjekje që t'u jepen përgjigje disa pyetjeve që dalin në këtë fushë dhe ngrihen hipoteza që mund të bëhen objekt studimi dhe analizash të mëtejshme.

Gjithashtu punimi do t'u vlente edhe institucioneve edukative dhe arsimore, organizatave të ndryshme qeveritare dhe joqeveritare, mediave etj. në punën e tyre për edukimin e ndërgjegjësimin e qytetarëve për rrezikun dhe për pasojat e veprave penale të ndërlidhura me sigurinë e informacionit, me synimin që veprimtaria e tyre të kontribuojë sa më mirë në funksion të parandalimit dhe të luftimit të veprave penale në fushën e informacionit.

Në tërë punën e bërë në këtë punim kam pasur synimin që me këto që përmenda këtu dhe me të tjera, jo vetëm të rris më tej kualifikimin tim shkencor e profesional, por edhe që ai të shërbejë në praktikë për ngritjen e nivelit shkencor dhe të efikasitetit të punës së organizatave dhe agjencive që merren me zbatimin e ligjit dhe me sigurinë kombëtare, por dhe të punonjësve të tyre në këtë fushë, për të cilën është e interesuar e gjitha shoqëria jonë.

Shpreh bindjen se hulumtimi i kësaj teme do të plotësohet edhe nga studiues, profesorë dhe akademikë të tjerë, nga funksionarë të tjerë të kësaj fushe, pasi rëndësia e kësaj çështjeje është jashtëzakonisht e madhe dhe ajo do të mbetet përherë një temë aktuale.

KAPITULLI 2: ASPEKTE TEORIKE DHE HISTORIKE TË SIGURISË SË INFORMACIONIT

2.1. Aspekte teorike të sigurisë së informacionit

Përkufizimi dhe rëndësia e informacionit

Informata apo informacioni ka të bëjë me njoftimin që marrim për diçka, me të dhëna për gjendjen e punëve në një fushë të caktuar, për veprimtarinë e dikujt, për një ngjarje (Fjalori i gjuhës së sotme shqipe, 1980: 721). Fjala informacion rrjedh nga gjuha latine *information*, që do të thotë formim, lajmërim, njoftim, sqarim, arsimim. Në përgjithësi, informacion është çfarëdo lloj lajmi apo tregimi, çfarëdo komunikim i shkruar apo gojor. Informacioni është diçka që mund të mësojmë, të njohim apo të kuptojmë.

Në mënyrë më të hollësishme, informacioni trajtohet nga shkenca e informacionit. Kjo shkencë është disiplina që studion informacionin, mbledhjen, analizën, rrjedhën e tij, si dhe mjetet e përpunimit të informacionit për qasje optimale dhe të përdorshmërisë. Ajo ka të bëjë me njohuritë në lidhje me mbledhjen, organizimin, ruajtjen, tërheqjen, interpretimin, transmetimin, transformimin dhe shfrytëzimin e informacionit. Këtu përfshihen përdorimi i kodeve për të qenë më efikas në transmetimin e mesazhit dhe studimi i pajisjeve të përpunimit të informacionit dhe teknikave të tilla, si kompjuterët dhe sistemet e tyre programore (Borko, 1968: 3-5).

Informacioni është një aset me vlerë për shoqërinë, për individin, për biznesin e organizatave, por, në veçanti, për sigurinë nacionale. Disponimi i informacioneve, njohja me to, përdorimi sa më efikas i tyre do t'i shërbente marrjes së vendimeve të

drejta dhe efikase në fushën që mbulon secili institucion, organizatë apo individ. Për këto arsye, çdo organizatë apo institucion në veprimtarinë e vet të përditshme krijon dhe disponon informacione që lidhen me veprimtarinë që zhvillon. Por, gjithashtu, ato kanë nevojë të sigurojnë pandërprerë sa më shumë informacione edhe nga burime të tjera, pasi kështu do të arrijnë më shumë rezultate. Këto përpjekje për marrje informacioni bëhen nën hijen e luftës që zhvillohet në vazhdimësi për ta njohur në mënyrën më të drejtë të mundshme situatën e cila na e shpjegon më së miri të vërtetën.

Informacioni ekziston në shumë forma. Ai mund të jetë i shtypur ose i shkruar në letër, i ruajtur në mënyrë elektronike, i transmetuar me postë ose duke përdorur mjete elektronike, i evidencuar në filma apo i folur. Karakteristikë e epokës në të cilën jetojmë është se informacioni dhe komunikimi po bëhen gjithnjë e më të varur nga interneti.

Karakteristikat kritike të informacionit

Vlera e informacionit vjen nga karakteristikat që ai zotëron. Kur një karakteristikë e informacionit ndryshon, vlera e këtij informacioni, ose rritet, ose ulet. Fjala këtu është për ato karakteristika që cilësohen si kritike. Këto janë: disponueshmëria, saktësia dhe vërtetësia e informacionit.

Disponueshmëria e një informacioni u mundëson përdoruesve të autorizuar apo sistemeve kompjuterike qasje në të, pa ndërhyrje të paligjshme ose pa pengesa për ta marrë atë në formatin e kërkuar. Këtu hyjnë informacionet që gjenden në arkiva, ato që gjenden në biblioteka në kategorinë ‘rezervat’ etj., ku hulumtuesve u kërkojnë identifikimin para hyrjes. Arkivistët, bibliotekarët mbrojnë përmbajtjen e informacionit që disponojnë dhe kujdesen që të shfrytëzohet sipas rregullave vetëm nga të autorizuarit.

Arkivat dhe bibliotekat duhet të marrin një identifikim mbrojtës përpara se mbrojtësi të ketë qasje të lirë në informacione dhe libra.

Saktësia e informacionit - Informacioni konsiderohet i saktë kur ai nuk ka gabime dhe e ka vlerën të cilën përdoruesi e pret. Nëse një informacion është modifikuar, me qëllim apo pa qëllim, ai nuk është i saktë. Përmendim këtu si shembull llogaritë rrjedhëse bankare. Ju supozoni se të dhënat që gjenden në llogarinë tuaj rrjedhëse paraqesin saktë gjendjen tuaj financiare. Por ndodh që në llogarinë tuaj të kontrolluar mund të ketë informacion të pasaktë, i cili rezulton ose nga gabimet ose nga ndërhyrjet e qëllimshme nga jashtë ose nga brenda institucionit.

Vërtetësia (origjinaliteti) e informacionit është cilësia ose gjendja e të qenit të vërtetë apo origjinal. Informacioni është autentik, kur ai është në gjendjen në të cilën është krijuar, vendosur, ruajtur ose transferuar, kur në të nuk ka asnjë ndryshim, heqje apo shtesë.

Vlera e konfidencialitetit të informacionit është veçanërisht e lartë kur është informacion personal rreth punonjësit, klientit apo pacientit. Individët të cilët punojnë në një organizatë presin që të dhënat e tyre personale do të mbeten konfidenciale. Problemet lindin kur kompanitë apo institucionet zbulojnë informacionin konfidencial. Ndonjëherë zbulimi i tij është i qëllimshëm, por ka raste kur zbulimi i informacionit konfidencial ndodh gabimisht, për shembull, kur ky informacion konfidencial shkëmbehet gabimisht me e-mail me dikë jashtë organizatës, në vend që ai të shkëmbehet me ndokënd brenda organizatës. Shembuj të tjerë të shkeljeve të konfidencialitetit janë kur një punonjës dërgon një dokument jashtë organizatës, ose një haker, i cili arrin të zbulojë fjalëkalimin e një baze të dhënash, vjedh informatat e ndjeshme për klientët, të tilla si emrat, adresat, numrat e kartave të kreditit etj.

Integriteti i informacionit. Informacioni ka integritet kur ai është i saktë, i plotë dhe i pandryshuar. Integriteti i informacionit është i kërcënuar, kur informacioni është i ekspozuar ndaj korrupsionit, kur nga një sistem informativ shkelen dhe neglizhohen rregullat dhe procedurat, pra, udhëzimet e shkruara për funksionimin normal të këtij sistemi, ose kur këto procedura të një organizate merren nga një përdorues i paautorizuar. Meqë edhe procedurat janë informacione, ato duhet të njihen mirë nga të gjithë anëtarët e organizatës vetëm në bazë të nevojës për të ditur.

Siguria e informacionit

Siguria e informacionit mund të përkufizohet si mbrojtja e informacionit nga qasjet e paautorizuara, nga transferimi, nga modifikimi dhe nga shkatërrimi aksidental ose i qëllimshëm i informacioneve që disponon një organizatë apo institucion. Sipas Blyth dhe Kovaçiç, "Siguria e informacionit është për të mbrojtur asetet e informacioneve nga shkatërrimi, nga degradimi, nga manipulimi dhe nga shfrytëzimi nga ndonjë kundërshtar" (Blyth & Kovacich, 2007: 3).

Siguria e informacionit ka qenë dhe mbetet një ndër prioritetet më të mëdha në çdo organizatë, qoftë ajo shtetërore apo joshtetërore, me synimin që informacioni të jetë "i sigurt, i lirë nga rreziku apo kërcënimi" (Whitman & Herbert & Mattord, 2011: 8).

Qëllimi i sigurisë së informacionit është që të sigurohen disponueshmëria e sistemeve dhe e të dhënave; të sigurohet konfidencialiteti i informacione, në mënyrë që asnjë person i paautorizuar të mos mund të ketë qasje në to, që çdo informacion të

mbetet konfidencial gjatë transmetimit të tij, duke siguruar, kështu, autenticitetin dhe integritetin e të dhënave.

Në fund të fundit, siguria e informacionit konsiston në mbrojtjen nga një gamë e gjerë kërcënimesh të vetë informacionit, si edhe të elementeve të tij kritike, që, siç i kemi përmendur, janë konfidencialiteti, integriteti dhe disponueshmëria e informacionit. Pikërisht këta janë dhe objekti kryesor i sigurisë së informacionit. Konkretisht:

Në kuptimin e sigurisë së informacionit, *konfidencialiteti* është fshehja e informacionit ose e burimeve të informacionit (Bishop, (2004: 2). Me zbatimin dhe respektimin e konfidencialitetit, sigurohet që informacioni të jetë në disponim vetëm për ata që me ligj u mundësohet për të pasur qasje në informacione.

Edhe karakteristika tjetër e informacionit, *integriteti* i tij, në kuadrin e sigurisë merr përparësi të veçantë, pasi kërcënimet kundër tij janë të shumta dhe me pasoja të rënda. Një kërcënim të madh për integritetin e informacionit përbën, për shembull, marrja e procedurave të një organizate. Fjala vjen, nëse një konsulent në një bankë, duke përdorur procedurat e qendrës kompjuterike bankare, arrin të mësojë lidhjet e fondeve, si pasojë e kësaj dobësie të sigurisë (mungesa e vërtetimit), do të kemi një dëm të madh, pasi kjo bankë mund të urdhërojë që të transferohen miliona dollarë nga llogaria bankare në llogarinë e konsulentit. Në këtë mënyrë, cenimi i integritetit të dhënave, procedurat e dobëta të sigurisë shkaktojnë humbje të shumta financiare.

Pasoja të rënda për sigurinë e informacionit sjell edhe prekja e *disponueshmërisë* së tij, gjë që ndodh kur informacionet përdoren nga subjekte të paautorizuara.

Në këto kushte, institucionet shtetërore ose joshtetërore, ku prodhohet, përpunohet, shpërndahet, transmetohet dhe ruhet informacioni i klasifikuar, kanë për detyrë që, në përputhje me vëllimin e tij, të marrin masat e nevojshme për sigurimin e

procedurave, të pajisjeve dhe të mjediseve të caktuara për këto qëllime. Pra, është fjala të bëhet me përparësi sigurimi fizik i të gjitha këtyre. Siguria fizike dhe administrative është e vlefshme për një organizatë për mbrojtjen e informacioneve. (Bagad & Dhotre, 2009: 1).

Me "sigurim fizik" kuptohet tërësia e masave organizative, fizike dhe teknike, për ruajtjen e zonave, të ndërtesave, të dhomave dhe të pajisjeve ku ruhet dhe administrohet informacioni i klasifikuar "sekret shtetëror". (Vendimi nr. 121, datë 15.3.2001, i Këshillit të Ministrave të Republika e Shqipërisë).

Ky lloj sigurimi është i domosdoshëm të jetë sa më cilësor, sepse informacionet secrete, që janë objekt kërcënimesh, duhen ruajtur në mënyrë rigoroze, me siguri maksimale, sepse vlera e tyre është mjaft e madhe kanë një rol të jashtëzakonshëm edhe në ruajtjen e sigurisë kombëtare. Për këto arsye, në kuadrin e forcimit të masave të sigurisë së informacionit, këto mjedise, ku ruhet dhe administrohet informacioni i klasifikuar, pajisen me kasaforta e kyçe automatike, dyert e zyrave kanë çelësa, brava dhe dryna të veçantë, të ndryshëm nga ata të përdorimit të zakonshëm, vulosen me dyllë dhe plastelinë, sigurohen mirë dritaret dhe mjediset e tjera përreth etj.

Por edhe këto masa nuk do të ishin të mjaftueshme, nëse nuk do të kishim standarde sa më të larta të sigurisë së informacioneve. Për krijimin dhe vendosjen e këtyre standardeve është e nevojshme të ndërtohen programe të sigurisë së informacioneve.

Ç'janë këto programe? "Në një përkufizim më të gjerë, një program i sigurisë së informacionit është një plan për të zbutur rrezikun lidhur me përpunimin e informacionit (Wylder, 2003: 4). Sipas Peltier, qëllimi i një programi sigurie të informacionit është për

të mbrojtur burimet e vlefshme të informacionit të një ndërmarrjeje apo organizate (Peltier, 2001: XIII).

Sot, në epokën e internetit, shumica e informatave përpunohen dhe ruhen në mënyrë elektronike. Kjo, për shumë arsye, është një metodë shumë më e avancuar se ruajtja në kopje fizike, por, gjithsesi, ajo e bën ruajtjen e të dhënave një sfidë të vërtetë. Sepse në kushtet e një ndërlidhjeje në zgjerim të pandërprerë, informacioni është i ekspozuar ndaj kërcënimeve dhe dobësive të shumëllojshme, të cilat vijnë duke u shtuar dhe duke u bërë më të sofistikuara e më të vështira për t'u zbuluar dhe për t'u parandaluar.

Kjo dikton nevojën që rrjetet e komunikimit të të dhënave dhe pajisjet e përpunimit të këtyre të dhënave, për shkak të përdorimit shumë të gjerë, duhet të jenë të siguruara mirë, sepse ato janë të ekspozuara ndaj kërcënimeve të jashtme, si edhe ndaj rrezikut të humbjes së të dhënave në rrjet, të rrjedhjes së informacionit. Humbja e të dhënave mund të shkaktohet, si nga gabimet e shfrytëzuesve, nga defektet në kod, nga aktivitetet me qëllim dëmtimi, nga dështimi i harduerit, ashtu dhe nga shkaqe natyrore (Strebe, 2004: 1.)

Në këto kushte, për sigurinë e informacionit është e rëndësishme siguria e rrjeteve elektronike, e cila përfshin të gjitha masat që duhen marrë për të parandaluar çfarëdo ndërhyrje të paautorizuar në rrjet. Për këtë duhen zbatuar një sërë kontrollesh të përshtatshme, përfshirë edhe politikat, proceset, procedurat, strukturat organizative dhe funksionet softuerike apo harduerike. Këto kontrolle duhet të implementohen, të monitorohen, të rishikohen dhe të përmirësohen kur është e nevojshme, për të siguruar që objektivat e veçanta të sigurisë së informacionit të përmbushen.

Mbrojtja penalo-juridike e informacioneve i është dhënë atyre normave me të cilat mbrohet prona, duke llogaritur edhe pronën intelektuale, të dhënat e fshehta specifike ose sendet trupore (Mohrenschlager, 1993: 332).

Institucionet dhe organizatat duhet të jenë plotësisht të vetëdijshme për domosdoshmërinë e sigurisë maksimale të informacionit që disponojnë dhe duhet t'u kushtojnë më shumë rëndësi burimeve, mjeteve dhe procedurave për mbrojtjen e aseteve të informacionit dhe të dhënave të sigurisë dhe të ngritet ky shqetësim më lart edhe nga ana e Qeverisë (Gross, Government CIO survey, 2006). Në këtë drejtim, trajnimi dhe edukimi i punonjësve në lidhje me procedurat e ruajtjes së informacionit është po aq i rëndësishëm sa edhe sigurimi fizik i informacionit.

Për të pasur një siguri maksimale të informacionit dhe për të parandaluar rreziqet që u kanosen informacionit dhe sigurisë së tij, kërkohet një qasje gjithëpërfshirëse e të gjitha institucioneve të vendit, përfshirë edhe Qeverinë.

Në këtë kontekst hartimi i një strategjie të sigurisë kombëtare që do të përmbledhë brenda saj dhe një strategji mbi sigurinë e informacionit është i domosdoshëm. Kjo strategji do të na detyrojë të reflektojmë mbi natyrën e vlerave që ne dëshirojmë dhe gjykojmë, e që duhen mbrojtur (Instituti për Demokraci dhe Ndërmjetësim për Çështje të Sigurisë, 2012: 102).

Kërcënimet ndaj sigurisë së informacionit

Shpesh dëgjojmë dhe lexojmë në media lajme lidhur me incidentet ndaj sigurisë së informacionit, të tilla si dëmtim të faqeve të internetit, hyrje të paautorizuara në sisteme kompjuterike nga hakerët, cenime të fshehtësisë së korrespondencës dhe të

bazave të të dhënave, zbulime dhe mosruajtje të informacioneve të klasifikuara, keqpërdorime dhe rrjedhje të informacionit etj. Për këto kërcënime ndaj informacionit, sot në kushtet e përparimit të teknologjisë, për ndërhyrje dhe për marrjen e informacioneve e të dhënave po përdoren metoda dhe teknika të shumta, nga ato më të rëndomta deri tek ato më të sofistikuara.

Për t'i parandaluar këto kërcënime dhe për t'u bërë ballë me atyre me qëllim që të dështojnë, menaxhmenti i institucionit duhet të jetë i mirë përgatitur dhe, që të marrë vendime të drejta dhe rezultative në lidhje me sigurinë e informacionit, duhet të jetë vazhdimisht i informuar dhe të ketë njohuri lidhur me kërcënimet e ndryshme që u bëhen sistemeve të informacionit.

Në kontekstin e sigurisë së informacionit, kërcënim është një objekt, person ose subjekt tjetër nga jashtë institucionit, që paraqet rrezik të vazhdueshëm për një aset të caktuar informacioni. Por siguria e informacionit mund të kërcënohet rëndë edhe nga brenda institucionit: nga politikat jo të përshtatshme që ndiqen për përpunimin dhe për ruajtjen e informacionit, nga pakujdesia për mirëmbajtjen e pajisjeve elektronike, por edhe nga gabimet njerëzore që mund të ndodhin gjatë punës etj.

Kërcënimet ndaj sigurisë informacionit mund të jenë:

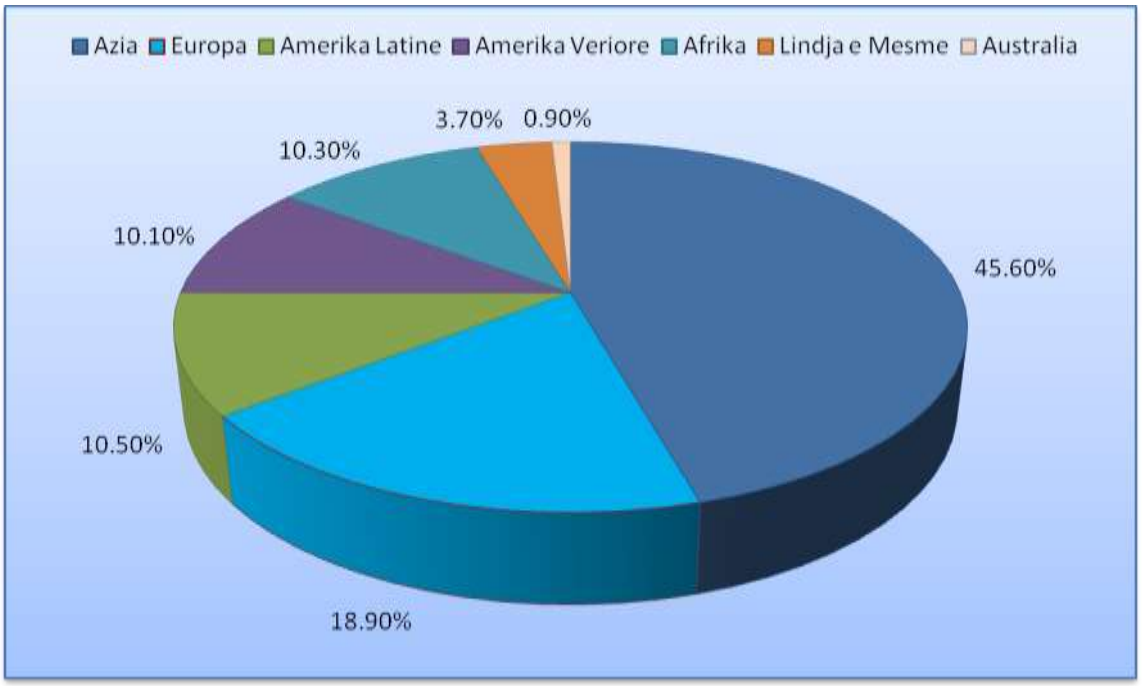
- Kërcënime nga burime të jashtme, dhe
- Kërcënime nga burime të brendshme.

Kërcënimet nga burimet e jashtme vijnë dhe shtohen kur organizata lidhet me internetin. Si të tilla mund të përmendim sulmet e qëllimshme softuerike, spiunazhin elektronik, shtrëngimin dhe shantazhin me informacione që bëhet nga jashtë etj.

Të tilla kërcënime janë prezente dhe vijnë duke u shtuar, pasi, në kushtet kur numri i përdoruesve të internetit vazhdon të rritet në mënyrë të shpejtë, interneti mbetet

platforma e një komunikimi thelbësor për organizatat terroriste dhe mbështetësit e tyre, duke bërë të mundur gjithnjë e më shumë përhapjen e një qasjeje anonimiteti dhe lidhje me një audiencë globale që mund të adresohen në një mënyrë në shënjestër konkrete (EUROPOL EU Terrorism Situation and Trend Raport 2013).

Sot në tërë botën investohet shumë dhe bëhen shpenzime marramendëse për arritjen dhe marrjen e informacioneve të rëndësishme dhe të bollshme, në rrugë të ligjshme, por, më së shumti, në rrugë e në forma të paligjshme dhe kriminale. Në këto kushte, në çfarëdo forme që të jetë informacioni dhe sado efikase dhe të përparuara të jenë rrugët dhe mjetet me të cilat ruhet, sado i lartë të jetë niveli i sigurisë së tij, përsëri janë gjithmonë prezente orvatjet, ndërhyrjet dhe veprimet konkrete për vjedhjen dhe përvetësimin e informacioneve që në më të shumtën e rasteve përfundojnë të suksesshme.



*Burimi: Internet World Stats.

Figura 1- Përdoruesit e internetit në nivel global

Në figurën 1 janë evidencuar përdoruesit e internetit në nivel global, sipas kontinenteve. Siç shihet, më 31.12.2014, ishin 3.079.339.857 përdorues të internetit në botë (Internet usage statistics, 2015).

Instituti i Sigurisë Kompjuterike (CSI), pas një sondazhi për krimet kompjuterike në vitin 2009, gjeti se 64 % e organizatave që i janë përgjigjur sondazhit kanë deklaruar se kanë pësuar infeksione, por vetëm 14 % e tyre treguan për depërtimin nga një sistem i huaj. Organizatat kanë raportuar humbje prej rreth 234.244 $ për zyrtar dhe, krahasuar me vitin 2001, humbjet kanë qenë 3 milionë $ më shumë **(**Whitman& Mattord, 2011: 44).

Si kërcënime nga brenda organizatës mund të përmendim ato rreziqe dhe dëmtime që i shkaktohen informacionit në mënyrë të qëllimtë ose jo të qëllimtë dhe që kanë të bëjnë me: politikat joadekuate të planifikimit organizativ të punës me informacionin, me dështimet apo defektet teknike harduerike, me gabimet njerëzore të personelit etj.

Çdo organizatë duhet t'u kushtojë prioritet kërcënimeve me të cilat përballet, të jashtme apo të brendshme, duke u bazuar në krijimin e situatën së sigurisë maksimale të informacionit, në strategjinë e saj organizative lidhur me rrezikun dhe me nivelet e ekspozimit ndaj rrezikut të pasurive të saj etj.

2.2. Historiku i sigurisë së informacionit

Informacionit është i vjetër sa vetë shoqëria njerëzore. Nevoja për informacione ka qenë e pranishme në të gjitha periudhat e zhvillimit të shoqërisë. Që nga dita kur njerëzit filluan të grumbullojnë informacione lidhur me fuqitë dhe synimet e klaneve, të

fiseve e të grupeve të ndryshme shoqërore ka lindur edhe nevoja për analizën e këtyre informacioneve, si dhe kanë nisur edhe kritikat lidhur me dobinë dhe efikasitetin e këtyre informacioneve.

Siguria e informacionit në shoqëritë e para njerëzore

Njerëzit në shoqërinë primitive, fillimisht, nuk kanë pasur asnjë fshehtësi, prandaj në këtë periudhë nuk ekzistonte nevoja që ata të bënin përpjekje për mbledhjen, ruajtjen e informacioneve dhe të fshehtësive të veta dhe as të zbulonin informacionet dhe fshehtësitë e të tjerëve. Njerëzit e parë, të cilët jetonin në kushtet elementare të ekonomisë grumbulluese, thjeshtë nuk posedonin kurrfarë fshehtësish, në kuptimin shoqëror, prandaj edhe veprimtaria për mbledhjen dhe ruajtjen e informatave në këtë periudhë ishte më pak e nevojshme.

Me zhvillimin e shoqërisë njerëzore në përgjithësi, me shfaqjen e klasave, me shfaqjen e tepricës në prodhim dhe të interesave të ndryshme mes njerëzve, lindi edhe nevoja e ruajtjes së fshehtësisë. Nga njëra anë, grupe shoqërore bënin përpjekje të ruanin fshehtësitë e veta dhe, nga ana tjetër, përpiqeshin që të zbulonin fshehtësitë e të tjerëve. Bazuar në këto zhvillime, në këtë fazë të zhvillimit të shoqërisë njerëzore rritet nevoja për mbledhje të informacioneve. Natyrisht, kjo nuk bëhej në formë të organizuar, siç e hasim në zhvillimet e më vonshme, me krijimin e shtetit si formë e organizimit shoqëror.

Grumbullimi i informacioneve dhe analiza e tyre, respektivisht, veprimtaria informative llogaritet ndër zanatet më të vjetra të njerëzimit (Dulles A., 2003:37).

Prej kohës së paraqitjes së shkrimeve të para, njerëzit e kanë kuptuar rëndësinë e informacionit, rëndësinë e ruajtjes së sekretit që përmban informacioni dhe rëndësinë e ruajtjes së besueshmërisë gjatë shkëmbimit të informacionit. Fillimisht, me formimin e fiseve të para u shfaq nevoja për më shumë ushqime dhe luftëtarët më të aftë u përdorën si vëzhgues të terrenit, në kërkim të kopeve me kafshë të egra. Kur filluan përplasjet e para midis fiseve, gjahtarët më të aftë përdoreshin si vëzhgues për të grumbulluar informacione në lidhje me armikun, forcën e tij dhe drejtimin e lëvizjes. Por këta gjahtarë-vëzhgues janë përdorur rast pas rasti. Pra, ky nuk ishte një shërbim i organizuar as me ndonjë strukture, as me një qëllim të qartë e të përcaktuar.

Gjithsesi, mbledhja e informacioneve përherë ka qenë e lidhur ngushtë me sigurinë njerëzore. Kuptohet, marrja e informacionit bëhej në forma dhe me mjete të thjeshta, të cilat, me kalimin e kohës, ato kanë ndryshuar. Por duhet thënë se edhe në kohët e hershme është menduar dhe vepruar jo vetëm për mbledhjen e informacionit, por edhe për sigurinë e tij, në veçanti, për ruajtjen e fshehtësisë së tij.

Është për t'u theksuar se gjatë zhvillimit historik të shoqërisë njerëzore një çështje ka mbetur dhe do të mbetet dominante, kërkimi i pandërprerë i informacioneve për atë se çka po ndodh dhe për atë që pritet të ndodhë. Kjo bëri prijësit, shtetet dhe komandat ushtarake të kuptonin nevojën dhe rëndësinë që ka mbledhja e grumbullimi sistematik i informative dhe për këtë u është dashur të krijojnë struktura dhe mekanizma për ta grumbulluar informacionin, por njëkohësisht, edhe për të ruajtur atë, si dhe për të siguruar besueshmërinë e informacionit gjatë shkëmbimit të tij. Historia flet se për një komunikim të sigurt, atëherë janë përdorur mjete për vulosje letrat a dokumentet e tjera, me shenja dhe simbole që shërbenin për të njohur vërtetësinë e dokumentit dhe besueshmërinë e tij. Njerëzit kanë marrë informata, i kanë ruajtur dhe kanë manipuluar

me to, po ashtu, kanë bartur informacionet që nga Sumerianet në Mesopotami rreth 3000 vjet para Krishtit. (Wieczorek, & Bons, 2014 :1-29).

Që nga koha e lashtë ishin të njohura shumë metoda të punës, të cilat u bënë të zakonshme për hartimin, grumbullimin dhe shpërndarjen e informacioneve ku me qëllim të sigurisë së informacionit ata e bënë shifrimin e informacioneve dhe shfrytëzimi i pëllumbave letërdërgues, por edhe zogj tjerë të trajnuar (duke përfshirë dallëndyshet) për bartjen e porosive. Por, edhe përkundër rolit të madh që kishte spiunazhi në kohën antike, nuk ekzistojnë shënime mbi ekzistencën e organeve ose organizatave të specializuara informative. (Abazoviq, 2006: 47). Edhe në shkrimet e shenjta flitet e tregohet në mënyrë të qartë për veprimtarinë informative. Kështu në Librin e Shenjtë, gjejmë*:*

"...Dhe perëndia i tha Moisiut duke folur: Dërgo njerëzit të vëzhgojnë tokën e Kanaanit, të cilën do t'ia dhuroj bijve të Izraelit; nga një njeri nga çdo fis, baballarët e tyre dërgoni, të gjithë krerët ndër ta. Dhe i dërgoj Moisiu nga toka Faraonike..Dhe duke i dërguar Moisiu për të spiunuar tokën Kanan, iu tha: shkoni këndej në jug, pastaj dilni në bjeshkë; dhe do të shikoni tokën çfarë është dhe çfarë populli jeton në të, është i fortë apo i dobët, i madh apo i vogël; dhe çfarë është toka në të cilën jeton, e mirë apo me gurë; në çfarë vendi jetojnë, nën tenda apo në qytete të forta; dhe çfarë është vetë toka, a është pjellore ose jopjellore, a *ka në të drunj apo nuk ka...."*

Punën zbuluese dhe kundërzbuluese shumë qartë e dallojmë edhe në Hadithin e të Dërguarit të Muhamedit as. (sipas Muslimit) ku qëndron:*"Ruajuni nga dyshimi, sepse dyshimi është fenomen më i rrejshëm. Mos lejoni që para jush të flitet keq për personat që nuk janë prezent. Mos e përcillni njëri-tjetrin"* (Abazoviq, 2006: 44).

Për ruajtjen e përmbajtjes dhe të sigurisë së informacioneve shumë herët filloi aplikimi i kodimit sekret të shkrimit të mesazheve, letrave dhe dokumenteve, sidomos të atyre informacioneve që përdoreshin gjatë luftërave. Fillimisht, ata që i krijuan kodet e ndryshme, do të kenë menduar se kodet e tyre janë të pathyeshme, ndaj dhe kanë kujtuar

se e kishin zgjidhur çështjen e sigurisë dhe të fshehtësisë së informacioneve të tyre. Por praktika tregoi se shumë shpejt ndodhi kundërveprimi, nisi çkodimi. Pra, bashkë me krijimin e kodeve, lindi edhe nevoja e thyerjes së tyre. Ky proces, kur rezultonte i suksesshëm, shkaktonte dëme të mëdha, por në radhë të parë krijoi pasiguri dhe brishtësi në aspektin e sigurisë së informacioneve. Kështu ka ndodhur gjatë gjithë historisë, kështu ndodh edhe sot. Edhe sistemet më komplekse të kodeve kanë arritur të deshifrohen.

Ndër kodet më të komplikuara, që ka njohur historia, është Shifra e Cezarit (Aliu, 2013).

Ky kod është përdorur nga Jul Cezari, kur ai dëshironte të dërgonte një mesazh sekret rreth planeve të tij ushtarake. Shifra e Cezarit ishte ndërtuar sipas këtij rregulli: në shkrimin e një mesazhi, çdo shkronjë zëvendësohej me shkronjën që ishte tri vende më poshtë saj në renditjen alfabetike. Për shembull, në vend të shkronjës B përdorej shkronja D. Në këtë mënyrë fjalët kamufloheshin, dilnin pa kuptim dhe mesazhi merrej i saktë vetëm nga ai të cilit i dërgohej dhe që punonte me të njëjtin kod.

Shifra e Cezarit ose, siç njihej ndryshe, ‘zhvendosja e Cezarit’, është përdorur shumë në atë kohë, ndonëse, në fakt, nuk kishte pse të ishte një kod kaq i komplikuar, pasi shumica e njerëzve nuk dinin të lexonin. Megjithatë, edhe pse i komplikuar, Kodi i Cezarit, rezultoi një nga kodet më të lehta për t’u thyer.

Nga sa thamë më sipër, del që qysh nga kohët më të lashta, njerëzimi ka bërë përpjekje që krahas preokupimit për sigurinë dhe fshehtësinë e informacionit, në kuadrin e pengimit të kriminalitetit në përgjithësi, ka vepruar edhe për të penguar e për të parandaluar edhe veprat penale të ndërlidhura me sigurinë e informacionit.

Siguria e informacionit në shoqërinë mesjetare (feudale)

Në Mesjetë, epoka ku mbizotëronte shoqëria me klasa dhe prona feudale, feudali më i fuqishëm dhe dominant ishte kisha katolike. Roli zotërues i kishës reflektohej, përveç të tjerash, edhe në grumbullimin dhe në analizën e informacioneve. Në këtë kuadër, është për t'u përmendur se në administrimin e informacioneve ajo vepronte me rigorozitet dhe rreptësi të madhe. Të bien në sy format e rënda të ndëshkimit që përdorte kisha ndaj atyre që bartnin informacionin te personat e tjerë në mënyrë të paautorizuar. Për raste të tilla shpesh here jepej dënimi me vdekje.

Në Mesjetë, për shkak të copëtimit feudal, nuk ekzistonin kushte të përshtatshme për zhvillimin e një veprimtarie të organizuar informative. Mirëpo, edhe në kushtet e copëtimit, të rivalitetit dhe të armiqësive, personat dhe grupet e caktuara, sidomos feudalëve gjenin një terren të favorshëm për marrjen dhe zbulimin e informatave – për këtë qëllim përdornin edhe luftën e vazhdueshme mes feudalëve për të arritur deri te informata.

Me zhvillimin e hovshëm të zejtarisë rriteshin akoma më shumë nevojat e shoqërisë për informacione nga më të ndryshme. Kjo solli nevojën që për gjetjen dhe marrjen e tyre punohej në mënyrë të organizuar dhe me njerëz të angazhuar posaçërisht me këtë veprimtari. Duke vlerësuar rëndësinë e informacionit, perandorët dhe monarkët, rekrutonin njerëz të besueshëm për të grumbulluar informacione nga burime të ndryshme dhe në bazë të këtyre të dhënave ndërmerrnin veprimet e duhura për të mirën e vet dhe në dëm të kundërshtarëve. Gjithashtu, ata mblidhnin informacione të brendshme, për mbajtjen nën kontroll të qytetarëve të tyre, për të shmangur ndonjë rebelim, në mënyrë që të mos u rrezikohej fronin dhe pushteti absolut.

Kështu, në këtë periudhë kemi organizimet e para të mbledhjes së informatave. Në vitin 1558, Elisabeta I Tudor erdhi në fronin e Anglisë. Ajo gjeti një vend të dobësuar dhe të izoluar dhe, për t'u bërë ballë vështirësive politike në rritje, si dhe për t'u mbrojtur nga armiqtë e saj të shumtë, ajo gjeti rrugën e përdorimit të spiunazhit, duke e praktikuar këtë në shkallë të gjerë. Veç të tjerash, ajo pati fatin të mbështetej te William Cecil, një kryeministër, i cili ishte veçanërisht i ndjeshëm ndaj çështjeve të sigurisë. Ai krijoi Organin Mbrojtës Shtetëror, një organizëm kompetent, si për spiunazhin jashtë vendit, ashtu edhe për kundërspiunazhin brenda vendit. Cecil do të përuronte edhe shërbimin e parë të „Shërbimit të Shifrimit". Pra, qysh në atë kohë kemi sistemin e shifrës, që shërbente për të siguruar informacionet, sekretet që përmbanin letërkëmbimet mbretërore, duke i bërë të pakuptueshme për kundërshtarët. Kjo arrihej përmes zëvendësimit të shkronjave apo futjes së nomenklaturave (fjalë dhe fraza kyçe). Po ashtu, ky shërbim nshifrimi shërbente edhe për të deshifruar mesazhet e kapura të armikut. (www.koha.net, parë më 29.11.2014)

Siguria e informacionit në shoqërinë bashkëkohore

Epoka bashkëkohore e informacionit fillon me sigurinë kompjuterike

Fillimet e veprave penale të ndërlidhura me sigurinë e informacionit e në këtë kontest edhe të kriminalitetit kompjuterik na shpien në zbulimin e vekut, në vitin 1801, nga ana e novatorit Jozef-Marie Jacqueardit, një fabrikant tekstili nga Franca. Kemi të bëjmë me një inovacion në sektorin e industrisë. Me ndihmën e kartelës së shpuar, mundësohej stampimi i mostrave të ndryshme në pëlhurë, në mënyrë automatike. Më vonë, gjatë viteve 1833, ky inovacion i shërbeu novatorit Charls Babbageu, të ndërtonte

makinën analitike dhe, njëkohësisht, të vinte edhe bazat e para teorike të punës së kompjuterëve modernë (Dragiqeviç, 1999:29).

Pas shumë përgatitjeve dhe eksperimenteve të njëpasnjëshme, në vitin 1944, Howard Aicken konstruktoi kompjuterin me emrin "*Mark 1*", ndërsa gjatë viteve 1946-1955, inxhinierët e njohur të asaj kohe, Echert, Mauchlay dhe Von Neumann, konstruktuan kompjuterin e parë elektronik, të njohur me emrin "*Electronic Numerical Integrator and Calculator*", i cili në atë periudhë ka shërbyer vetëm për qëllime shkencore (Dragiqeviq, 2004:10).

Por historia e shoqërisë tregon se zbulimet dhe zhvillimet në teknologji shoqërohen edhe me vepra që ecin në drejtim të kundërt, deri edhe me vepra që klasifikohen si krime. Lidhur me këtë, autori E. H. Sutherlland, në punimin e tij "Is *White Collar Crime*", duke folur për to, fillimet e paraqitjes së kriminalitetit kompjuterik i gjen te paraqitja e kriminalitetit të Jakave të Bardha në fillim të shekullit XX (Vasik, 1991:24).

Më vonë, në vitin 1960, Departamenti i Mbrojtjes (SHBA) ARPA (Advanced Research Project Agency) filloi të shqyrtojë mundësinë për krijimin e një sistemi komunikues me rritje të sigurt, për të mbështetur shkëmbimin e informatave të ushtrisë (Samuel C., 2009:7). Larry Roberts, i njohur si themeluesi i internetit, ka zhvilluar projektin e quajtur ARPANET (Whitman & Mattord, 2011: 4.)

Paraardhësi i internetit të sotëm ARPANET ishte një rrjet super, që u krijua në përgjigje të kërcënimit të mundshëm të sulmit bërthamor nga Bashkimi Sovjetik (Blank 2004:3).

Nevojat në rritje për të ruajtur sigurinë kombëtare të shteteve të veçanta, diktuan përsosjen e teknologjisë për të arritur në sigurinë më të ndërlikuar dhe më të sofistikuar kompjuterike mbrojtëse.

Gjatë këtyre viteve të hershme, siguria e informacionit përbëhej kryesisht prej sigurisë fizike dhe prej skemave të thjeshta të klasifikimit të dokumenteve. Rëndësi parësore i kushtohej mbrojtjes nga kërcënimet ndaj sigurisë fizike, si vjedhja e pajisjeve, spiunazhi kundër produkteve të sistemeve, sabotimi etj. Departamenti i Agjencisë për Mbrojtjen e projektit kërkimor (ARPA) filloi shqyrtimin e krijimit të një sistemi të rrjetit të komunikimit për të mbështetur dhe për ta bërë sa më të sigurt shkëmbimin e informacioneve të ushtrisë.

Kompjuterët nuk lidheshin me njëri-tjetrin, që të mund të shkëmbenin informacione mes tyre. Këto shkëmbeheshin me disqe me kapacitet tejet të vogël. Kjo njihej me emrin "Sneakernet". Në vitet 1960 u zhvilluan sistemet e para që bënë të mundur bartjen e informatave në formë paketash brenda një rrjeti të izoluar. U zhvillua projekti ARPANET, që në vitin 1972 riemërohet DARPA. Ky njihet si fillimi i teknologjisë "packet switchin". Në këtë kohë, shumë kompani zhvilluan protokolle dhe teknologji të ndryshme, që shfrytëzoheshin në rrjetet e tyre të komunikimit.

Por përdorimi i standardeve dhe i protokolleve jo të njëjta, e bënte të pamundur komunikimin mes rrjeteve të kompanive. Gjatë viteve 1970-1980, Arpanet u popullarizua shumë dhe u rrit në përmasa të mëdha përdorimi i tij, por, njëkohësisht, u rrit edhe potenciali për keqpërdorimin e tij. Kështu që rriten edhe problemet e sigurisë së informacionit me Arpanet, probleme që kryesisht ndërlidheshin me kontrollet, me masat për të mbrojtur të dhënat nga përdoruesit e paautorizuar, me strukturën e dobët të

fjalëkalimit, me mungesën e procedurave të sigurisë dhe me identifikimin e përdoruesve inekzistentë.

Në fund të shekullit XX, rrjetet kompjuterike u bënë më të zakonshme, po ashtu edhe lidhja e këtyre rrjeteve me njëra-tjetrën. Kjo ndikoi në rritjen e shtrirjes së internetit dhe të rrjeteve globale. Në vitin 1990 interneti është vënë në dispozicion të publikut të gjerë dhe u lidh gjerësisht te kompjuterët (http://www.tcpipguide.com/free/t_History of the OSI, Reference Model.htm) parë më 05.05.2013.). Ai u bë teknologji e përhapur pothuajse në çdo cep të globit me një rritje të konsiderueshme të numrit të përdoruesve. Sot shoqëritë moderne janë bërë të varura nga kompjuterët, sistemet kompjuterike dhe rrjetet me shërbimet vitale, të varura nga interneti. Ky evolucion digjital sot jo vetëm infrastrukturën civile, por edhe Forcat e Armatosura (Roscini, 2014:1). Sot informacioni dhe teknologjia informatike prekin çdo aspekt të jetës dhe të njerëzimit pa marrë parasysh vendndodhjen. Aktivitetet njerëzore në fushën e biznesit dhe fusha të tjera kanë përfitim të madh prej këtij revolucioni informatikë. Interneti ka lehtësuar kontaktet dhe shkëmbimin e mesazheve të menjëhershme. Nëpërmjet tij publiku i gjerë mund të ndjekë e të realizojë, nga shtëpia, biznese dhe punë të ndryshme përmes e-mailit, rrjeteve sociale, si Facebook, Friendster, që bëjnë të mundur qasjen në të dhënat personale (Ross, 2010:24). Teknologjia moderne e informimit dhe e komunikimit bën të mundshme që individët në mbarë botën të komunikojnë aty për aty me njëri-tjetrin dhe mundëson transferimin e menjëhershëm të informacionit në largësi të mëdha.

Informacioni, i trajtuar në të gjitha format e mundshme, elektronike apo tradicionale, përbën një pasuri të vërtetë, si për individët, ashtu dhe për organizatat shtetërore apo private. Ai, me të drejtë konsiderohet një burim strategjik rreth të cilit

zhvillohet ajo që sot quhet shoqëria e informacionit. Teknologjia dhe inovacionet e lidhura me të, kanë qenë dhe janë në bazën e ndryshimeve të thella në shoqërinë njerëzore: dje, me inovacionet në fushat e energjisë, sot, me mënyrat e larmishme të komunikimit të njohurive dhe të informacioneve nëpërmjet teknologjive të reja të telekomunikacionit. Sot, shoqëria e informacionit, si një vazhdimësi e shoqërisë industriale të disa viteve më parë, vë në qendër të saj informacionin dhe njohuritë, si dhe këmbimin dhe përcjelljen e tyre pa limite gjeografike dhe kohore. Teknologjitë e telekomunikacionit, që kanë një përdorim mjaft të gjerë, janë një vektor shumë i rëndësishëm dhe i pashmangshëm për shumicën e aktiviteteve të shoqërisë. Ky realitet ilustrohet me vendin gjithnjë e më të rëndësishëm që po zë në jetën tonë të përditshme ajo që quhet hapësira virtuale, e cila po thyen gjithnjë e më shumë kufijtë tradicionalë kohorë dhe gjeografikë dhe po transformon mënyrën tonë të jetuarit e të menduarit.

Por arritjet dhe zhvillimet e mëdha në aspektin tekniko-teknologjik, ekspansioni i shpejtë i teknologjisë informative dhe automatizimi i proceseve të punës në të gjitha sferat e jetës shoqërore dhe ekonomike, nga njëra anë, kanë sjellë një numër të madh lehtësirash, ndërsa në anën tjetër, kur këto arritje teknologjike keqpërdoren në mënyrë të paramenduar, krijojnë një numër problemesh dhe rreziqesh, si për individë dhe grupe, ashtu edhe për shoqërinë në përgjithësi. Revolucioni informatikë dhe interneti, me mundësitë e mëdha që kanë, kanë krijuar terren të favorshëm edhe për keqbërësit, të cilët, duke i njohur këto mundësi, i përdorin ato për të kryer vepra të papranueshme dhe të paligjshme. Siç thotë Vula, revolucioni informatikë dhe interneti, nga ky aspekt, u kanë hapur derë sjelljeve antishoqërore dhe kriminale, që më parë nuk kanë qenë të mundura (Vula: 2010, fq. 26).

Dhe, në realitet shohim që interneti ka sjellë edhe pasiguri në komunikim te miliona rrjete kompjuterike, por edhe në informacion. Tani siguria e ruajtjes së informacionit e çdo kompjuteri është e kushtëzuar me nivelin e sigurisë së çdo kompjuteri tjetër me të cilën ai është i lidhur. Madje, përmes komunikimeve elektronike dhe mesazheve mundë të kryhen edhe kërcënime, si dhe sulme kibernetike, duke vënë në rrezik sigurinë e informacionit, madje edhe sigurinë kombëtare. Ky problem bëhet edhe më i mprehtë kur shohim që ka një shqetësim në rritje rreth shteteve që angazhohen në luftë për përvetësim të informacionit. Aferat e ndryshme të publikimeve të informacioneve sekrete e pasqyrojnë më së miri këtë shqetësim.

Duke qenë se mbrojtja e vendit, siguria kombëtare dhe siguria njerëzore është qëllim themelor i të gjitha shteteve dhe i institucioneve ndërkombëtare, që merren me mbrojtjen e të drejtave të njeriut, qeveritë dhe organizatat e ndryshme janë bërë më të vetëdijshme për nevojën për të mbrojtur sistemet e kontrollit të shërbimeve dhe të infrastrukturave të tjera kritike nga kërcënimet në rritje që vijnë nga sulmet kibernetike.

Në botën bashkëkohore mënyrat e marrjes së informacionit janë të ndryshme dhe janë të bazuara në legjislacionin në fuqi, ku qëllimi përfundimtar është askush nuk pyet sesi është arritur deri te informacioni, ndërsa në rast se dështohet nga informacionet e mangëta apo jo të sakta, atëherë kjo do të rezultojë me dështime të përmasave të mëdha.

Individë, organizata madje edhe shtete, duke përfituar nga mundësitë e reja dhe të shumta që ofrojnë sistemet kompjuterike, nuk ngurrojnë të shkelin ligjet, madje edhe rregullat e marrëveshjet ndërkombëtare dhe kryejnë me paramendim dhe në mënyrë të qëllimtë vepra të ndryshme të kriminalitetit tradicional në mënyrë jo tradicionale.

E kemi fjalën për krimet kibernetike ndaj infrastrukturës e teknologjisë informative. Megjithëse fusha e krimeve kibernetike funksionon mbi bazën e principeve themelore të njëjta me ato të krimeve të tjera, mund të themi sulmet kibernetike janë shumë të sofistikuara dhe të kushtueshme. Ato janë shtuar në përmasa shqetësuese dhe paraqesin një rrezik global në tërë botën, jo vetëm për sigurinë e informacionit, por edhe për sigurinë kombëtare të vendeve të veçanta. Si pasojë e sulmeve kibernetike në Estoni dhe Gjeorgji në vitet 2007 dhe 2008, NATO-ja, pranoi se siguria kibernetike duhet të vendoset në krye të sfidave të reja të sigurisë që do të trajtohet në vitet e ardhshme.

Sot hakerët reflektojnë dobësitë e sistemit ligjor, mbrojtës dhe të kapaciteteve hetuese, duke tentuar në vazhdimësi të depërtojnë te informacionet e klasifikuara.

Përballë rreziqeve që vijnë nga këto sulme, informacioni, si një motor ekonomik i zhvillimit, është një e mirë jomateriale që kërkon një mbrojtje në lartësinë e vlerave dhe rëndësisë së tij, si nga ana e individëve, e organizmave të specializuara, dhe mbi të gjitha, nga ana e shtetit. Sepse krime të tilla, që synojnë manipulimin, fshirjen, modifikimin, survejimin, spiunazhin e informacioneve që qarkullojnë në rrjetet e komunikimit, mund të prekin drejtpërdrejt jo vetëm interesat e një individi, të një organizmi, por dhe të një shteti. Për këtë arsye, siguria e informacionit është e lidhur drejtpërdrejt edhe me sovranitetin e një shteti. Ajo ka të bëjë me mbrojtjen e infrastrukturave kritike, të sistemeve dhe të rrjeteve kompjuterike, por, mbi të gjitha, edhe të pasurive të kombit, të të mirave materiale dhe jomateriale, me një fjalë: me mbrojtjen e vlerave kombëtare.

Kjo dikton që në kuadrin e sigurisë kombëtare, të shihet me përparësi edhe realizimi i sigurisë maksimale të informacionit. E themi këtë, sepse nuk mungojnë rastet kur në rrethet e specialistëve të sigurisë, problematika e sigurisë së informacionit

trajtohet herë si një problem thjesht teknik, herë si një problematikë virtuale dhe herë demagogji. Fatkeqësisht, faktet tregojnë i kanë dhënë të drejtë vetëm pjesërisht kësaj mënyre të menduari. Në të vërtetë, këto sulme virtuale kanë pasur pasoja më se reale, me një bilanc shumë negativ për organizmat publikë apo privatë.

Prandaj mbetet një përparësi kontrolli dhe mbikëqyrja e rreptë e sistemeve informatike dhe e rrjeteve kompjuterike nga ana e strukturave të posaçme shtetërore. Qeveritë duhet të realizojnë survejime në një masë të konsiderueshme dhe për këtë ato i kanë të gjitha mundësitë, i gjejnë këto tek infrastruktura e teknologjisë informatike. Përmes përdorimit të mjeteve të avancuara teknologjike, shërbimet e inteligjencës mund të mbledhin informata në shkallë të madhe, mbledhjen e shumë më shumë informatave sesa ato që mund t'i absorbojnë dhe t'i analizojnë (Collins & Taylor, 2013:318).

KAPITULLI 3: ASPEKTI JURIDIKO-PENAL I VEPRAVE PENALE TË NDËRLIDHURA ME SIGURINË E INFORMACIONIT

3.1. Vështrime hyrëse

Veprat penale të ndërlidhura me sigurinë e informacionit janë ato vepra, me kryerjen e të cilave rrezikohen liritë dhe të drejtat njerëzore, vlerat shoqërore të garantuara dhe të mbrojtura me Kushtetutën e Republikës së Kosovës dhe me të drejtën ndërkombëtare. Edhe pse nuk kemi një përkufizim unik për këto vepra, nisur nga karakteristikat dhe veçoritë e tyre, veprat penale të ndërlidhura me sigurinë e informacionit mund t'i kuptojmë si çdo aktivitet, në të cilin kompjuterët apo rrjetet shërbejnë si mjete ose objekte sulmi për ushtrimin e aktivitetit kriminal, ndaj të cilit duhet të ndërmerren të gjitha masat preventive ligjore të duhura për luftimin e tyre.

Rrezikshmëria shoqërore e këtyre veprave penale është shumë e lartë, sepse me kryerjen e tyre rrezikohen informacionet e klasifikuara dhe shkaktohen pasoja të rënda, që rezultojnë drejtpërdrejt me rrezikimin jo vetëm të sigurisë së qytetarëve të një vendi, por edhe të sigurisë kombëtare të atij vendi.

Karakteristikë kryesore e veprave penale të ndërlidhura me sigurinë e informacionit është efekti global i tyre. Për këtë arsye, kërkohet një fokus ndërkombëtar, pasi autorët e krimit me rastin e konsumimit të këtyre veprave penale veprojnë dhe shfrytëzojnë metoda nga më të ndryshmet që nuk kufizohen në njësi të veçanta territoriale. Ata mund të veprojnë në një vend të caktuar, ndërsa objekti i krimit të tyre, pra viktima, mund të ndodhet në një vend tjetër.

Të tilla vepra janë: hyrja e paautorizuar në sisteme kompjuterike, përgjimi i paligjshëm i të dhënave kompjuterike, ndërhyrja në të dhënat kompjuterike, ndërhyrja në sistemet kompjuterike, abuzimi me pajisjet kompjuterike, përhapja e viruseve dhe veprime të tjera, që rrezikojnë programet kompjuterike.

Dallimi mes krimeve tradicionale dhe veprave penale të ndërlidhura me sigurinë e informacionit është i dukshëm. Për shkak se kryerja e këtyre veprave penale mund të ndodhë larg vendit të ngjarjes dhe ngaqë provat për to janë më të paqëndrueshme, parandalimi dhe luftimi i këtij lloji të sofistikuar të krimit është më sfidues për organet e rendit. Kjo ndonjëherë dikton nevojën që, krahas angazhimeve të autoriteteve vendore, të kërkohet edhe ndihma juridike ndërkombëtare për marrjen e informacioneve të nevojshme për ndjekje penale.

Këto vepra i karakterizon vështirësia për t'u zbuluar dhe për t'u ndjekur, sepse, si të sofistikuara që janë, pasojat që shkaktojnë ato janë shumë të mëdha, saqë krijojnë pengesa të shumta për t'i hetuar. Tjetër veçori e këtyre veprave penale është se ato mund të konsumohen nga autorë prej një vendi tjetër, pra, jo nga vendi ku ndodhet viktima dhe ku shkaktohet dëmi, gjë që sjell vështirësi të tjera për hetimin e tij, sepse duhet komunikim, miratim dhe bashkëpunim me autoritetet e shtetit tjetër ku ka vepruar autori i krimit.

Veprat penale që ndërlidhen me sigurinë e informacionit dhe që kryhen përmes përdorimit të kompjuterit apo të sistemeve kompjuterike, mund të përdoren edhe për kryerjen e krimeve tradicionale, siç janë: mashtrimi, kërcënimi, falsifikime dokumentesh, vjedhja, shkelja e së drejtës së privatësisë, shkelja e të drejtës së autorit etj. Pra, kemi të bëjmë edhe me abuzimin me teknologjinë informatike.

Në përputhje me të gjitha këto veçori të krimeve duhet dhënë përgjigjja e duhur ligjore. Kjo është një çështje me rëndësi për t'u përballuar dhe për t'u studiuar, që kërkon një qasje serioze jo vetëm të autoriteteve dhe të ekspertëve vendorë, por edhe të atyre të komunitetit ndërkombëtar, për luftimin dhe parandalimin e këtyre vepra penale me shtrirje ndërkombëtare.

3.2. Karakteristikat juridiko-penale të veprave penale të ndërlidhura me sigurinë e informacionit, sipas Kodit Penal të Kosovës

Zhvillimi i teknologjive të reja informatike mundëson ruajtjen e sigurisë së informacionit, por në të njëkohësisht ajo lejon shfaqjen e rreziqeve serioze. Ndaj shoqëria është e vetëdijshme për këtë përdorim të dyfishtë të teknologjive informatike, duke nënkuptuar që, krahas dobisë së madhe që sjell, kjo teknologji mundëson edhe kryerjen e veprave penale kundër sigurisë së informacionit, si edhe të veprave tjera penale të rënda, siç është terrorizmi ndërkombëtar. Për këto arsye, organizata të specializuara vendore dhe ndërkombëtare kanë punuar dhe punojnë në vazhdimësi për gjetjen e mënyrave sa më efikase për të parandaluar përdorimin e teknologjive informatike për kryerje krimesh dhe aktesh që rrezikojnë sigurinë ndërkombëtare.

Veprat penale të ndërlidhura me sigurinë e informacionit lidhen me një gamë të gjerë krimesh dhe shpërdorimesh të teknologjisë së informacionit, ku incidentet e raportuara më rëndom janë ato që përfshijnë programuesit e paautorizuar të programeve kompjuterike dhe viruset e kompjuterit.

Në Republikën e Kosovës, veprat penale të ndërlidhura me sigurinë e informacionit nuk janë të parapara me një kod apo ligj të vetëm, por trajtohen në disa ligje. Disa prej tyre janë të parashikuara në Kodin Penal të Kosovës, disa të tjera në Ligjin për Parandalimin dhe Luftimin e Krimeve Kibernetike, ndërsa një vepër e tillë parashikohet edhe në Kodin Penal, edhe Ligjin për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë. Mendojmë se një tablo e tillë që gjendet në legjislacionin e Kosovës paraqet një praktikë jo të mirë legjislative që duhet rregulluar. Zgjidhja është përfshirja e të gjitha veprave penale të kësaj natyre në një kapitull të veçantë në Kodin Penal të Kosovës.

Për lehtësi studimi, po i trajtojmë të ndara karakteristikat juridiko-penale të veprave penale të ndërlidhura me sigurinë e informacionit të parapara me Kodin Penal të Kosovës, nga karakteristikat juridiko-penale të krimeve kibernetike.

Elementet konstituive të veprave penale të ndërlidhura me sigurinë e informacionit

Veprat penale të ndërlidhura me sigurinë e informacionit janë vepra apo sjellje të individëve apo organizatave të caktuara, që shkaktojnë pasoja në dëm të vlerave themelore të njeriut, të shoqërisë dhe të sistemit juridik. Varësisht prej shkallës së rrezikimit të vlerave, mbrojtja juridike-penale ndaj këtyre veprave është parashikuar në legjislacionin penal, përkatësisht në Kushtetutën e Kosovës, në Kodin Penal të Kosovës, në Kodin e Procedurës Penale të Kosovës, në Ligjin për Mbrojtjen e të Dhënave Personale, në Ligjin për Parandalimin dhe Luftimin e Krimeve Kibernetike, në Ligjin

për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë, por edhe në ligje tjera të aplikueshme.

Si çdo vepër penale me pasoja juridike, edhe veprat penale të ndërlidhura me sigurinë e informacionit përmbajnë në vete elemente themelore apo të përgjithshme, pa të cilat nuk do të përkufizoheshin si vepra penale. Ato janë: elementet objektive dhe elementet subjektive.

Elementet objektive të këtyre veprave penale i përbëjnë: veprimi i njeriut, kundërligjshmëria, përcaktueshmëria e veprës penale me ligj dhe rrezikshmëria shoqërore, ndërsa elementet subjektive janë përgjegjësia penale ose fajësia e autorit të krimit.

Kundërligjshmërinë e veprave penale të ndërlidhura me sigurinë e informacionit e karakterizon aspekti formal i veprës penale, i parashikuar në nenin 7 të Kodit Penal të Kosovës, në të cilin thuhet shprehimisht se: për t'u konsideruar vepër penale, ajo duhet të jetë e kundërligjshme dhe e përcaktuar me ligj, duke i përfshirë këtu tiparet dhe sanksionet. Për luftimin e kriminalitetit, veprat që konsiderohen të dëmshme për shoqërinë duhet të jenë të përcaktuara me ligj, me konventa ndërkombëtare, me kushtetutë, me kode dhe të jenë të përcaktuara si vepra që i dëmtojnë apo i rrezikojnë të mirat juridike të njeriut apo të shoqërisë (Salihu, 2008: 183).

Përcaktueshmëria e me ligj e veprave penale të ndërlidhura me sigurinë e informacionit siguron parimin e legalitetit:"nullum crimen, nulla poena sine lege", njëkohësisht, edhe respektimin e lirive, të drejtave dhe sigurisë e barazisë së qytetarëve, ngase përmes respektimit të parimit të ligjshmërisë në fushën e së drejtës penale nga organet e drejtësisë, sigurohen funksionimi i shtetit ligjor dhe parandalimi i arbitraritetit.

Në rastin tonë kemi të bëjmë me zbatimin e dispozitave për mbrojtjen e të dhënave personale (Ligji për Mbrojtjen e të Dhënave Personale, Prishtinë, 2010).

Elementi subjektiv apo përgjegjësia penale, gjegjësisht fajësia e autorit të veprës penale, si element kumulativ i figurës së këtyre veprave, duhet të jetë i shprehur për t'u konsideruar vepra si vepër penale. Prandaj, përveç të provuarit se i pandehuri shkakton dëmin (actus reus), duhet të provohet që ai është përgjegjës për shkaktimin e dëmit (mens rea) (Herring, 2013: 30). Meqë përgjegjësia penale konsiderohet si çështje subjektive, psikike e autorit të veprës penale, në shumë aspekte ajo dallon nga elementet e tjera të veprës penale (Salihu, 2008: 275). Marrë në tërësi, personi është fajtor në rast se e kryen veprën me dashje ose nga pakujdesia.

Për t'u konsideruar personi penalisht i përgjegjshëm, duhet që veprën ta ketë kryer me fajin e tij. (Salihu, 2014: 71).

Elemente konstituive të këtyre veprave penale konsiderohen veprimi ose mosveprimi. Pra, këto vepra penale kryhen me veprim, por edhe me mosveprim.

Përgjegjësia penale e autorëve të këtyre veprave

Veprat penale mund të kryhen me dashje dhe nga pakujdesia. Veprat penale të ndërlidhura me sigurinë e informacionit kryhen, zakonisht, me dashje, por ka edhe raste kur këto vepra penale kryhen nga pakujdesia. Shembull të kryerjes së veprës penale nga pakujdesia kemi rastin kur një zyrtar që ka qasje në informacionet e klasifikuara, në mënyrë të gabuar shpërndan përmes emalit një informacion duke gabuar pa dashje

adresën e zyrtarit të cilit duhet t'ia dërgonte dhe ia dërgon atë një personi të paautorizuar. Ky gabim i zyrtarit mund të paraqesë rrezik për sigurinë nacionale.

Personi që kryen veprën penale konsiderohet penalisht i përgjegjës nëse në kohën e kryerjes së veprës ai ka qenë i përgjegjshëm dhe i fajshëm.

Aspekte krahasuese të veprave penale të ndërlidhura me sigurinë e informacionit me vështrim të posaçëm tek analiza e figurave penale

Në Kodin Penal janë të parashikuara pesëmbëdhjetë vepra penale që ndërlidhen me sigurinë e informacionit. Është karakteristike se disa nga këto vepra penale janë të ndërlidhura drejtpërdrejt me sigurinë e informacionit, ndërsa disa tjera ndërlidhen me sigurinë e informacionit në mënyrë të tërthortë.

Veprat penale të ndërlidhura me sigurinë e informacionit të cilat janë të parapara me Kodin Penal të Kosovës janë:

1. Zbulimi i informacioneve të klasifikuara dhe mosruajtja e informacioneve të klasifikuara
2. Sabotimi;
3. Spiunazhi;
4. Rrezikimi i rendit kushtetues me shkatërrimin apo dëmtimin e instalimeve dhe pajisjeve publike;
5. Cenimi i fshehtësisë së korrespondencës dhe i bazave të të dhënave kompjuterike;
6. Zbulimi i paautorizuar i informacionit konfidencial;
7. Përgjimi i paautorizuar;

8. Fotografimi dhe incizime tjera të paautorizuara;

9. Shkelja e urdhrave për masat e fshehura ose teknike të vëzhgimit ose hetimit;

10. Komunikimi i paautorizuar i sekretit tregtar;

11. Shmangia e masave teknologjike;

12. Hyrja në sistemet kompjuterike;

13. Asgjësimi, dëmtimi ose heqja e instalimeve publike;

14. Keqpërdorimi i informacionit zyrtar dhe

15. Zbulimi i fshehtësisë zyrtare.

Rrezikimi i rendit kushtetues me shkatërrimin apo dëmtimin e instalimeve dhe të pajisjeve publike (Neni 129)

Vepra penale "*Rrezikimi i rendit kushtetues me shkatërrimin apo dëmtimin e instalimeve dhe të pajisjeve publike*" është e parashikuar në kuadër të veprave penale kundër rendit kushtetues dhe sigurisë së Republikës së Kosovës.

Neni 129 konsideron vepër penale veprimet që ndërmerren me qëllim të rrezikimit të rendit kushtetues apo të sigurisë së Republikës së Kosovës, siç janë djegia ose shkatërrimi apo dëmtimi në çfarëdo mënyre tjetër i zonës industriale, bujqësore ose ndonjë zone tjetër ekonomike, i sistemit të trafikut, i lidhjeve të telekomunikimeve, i pajisjeve publike të ujit, të ngrohjes, të gazit apo të energjisë, i digave, i depove apo i ndonjë ndërtese tjetër të rëndësishme për sigurinë, për furnizimin e qytetarëve, për ekonominë apo për funksionimin e shërbimeve publike.

Figura e veprës penale "Rrezikimi i rendit kushtetues me shkatërrimin apo dëmtimin e instalimeve dhe të pajisjeve publike" - Këtë vepër penale e kryen kushdo që me qëllim të rrezikimit të rendit kushtetues apo të sigurisë së Republikës së Kosovës, djeg ose shkatërron apo dëmton në çfarëdo mënyre tjetër zonën industriale, bujqësore ose ndonjë zonë tjetër ekonomike, sistemin e trafikut, lidhjet e telekomunikimeve, pajisjet publike të ujit, të ngrohjes, të gazit apo të energjisë, digat, depot apo ndonjë ndërtesë tjetër të rëndësishme për sigurinë, për furnizimin e qytetarëve, për ekonominë apo për funksionimin e shërbimeve publike. Nga ky përkufizim i kësaj vepre penale shihet se këtu bëhet fjalë për shkatërrimin apo për dëmtimin e objekteve që kanë rëndësi shumë të madhe për ekonominë dhe për jetën normale të qytetarëve (Salihu & Zhitia& Hasani, 2014: 375).

Nga ana objektive krimi kryhet me anë të veprimeve ose të mosveprimeve të kundërligjshme, që rezultojnë me shkatërrimin apo dëmtimin e objekteve që kanë rëndësi shumë të madhe për ekonominë dhe për jetën normale të qytetarëve.

Nga ana subjektive, krimi kryhet me dashje të drejtpërdrejtë dhe me qëllim të rrezikimit të rendit kushtetues apo të sigurisë së Republikës së Kosovës, qëllim që e dallon këtë vepër penale nga veprat e përgjithshme të dëmtimit të pasurisë së huaj, si dhe nga veprat e rrezikimit të përgjithshëm të njerëzve dhe të pasurisë.

Subjekt i krimit është çdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm i cili, me veprimet apo mosveprimet e tij rrezikon rendin kushtetues duke shkatërruar apo dëmtuar instalimet dhe pajisjet publike.

Kjo vepër penale ndërlidhet me sigurinë e informacionit në rastet kur veprimet me të cilat kryhet ajo rezultojnë me shkatërrimin e instalimeve publike, siç janë: rrjeti elektrik, pajisjet e telekomunikimit që kanë rëndësi të posaçme për funksionimin e

shumë veprimtarive ekonomike dhe për jetën e njerëzve në përgjithësi. Me asgjësimin apo dëmtimin e këtyre instalimeve mund të shkaktohen pasoja të ndryshme të dëmshme në furnizimin me energji, gjë që paraqet edhe bazën e këtij inkriminimi të kësaj vepre penale (Kodi Penal i Kosovës, neni 129).

Veprimi i kryerjes së kësaj vepre penale është përcaktuar në mënyrë alternative si asgjësim, dëmtim ose heqje e instalimeve të përmendura më sipër. Kjo vepër penale kryhet nëse shkaktohet çfarëdo vështirësie, si pasojë e veprimit të paligjshëm të autorit.

Shembull: nëse qëllimisht në dhomën e të dhënave të një organizate të sigurisë vendosin në pajisje, materie, që pengojnë funksionimin normal të tyre, çkyçin nga rrjeti i rrymës pajisjet klimatike dhe, si pasojë, shkaktohet dëmtim i rëndë i të gjitha pajisjeve teknologjike. Pjesë e këtyre pajisjeve teknologjike janë edhe pajisjet kompjuterike, harduerët, softuerët dhe pajisje tjera, në të cilat ruhen programe dhe baza të të dhënave që përmbajnë informacione të rëndësishme. Pjesë e këtyre informacioneve janë edhe informacionet e klasifikuara në nivele të ndryshme të sigurisë dhe të qasjes. Në këtë rast, pasoja nuk ndërlidhet vetëm me vlerën e pajisjeve teknologjike, por pasoja më e rëndë konsiston në rrezikimin dhe në asgjësimin e informacioneve të klasifikuara, që ndikojnë drejtpërdrejt edhe në rrezikimin e sigurisë kombëtare.

Bazuar në shembullin e dhënë më lart, objekt veprimi i veprave të tilla penale janë pajisjet publike, që shërbejnë për analizën, përpunimin dhe ruajtjen e informacioneve, përfshirë edhe informacionet e klasifikuara, dhe përmbushjen e nevojave të një numri të papërcaktuar njerëzish apo për ushtrimin e veprimeve të caktuara të sigurisë. Në këtë rast, pajisjet publike që janë objekt i kësaj vepre penale, janë të asaj natyre që, me asgjësimin, dëmtimin ose në përgjithësi me bërjen të

papërdorshme të tyre, si rregull shkaktohet çrregullim në fushën e sigurisë, për shkak të vështirësive që krijohen në funksionimin e Agjencive të Sigurisë.

Ndërlidhja e kësaj vepre penale me sigurinë e informacionit ka të bëjë edhe me veprimin e heqjes së pajisjeve të teknologjisë informatike dhe nxjerrjes së tyre jashtë funksionit. Heqja e instalimeve mbrojtëse, në aspektin e këtij inkriminimi, nënkupton zhvendosjen, dislokimin në një vend tjetër prej ku ato zakonisht gjenden, duke pamundësuar kështu përdorimin e tyre në përgjithësi apo përdorimin e tyre me kohë në rast nevoje. Ky dislokim i instalimeve mbrojtëse krijon mundësi për qasje të paautorizuar në informacione dhe për keqpërdorim të këtyre informacioneve.

Sabotimi (Neni 130)

Sabotimi është veprimtari e paramenduar dhe e fshehtë, me qëllim që t'i shkaktohen dëme materiale, organizatës ekonomike ose ekonomisë nga persona, grupe ose organizata të cilat punojnë në objektet në të cilat kryhen dëmet. Në fillim, sabotimi ishte formë e aksionit të drejtpërdrejtë në luftën për të drejtat e punëtorëve por, me kohë, mori shumë forma të tjera, kundërshtimi i qetë i punës, paralizimi i makinave, rrënimi i fabrikave dhe pajisjeve etj. (Dragutin, 1982: 78). Synimi i sabotatorëve është që me punën e tyre, por edhe duke mos dalë në punë, të shkaktojnë sa më shumë dëme dhe njëkohësisht të krijohet përshtypja se dëmi erdhi rastësisht, nga pakujdesia, nga materiali i keq të teknologjisë ose konstruksionit të pajisjes.

Vepra penale "*Sabotimi*" është e parashikuar në kuadër të veprave penale kundër rendit kushtetues dhe sigurisë së Republikës së Kosovës (Kodi Penal i Kosovës,

Kapitulli XIV). Dispozita e nenit 130 konsideron vepër penale veprimet e kundërligjshme që ndërmerren me qëllim të rrezikimit të rendit kushtetues apo të sigurisë së Republikës së Kosovës siç janë:

a) moskryerja e detyrës zyrtare në mënyrë të ndërgjegjshme apo dëmtimi i mjeteve të prodhimit gjatë ushtrimit të detyrës zyrtare;
b) shkatërrimi apo dëmtimi i instalimeve ose i ndërtesave;
c) shkatërrimi apo dëmtimi në sasi të mëdha i produkteve, i mallrave apo i materialeve;
d) shkaktimi i ndërprerjes të procesit të prodhimit dhe vlera e dëmeve apo e shkatërrimit tejkalon pesëdhjetëmijë euro.

Figura e veprës penale të sabotimit - Veprën penale të sabotimit e kryen kushdo që, me qëllim rrezikimin e rendit kushtetues apo të sigurisë së Republikës së Kosovës, nuk e kryen në mënyrë të ndërgjegjshme detyrën zyrtare apo kushdo që gjatë ushtrimit të detyrës zyrtare dëmton mjetet e prodhimit, shkakton shkatërrimin apo dëmtimin e instalimeve ose të ndërtesave, shkakton shkatërrimin apo dëmtimin në sasi të madhe të produkteve, të mallrave apo të materialeve ose shkakton ndërprerjen e procesit të prodhimit dhe vlera e dëmit apo e shkatërrimit tejkalon pesëdhjetëmijë euro. (Salihu & Zhitia & Hasani, 2014: 376).

Karakteristikë themelore e kësaj vepre penale është se ajo kryhet në mënyrë të fshehtë dhe se sabotimi mund të kryhet edhe në rastet e ushtrimit të detyrave zyrtare në organet shtetërore, ku nëpërmjet sabotimit dëmtohen apo shkatërrohen pajisjet e teknologjisë informatike në të cilat ruhen informacionet e klasifikuara.

Nga ana objektive, ky krim kryhet vetëm me dashje, me anë të veprimeve ose të mosveprimeve të kundërligjshme, që çojnë në rrezikimin e rendit kushtetues dhe të sigurisë së Republikës së Kosovës, i cili edhe është qëllim i posaçëm i kësaj vepre penale.

Nga ana subjektive, ky krim kryhet me dashje të drejtëpërdrejtë vetëm nga persona të punësuar në ekonomi apo në ndonjë organ shtetëror në nivel qendror apo lokal. Personi që kryen këtë vepër penale (sabotuesi), gjatë ushtrimit të punës dhe detyrave të veta vepron në mënyrë të fshehtë dhe me zgjuarsi, nga njëra anë, shkakton pasoja të rënda me dëmtimin dhe shkatërrimin e instalimeve dhe të mjeteve të punës, ndërsa, nga ana tjetër, bën përpjekje që të krijojë tek të tjerët bindje së po e kryen punën me profesionalizëm të lartë.

Subjekt i këtij krimi është çdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm, ai që me veprimet apo me mosveprimet e tij rrezikon rendin kushtetues dhe sigurinë e Republikës së Kosovës.

Elementet e kësaj vepre penale, që ndërlidhen me sigurinë e informacionit, kanë të bëjnë me rrezikimin e rendit kushtetues apo të sigurisë së Republikës së Kosovës, sepse autori i saj, siç sanksionohet në Kodin Penal të Kosovës, duke mos e kryer në mënyrë të ndërgjegjshme detyrën apo që gjatë ushtrimit të detyrës dëmton mjetet dhe shkakton shkatërrimin apo dëmtimin e instalimeve ose të ndërtesave, shkakton shkatërrimin apo dëmtimin në sasi të mëdha të programeve softuerike, që përmbajnë baza të të dhënave me rëndësi nacionale, sepse këto baza të të dhënave përmbajnë informacione të klasifikuara (Kodi Penal i Kosovës, neni 130).

Kjo kategori e kërcënimit ndaj informacionit përfshin edhe sabotimin e qëllimshëm të një sistemi kompjuterik, edhe aktet e vandalizmit për të shkatërruar asetet

e informacioneve ose për të dëmtuar imazhin e një organizate. Këto akte të sabotatorit mund të shkojnë nga sabotimet në përmasa të vogla, deri te sabotimet kundër një organizate të tërë.

Edhe pse nuk janë domosdoshmërisht financiarisht shkatërruese, sulmet ndaj imazhit të një organizate janë serioze. Sulmet në një ueb-faqe të organizatës mund të dëmtojnë besimin dhe reputacionin e saj. Punonjësit e organizatave të sigurisë që kryejnë këto sulme veprojnë në kundërshtim me rregulloret e punës dhe me ligjet në fuqi. Motivi i tyre për të sabotuar mund të jetë dëshira e tyre për t'i shkaktuar dëm jo vetëm organizatës së sigurisë ku punojnë, por edhe sigurisë kombëtare. Një kategori tjetër e autorëve të kësaj vepre e gjejnë motivin për sabotim te pasurimi i tyre, duke u vënë nën shërbim të shërbimeve të huaja të inteligjencës.

Në këto kushte shumë shtete po i forcojnë masat e sigurisë me qëllim mbrojtjen e informacioneve, të komunikimit dhe të rrjeteve të infrastrukturave fizike.

Spiunazhi (Neni 131)

Spiunazhi njihet si një ndër krimet më të lashta në vende të ndryshme, përfshirë edhe Kosovën. Në lidhje me rëndësinë e spiunazhit, Napoleoni ka thënë: *"Një spiun i mirë është ekuivalent i 20.000 ushtarëve"*. (Colins, 2006: 313).

Si një vepër penale që paraqet rrezikshmëri të theksuar shoqërore, vepra penale e spiunazhit është e parashikuar në kuadër të veprave penale kundër rendit kushtetues dhe të sigurisë së Republikës së Kosovës në Kodin Penal të Kosovës, Kapitulli XIV.

Neni 131 i këtij Kodi konsideron vepër penale:

a) komunikimin, dorëzimin apo bërjen të arritshme të sekretit shtetëror shtetit të huaj, organizatës së huaj apo personit që u shërben atyre;

b) Krijimin apo drejtimin (udhëheqjen) e shërbimit informativ në Republikën e Kosovës, i cili shërbim punon për shtetin apo organizatën e huaj;

c) Hyrjen në shërbimin informativ të huaj, mbledhjen e të dhënave për të apo në ndonjë mënyrë tjetër veprimet me të cilat ndihmohet puna e shërbimit të tillë;

d) Mbledhjen e të dhënave apo të dokumenteve të klasifikuara me qëllim që t'ia komunikojë dhe t'ia dorëzojë shtetit të huaj, organizatës së huaj apo personit që u shërben atyre dhe

c) Shkaktimin e pasojave të rënda për sigurinë ose për fuqinë ekonomike apo ushtarake të shtetit.

Figura e veprës penale të spiunazhit - Veprën penale të spiunazhit e kryen kushdo që komunikon, dorëzon apo ia bën të arritshme sekretin shtetëror një shteti të huaj, një organizate të huaj apo një personi që u shërben atyre; kushdo që krijon apo udhëheq shërbimin informativ, mbledh të dhëna dhe e ndihmon këtë shërbim që punon për shtetin apo organizatën e huaj, që vepron në Republikën e Kosovës.

Në këto mënyra veprimi përfshihen të gjitha format e veprimit apo të mosveprimit me të cilat autori i krimit, me vetëdije dhe me vullnet, i krijon një personi tjetër, mundësi, qasje në të dhënat sekrete. Rrjedhimisht, kjo vepër kryhet duke i komunikuar apo i dorëzuar në mënyrë të rëndomtë, apo kur i mundëson personit tjetër të paautorizuar të ketë qasje në dokumentet sekrete. Mundësimi që një personi tjetër të paautorizuar të ketë qasje në informacione të klasifikuara, për shembull, duke i lënë dokumentet në tavolinë, duke mos i mbyllur ato në kasafortë apo duke i lënë në një vend

ku është marrë vesh me personin i cili i fotografon apo i fotokopjon ato dokumente (Salihu & Zhitia& Hasani, 2014: 378).

Kjo vepër mund të kryhet edhe në mënyrë periodike, për shembull, gjatë tërë vitit, kohë pas kohe, në data të caktuara, i komunikon apo i dorëzon fotokopje të dokumenteve të klasifikuara. Nëse këto të dhëna sekrete kanë qenë të destinuara për të njëjtin shtet dhe nëse janë kryer në vazhdimësi kohore, konsiderohet se me këtë veprim është kryer një vepër penale, vepër penale e vazhduar. Nuk ka rëndësi se në çfarë mënyrë autori ka pasur qasje në të dhënat sekrete, rëndësi ka kryerja e veprës. Përkatësisht, vepër penale e vazhduar konsiderohet, si në rastet kur të dhënat sekrete i janë besuar personit që kryen veprën, ashtu edhe në rastet kur ai rastësisht ka pasur qasje në to (Bacic, F. & Sheparovic Z., (1997 : 26).

Me mbledhje të të dhënave sekrete nënkuptohen veprimet me të cilat u mundësohet qasje në të dhëna të besueshme shtetit të huaj, organizatës së huaj apo personit që u shërben atyre. Veprime të mbledhjes së të dhënave sekrete konsiderohen shikimi vizual i këtyre të dhënave, fotografimi, incizimi, marrja e tyre etj.

Nga ana objektive, ky lloj krimi kryhet me anë të veprimeve ose mosveprimeve të kundërligjshme, si dhënia e informatave sekrete me karakter ushtarak apo të çdo lloji tjetër (politik, ekonomik) një fuqie të huaj, për të cenuar pavarësinë e vendit (Elezi, 2009:369).

Nga ana subjektive, krimi i këtij lloji kryhet me dashje të drejtpërdrejtë dhe me qëllim për t'ia dorëzuar informatat sekrete një fuqie të huaj apo agjenturës së saj, me qëllim cenimin e sigurisë kombëtare dhe të pavarësisë së vendit.

Subjekt i këtij krimi është çdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm, i cili mbledh, vlerëson dhe analizon informacione

sekrete për t'ia dorëzuar një shteti të huaj informatat me karakter sekret, ushtarak ose civil, që i janë besuar për ruajtje ose administrim.

Motivet e kryerjes së këtij krimi mund të jenë të ndryshme: interesi material, karrierizmi, urrejtja ndaj shtetit etj., të gjitha kundër Kosovës.

Edhe format e kryerjes së kësaj vepre penale janë të ndryshme jo vetëm në aspektin e anës objektive të kryerjes së saj, por edhe nga lloji dhe masa e dënimit që ligji parashikon për secilën. Për shembull dënimi penal me burgim ashpërsohet nëse vepra penale kryhet në kohë lufte, kur është prezent rreziku i pashmangshëm për luftë, gjatë konfliktit të armatosur apo nëse zbulimi i sekretit shtetëror ka të bëjë me sigurinë e Republikës së Kosovës (Kodi Penal i Kosovës, Neni 131).

Formë jashtëzakonisht e rëndë e spiunazhit konsiderohet ajo vepër penale që rezulton me rrezikimin e jetës së një apo më shumë personave, me vdekjen e një apo më shumë personave, vepra që shoqërohet me dhunë të rëndë, ose me shkatërrim në shkallë të madhe, ose me rrezikim të sigurisë ekonomike dhe ushtarake të Kosovës.

Si formë e posaçme e spiunazhit është parashikuar krijimi në territorin e Kosovës të një shërbimi informativ apo udhëheqja e këtij shërbimi, për një shtet apo organizatë të huaj, shërbim ky që do të spiunojë Kosovën. Kjo formë spiunazhi është vepër kundër sigurisë së vendit tonë.

Zbulimi i informacioneve të klasifikuara dhe mosruajtja e tyre – Neni 132

Informacionet, në përgjithësi, dhe informacionet e klasifikuara, në veçanti, kanë rëndësi të madhe për sigurinë kombëtare të secilit shtet, prandaj ligjvënësi e ka

parashikuar këtë vepër penale me qëllim të ruajtjes së informacioneve të klasifikuara dhe të ruajtjes së interesave të sigurisë së vendit. Kjo vepër e plotëson mbrojtjen e sigurisë dhe të pavarësisë së vendit tonë.

Në aspektin e mbrojtjes së sigurisë dhe të pavarësisë së vendit, kjo vepër penale nuk dallon nga vepra penale e spiunazhit. Mirëpo në aspektin e motivit dhe qëllimit, kjo vepër dallon nga vepra e spiunazhit, pasi në këtë rast zbulimi i të dhënave apo i dokumenteve që konsiderohen sekrete shtetërore nuk bëhet me qëllim që t'i dorëzohen një shteti të huaj, një organizate apo një personi që vepron për shtetin e huaj. Por sipas përkufizimit të saj, kjo vepër quhet e kryer nëse personi i caktuar, i cili në ndonjë mënyrë është njoftuar, ka dijeni për ndonjë të dhënë të karakterit shtetëror, këtë e zbulon. (Salihu & Zhitia& Hasani, 2014: 381).

Objekt i trajtimit të kësaj vepre penale janë marrëdhëniet juridike të vendosura me Ligjin për Klasifikimin e Informacioneve dhe për Verifikimin e Sigurisë. Këto marrëdhënie juridike janë të mbrojtura posaçërisht me legjislacionin penal nga veprime ose mosveprime kriminale dhe kanë për qëllim ruajtjen e informacioneve të klasifikuara si konfidenciale, sekrete dhe tepër sekrete dhe që paraqesin sekret shtetëror. Në Kodin Penal kjo vepër penale është e parashikuar në kuadër të veprave penale kundër rendit kushtetues dhe sigurisë së Republikës së Kosovës. (Kodi Penal i Kosovës, Kapitulli XIV).

Për këtë vepër penale në Kodin Penal nuk është paraparë dënimi që mund të jepet, por aty përcaktohet se për këtë vepër penale autori dënohet sipas Ligjit për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë. Kjo paraqet një paqartësi juridike, sepse, parimisht, një vepër penale nuk mund të parashihet me dy ligje të aplikueshme, siç ndodh me veprën penale "Zbulimi i informacioneve të klasifikuara dhe

mosruajtja e informacioneve të klasifikuara", e cila është e parashikuar edhe në Kodin Penal të Kosovës, edhe në Ligjin për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë. Kjo vepër penale nuk duhet të figurojë fare në Ligjin për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë, sepse, sipas kritereve elementare për ndërtimin e ligjeve, në përgjithësi, dhe të ligjeve penale, në veçanti, nuk rekomandohet që e njëjta vepër penale të parashihet në dy apo më shumë ligje.

Figura e veprës penale "Zbulimi i informacioneve të klasifikuara dhe mosruajtja e tyre - Sipas nenit 132 të Kodit Penal, përcaktohen si veprim i kundërligjshëm që përbën vepër penale, zbulimi ose mosruajtja e informacionit të klasifikuar. Nga ky përkufizim rezulton se kjo vepër penale kryhet në dy situata. Në situatën e parë kryhet kur personi e zbulon informacionin e klasifikuar. Ndërsa në situatën e dytë kryhet kur informacionin e klasifikuar personi nuk e ruan dhe, si pasojë, e kësaj mosruajtjeje, u mundësohet personave të paautorizuar që të njoftohen apo të kenë qasje në këtë informacion.

Elementi thelbësor i kësaj vepre qëndron në faktin se autori i këtij krimi sillet në mënyrë të papërgjegjshme ndaj obligimit që ka për ruajtjen e sekretit. Këtu është fjala për shkelje të rëndë të obligimit për ta ruajtur sekretin, që është i karakterit shtetëror. Rrezikshmëria e kësaj vepre konsiston në faktin se me shkeljen e këtij obligimi krijohet mundësia, edhe pse kjo nuk është dëshirë e as qëllim i autorit të veprës, që shteti i huaj të ketë qasje në të dhënat që janë sekrete shtetërore (Bacic, F. & Sheparovic Z., (1997: 26).

Në Ligjin për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë, neni 50 përcakton si veprime të kundërligjshme që përbëjnë vepër penale:

a) Publikimin e paautorizuar dhe mosmbrojtjen e informacionit të klasifikuar si "Konfidenciale",

b) Publikimin e paautorizuar dhe mosmbrojtjen e informacionit të klasifikuar si "Sekret",

c) Publikimin e paautorizuar dhe mosmbrojtjen e informacionit të klasifikuar si "Tepër Sekret".

Nga ana objektive, krimi kryhet me anë të veprimeve ose mosveprimeve të kundërligjshme, që konsistojnë në dhënien e informatave të klasifikuara si konfidenciale, sekrete dhe tepër sekrete një fuqie të huaj, për të cenuar pavarësinë e vendit. Informatat e klasifikuara sigurohen nga personat e paautorizuar përmes qasjes së paligjshme në informacione, përmes fotokopjimit, fotografimit të dokumenteve, deshifrimit të kodit, përmes bisedave me persona që i kanë informatat e klasifikuara. Dhënia në mënyrë të kundërligjshme e informacioneve të klasifikuara bëhet me gojë, me telefon, me shkrim me shifra të koduara dhe në çdo mënyrë tjetër. Kështu, për shembull, dhënia e një mikrofilmi, ku janë fotografuar objekte me karakter sekret ushtarak, nga personi të cilit i është besuar ruajtja e mikrofilmave, përbën shkelje të rregullave të caktuara për ruajtjen e informatave me karakter sekret ose që japin informata sekrete sipas porosisë së zbulimeve të huaja (Elezi, 2009:371).

Nga ana subjektive, ky lloj krimi kryhet me dashje të drejtpërdrejtë për t'ia dorëzuar informatat sekrete një fuqie të huaj apo agjenturës së saj, me qëllim cenimin e sigurisë kombëtare dhe të pavarësisë së vendit.

Subjekt i krimit është çdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm, që punon në organe shtetërore dhe ka qasje në sekrete

shtetërore, i janë besuar për ruajtje ose administrim informata me karakter sekret, ushtarak ose civil, por që i publikon ato në mënyrë të paautorizuar dhe nuk e mbron informacionin e klasifikuar.

Motivet mundë të jenë të ndryshme: interesi material, karrierizmi, urrejtja për vendin etj., të gjitha këto të motivuara kundër Kosovës.

Cenimi i fshehtësisë së korrespondencës dhe të bazave të të dhënave kompjuterike (Neni 202)

Një ndër të drejtat kushtetuese të personit është edhe ruajtja e fshehtësisë së korrespondencës së tij (Kushtetuta e Kosovës, neni 36), shkelja e së cilës në Kodin Penal parashikohet si vepër penale.

Fshehtësia e letrave, e telegrameve, e faksimileve ose e ndonjë dokumenti tjetër të mbyllur apo dërgese, që i destinohet një personi tjetër, është e garantuar me legjislacionin vendor dhe atë ndërkombëtar dhe mbrohet edhe me të drejtën penale.

Me globalizimin e shoqërisë, sot koncepti i jetës private ka ndryshuar. Është e pamundur pjesëmarrja jonë në këtë detyrë, në një numër organesh me shumë të dhëna personale dhe pa qasjen tonë në informacionet e të tjerëve (Mendel, 2012:102).

Shpërndarja e informacioneve në të gjitha fushat ku përfshihen personat ka marrë përmasa të tilla që tani është e qartë se njerëzit e duan këtë shpërndarje dhe se dhënia e informacionit, dhënia e pëlqimit për të ndarë informacionin rreth tyre është shumë më e lehtë sesa në të kaluarën. (Lessig, 2013:181).

Kushtetuta e Republikës së Kosovës përkufizon qartë që çdokush të gëzojë të drejtën që t'i respektohet jeta private dhe familjare, pacenueshmëria e banesës dhe fshehtësia e korrespondencës, e telefonisë dhe e komunikimeve të tjera. Përjashtimisht, këto të drejta mund të kufizohen vetëm përkohësisht dhe në bazë të vendimit të një gjykate, kur është e domosdoshme të udhëhiqet ndonjë procedurë penale dhe në rastet kur e kërkojnë interesat kombëtare dhe shtetërore (Kushtetuta e Republikës së Kosovës, neni 36).

Vepra penale "*Cenimi i fshehtësisë së korrespondencës dhe të bazave të të dhënave kompjuterike*" është e parashikuar në kuadër të veprave penale kundër lirive dhe të drejtave të njeriut (Kodi Penal i Kosovës, Kapitulli XVII). Të dhëna kompjuterike janë të gjitha shkresat, fotografitë, planet, sekretet e biznesit, sekretet zyrtare, shënimet, porositë, llogaritë e ndryshme, procesverbalet e ndryshme, raportet e ndryshme, me fjalë të tjera, çdo shënim që gjendet në kompjuter, përveç shënimeve për karakteristikat teknike të kompjuterit.

Ndryshe nga pacenueshmëria e banesës, pacenueshmëria e korrespondencës nuk mund të kufizohet asnjëherë pa ndonjë vendim të gjykatës.

Objekti i kësaj vepre penale janë marrëdhëniet juridike të vendosura nga shteti për të ruajtur fshehtësinë e korrespondencës dhe të bazave të të dhënave kompjuterike nga veprimet apo mosveprimet kriminale.

Objekt i sulmit tek kjo vepër penale janë letrat e mbyllura, faksimilet, telegramet, dokumentet tjera të mbyllura, deklaratat, porositë, shënimet dhe përmbajtjet tjera të dërguara me mjetet elektronike. Objekt i mbrojtjes në këtë vepër penale është fshehtësia e materialeve të tilla, si një e drejtë e garantuar me kushtetutë.

Objekti sulmues është kompjuteri si mjet elektronik i korrespondencës. Veprimet e kryerjes së krimit janë paraqitur në mënyrë alternative me depërtimin në bazën e të dhënave kompjuterike të personit tjetër, me shfrytëzimin e të dhënave që gjenden në të dhe me vënien e këtyre të dhënave personit tjetër.

Nga ana objektive, kjo vepër kryhet me veprime ose me mosveprime të kundërligjshme, me forma dhe mënyra të ndryshme, si: me agjësim, me mosdorëzimin e letrave në destinacion, me hapjen dhe leximin e tyre apo të çdo korrespondence tjetër, si dhe me ndërprerjen ose vënien nën kontroll të aparateve telefonike, dëgjimi i bisedave telefonike, telegrafike ose të çdo mjeti tjetër telekomunikimi.

Subjekt i kësaj vepre penale është çdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm.

Nga ana subjektive, vepra mund të kryhet me dashje të drejtpërdrejtë ose të tërthortë.

Në legjislacionin tonë penal ekzistojnë disa forma themelore të kësaj vepre penale, të ndryshme për nga mënyra e kryerjes dhe e qëllimit të autorit. Mirëpo tek të gjitha format e kësaj vepre penale objekt i sulmit është një: letër e huaj, telegram, faks, dokumenti tjetër i mbyllur, apo dërgesë e personit tjetër (Salihu & Zhitia& Hasani, 2014: 553).

Kjo vepër penale mund të kryhet në disa mënyra. Ajo realizohet: me hapjen e paautorizuar të letrave të huaja, të telegrameve apo të ndonjë dokumenti tjetër të mbyllur, të ndonjë dërgese apo komunikim elektronik të personit tjetër; me cenimin, në ndonjë mënyrë tjetër, të fshehtësisë së materialeve të tilla; kur pa autorizim mban, fsheh, asgjëson ose i dorëzon një personi tjetër, letrën, telegramin, faksimilen, komunikimin elektronik, ndonjë dokument tjetër të mbyllur ose dërgesë të dikujt tjetër.

Figura e veprës penale "Cenimi i fshehtësisë së korrespondencës dhe të bazave të të dhënave kompjuterike" - Sipas nenit 202 të Kodit Penal të Kosovës, përcaktohen si veprim i kundërligjshëm që përbën vepër penale: hapja pa autorizim e letrës, e telegramit, e faksimileve ose e ndonjë dokumenti tjetër të mbyllur a dërgese të personit tjetër, ose, cenimi, në ndonjë mënyrë tjetër, i fshehtësisë së materialeve të tilla; mbajtja, fshehja, asgjësimi ose dorëzimi i një personi tjetër i letrës, i telegramit, i faksimiles apo i dërgesës të dikujt tjetër.

Për të pasur figurën e veprës penale të kryer, mjafton një nga format apo mënyrat e treguara më lart, pa qenë nevoja për ardhjen e ndonjë pasoje tjetër.

Të gjitha këto forma janë të kundërligjshme, përveç rasteve kur organet shtetërore, të caktuara me detyra për zbulimin dhe luftimin e kriminalitetit, janë të autorizuara me ligj të marrin masa për përgjime, sipas dispozitave ligjore të posaçme (Elezi & 2009:180)

Me letër të huaj kuptojmë çdo letër që ka një përmbajtje dhe është e mbyllur dhe përmbajtja e saj nuk mund të kuptohet pa u mënjanuar pengesat dhe e adresuar personit të caktuar. Ato janë: letra e huaj, telegrami, faksi, një dokument tjetër i mbyllur apo dërgesë e personit tjetër ose komunikim i personit tjetër (Bacic & Pavlovic, 543).

Cenimi në ndonjë mënyrë tjetër i fshehtësisë së letrës, të dokumentit, të dërgesës postare dhe asaj elektronike etj. është njohja me përmbajtjen e tyre me anë të mjeteve kimike, përdorimit të rrezeve ultraviolet apo me metoda tjera teknike. Që kjo formë të quhet vepër penale, duhet që autori ta ketë mësuar përmbajtjen e korrespondencës. Nëse ai nuk e ka mësuar atë, atëherë nuk ekziston edhe vepra penale. Fshehja, mbajtja dhe asgjësimi i letrave, i dokumenteve, i telegrameve, i faksimileve ose i dërgesave elektronike është mënyrë tjetër e kryerjes së kësaj vepre penale. Tek kjo formë e veprës

penale kemi të bëjmë me mënyrat e ndryshme të posedimit të paautorizuar të korrespondencave (Salihu & Zhitia& Hasani, 2014: 555).

Paragrafi 1, i nenit 202, përcakton këto veprime të kundërligjshme që përbëjnë vepër penale:

a) Hapja e paautorizuar e letrës, e telegramit, e faksimiles apo e ndonjë dokumenti tjetër të mbyllur ose e dërgesës, e komunikimit elektronik të personit tjetër,
b) Cenimi i fshehtësisë së materialeve,
c) Mbajtja e paautorizuar, fshehja, asgjësimi ose dorëzimi i letrës, i telegramit, i faksimiles, i komunikimit elektronik, i ndonjë dokumenti tjetër të mbyllur apo i një dërgese një personi tjetër.

Paragrafi 2, i nenit 202, përcakton veprim të kundërligjshëm që përbën vepër penale, ndërhyrjen e paautorizuar në bazën e të dhënave kompjuterike të personit tjetër, shfrytëzimin dhe vënien e këtyre të dhënave kompjuterike në dispozicion personit tjetër. Ky veprim mund të bëhet në mënyra të ndryshme, me përcjellje elektronike tek kompjuteri i personit tjetër, me dhënien në dorë personit tjetër, me anë të kopjimit, incizimit etj. Që ky veprim të përbëjë vepër penale, duhet që ai të jetë ndërmarrë pa autorizim ose në mënyrë të kundërligjshme. Për ekzistimin e kësaj forme të veprës penale mjafton që të dhënat e nxjerra nga kompjuteri i personit të huaj të shfrytëzohen pa autorizim ose në mënyrë të kundërligjshme.

Forma e kualifikuar e këtyre veprave penale themelore ekziston, kur ato kryhen me qëllim të përfitimit të dobisë pasurore (dobi materiale dhe jomateriale) për vete ose

për tjetrin apo për t'i shkaktuar tjetrit dëm, si edhe kur vepra kryhet nga personi zyrtar gjatë ushtrimit të detyrës zyrtare (Kodi Penal i Kosovës, Neni 202).

Figura e krimit e cekur në paragrafin 3 dhe 4 të nenit 202, për nga forma janë më të rënda, pasi vepra penale konsiderohet e kryer në raste kur autori e kryen atë për përfitimi të dobisë pasurore për vete ose për një person tjetër apo për t'i shkaktuar dëm personit tjetër (Neni 202, Paragrafi 3, Kodi Penal) .

Formë tjetër e rëndë e kësaj vepre penale konsiderohet kur ajo kryhet nga personi zyrtar në keqpërdorim të pozitës apo të autorizimeve të tij (Kodi Penal i Kosovës, Neni 202, Paragrafi 4).

Mënyrë tjetër e kryerjes së kësaj vepre penale është edhe kur korrespondenca i dërgohet një personi tjetër, të cilit nuk i është adresuar.

Rast nga praktika gjyqësore e Gjykatës Evropiane të të Drejtave të Njeriut

Hartimi i legjislacionit vendor është në përputhje edhe me aktet kryesore ndërkombëtare në fushën e mbrojtjes së lirive dhe të drejtave të njeriut, pasi *cenimi i fshehtësisë së korrespondencës dhe të bazave të të dhënave kompjuterike* përbën cenim apo shkelje edhe të dispozitës së nenit 8 (E drejta për respektimin e jetës private dhe familjare) të Konventës Europiane për të Drejtat e Njeriut.

Praktika gjyqësore e Gjykatës Europiane për të Drejtat e Njeriut (GJEDNJ) është mjaft e zhvilluar. Ajo ka konstatuar se e drejta për të respektuar korrespondencën e një personi është një e drejtë që ka lidhje me komunikimet e pandërprera e të pacensuruara me të tjerët. Më 23 korrik 1992, Silvestru Cotlet, shtetas rumun, u gjet fajtor, nga një gjykatë rrethi, për kryerjen e një vrasjeje dhe u dënua prej saj me 17 vjet burg. Z. Cotlet

u dërgua në burgun e Drobeta Turnu-Severin dhe në vijim u transferua në disa burgje. Në nëntor 1995, i dënuari dërgoi nga burgu një kërkesë për Komisionin Europian të të Drejtave të Njeriut, duke u ankuar për karakterin e padrejtë të procesit që kishte çuar në dënimin e tij. Z. Cotlet, në bazë të nenit 8 të Konventës Europiane për të Drejtat e Njeriut, iu drejtua edhe GJEDNJ-së, për ndërhyrje në korrespondencën e tij me institucionet e Konventës, përfshirë këtu vonesat në dërgimin e letrave të tij me Gjykatën dhe me Komisionin, hapjen e letrave që ai u dërgonte këtyre institucioneve etj. (Cotlet kundër Rumanisë, kërkesa numër 38565/95).

GJEDNJ në çështjen *Cotlet kundër Rumanisë (kërkesa numër 38565/95),* për sa u përket vonesave të korrespondencës kishte vënë re se ndërmjet nëntorit 1995 dhe tetorit 1995 korrespodencës së z. Cotlet i ishte dashur ndërmjet 1 muaj e 1 ditë deri në 2 muaj e 6 ditë për të arritur në destinacion. Sipas mendimit të Gjykatës, këto vonesa përbënin ndërhyrje ndaj të drejtës së tij për respektimin e korrespondencës, ndaj, në këtë rast, Gjykata vendosi se ka pasur shkelje të Konventës (*Cotlet kundër Rumanisë kërkesa numër 38565/95, faqe 467*). Ndërsa lidhur me çështjen e hapjes së korrespondencës së z. Cotlet me Komisionin dhe Gjykatën, GJEDNJ ka konstatuar faktin që letrat e z. Cotlet ishin hapur dhe se kjo përbënte një ndërhyrje në të drejtën e tij për respektimin e korrespondencës (*Cotlet kundër Rumanisë kërkresa numër 38565/95, faqe 467*).

Edhe në rastin *Lavents kundër Letonisë (kërkesa numër 58442/00)* GJEDNJ kishte vlerësuar se ka pasur ndërhyrje në të drejtën e z. Lavents për respektimin e korrespondencës. Gjykata ka vënë në dukje se masa në fjalë, pra, bllokimi dhe kontrolli i korrespondencës, ishte urdhëruar nga një gjyqtar në bazë të Kodit të Procedurës Penale, i cili autorizonte marrjen e masave të tilla në rastin e personave të akuzuar për vepra penale të një rrezikshmërie të madhe. Sipas Mendimit të Gjykatës, kjo dispozitë u

krijonte gjykatave një hapësirë mjaft të madhe, duke parashikuar vetëm llojet e veprave penale për të cilat kjo masë gjen zbatim, por duke mos specifikuar periudhën e vlefshmërisë së masës ose arsyet subjektive që mund të kërkojnë vendosjen e saj (*Lavents kundër Letonisë, kërkesa 58442/00, faqe 229*).

Zbulimi i paautorizuar i informacionit konfidencial (Neni 203)

Në sferën e marrëdhënieve të ndryshme në të cilat hyjnë individët, ekzistojnë situata të tilla në të cilat duhet të ekzistojë një shkallë e besimit midis pjesëmarrësve në këto marrëdhënie, në mënyrë që pa pengesa të realizohet qëllimi për shkak të të cilit individët kanë hyrë në ato marrëdhënie (Salihu, 2009: 169).

Ruajtja e fshehtësisë zyrtare dhe profesionale e informacionit konfidencial është obligim ligjor i secilit punonjës. Ky obligim derivon nga ligjet e aplikueshme të secilit vend, ndërsa në mënyrë specifike është i rregulluar me rregullore dhe me procedurat standarde të veprimit të secilit institucion. Zgjedhja ligjore është e ndryshme, varësisht nga vendet e ndryshme. Disa vende fillojnë nga konstatimi se zbulimi i fshehtësisë së informacionit konfidencial duhet të shkaktojë pasojë, ndërsa disa të tjera këtë kusht nuk e kërkojnë dhe parashohin forma të posaçme të kësaj vepre penale. Mosruajtja e informacionit konfidencial dhe zbulimi i paautorizuar i tij shkakton pasoja penalo-juridike.

Vepra penale "*Zbulimi i paautorizuar i informacionit konfidencial"* është e parashikuar në kuadër të veprave penale kundër lirive dhe të drejtave të njeriut në Kodin

Penal të Kosovës, Kapitulli XVII). Me këtë normë penalo-juridike mbrohet fshehtësia e disa profesioneve të cilat sipas dispozitave ligjore apo etike janë të ndaluara të zbulohen.

Figura e veprës penale "Zbulimi i paautorizuar i informacionit konfidencial" - Sipas nenit 203 të Kodit Penal, përcaktohen si veprim të kundërligjshëm, që përbën vepër penale, zbulimin e paautorizuar të informacionit konfidencial nga avokati, nga mbrojtësi, nga mjeku apo personi tjetër që është vënë në dijeni gjatë ushtrimit të profesionit të vet dhe që është ligjërisht i detyruar ta mbajë në fshehtësi. Veprimi i kryerjes së kësaj vepre penale ka të bëjë me zbulimin e informacionit të besueshëm, gjatë ushtrimit të profesionit. Me zbulim të informacionit kuptojmë veprimet me të cilat i mundësohet personit tjetër të mësojë përmbajtjen e informacionit të besueshëm. Shpesh, zbulimi i informacionit konfidencial bëhet duke ia treguar personit tjetër, por ekzistojnë edhe mënyra tjera, sikurse janë: mundësia e shikimit të dokumentacionit që përmban informacionin, dërgimi i shkresave, leximin e tyre një personi tjetër, vënia në shikim për persona të tjerë në raste ligjëratash, shpjegimesh apo diskutimesh me ta etj (Salihu & Zhitia & Hasani, 2014: 556). Kjo vepër penale quhet e kryer kur informacioni i besueshëm zbulohet pa autorizimin e personit për të cilin ka të bëjë informacioni, që është përcaktuar si i besueshëm në bazë të ligjit apo kodit të etikës.

Nga ana objektive, vepra penale kryhet me zbulimin e informacionit të besueshëm, gjatë ushtrimit të profesionit.

Pasoja e kësaj vepre penale është zbulimi i informacionit. Pasoja mund të shkaktohet në momentin e ndërmarrjes së veprimit të kryerjes së veprës penale ose në momentin e leximit të informacionit.

Subjekt i këtij krimi është çdo person që ka kryer veprimet e parashikuara me këtë vepër penale, person i cili është i përgjegjshëm dhe ka mbushur moshën për përgjegjësi penale.

Nga ana subjektive ky lloj krimi kryhet me dashje, të drejtpërdrejtë, për të kryer veprimet e parapara për këtë vepër penale.

Shënimet, shkresat dhe dokumentet që paraqesin fshehtësi personale, profesionale, ushtarake, shtetërore apo fshehtësi biznesi dhe zbulimi i tyre mbrohen me ligje të veçanta, ngaqë interesi shoqëror dhe personal e kërkon që ato shënime apo të dhëna të mos zbulohen, madje, edhe ato që konsiderohen si fshehtësi personale e cila iu është besuar apo kanë mësuar personat e caktuar gjatë ushtrimit të detyrës së tyre. Me këtë normë juridike, praktikisht, mbrohet fshehtësia profesionale. (Salihu & Zhitia & Hasani, 2014: 558).

Sipas përkufizimit të kësaj vepre penalo-juridike, këtë krim mund ta kryejnë avokati, mjeku apo personi tjetër që, pa autorizim, zbulon informacionin konfidencial për të cilin është vënë në dijeni gjatë ushtrimit të profesionit të vet dhe që është ligjërisht i detyruar ta mbajë në fshehtësi. Ky obligim vlen vetëm për personat e caktuar gjatë ushtrimit të profesionit të tyre.

Objekti mbrojtës i kësaj vepre penale janë faktet që kanë të bëjnë me jetën e personit. Prandaj, kjo normë juridike ofron mbrojtje të fshehtësisë personale (individuale) dhe jo fshehtësi të tjera. Kështu, sipas objektit mbrojtës të kësaj vepre penale, me fshehtësi nënkuptojmë ato fakte ose rrethana të jetës së personit për të cilin flet dokumenti konfidencial, që janë mësuar gjatë ushtrimit të profesionit, dhe personi për të cilin kanë të bëjnë faktet apo rrethanat nuk dëshiron t'i zbulohen (Salihu & Zhitia & Hasani, 2014: 558).

Për ekzistimin e kësaj vepre penale nuk është e rëndësishme se si janë mësuar fshehtësitë, por patjetër është e nevojshme që deri tek mësimi i fshehtësive ka ardhur gjatë ushtrimit të profesionit. Nëse deri tek informacioni i besueshëm është ardhur jashtë ushtrimit të profesionit, përmes kolegut, mikut etj., kjo vepër penale nuk do të ekzistojë, sepse mungon elementi i kësaj figure të veprës penale.

Pasoja e veprës penale është caktuar me vetë veprimin e kryerjes së saj, respektivisht pasoja është me vetë faktin se është zbuluar informacioni. Ajo mund të shkaktohet, ose në momentin e ndërmarrjes së veprimit të kryerjes së veprës penale, ose në momentin e mësimit të informacionit.

Sipas nenit 203 të Kodit Penal të Kosovës, personi që ka zbuluar informacionin konfidencial nuk është penalisht përgjegjës, nëse ai e ka zbuluar atë ngaqë e kërkon interesi i përgjithshëm, i cili peshon më shumë, sesa moszbulimi i atij informacioni konfidencial.

Nëse autori e ka zbuluar informacionin në interes të përgjithshëm dhe në rastin e dytë, kur interesi i personit tjetër është me peshë më të madhe sesa interesi i moszbulimit, lejohet mundësia e përjashtimit të përgjegjësisë penale të kryerësit. Zbulimi i informacionit konfidencial është me interes të përgjithshëm, zakonisht, atëherë kur kemi të bëjmë me ndonjë sëmundje ngjitëse, për ta evituar zgjerimin e saj. Dispozitat ligjore rrallëherë përmbajnë detyrim për zbulimin e informacioneve të tilla, por më shpesh ajo ekziston te disa dispozita të veçanta, për shembull, në Kodin Penal, kur personi gjatë ushtrimit të detyrës zbulon se është duke u përgatitur kryerja e veprës së rëndë penale (Kodi Penal i Kosovës, Neni 203).

Interesi i përgjithshëm duhet të jetë i përcaktuar me ligj apo me akte ligjore, që autorizojnë persona të caktuar të zbulojnë informacionin. Për shembull, është obligim i

qytetarit, i personit zyrtar dhe i avokatit të zbulojnë informacionin për përgatitjen e veprës së rëndë penale.

Në raste të tjera, nevoja e zbulimit të informacionit të besueshëm paraqitet për shkak se zbulimi i tij është në interes të personit tjetër, ndaj interesi i zbulimit ka peshë më të madhe, sesa interesi i moszbulimit. Për shembull, nëse personi vuan nga sëmundja e AIDS dhe dëshiron të martohet me personin tjetër, i cili nuk di për sëmundjen (Salihu & Zhitia & Hasani, 2014: 559).

Rast nga praktika gjyqësore e Gjykatës Europiane të të Drejtave të Njeriut

Në çështjen *Godelli kundër Italisë*, GJEDNJ ka vendosur unanimisht se ka pasur një shkelje të Nenit 8 (E drejta për respektimin e jetës private dhe familjare) të Konventës Europiane për të Drejtat e Njeriut, pasi sistemi italian nuk merr parasysh interesat e fëmijës, bazuar në ligjin Nr. 184/1983, që garanton të drejtën për të mbajtur sekret origjinën e fëmijës, në mungesë të autorizimit të shprehur nga autoriteti gjyqësor.

GJEDNJ konsideroi, ndër të tjera, se nuk ishte vendosur një balancë e drejtë midis interesave në fjalë që në legjislacion, për rastin kur nëna kishte vendosur të mos zbulojë identitetin e saj, nuk i ka lejuar një fëmijë që nuk ishte njohur zyrtarisht në lindje dhe u miratua më pas të kërkojë ose informacion lidhur me origjinën e tij ose të saj, ose zbulimin e identitetit të nënës lindëse me pëlqimin e këtij të fundit (*Godelli kundër Italisë, aplikimi nr: 33783/09*).

Gjykata vuri në dukje se Neni 8 i Konventës Europiane për të Drejtat e Njeriut e mbron të drejtën për identitetin dhe zhvillimin personal; paraqitjen e së vërtetës në lidhje me identitetin personal të dikujt, duke përfshirë identitetin e prindërve të ndokujt,

ishte një faktor kontribues në këtë zhvillim. Rrethanat në të cilat një fëmijë ka lindur ishte pjesë e fëmijërisë dhe e jetës private të të rriturit, të garantuara me këtë nen.

Gjykata përsëriti se çështja e qasjes në informacionin lidhur me origjinën e dikujt dhe me identitetin e prindërve natyrorë të dikujt nuk ishte i natyrës së njëjtë me atë të qasjes në të dhënat e rastit lidhur me një fëmijë në përkujdesje ose me dëshmi të atësisë së pretenduar. Znj. Godelli kishte kërkuar për të gjetur nënën e saj, e cila e kishte braktisur atë që në lindje dhe kishte kërkuar shprehimisht që identiteti i saj të mbahet sekret. Interesat në fjalë ishin: interesi i nënës në ruajtjen e anonimatit të saj; interesi i fëmijës për të mësuar origjinën e vet; dhe interesi i përgjithshëm në parandalimin e aborteve të paligjshme dhe braktisjen e fëmijëve.

Gjykata theksoi se interesi i një individi për zbulimin e prejardhjes së tij ose të saj nuk humbet me kalimin e moshës, por është krejt e kundërta. Edhe pse në moshë 69-vjeçare personaliteti i zonjës Godelli, tashmë, ishte formuar, megjithatë, ajo kishte treguar një interes të vërtetë në zbulimin e identitetit të nënës së saj; një sjellje e tillë implikon vuajtje mentale dhe psikologjike.

Megjithatë, për aq sa legjislacioni italian nuk i ka lejuar një fëmije, që nuk ishte njohur zyrtarisht në lindje dhe të cilit më pas iu miratua e drejta për të kërkuar, ose qasje në mosidentifikimin e informacionit në lidhje me origjinën e tij apo të saj, ose zbulimin e identitetit të nënës, Gjykata konsideroi se autoritetet italiane kishin dështuar në arritjen e një ekuilibri të drejtë ndërmjet interesave në rrezik dhe kishte tejkaluar vlerësimin e tyre. Prandaj, ka pasur një shkelje të Nenit 8 të Konventës Europiane për të Drejtat e Njeriut (*Godelli kundër Italisë, aplikimi nr: 33783/09*).

Përgjimi i paautorizuar (Neni 204)

Vepra penale "*Përgjimi i paautorizuar*" është e parashikuar në kuadër të veprave penale kundër lirive dhe të drejtave të njeriut në Kodin Penal të Kosovës, Kapitulli XVII. Qëllimi inkriminues i kësaj vepre penale në legjislacionin tonë penal është mbrojtja e jetës private të njeriut, respektivisht, të jetës intime. Fjala është për të drejtën personale për komunikim privat me personin tjetër (Salihu & Zhitia & Hasani, 2014: 560). Sipas mënyrës së kryerjes së kësaj vepre penale kemi të bëjmë me përgjimin e paautorizuar apo me përgjimin tonik të zërave dhe incizimin e bisedës së huaj, ose ia mundëson personit tjetër të njoftohet me përmbajtjen apo me deklaratën që është përgjuar në mënyrë tonike ose incizuar. Që të kemi vepër penale, duhet që të gjitha këto veprime të jenë ndërmarrë pa autorizim.

Figura e veprës penale "Përgjimi i paautorizuar" - Sipas nenit 204 të Kodit Penal të Kosovës, veprime të kundërligjshme që përbëjnë vepër penale përcaktohen: përgjimi i paautorizuar, përgjimi tonik ose incizimi i paautorizuar i bisedës apo i deklaratës, ose mundësimi personit tjetër të jetë në dijeni për bisedën apo për deklaratën që është përgjuar pa autorizim. Veprimet si: përgjimi, përgjimi tonik dhe incizimi i bisedave apo i deklaratave që nuk i përkasin autorit të veprës paraqesin formën e parë e kësaj vepre penale. Për të ekzistuar kjo vepër penale duhet të ekzistojë elementi qenësor i saj, kundërligjshmëria, e cila shprehet me mosekzistimin e autorizimit për përgjim, për përgjimin tonik ose për incizimin e bisedës a të deklaratës. Bisedat a deklaratat duhet të kenë përmbajtje që prekin jetën private të personit. Përgjimi, përgjimi tonik ose incizimi i bisedave a deklaratave që kanë të bëjnë me biseda politike, zyrtare, afariste,

profesionale e biseda tjera që nuk prekin jetën private, nuk përbëjnë vepër penale (Salihu & Zhitia & Hasani, 2014: 555).

Nga ana objektive, kjo vepër penale kryhet me përgjim të paautorizuar, përgjim tonik ose incizim të paautorizuar të bisedës a të deklaratës ose mundësimin personit tjetër që të jetë në dijeni për bisedën apo deklaratën që është përgjuar pa autorizim.

Pasoja e kësaj vepre është përcaktuar me vetë veprimin e kryerjes së saj, domethënë me përgjim të paautorizuar, përgjim tonik dhe incizim të bisedave a deklaratave të huaja.

Subjekt i këtij krimi është çdo person që ka bërë përgjimin e paautorizuar, përgjimin tonik apo incizimin, por mund të jetë edhe personi tjetër, i cili ka qenë i vetëdijshëm se e po vë në dijeni personin tjetër me bisedën a deklaratën që është incizuar apo përgjuar pa autorizim.

Nga ana subjektive ky krim kryhet me dashje të drejtpëdrejtë apo eventuale për të kryer veprimet e parapara të kësaj vepre penale.

Vepra në fjalë mund të kryhet për motive të ndryshme: përfitime materiale, hakmarrje, urrejtje, kureshtje apo për qëllime tjera. Po ashtu, për ekzistimin e kësaj vepre penale nuk është e rëndësishme as rrethana që ajo që është përgjuar apo incizuar ka qenë më parë e njohur për personin tjetër. Për këtë arsye, në përkufizimin e kësaj vepre penale nuk gjendet qëllimi i autorit për ta kryer këtë vepër penale. Në rastet kur biseda dhe incizimi bëhen publike pas përgjimit ose incizimit të paautorizuar, ndjekja penale bëhet me autorizim të personit të përgjuar ose incizuar. Në këto raste, për shkak të rëndësisë së vogël shoqërore të veprës penale, ndjekja penale nuk duhet të fillohet dhe, nëse është filluar, duhet të pushohet.

Kjo vepër penale kryhet edhe me mundësinë që i krijohet personit tjetër që të njoftohet me përmbajtjen e bisedës a të deklaratës që është përgjuar, përgjuar me ton apo e incizuar pa autorizim. Esenca e kësaj forme është personi tjetër të jetë vënë në dijeni me atë që është marrë pa autorizim. Personi i pa thirrur mund të vihet në dijeni duke ia komunikuar përmbajtjen e bisedës apo të deklaratës me gojë, duke ia mundësuar shikimin apo dëgjimin e incizimit, duke ia dërguar incizimin me mjete tjera teknike, duke ia dorëzuar incizimin dhe me mënyra tjera.

Dispozita e nenit 204, te paragrafi 2, përcakton rrethanat rënduese në rastet kur vepra penale kryhet nga personi zyrtar gjatë ushtrimit të detyrës. Forma kualifikuese e kësaj vepre penale bëhet për shkak të cilësive që ka autori i veprës penale. Nëse vepra penale kryhet nga personi zyrtar gjatë ushtrimit të detyrës zyrtare, ajo bëhet e kualifikuar dhe, për të sanksioni penal është parashikuar më i rëndë.

Rast nga praktika gjyqësore e Gjykatës Europiane të të Drejtave të Njeriut

Masat e përgjimit të fshehtë janë pjesë e numrit gjithnjë në rritje të padive në GJEDNJ (Roagna, 2012:40). Në këtë fushë, zhvillimet teknologjike kanë detyruar Gjykatën të krahasojë parimet tradicionale të Nenit 8 të Konventës Europiane për të Drejtat e Njeriut me metodat e sofistikuara të ndërhyrjes në jetën private. Në vitin 2010, Gjykata dha gjykimin e saj të parë lidhur me përgjimin GPS në kontekstin e hetimeve penale (*Uzun kundër Gjermanisë*, *aplikacioni numër 35623/05*).

Fotografimi dhe incizimet tjera të paautorizuara (Neni 205)

Kjo vepër penale është e parashikuar në kuadër të veprave penale kundër lirive dhe të drejtave të njeriut dhe vetëm sa e plotëson qëllimin kushtetues së Republikës së Kosovës për ruajtjen integritetit personal, jetën private dhe të drejtat personale të individit (Kodi Penal i Kosovës, Kapitulli XVII).

Sot, çdo ditë, posaçërisht në vendet me një sundim të brishtë të ligjit, me shfrytëzimin e videove dhe me vëzhgim në mënyrë drastike shkelen e drejta e privatësisë dhe integriteti i garantuar me kushtetutë. Shembull: ekziston vepra penale "*Fotografimi dhe incizime tjera të paautorizuara*", kur personi, pa autorizim, ka publikuar përmes faqes së internetit dhe telefonave mobilë foto, ku duket personi i dëmtuar në situata dhe pamje të palakmueshme, që cenojnë dinjitetin dhe moralin njerëzor. Sidomos mediat hulumtuese, gazetarë, emisione të tjera humoristike individë etj, krejt me pretekstin se po zbulojnë dukuritë negative në shoqëri, duke përdorur mjete të sofistikuara, në fakt, cenojnë të drejtën e privatësisë, përfshirë edhe jetën intime të njerëzve. Prej këtyre veprimeve janë shkaktuar pasoja shumë të rënda, vetëvrasje, vrasje e deri te shkatërrimi i jetës së individëve, krejt me motivacion dhe nën emrin e gazetarisë apo të mediave investiguese (Salihu & Zhitia & Hasani, 2014: 562).

E drejta e privatësisë përfshin disa të drejta të tjera, që parashihen në Paktin Ndërkombëtar për të Drejtat Civile dhe Politike (Pakti Ndërkombëtar për të Drejtat Civile dhe Politike, neni 17). Deklarata Universale për të Drejtat e Njeriut parashikon: "*Askush nuk bën t'i ekspozohet ndërhyrjes arbitrare dhe të paligjshme në jetën private, familje, banesë apo letërkëmbim dhe as sulmeve të kundërligjshme në nderin dhe reputacionin dhe ka të drejtë në mbrojtje ligjore nga ndërhyrja dhe sulmi i tillë"*

(Deklarata Universale për të Drejtat e Njeriut, neni 12). Megjithatë, sot e drejta e privatësisë cenohet nga kryerja e disa veprave penale, ndër të cilat është edhe fotografimi dhe incizimet e tjera të paautorizuara. Këto të drejta janë të mbrojtura edhe me dokumente tjera ligjore, ndër të cilat edhe me Konventën Europiane për të Drejtat dhe Liritë Themelore të Njeriut, që garanton të drejtën e respektimit të jetës private dhe familjare. Por, në praktikë, kjo e drejtë nuk respektohet ashtu siç përcaktohet në ligjet e aplikueshme dhe ka raste kur ajo cenohet pikërisht nga ata që janë të ngarkuar për ta garantuar atë. Gjersa sot nga cenimi i kësaj të drejte nuk kursehen as liderët botërorë, atëherë respektimi i kësaj të drejte për qytetarët e thjeshtë të një shteti shpeshherë vihet në pikëpyetje.

Kjo çështje ka hapur shumë debate individuale, por edhe debate dhe pakënaqësi edhe në nivelet më të larta shtetërore dhe ndërkombëtare, sidomos pas publikimit të disa të dhënave mbi përgjimet e telekomunikimeve të disa liderëve botërorë. Në aspektin global, shqetësim të madh ka shkaktuar, për shembull, publikimi i të dhënave personale të disa liderëve botërorë dhe i të dhënave tjera të klasifikuara. Shkelja e së drejtës së privatësisë ka arritur kulmin në faktin që viktima të saj nuk janë vetëm qytetarët e thjeshtë, por edhe liderë botërorë, të cilët kanë fuqi politike dhe juridike. Për të mos ekzistuar ndonjë lajthitje, sot ekzistojnë shumë çështje të diskutueshme lidhur me shfrytëzimin e video-incizimeve. Te shumica e shteteve video-incizimet mund të përdoren në proceset gjyqësore si prova materiale dhe është i qartë ligji se kur dhe në cilat kushte mund të bëhen incizimet me video-kamera. Asnjë ligj nuk lejon hyrjen e kundërligjshme në pronën private me video-kamerë ose regjistrues. Me pronë private, konsiderohet çdo hapësirë ku individi e ka pushtetin faktik apo të drejtën e shfrytëzimit, madje edhe dhoma e hotelit pa marrë parasysh shtrirjen kohore. Në shumë raste, video-

incizimet janë të lejuara në vendet publike, në rastet zyrtare, por jo incizimet e fshehura për qëllime private (Salihu & Zhitia & Hasani, 2014: 562).

Fokus primar tek kjo vepër penale është ruajtja e integritetit personal, e jetës private dhe e të drejtave personale të individit. Kështu, ligjvënësi me këtë normë juridike i sanksionon veprimet e fotografimit dhe incizimet e paautorizuara, që cenojnë integritetin, jetën private dhe të drejtat personale.

Figura e veprës penale "Fotografimi dhe incizime tjera të paautorizuara" - Sipas nenit 205 të Kodit Penal të Kosovës, përcaktohen si veprim i kundërligjshëm që përbën vepër penale: fotografimi, incizimi filmik, incizimi me video ose ndonjë incizim tjetër i paautorizuar i personit tjetër në banesën e tij personale ose në ndonjë vend tjetër, ku personi ka pritje të arsyeshme për privatësi, veprime këto mënyrë që cenojnë thellësisht privatësinë e tjetrit.

Me këtë normë juridike janë parashikuar dy forma të kësaj vepre penale: fotografimi, incizimi filmik, incizimi me video ose ndonjë incizim tjetër; dhe mundësimi i personit tjetër që të njihet me ato që janë fotografuar apo incizuar pa autorizim.

Veprimi i kryerjes tek kjo vepër penale ka të bëjë me fotografimin e personit tjetër me aparat fotografik, me kamera ose me çdo aparat tjetër bashkëkohor, dhe, pastaj, bërja e fotografive në mënyrat më të reja tekniko-teknologjike, të cilat tani, me zhvillimin e kibernetikës, janë të shumta.

Veprim tjetër alternativ, me të cilin kryhet kjo vepër penale, është incizimi filmik, që bëhet me kamera, dhe, pastaj, shiriti celuloid zbërthehet dhe mund të riprodhohet e tërë ngjarja e incizuar e personit apo e personave tjerë. Po ashtu kemi edhe

një veprimi tjetër të kryerjes së kësaj vepre penale: incizimin me video-kamera të llojeve të ndryshme, që tani janë të shumta.

Objekt i sulmit i kësaj vepre penale është personi tjetër, respektivisht, personi që fotografohet apo incizohet me aparate të llojeve të ndryshme. Për të ekzistuar kjo vepër penale duhet që fotografimi apo incizimi të jenë bërë në banesën e tij personale, pa pëlqimin e tij. Me banesën private kuptohet çdo vend ku subjekti ka qëndrimin e përkohshëm apo të përhershëm. Çdo vend (oborr, kopsht, shtëpi, madje, edhe dhomë hoteli, ku subjekti pasiv ka qëndrim të përkohshëm ose të përhershëm). Fotografimi, incizimi në vendet publike, në veprimtari zyrtare, në tubime shkencore e të tjera të ngjashme, janë të lejuar edhe pa pëlqimin e personit ndaj të cilit ndërmerren veprimet e kryerjes së kësaj vepre penale.

Edhe tek kjo vepër penale kundërligjshmëria mund të përjashtohet kur fotografimi, incizimi bëhen në bazë të ligjit dhe të procedurës së parashikuar me ligj apo me autorizimin e personit që i lejon këto veprime. Autorizimi duhet të jepet me vetëdije dhe me dashje. Kundërligjshmëria nuk përjashtohet, nëse autorizimi ka rrjedhur nga një i mitur apo nga personi që nuk ka pasur aftësi të logjikojë për pasojën e kësaj vepre penale.

Element tjetër i kësaj vepre penale është pasoja e saj që ka të bëjë me cenimin (ndërhyrjen) thellësisht të jetës private të personit që incizohet apo fotografohet. Se sa thellësisht është cenuar jeta private, këtë e vërteton gjykata për secilin rast konkret.

Kjo formë e veprës penale kryhet vetëm me dashje të drejtpërdrejtë të autorit. Ajo konsiderohet e kryer në momentin kur fotografia apo incizimi është bartur në materialin riprodhues.

Paragrafi 2 konsideron vepër penale shfaqjen apo dhënien personit të tretë të qasjes në fotografinë, në filmin, në videokasetën apo në ndonjë incizim tjetër të marrë në shkelje të paragrafit të këtij neni. Me dhënie të qasjes kuptohet çdo mënyrë e mundësimit të njohjes me materialet e riprodhuara (fotografi, incizime, filmime ose video), si, për shembull, tregimi i filmit përmes projektorit, i fotografisë, shitja ose shpërndarja e fotografive apo incizimeve përmes mjeteve elektronike, shtypit, kompjuterëve ose sms-ve etj. (Kodi Penal i Kosovës, Neni 205).

Vepra penale e kësaj forme kryhet me faktin kur fotografia ose incizimi filmik apo video- incizimi i është mundësuar personit tjetër për ta parë. Nuk kërkohet të dihet motivi i atij që kryen veprën, por nëse dihet motivi, kjo mund të ndikojë në masën e dënimit. Nëse janë bërë shumë fotografi apo shumë incizime vetëm nga një person, kemi vetëm një vepër penale.

Autori i kësaj vepre penale mund të jetë çdo person. Vepra kryhet me dashje, çka përfshin vetëdijen për pasojën e veprës penale dhe se fotografimi, incizimi pa autorizim në qëndrimin privat të personit tjetër është i sanksionuar.

Paragrafi 3 i këtij neni përmban format kualifikuese në rastet kur kjo vepër penale kryhet nga personi zyrtar gjatë ushtrimit të detyrës zyrtare bëhet e kualifikuar dhe për këtë dënimi penal me burgim ashpërsohet.

Paragrafi 4 përcakton se nuk ka përgjegjësi penale, nëse fotografimi ose incizimi bëhet me qëllim për të zbuluar veprën penale dhe autorët e saj ose për t'i evidencuar si dëshmi në polici, në prokurori ose në gjykatë dhe nëse fotografitë dhe incizimet u dorëzohen këtyre organeve. Ndërsa në paragrafin e 5-të të këtij neni është parashikuar konfiskimi i pajisjeve të përdorura për kryerjen e veprës penale.

Rast nga praktika gjyqësore e Gjykatës Europiane të të Drejtave të Njeriut

Në çështjen *Mitkus kundër Letonisë*, shtetasi i Letonisë ishte ankuar se redaksia e një gazete në një artikull të saj kishte zbuluar informacionin në lidhje me infeksionin e tij me HIV dhe kishte publikuar foton e tij. Në këtë rast, GJEDNJ kishte konstatuar se shtetasit letonez i është shkelur e drejtat e tij sipas Nenit 8 (E drejta për respektimin e jetës private) etj. (*Mitkus kundër Letonisë, aplikimi numër 7259/03*).

Në çështjen *Peck kundër Mbretërisë së Bashkuar (kërkesa numër 44647/98)*, GJEDNJ kishte ardhur në përfundim se, ndërsa z. Peck ecte i vetëm nëpër rrugët e qytetit me një thikë kuzhine në dorë dhe tentoi të vriste veten duke prerë damarët e dorës, ai nuk kishte vënë re se ishte filmuar nga kamera e një televizioni me rrjet të mbyllur (TVM), e instaluar nga Këshilli Bashkiak i Brentwood-it. Fotografitë e z. Peck, ku fytyra e z. Peck nuk ishte mbuluar fare, ishin shpërndarë në disa revista dhe televizione. Në këtë rast Gjykata vuri në dukje se, pasi filmimet e TVM iu dhanë mediave, në transmetimin e tyre veprimet e z. Peck nuk mund të shiheshin më si sjellje të një kalimtari të zakonshëm, as nuk kishim të bënim me një regjistrimi për arsye sigurie. Ajo konstatoi se ato filmime përbënin një shkelje serioze të së drejtës së kërkuesit për respektimin e jetës së tij private (*Peck kundër Mbretërisë së Bashkuar, kërkesa numër 44647/98, faqe:508*).

Një çështje tjetër mjaft interesante që pasuron praktikën gjyqësore lidhur me nenin 8 të Konventës Europiane për të Drejtat e Njeriut është edhe çështja *Haldimann dhe të tjerë kundër Zvicrës (Kërkesë no 21830/09)*, e cila u fillua me kërkesën no. 21830/09, drejtuar kundër Konfederatës së Zvicrës, nga katër shtetas: Ulrich Mathias Haldimann (kërkuesi i parë), Hansjörg Utz (kërkuesi i dytë), Monika Annemarie Balmer (kërkuesja e tretë) dhe Fiona Ruth Strebel (kërkuesja e katërt). Kërkuesja e tretë,

redaktore, përgatiti një emision mbi praktikat në fushën e shitjeve të produkteve të sigurimit të jetës. Ajo ra dakord me redaktorin përgjegjës për emisionin (kërkuesi i dytë) dhe me kryeredaktorin e SF DRS (kërkuesi i parë) të regjistronte me kamera të fshehtë bisedat midis klientëve dhe agjentëve, për të provuar mangësitë e këtyre të fundit. Ai vendosi t'i regjistronte bisedat në një apartament privat, pastaj t'i komentonte nga një specialist i sigurimeve (*Haldimann dhe të tjerë kundër Zvicrës*).

Kërkuesja e katërt, gazetare e SF DRS, ra dakord për një bisedë me agjentin e sigurimeve të ndërmarrjes X, bisedë që u zhvillua në 26 shkurt 2003. Ajo pretendoi se ishte një kliente që interesohej për nënshkrimin e një kontrate për sigurimin e jetës. Në dhomën ku do të bëhej biseda u instaluan dy kamera të fshehta audio-vizuale, që e transmetuan regjistrimin e bisedës në një dhomë ngjitur, ku ishte kërkuesja e tretë dhe specialisti i sigurimeve. Në këtë dhomë gjendeshin edhe një kameraman dhe një teknike, të ngarkuar për të regjistruar vlerësimin e bisedës nga eksperti.

Më pas, kërkuesi i parë dhe i dytë vendosën ta transmetojnë pjesërisht bisedën e regjistruar në një nga emisionet e ardhshme të "Kassensturz". Në fakt, kërkuesit e mbuluan fytyrën e agjentit, në mënyrë të tillë që vetëm ngjyra e flokëve dhe e fytyrës si dhe veshjet mund të dalloheshin ende pas këtij transformimi të figurës së pikselizuar. Edhe zëri i tij ishte ndryshuar. Në rastin e çështjes, Gjykata konstaton se kërkuesit kanë regjistruar një bisedë që përmban imazhe dhe zërin e një gjoja negocimi midis agjentit të sigurimeve dhe gazetares. Për mendimin e Gjykatës, regjistrimi në vetvete u ka shkaktuar vetëm një cenim të kufizuar interesave të agjentit të sigurimeve, pasi vetëm një rreth i kufizuar personash kanë pasur akses për ta dëgjuar regjistrimin, çka e pranon edhe qeveria (*Haldimann dhe të tjerë kundër Zvicrës*).

Shkelja e urdhrave për masat e fshehura ose teknike të vëzhgimit ose të hetimit (Neni 206)

Vepra penale "*Shkelja e urdhrave për masat e fshehura ose teknike të vëzhgimit ose të hetimit*" është e parashikuar në kuadër të veprave penale kundër lirive dhe të drejtave të njeriut. (Kodi Penal i Kosovës, Kapitulli XVII).

Figura e veprës penale "Shkelja e urdhrave për masat e fshehura ose teknike të vëzhgimit ose të hetimit - Sipas nenit 206 të Kodit Penal të Kosovës, përcaktohen si veprim i kundërligjshëm që përbën vepër penale: shkelja e urdhrave për masat e fshehura ose teknike të vëzhgimit ose të hetimit nga e zyrtari policor i autorizuar që zbaton një urdhër gjyqësor ose prokurorial për masat e fshehura ose teknike të vëzhgimit ose të hetimit, në shkelje të ligjit. Këtë vepër penale e kryen edhe personi i cili zbulon informatën që do të dëmtojë efikasitetin e zbatimit të një urdhri për masat e fshehura ose teknike të vëzhgimit ose të hetimit.

Autor i kësaj vepre penale është edhe personi përgjegjës për operimin e telekomunikimeve, të rrjeteve kompjuterike ose të shërbimeve postare, apo punonjësi i një institucioni financiar, që nuk ndërmerr veprimet e duhura për të lehtësuar zbatimin e urdhrit për përgjimin e telekomunikimeve, për përgjimin e komunikimeve me anë të rrjetit kompjuterik, kontrollin e dërgesave postare, regjistrimin e thirrjeve telefonike ose zbulimin e të dhënave financiare.

Ndërlidhja e kësaj vepre penale me sigurinë e informacionit konsiston te fakti i cenimit të sigurisë së informacionit, respektivisht, nxjerrja e informacionit jashtë rrethit të personave që duhet të dinë për të.

Veprimet me të cilat mund të kryhet kjo vepër penale janë të shumta, andaj ligjvënësi edhe nuk ka pasur mundësi t'i përcaktojë të gjitha ato veprime të mundshme. Për këtë, thuhet se zbatimi i një urdhri gjyqësor në kundërshtim me nenet përkatëse të Kodit të Procedurës Penale, pra, çdo veprim që cenon dispozitat përkatëse të këtij Kodi për zbatimin e masave të fshehta ose teknike të vëzhgimit është veprim me të cilin kryhet kjo vepër penale (Salihu & Zhitia & Hasani, 2014: 565). Këtë vepër penale mund ta kryejë edhe personi tjetër që e nxjerr informacionin me të cilin dëmton efikasitetin e zbatimit të urdhrit për masat e fshehta ose teknike të vëzhgimit ose të hetimit. Këtë formë të veprës penale mund ta kryejë secili person që ka qasje ose ka arritur deri tek informacioni me të cilin do të dëmtojë efikasitetin e zbatimit të urdhrit. Veprimi i kryerjes së kësaj vepre penale në këtë rast është nxjerrja e informacionit, domethënë, zbulimi ose bërja me dije personit tjetër për informatat që gjenden në urdhrin lidhur me masat e fshehta ose teknike të vëzhgimit ose të hetimit.

Zakonisht personat potencialë për kryerjen e kësaj vepre penale janë: gjyqtari, prokurori, polici, mbajtësi i procesverbalit, personeli i gjykatave, i prokurorisë, punëtori i post-telekomunikimit dhe çdo person që, në një mënyrë apo tjetër, ka arritur deri tek informacioni (Salihu & Zhitia & Hasani, 2014: 566).

Komunikimi i paautorizuar i sekretit tregtar (Neni 292)

Sot i kushtohet kujdes i veçantë sekretit të afarizmit dhe sekretit tregtar në marrëdhëniet afariste ndërkombëtare e, posaçërisht, në format e pronësisë industriale.

Nevoja e mbrojtjes së tyre shprehet me rastin e lidhjes së llojeve të reja të kontratave: "joint venture, leasing, factoring, franchising" (Salihu & Zhitia & Hasani, 2014: 809).

Në kontrata shtohen dispozita të posaçme lidhur me sekretin e afarizmit apo të tregtisë, me qëllim shmangien e pasojave të dëmshme që shkakton zbulimi apo kumtimi i sekretit. Vepra penale "Komunikimi i paautorizuar i sekretit tregtar" është e parashikuar në kuadër të veprave penale kundër ekonomisë, në Kodin Penal të Kosovës, Kapitulli XXV.

Shprehja "sekret afarist" nënkupton të dhënat që janë cilësuar si të tilla me ligj ose me dispozita të organizatës së biznesit ose të personit juridik dhe që paraqesin sekretin e prodhuesit, rezultatin e punës hulumtuese ose të dizajnimit, të dhëna financiare, afariste, shkencore, teknike, ekonomike apo inxhinierike, përfshirë plane, formula, dizajne, prototipe, metoda, teknika, procese, procedura, programe, kode ose të dhëna tjera, për të cilat pronari ka ndërmarrë masa të arsyeshme për t'i mbajtur sekret dhe zbulimi i tyre personit të paautorizuar mund të ketë efekte të dëmshme për interesat ekonomike të organizatës së biznesit apo të personit juridik (Kodi Penal i Kosovës, Neni 292).

Shprehja "sekret tregtar" nënkupton të dhënat që janë cilësuar si të tilla me ligj ose me dispozita të organizatës së biznesit ose të personit juridik dhe të cilat paraqesin sekretin e prodhuesit, rezultatin e punës hulumtuese ose të dizajnimit, të dhëna financiare, afariste, shkencore, teknike, ekonomike apo inxhinierike, përfshirë plane, formula, prototipe, metoda, teknika, procese, procedura, programe, kode ose të dhëna tjera për të cilat pronari ka ndërmarrë masa të arsyeshme për t'i mbajtur sekret dhe zbulimi i tyre personit të paautorizuar mund të ketë efekte të dëmshme për interesat

ekonomike të organizatës së biznesit apo të personit juridik. (Kodi Penal i Kosovës, Neni 292).

Këtë vepër e kryen kushdo që në shkelje të detyrave të tij për ruajtjen e sekreteve afariste apo tregtare, ia kumton apo ia përcjell personit tjetër të dhënat lidhur me sekretet afariste apo tregtare ose në ndonjë mënyrë tjetër ia mundëson ndonjë personi të paautorizuar qasjen në të dhënat e tilla ose mbledh të dhëna të tilla, me qëllim që t'ia përcjellë personit të paautorizuar. (Kodi Penal i Kosovës, Neni 292).

Figura e veprës penale "Komunikimi i paautorizuar i sekretit tregtar" - Sipas nenit 292 të Kodit Penal të Kosovës, përcaktohen si veprim i kundërligjshëm që përbën vepër penale: kumtimi i sekretit të afarizmit apo atij tregtar, përcjellja e sekretit personit tjetër dhe bërja e mundshme në qasjen a mbledhjen e të dhënave të tilla personit tjetër, me qëllim që t'ia dorëzojë personit të paautorizuar. Kumtimi i sekretit realizohet me veprimin me të cilin njoftohet personi tjetër me përmbajtjen e shënimeve. Kumtimi mund të bëhet me gojë, me shkrim apo në ndonjë mënyrë tjetër të përshtatshme.

Përcjellja e të dhënave ka të bëjë me dhënien ose me krijimin e mundësive për të arritur në posedimin e të dhënave, që paraqesin sekret, personit të paautorizuar. Përcjellja, kryesisht ka të bëjë me dorëzimin e dokumentacionit sekret të afarizmit apo të sekretit tregtar (Salihu & Zhitia & Hasani, 2014: 811).

Veprimi me të cilin kryhet kjo vepër penale konsiston në sigurimin e kundërligjshëm të të dhënave që ruhen si sekret tregtar. Depërtimi te këto të dhëna realizohet në disa mënyra, si: modifikimet dhe ndërhyrjet e paautorizuara në të dhënat kompjuterike, hapja e kasafortave, ku ruhen të dhënat, përgjimi i bisedave telefonike etj.

Rrethana rënduese tek kjo vepër penale ekziston kur autori, me qëllim të përdorimit në mënyrë të paautorizuar, arrin në mënyrë të kundërligjshme te të dhënat që

ruhen si sekrete të afarizmit apo të tregtisë dhe që janë të një rëndësie të veçantë; kur të dhënat e këtilla i përcillen personit tjetër, me qëllim që ky t'i nxjerrë ato jashtë territorit të Republikës së Kosovës. Rëndësia e posaçme e të dhënave duhet të vërtetohet për secilin rast konkret, varësisht nga natyra e tyre, nga pasoja që është shkaktuar apo ku ka mundur të shkaktohet me kumtimin ose me përdorimin e tyre dhe të rrethanave tjera. Këto të dhëna shënohen si "sekret", "sekret i besueshëm" dhe "të dhëna sekrete të rëndësisë së veçantë" (Salihu & Zhitia & Hasani, 2014: 811).

Rast nga praktika gjyqësore

Nuk ekziston vepra penale, kumtimi i paautorizuar i sekretit të punës kur autori, si operator teknolog i makinave përpunuese të informacionit, e ka njohur teknologun privat të makinave elektrike në ndërmarrjen e vet dhe, mbi këtë bazë, ai ka ndërtuar një tavolinë montuese dhe disa vegla për makina elektrike; kur të dhënat, me të cilat i pandehuri e ka njoftuar prodhuesin privat, nuk janë ruajtur sipas dispozitave të ndërmarrjes si sekret i punës, që cilat konsiderohen si rezultat hulumtues i punës së konstruksionit. I pandehuri e ka ndërtuar makinën montuese dhe veglat bazë të zgjedhjeve të veta, që i ka arritur mbi bazën e njohurive të veta si ekspert dhe me rastin e punimit nuk shërbyer me të arriturat hulumtuese të ndërmarrjes së vet. (*Aktgjykimi i Gjykatës së Qarkut në Bjellovar KZ.nr. 328/91, dt. 29.05.1991*)

Shmangia e masave teknologjike (Neni 297)

Kjo vepër penale më parë nuk ka qenë e parashikuar në sistemin tonë penal. Në ligjin për të drejtat e autorit parashikohen një sërë masash mbrojtëse të teknologjisë apo menaxhimi i të dhënave në mënyrë elektronike. Kjo vepër penale konsiston në shtrirjen e mbrojtjes penale të masave teknologjike ose të heqjes apo ndryshimit të të drejtave elektronike për menaxhimin e të dhënave, sikurse parashihet në dispozitat e ligjit për të drejtat e autorit dhe të drejtave të tjera të përafërta (Salihu & Zhitia & Hasani, 2014: 825).

Vepra penale "*Shmangia e masave teknologjike*" është e parashikuar në kuadër të kapitullit të veprave penale kundër ekonomisë në Kodin Penal të Kosovës, Kapitulli XXV. Këtë vepër e kryen kushdo që kryen vepër të shmangies së ndonjë prej masave efektive mbrojtëse të teknologjisë ose heqjen apo ndryshimin e të drejtave elektronike për menaxhimin e të dhënave, siç parashihet në dispozitat e Ligjit për të drejtat e autorit dhe të drejtat e tjera të përafërta (Kodi Penal i Kosovës, Neni 297).

Figura e veprës penale "Shmangia e masave teknologjike" - Sipas nenit 297 të Kodit Penal të Kosovës, përcaktohen si veprim i kundërligjshëm që përbën vepër penale: shmangia e masave teknologjike të parapara për funksionimin e rregullt të pajisjeve të telekomunikimeve, të pajisjeve të teknologjisë informatike, të pajisjeve që janë të vendosura në ndonjë ndërtesë tjetër të rëndësishme, për sigurinë e informacionit, siç janë dhomat e të dhënave apo siç quhen ndryshe Data Center.

Në dhomat e të dhënave kërkohet që çdo ditë të realizohet kontrollimi i masave teknologjike dhe një mbikëqyrje konstante, për të garantuar funksionim normal të të gjitha pajisjeve. Kjo mundëson që shërbimet mbështetëse, si ato të ngrohjes, të

ventilimit dhe të kondicionimit, të energjisë, të ujit dhe shërbimet tjera, të kenë një funksionim të rregullt dhe të sigurt. Secili prej këtyre shërbimeve duhet të menaxhohet në mënyrë të duhur, për të parandaluar dëmtimin e informacionit dhe sistemet e informacionit.

Nga ana objektive, vepra penale kryhet me shmangien e masave teknologjike të parapara për funksionimin e rregullt të pajisjeve të telekomunikimeve, të pajisjeve të teknologjisë informatike apo të pajisjeve të tilla të vendosura në ndonjë ndërtesë tjetër.

Pasoja e veprës penale është përcaktuar me vetë veprimin e kryerjes së kësaj vepre penale, që është shmangia e masave teknologjike të parapara për funksionimin e rregullt të pajisjeve.

Subjekt i krimit është çdo person i cili me veprimet apo mosveprimet e tij ka bërë shmangien e masave efektive mbrojtëse të teknologjisë.

Nga ana subjektive, krimi kryhet me dashje të drejtpërdrejtë për të kryer veprimet e parashikuara me këtë vepër penale.

Elementet që ndërlidhen me sigurinë e informacionit tek kjo vepër penale kanë të bëjnë me menaxhimin jo të duhur të masave teknologjike në vendet dhe në objektet ku ndodhen pajisjet e teknologjisë informatike në të cilat ruhen informacionet e klasifikuara. Edhe moskontrollimi i temperaturës, i filtrimit, i lagështisë dhe i energjisë elektrike shkakton pasoja, sepse temperatura dhe sistemet kompjuterike të filtrimit janë elektronike dhe, si të tilla, mund të dëmtohen nga temperatura ekstreme. Temperaturat e ulëta mund të dëmtojnë pajisjet teknologjike: kompjuterët, harduerët kompjuterikë; nivelet e larta të lagështisë krijojnë probleme, nivelet e ulëta të lagështisë mund të rrisin sasinë e elektricitetit statik në mjedis dhe të gjitha këto së bashku shkaktojnë probleme dhe dëme.

Hyrja në sistemet kompjuterike (Neni 339)

Vepra penale "*Hyrja në sistemet kompjuterike*" është e parashikuar në kuadër të kapitullit të veprave penale kundër pasurisë në (Kodin Penal të Kosovës, Kapitulli XXVII. Kjo vepër penale paraqet formën e të ashtuquajturit kriminalitet kompjuterik. Me këtë inkriminim ruhet dhe sigurohet shfrytëzimi i papenguar i të dhënave adekuate kompjuterike apo i programeve.

Kompjuteri dhe shfrytëzimi i tij në shumë lëmenj të jetës përbën një ndër zbulimet më të mëdha në dy dekadat e fundit të shekullit XX. Përfitimet dhe favoret e përdorimit të tij në informatikë, në ekonomi, në shkencë etj., janë shumë të mëdha për çdo individ dhe për mbarë njerëzimin. Mirëpo, me keqpërdorimin e tij mund të kryhen edhe shumë vepra penale, madje, shumë të rënda. (Salihu & Zhitia & Hasani, 2014: 811). Sipas natyrës së tyre, disa nga veprat penale që bëjnë pjesë në kriminalitetin kompjuterik, për nga elementet e tyre, janë të përafërta me veprën penale të dëmtimit të pasurisë së huaj dhe me veprën penale të mashtrimit, nëse kryhen me qëllim të njëjtë.

Figura e veprës penale "Hyrja në sistemet kompjuterike" - Sipas nenit 339 të Kodit Penal të Kosovës, përcaktohen si veprim i kundërligjshëm që përbën vepër penale: ndryshimi, publikimi, shlyerja, asgjësimi apo shkatërrimi i paautorizuar i të dhënave kompjuterike, i programeve kompjuterike apo hyrja e paautorizuar, në çfarëdo mënyre tjetër, në sistemin kompjuterik, me qëllim që t'i sjellë vetes ose personit tjetër dobi pasurore të paligjshme apo t'i shkaktojë dëme personit tjetër.

Veprimi i kryerjes së kësaj vepre penale është përcaktuar në mënyrë alternative dhe kjo konsumohet me ndërmarrjen e cilitdo nga veprimet e përshkruara më lart. Në esencë, bëhet fjalë për veprime, qëllimi i të cilave është pamundësimi i shfrytëzimit të

papenguar të të dhënave dhe të programeve kompjuterike. Parimisht, veprimi ndërmerret fshehtas, për shembull, dërgimi i të ashtuquajturve viruse kompjuterike dhe të ngjashme, por mund të kryhet edhe me ndërrimin e të dhënave dhe të programeve kompjuterike, përkatësisht, me asgjësimin e tyre, për shembull, me shlyerjen e të dhënave. Me këtë vepër janë inkriminuar publikimi i paautorizuar i të dhënave dhe i programeve kompjuterike. Kjo vepër penale konsumohet edhe kur të dhënat dhe programet kompjuterike janë të mbrojtura, edhe kur ato nuk janë të mbrojtura. (Salihu & Zhitia & Hasani, 2014: 811).

Qasja e paautorizuar e të dhënave "i referohet një skenari në të cilin një person qaset në të dhëna në mënyrë të paautorizuar apo pa leje për qasje. Një skenar i zakonshëm është kur dikush që ka qasje të ligjshme të të dhënave zgjedh, ose kur personi qaset në të dhënat në të cilat ai nuk është i autorizuar për të hyrë, ose kur ai i përdor këto të dhënat në një mënyrë tjetër nga ajo që ka qenë i autorizuar. (Eastom & Taylor, 2011: 12).

Për të ekzistuar kjo vepër penale, duhet që veprimet e përshkruara më lart të jenë ndërmarrë pa pasur autorizim për to. Veprimi i kundërligjshëm është element konstituiv i veprës; përpos kësaj, është e nevojshme që veprimet të jenë ndërmarrë me qëllim të posaçëm: përfitimi për vete apo për tjetrin të dobisë pasurore të kundërligjshme ose dëmtimi i tjetrit.

Dënimi penal me burgim ashpërsohet kur bëhet fjalë për formën e rëndë të kësaj vepre penale, që është e parashikuar në paragrafin 2, i cili konsideron vepër penale hyrjen e paautorizuar në sistemin kompjuterik dhe nga kjo autori realizon dobi pasurore ose tjetrit i shkakton dëm material që tejkalon 10.000 €.

Te qasja apo tek hyrja e paautorizuar në sisteme kompjuterike, karakteristikë e përbashkët është se autori i krimit nuk është i autorizuar për t'u qasur në të dhënat as për t'i përdorur të dhënat në mënyrën në të cilën ai ose ajo është duke i përdorur ato. (Eastom & Taylor, 2011:19).

Objekt i kësaj vepre penale janë marrëdhëniet juridike për të siguruar funksionimin e sistemit kompjuterik nga ndërhyrjet, të mbrojtura posaçërisht nga legjislacioni penal.

Nga ana objektive, vepra penale kryhet me ndërhyrje në sistemin kompjuterik nëpërmjet krijimit të pengesave serioze dhe të paautorizuara, si: futjes, dëmtimit, shtrembërimit, ndryshimit apo fshirjes së të dhënave. (Elezi, 2009:560).

Pasojat janë mosfunksionimi i sistemit kompjuterik nga hyrjet e paautorizuara.

Subjekt i krimit është çdo person që kryen veprimet e parashikuara me këtë vepër penale, person që është i përgjegjshëm dhe ka mbushur moshën për përgjegjësi penale.

Nga ana subjektive, krimi kryhet me dashje, si rregull me dashje të drejtpërdrejtë, për të kryer veprimet e parashikuara me këtë vepër penale.

Rast nga praktika gjyqësore e Gjykatës Europiane të të Drejtave të Njeriut

Praktika gjyqësore çështja *Copland kundër Mbretërisë së Bashkuar,* filloi në vijim të një ankese (nr. 62617/00) nga Znj. Lynette Copland (kërkuesja), kundër Mbretërisë së Bashkuar të Britanisë së Madhe dhe Irlandës Veriore. Në vitin 1991, kërkuesja ishte e punësuar në Kolegjin Carmathenshire (Kolegji). Kolegji është një organ statutor i administruar nga shteti me pushtet procesues sipas seksioneve 18 dhe 19 të Ligjit për Arsimin e Vazhdueshëm dhe të Lartë të vitit 1992 në lidhje me ofrimin e

arsimit të vazhdueshëm dhe të lartë (*Copland kundër Mbretërisë së Bashkuar, kërkesa nr. 62617/00*).

Në vitin 1995 kërkuesja u bë asistente personale e drejtorit të Kolegjit (DK) dhe prej fundit të atij viti asaj iu kërkua të punonte afër drejtorit të ri kryesor (DK) të sapoemëruar.

Rreth muajit korrik të vitit 1998, gjatë periudhës së pushimit vjetor, kërkuesja vizitoi një kampus tjetër të Kolegjit me një drejtor mashkull. Më pas, ajo mori vesh që DK kishte kontaktuar kampusin për të pyetur lidhur me vizitën e saj dhe kuptoi që ai po sugjeronte një raport të pahijshëm mes saj dhe drejtorit (*Copland kundër Mbretërisë së Bashkuar, kërkesa nr. 62617/00*).

Gjatë punësimit të saj, telefoni, e-maili dhe përdorimi i internetit nga kërkuesja iu nënshtruan monitorimit, me nxitjen e DK. Sipas qeverisë, ky monitorim u zhvillua në mënyrë që të sigurohej nëse kërkuesja po i përdorte ambientet e Kolegjit më tepër për qëllime personale. Qeveria deklaroi se monitorimi i përdorimit të telefonit kishte të bënte me analizën nga Kolegji të faturave telefonike, ku tregoheshin numrat e thirrur, datat dhe ora e thirrjeve, si dhe kohëzgjatja dhe kostoja e tyre. Gjithashtu, kërkuesja besonte se kishte pasur regjistrime të hollësishme dhe të plota të kohëzgjatjes së thirrjeve, numrit të thirrjeve të bëra dhe të pranuara, si dhe numrat e telefonave të personave që e kishin thirrur atë. Ajo deklaroi që, të paktën, në një rast, DK kishte marrë vesh emrin e një individi me të cilin ajo kishte pasur telefonata hyrëse dhe dalëse. Qeveria parashtroi që monitorimi i përdorimit të telefonit ndodhi për një periudhë disa-mujore deri rreth datës 22 nëntor 1999. Kërkuesja deklaroi që përdorimi i telefonit të saj u monitorua për një periudhë prej rreth tetëmbëdhjetë muajsh, deri në nëntor 1999. Edhe përdorimi i internetit nga kërkuesja u monitorua nga DK. Qeveria pranoi që ky

monitorim kishte të bënte me analizimin e faqeve të internetit të vizituara, kohët, datat e vizitave në faqet e internetit dhe kohëzgjatja e secilës vizitë, dhe që ky monitorim ndodhi nga tetori deri në nëntor 1999. Kërkuesja nuk komentoi mbi mënyrën në të cilën ishte monitoruar përdorimi i internetit prej saj, por deklaroi se ai kishte ndodhur gjatë një periudhe më të gjatë kohore, sesa periudha e pranuar nga qeveria.

Sipas praktikës gjyqësore të Gjykatës, thirrjet telefonike nga ambientet e punës mbulohen *prima facie* nga nocionet e "jetës private" dhe "korrespondencës" për qëllime të nenit 8 § 1 (shih: Halford, cituar lart, § 44, dhe Amann kundër Zvicrës [GC], nr. 27798/95, § 43, KEDNJ 2000-II). Logjikisht, rrjedh që emailet e dërguar nga puna duhet të mbrohen, po ashtu, nga neni 8, ashtu siç duhen mbrojtur edhe informacionet e përftuara nga monitorimi i përdorimit personal të internetit.

Në rastin konkret, kërkueses nuk i ishte dhënë paralajmërim që thirrjet e saj do të mund të monitoroheshin, prandaj ajo, me të drejtë, priste të kishte privatësi në thirrjet telefonike që bënte nga telefoni i punës (shih: Halford, § 45). E njëjta pritje duhet zbatuar edhe lidhur me përdorimin nga kërkuesja të emailit dhe të internetit. Për këto arsye, gjykata njëzëri vendos që ka pasur shkelje të nenit 8 të Konventës (*Copland kundër Mbretërisë së Bashkuar, kërkesa nr. 62617/00*).

Asgjësimi, dëmtimi ose heqja e instalimeve publike (Neni 366)

Vepra penale "*Asgjësimi, dëmtimi ose heqja e instalimeve publike"* është e parashikuar në kuadër të kapitullit të veprave penale kundër sigurisë së përgjithshme të njerëzve dhe pasurisë në Kodin Penal të Kosovës, Kapitulli XXIX.

Figura e veprës penale "Asgjësimi, dëmtimi ose heqja e instalimeve publike" - Sipas nenit 366 të Kodit Penal të Kosovës, konsiderohen vepër penale veprimet me të cilat rrezikohen rendi kushtetues apo siguria e Republikës së Kosovës, si: djegia ose shkatërrimi apo dëmtimi në çfarëdo mënyre i zonës industriale, i zonës bujqësore ose i ndonjë zone tjetër ekonomike, i sistemit të trafikut, i lidhjeve të telekomunikimeve, i pajisjeve publike të ujit, të ngrohjes, të gazit apo të energjisë, i digave, i depove apo i ndonjë ndërtese tjetër të rëndësishme për sigurinë, për furnizimin e qytetarëve, për ekonominë apo për funksionimin e shërbimeve publike.

Format e ndryshme të kryerjes së kësaj vepre penale dallojnë, jo vetëm në anën objektive të kryerjes së saj, por edhe nga lloji dhe masa e dënimit që ligji parashikon për secilën formë të tyre. Dënimi penal me burgim ashpërsohet, nëse veprimet e përmendura më lart, me të cilat rrezikohet rendi kushtetues apo siguria e Republikës së Kosovës, rezultojnë me dëm substancial pasuror apo material, me lëndim të rëndë trupor apo me vdekje të një apo më shumë personave.

Elementet që ndërlidhen me sigurinë e informacionit te kjo vepër penale kanë të bëjnë me rendin kushtetues apo me sigurinë e Republikës së Kosovës, me shkatërrimin e lidhjeve të telekomunikimeve, të ndonjë ndërtese tjetër të rëndësishme për sigurinë e informacionit, siç janë dhomat e të dhënave. Edhe moskontrollimi i temperaturës, i filtrimit, i lagështisë dhe i energjisë elektrike statike, shkakton pasoja, sepse temperatura dhe sistemet kompjuterike të filtrimit janë elektronike dhe, si të tilla, mund të dëmtohen nga temperaturat ekstreme.

Objekt i kësaj vepre penale janë marrëdhëniet juridike të vendosura për ruajtjen dhe mirëmbajtjen e mjeteve, të pajisjeve, të aparaturave, të sistemit të trafikut, të lidhjeve të telekomunikimeve, të pajisjeve publike të ujit, të ngrohjes, të gazit apo të

energjisë, të digave, të depove apo të ndonjë ndërtese tjetër të rëndësishme për sigurinë, për furnizimin e qytetarëve, për ekonominë apo për funksionimin e shërbimeve publike.

Nga ana objektive, vepra penale kryhet me veprime aktive të kundërligjshme, që shprehen me asgjësimin, dëmtimin ose me heqjen e instalimeve publike. Me asgjësim kuptohet shkatërrimi i tyre, nxjerrja jashtë përdorimit me anë djegieje, thyerjeje, prishjeje etj. Me dëmtim kuptohet prishja e pjesshme e mjeteve, e pajisjeve që mund të riparohen dhe të vihen përsëri në përdorim.

Subjekt i kësaj vepre penale mundë të jetë çdo person të cilit i janë besuar për ruajtje dhe administrim pajisjet dhe i cili ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm.

Nga ana subjektive, krimi kryhet me dashje të drejtpërdrejtë dhe me qëllim që të asgjësohen dhe të dëmtohen pajisjet duke dobësuar funksionimin dhe aftësinë mbrojtëse të organizatës.

Rast nga Praktika Gjyqësore e Kosovës

"Kur të akuzuarit si pronarë të ndërmarrjes "N" me rastin e gërmimit të themeleve për ndërtimin e një objekti ndërtimor nuk kanë ndërmarrë masat e duhura për mbrojtjen e instalimeve nëntokësore dhe mbrojtjen e rrjetit të ujësjellësit dhe, si pasojë e këtij lëshimi, bageristi, me rastin e gërmimit, ka dëmtuar kabllot dhe tubin e ujit, duke i shkaktuar dëm kompanisë së ujërave dhe një pjesë të qytetit për një kohë e ka lënë pa ujë dhe pa rrymë, në këtë rast nuk ka konsumuar elementet e veprës penale të parashikuar nga neni 292, par. 2, lidhur me par.1, të KPK, kryhet vetëm me veprim, ndërsa të dëmtuarit kishin abstenuar nga ndërmarrja e veprimeve që kishin për obligim t'i ndërmerrnin, d.m.th veprimet e tyre në situatën konkrete mund të vihen vetëm në

ndonjërën nga normat juridike që i sanksionon veprat penale me mosveprim, nëse janë përmbushur elementet qenësore të veprës penale konkrete. (Gjykata e Qarkut në Pejë, Ap.nr.100/2010, datë 31.10.2011 dhe aktgjykimi i Gjykatës Supreme Pkl. Nr. 5/2012, datë 21.2.2012).

Keqpërdorimi i informacionit zyrtar (Neni 423)

Përmes dispozitës së nenit 423 të Kodit Penal të Kosovës, ligjvënësi ka synuar të mbrojë dhe të ruajë informatën zyrtare nga keqpërdorimi.

Termi 'informatë zyrtare' nënkupton informatën në të cilën personi ka qasje, si rezultat i detyrës apo i punës së tij, dhe që nuk është bërë publike. (Kodi Penal i Kosovës, Neni 423).

Vepra penale e keqpërdorimit të informatës zyrtare është e parashikuar në kuadër të kapitullit për korrupsionin zyrtar dhe për veprat penale kundër detyrës zyrtare (Kodi Penal i Kosovës, Kapitulli XXXIV).

Figura e veprës penale "Keqpërdorimi i informacionit zyrtar" - Sipas nenit 423 të Kodit Penal, përcaktohet si veprim i kundërligjshëm që përbën vepër penale keqpërdorimi i informatës zyrtare nga personi zyrtar, me qëllim që të fitojë për vete apo për personin tjetër ndonjë përparësi që nuk i takon.

Dënimi penal me burgim për këtë vepër penale ashpërsohet, kur bëhet fjalë për format më të rënda të saj, që janë të parashikuara në paragrafët 2, 3 dhe 4, nëse informata zyrtare ka të bëjë me ndonjë veprim të prokurimit apo me ndonjë ankand publik dhe nëse vepra penale rezulton me dobi pasurore apo me humbje në vlerën që tejkalon pesëmijë euro dhe pesëdhjetëmijë euro.

Objekti mbrojtës i kësaj vepre penale është detyrimi i personit të caktuar për ruajtjen e informatës zyrtare, ndërsa objekti i sulmit është përmbajtja e informatës zyrtare, respektivisht, të dhënat konkrete të informatës.

Këtë vepër penale mund ta kryejë vetëm personi zyrtar, ajo kryhet vetëm me dashje, e cila përfshin edhe faktin që autori e di se ai po keqpërdor një informatë zyrtare, që nuk i është bërë e njohur publikut ende dhe se, me dhënien e kësaj informate, ai apo ajo do t'i sjellë favore apo dëm dikujt. (Salihu & Zhitia & Hasani, 2014: 1223).

Tek kjo vepër penale autori keqpërdor informatën zyrtare, me qëllim që vetes apo tjetrit t'i sjellë ndonjë përparësi. Pra, në rastin konkret bëhet fjalë për një informatë të tillë të rëndësishme për ndonjë raport juridik, në të cilën personi zyrtar ka qasje në bazë të punës a detyrës së tij dhe informata apo e dhëna nuk e ka statusin e sekretit shtetëror, por nuk është publikuar ende, dhe kjo informatë nga personi zyrtar përcillet tek persona të tjerë me qëllim të realizimit të ndonjë përparësie për vete apo për një person tjetër. (Salihu & Zhitia & Hasani, 2014: 1223).

Forma cilësuese e kësaj vepre penale konsumohet nëse informata zyrtare ka të bëjë me prokurimin apo ankandin publik, domethënë bëhet fjalë për tenderime të ndryshme, ku personi zyrtar i keqpërdor informatat, që i ka siguruar në bazë të punës apo detyrës së tij, duke ua përcjellë këto informata personave, që marrin pjesë në ankand publik apo në tender, me qëllim që t'u sjellë atyre personave përparësi, favore. (Salihu & Zhitia & Hasani, 2014: 1224).

Nëse veprën penale e kryen personi zyrtar i cili keqpërdor informatën zyrtare me qëllim që për vete apo për personin tjetër të fitojë ndonjë përparësi që nuk i takon dhe dobia pasurore apo humbja në vlerën pasurore tejkalon 50.000 euro, atëherë kjo paraqet rrethanë rënduese. (Kodi Penal i Kosovës, Neni 423).

Zbulimi i fshehtësive zyrtare (Neni 433)

Vepra penale "*Zbulimi i fshehtësive zyrtare*" është e parashikuar në kapitullin e veprave penale lidhur me korrupsionin zyrtar dhe me veprat penale kundër detyrës zyrtare (Kodi Penal i Kosovës, Kapitulli XXXIV). Nisur nga fakti se te kjo vepër penale bëhet fjalë për mbrojtjen e fshehtësisë së të dhënave të caktuara, mund të thuhet se këtu, së pari, mbrohen ato interesa që qëndrojnë pas këtyre fshehtësive, interesa që do të rrezikoheshin me cenimin e detyrës së ruajtjes së fshehtësisë; së dyti, kur këto interesa nuk janë të rëndësishme, atëherë bëhet fjalë për mbrojtjen e kësaj fshehtësie, më së shpeshti, për ruajtjen e besimit të publikut për paanshmërinë e shërbimit, që është gjithnjë parakusht për funksionimin normal të shërbimit dhe të institucionit.

Interesi i shërbimit, përkatësisht, trajtimi i fshehtë i ndonjë të dhëne apo fakti, imponojnë nevojën që të sigurohet dhe të ruhet fshehtësia e të dhënave të caktuara, të mësuara nga personi zyrtar gjatë ushtrimit të detyrës. Në të kundërtën, zbulimi apo kumtimi i tyre mund të rrezikojë kryerjen e rregullt dhe efikase të shërbimit dhe, në përgjithësi, besimin e opinionit ndaj profesionalizmit dhe funksionimit të paanshëm të shërbimeve dhe të institucioneve publike. Kjo është arsyeja për të cilën këtyre të dhënave, përpos formave të tjera mbrojtëse, u është siguruar edhe mbrojtja penalo-juridike.

Figura e veprës penale "Zbulimi i fshehtësive zyrtare" - Sipas nenit 433 të Kodit Penal të Kosovës, përcaktohen si veprim i kundërligjshëm që përbën vepër penale: kumtimi dërgimi ose, në ndonjë mënyrë tjetër, vënia në dispozicion, nga personi zyrtar, pa pasur autorizim, ose sigurimi i informatës, që përbën fshehtësi zyrtare, personit tjetër, me qëllim që t'ia përcjellë ndonjë personi të paautorizuar.

Vepra penale *"Zbulimi i fshehtësive zyrtare"* ekziston kur personi zyrtar apo personi përgjegjës, pa pasur autorizim, ia kumton, ia kalon ose, në ndonjë mënyrë tjetër, ia bën të qasshme personit tjetër të dhënat që paraqesin fshehtësi zyrtare ose i siguron të dhëna të tilla me qëllim që ato t'ia bartë personit të paautorizuar (Kodi Penal i Kosovës, Neni 433).

Kjo vepër penale kryhet nga personi zyrtar, domethënë ai është subjekt i veprës. Por autor i kësaj vepre mund të jetë edhe personi, të cilit ndërkohë i ka pushuar statusi i personit zyrtar, por ia kumton ndonjë personi tjetër të dhënat që paraqesin fshehtësi, për të cilat ai ka marrë dijeni në kohën kur e kishte statusin e personit zyrtar a të personit përgjegjës (Kodi Penal i Kosovës, Neni 433). Obligimi i ruajtjes së fshehtësisë zyrtare edhe në rastet e pushimit të statusit zyrtar të personit, parashihet edhe me Ligjin për Klasifikimin e informacioneve dhe Verifikimin e sigurisë, edhe me Ligjin nr. 2004/34, Ligji Kundër Korrupsionit, Neni 44, i cili parashikon detyrimin e ruajtjes së fshehtësisë zyrtare edhe 15 vjet pas pushimit të statusit të personit zyrtar

Tek kjo vepër penale veprimi i kryerjes është përcaktuar në mënyrë alternative si kumtim, bartje e të dhënave të tilla, që paraqesin të dhëna të fshehta, apo bërje e tyre të qasshme tjetrit në ndonjë mënyrë tjetër, si dhe sigurimi i të dhënave të tilla, me qëllim që t'i dorëzohen personit të paautorizuar, këto të dhëna duhet t'i kumtohen tjetrit. Me shprehjen "tjetrit" në kuptim të kësaj vepre penale duhet kuptuar çdo person fizik apo juridik, i cili nuk është i autorizuar as të dijë për të dhëna të tilla dhe as të mësojë përmbajtjen e tyre.

Objekt i veprimit të këtij krimi janë të dhënat e besueshme që paraqesin fshehtësi zyrtare. Fshehtësi zyrtare konsiderohen informacionet ose dokumentet e shpallura me ligj si të tilla, po ashtu, dispozita të tjera të nxjerra me vendim të organit

kompetent dhe që në bazë të ligjit konsiderohen fshehtësi zyrtare, dokumente këto, zbulimi i të cilave ka shkaktuar ose mund të shkaktojë pasoja të dëmshme. Pra, të dhënat që formalisht nuk janë shpallur fshehtësi, pavarësisht nga rëndësia e tyre, nuk mund të trajtohen si fshehtësi, në kuptim të kësaj vepre penale (Kodi Penal i Kosovës, Neni 43). Nuk konsiderohen fshehtësi zyrtare informatat apo dokumentet që janë të drejtuara në cenimin e rëndë të të drejtave themelore të njeriut ose moszbulimi i të cilave do të mund të rrezikonte rendin kushtetues apo sigurinë e Republikës së Kosovës; ose informatat dhe dokumentet që kanë për qëllim fshehjen e auorit të veprës.

Figura e këtij krimi, e cekur në paragrafin 2 të nenit 433, për nga forma janë më të rënda në ato raste kur autori (personi zyrtar) e kryen këtë vepër për përfitim personal ose me qëllim të publikimit apo të shfrytëzimit të informacionit jashtë Republikës së Kosovës.

Forma e cilësuar e kësaj vepre penale ekziston kur kumtimi, bartja e fshehtësive zyrtare bëhet për përfitim material. Vepra ka natyrë korruptive, sepse kryhet për motive leverdie. (Kodi Penal i Kosovës, Neni 433).

Forma e cilësuar ekziston kur autori ka për qëllim që të dhënat e tilla t'i publikojë apo t'i shfrytëzojë jashtë territorit të Kosovës. Te kjo formë e cilësuar kërkohet dashja, si në raport me përfitimin personal, ashtu edhe, përkitazi, me rëndësinë e të dhënave të tilla dhe me përdorimin e tyre jashtë shtetit të Kosovës (Kodi Penal i Kosovës, Neni 4).

Rast nga praktika gjyqësore e Gjykatës Themelore të Prizrenit

Një ish-zyrtar i një organizate të sigurisë është dënuar për veprën penale të zbulimit të fshehtësive zyrtare. Zyrtari, nga viti 2009 në vazhdimësi, pa pasur autorizim,

ka bartur në mënyrë elektronike në email-et e tij privat informacionet dhe pastaj u ka mundësuar personave të paautorizuar të kenë qasje në këto informacione, persona që kanë pasur qasje në adresën e tij dhe fjalëkalimin e tij (https://kallzo.com)

3.3. Veprat penale të ndërlidhura me sigurinë e informacionit të kryera me anë të mjeteve të teknologjisë informatike

Teknologjia informatike, respektivisht, pajisjet e saj, si kompjuteri dhe sistemet kompjuterike, janë bërë pjesa më vitale me të cilat sot realizohen detyra të ndryshme në procesin e punës. Nuk ka dyshim që kompjuterët si mjete të fuqishme teknike, janë të përfshirë në çdo sferë, si ajo ekonomike, ushtarake, mjekësore dhe fusha të tjera. (Vula, 2010: 164).

Por, siç e kemi përmendur edhe më parë, kompjuterët shfrytëzohen edhe për kryerje krimesh. Shfrytëzimi i kompjuterit në fushën kriminale bëhet në pesë mënyra themelore: kompjuteri përdoret si objekt sulmi, si mjet i kryerjes së veprës penale, si mjet për planifikim, fshehje ose udhëheqje me kriminalitetin, si simbol për mashtrim dhe si mjet për ndalimin, sqarimin dhe provimin e veprave penale. (Bequaj, 1983: 16).

Veprat penale të ndërlidhura me sigurinë e informacionit të kryera me anë të mjeteve të teknologjisë informative, mundësohen nga shpikjet e teknologjisë së re dixhitale. Me zhvillimet që ka marrë industria elektronike, me shtimin e prodhimit të kompjuterëve, të shitjes së tyre dhe blerjes nga ana e konsumatorëve, rriten edhe mundësitë për lloje të reja të këtyre veprave penale. Madje, kriminaliteti kompjuterik ka marrë edhe karakter global. Për këtë arsye, veprimi i përgjithshëm për parandalimin dhe

luftimin e tij nënkupton ndërtimin e urave të bashkëpunimit dhe veprim të koordinuar midis shteteve, pra, edhe midis Shqipërisë dhe Kosovës, në mënyrë që edhe te ne të vendosen standarde ndërkombëtare në fushën e mbrojtjes dhe të sigurisë së sistemeve informative, standarde që do të garantonin sukses dhe një perspektivë kombëtare të qëndrueshme në luftimin e kërcënimeve nga krimet kibernetike.

Duke ditur pasojat që sjellin krimet e kryera me mjete të teknologjisë informatike, shtetet obligohen të ndërmarrin hapa konkretë për parandalimin dhe luftimin e veprave penale të ndërlidhura me sigurinë e informacionit të kryera me këto mjete. Edhe Republika e Kosovës, përkatësisht, institucionet përgjegjëse të saj, kanë ndërmarrë hapat e nevojshëm për të penalizuar të gjitha veprimet kundërligjore në këtë drejtim.

Për zbulimin e veprave penale të ndërlidhura me sigurinë e informacionit, të kryera me anë të mjeteve të teknologjisë informatike, rol të rëndësishëm ka forenzika e internetit. Teknikat e forenzikës së internetit ndihmojnë në lokalizimin e informacionit që qëndron i fshehur në çdo mesazh, e-mail, dhe ueb faqe të internetit. Për t'i zbuluar të dhëna në lidhje me njerëzit dhe kompjuterët e përfshirë në krimet e internetit, ekspertët e forenzikës së internetit përdorin kombinime të teknikave të përparuara informatike dhe të tjera metoda.

Disa nga këto vepra penale janë krimet kibernetike, si: hakingu, krijimi dhe distribuimi i viruseve, pirateria e softuerëve, shkarkimet e paligjshme, vjedhjet e identitetit etj.

Krimet kibernetike

Krimet kibernetike përbëjnë një ndër kërcënimet themelore për sigurinë globale dhe atë kombëtare, në përgjithësi, dhe për sigurinë e informacionit, në veçanti. Krimi kibernetikë është një rrezik i qartë dhe i pranishëm që është kthyer në një epidemi të heshtur digjitale globale (Buckland B., 2015:9).

Krimet kibernetike paraqesin një nga sfidat më serioze për shoqërinë e sotme. Ky fenomen prek jo vetëm aktivitetet e institucioneve publike dhe private, por edhe njerëzit e thjeshtë, në aktivitetin e tyre të përditshëm, në sferën e tyre private apo profesionale. Zhvillimi i hovshëm i teknologjisë informatike, i internetit dhe arritjet e mëdha në këtë fushë, u krijojnë mundësi sjelljeve antishoqërore dhe kriminale, që më herët nuk kanë qenë të mundura. Sistemet e sotme kompjuterike ofrojnë mundësi të reja për shkeljen e ligjit, duke krijuar potenciale që shtyjnë individët në kryerjen e formave të ndryshme të kriminalitetit tradicional në mënyrë jotradicionale.

Krimet kibernetike mund të shfaqen në forma të ndryshme, varësisht nga mënyra e kryerjes dhe nga qëllimi i atyre që i kryejnë veprat penale, përfshirë edhe mashtrimin online, vjedhjen dhe terrorizmin kompjuterik.

Globalizimi i teknologjisë dhe përparimet revolucionare të Teknologjisë së Komunikimit dhe Informacionit lehtësojnë kryerjen e krimeve kompjuterike, duke ndikuar kështu në rritjen e aktivitetit kriminal kibernetikë. Ato janë një nga shkaqet kryesore që sot kriminaliteti kibernetikë është një e keqe e pranishme ndërkombëtare. Ai kapërcen kufijtë kombëtarë dhe ka marrë forma të krimit të organizuar, duke u bërë një shqetësim global. Një sulm kibernetikë mund të shkatërrojë një vend, pa qenë nevoja që

personeli të dërgohet në atë vend. Mund të themi se sulmet kibernetike janë bërë një formë e re lufte të përhershme.

Interneti, si mjet dhe përçues i një aktiviteti të tillë kriminal i jep atij karakter transnacional. Ky fakt nxjerr nevojën që për luftimin e krimeve kompjuterike të bëhen përpjekje të bashkërenduara ndërkombëtare dhe në këtë drejtim janë bërë edhe hapa konkretë. Për shembull, "Në nivelin ndërkombëtar, krimi i teknologjisë së lartë është një prej pesë prioriteteve më kryesore të Interpolit" (Broadhurst, R.& P. Grabosky, 2005: 37).

Rritja e kërcënimeve nga krimet kibernetike në vendet e Bashkimit Europian, ka bërë që krimet kibernetike të marrin përparësi në strategjinë e brendshme të sigurisë së Bashkimit Europian, si edhe për Europolin (EUROPOL Making Europe Safer, 2012). Që nga viti 2006 deri në vitin 2011 janë shënuar një numër i konsiderueshëm incidentesh të dyshuara për krime kibernetike në nivel ndërkombëtar ndërmjet shteteve, siç janë rastet e sulmeve në Estoni dhe Gjeorgji (Cornish, 2010: 2).

Gjithashtu, Bashkimi Europian ka ndërmarrë një sërë veprimesh për harmonizimin e ligjeve për luftimin e krimit kibernetikë. Fillimisht, në vitet '90, ka adoptuar direktivën për mbrojtjen e individëve në lidhje me procesimin e të dhënave personale dhe me lëvizjen e të dhënave të tilla, duke u fokusuar në konfidencialitetin dhe në sigurinë e tyre kundër dëmtimeve, ndryshimeve, qasjes apo formave të tjera të procesimit të kundërligjshëm (Direktiva 95/46/EC e Parlamentit Europian dhe e Këshillit, 1995). Në vazhdim, ka adoptuar Direktivën 97/66/EC lidhur me procesimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e telekomunikimeve (Direktiva 95/46/EC e Parlamentit Europian dhe e Këshillit, 1997), me synimin që të kërkohet nga vendet anëtare të nxjerrin rregullore dhe të sigurojnë konfidencialitetin e

komunikimeve, ndalimin e llojeve të ndryshme të përgjimit të paautorizuar. Së fundi, Bashkimi Europian miratoi një instrument detyrues, vendimin kornizë të Këshillit, 2005/222/JHA5, për sulmet kundër sistemeve të informacionit, me të cilin penalizohen veprimet e kundërligjshme në ndërhyrjen në sisteme informative, në ndërhyrjen në sisteme apo ndërhyrjet në të dhënat kompjuterike, si dhe nxitja, ndihma dhe përkrahja e këtyre veprave apo vetëtentimi për kryerjen e tyre (Vendimi kornizë 2005/222/JHA i Këshillit të BE-së 2005).

Krimi kibernetik konsiston në veprim kundërligjor, që përfshin kompjuterin, sistemet e tij ose aplikacionet e tij. Pajisjet kompjuterike mund të përdoren për kryerjen e krimeve në tri mënyra: si vegla të krimit, si cak i krimit dhe si vegël dhe cak i krimit.

Përpos Ligjit për Parandalimin dhe Luftimin e Krimit Kibernetikë, ligjet e tjera të aplikueshme, që lehtësojnë luftimin e grupeve kriminale dhe të individëve që kryejnë vepra penale të kësaj natyre, janë: Kodi Penal i Kosovës, Kodi i Procedurës Penale të Kosovës, Ligji për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë, Ligji për Komunikime Elektronike, dispozitat e tjera të dala nga konventat dhe ligje të tjera, që rregullojnë veprimet policore, Strategjia Nacionale Kundër Krimit të Organizuar dhe strategji tjera nacionale dhe sektoriale.

Krimi kibernetikë përkufizohet si një aktivitet kriminal i zhvilluar në rrjet, që ka si objekt apo si mënyrë të kryerjes së tij keqpërdorimin e sistemeve kompjuterike dhe të dhënave kompjuterike (Ligji për Parandalimin dhe Luftimin e Krimeve Kibernetike, Neni 3). Krim kompjuterik konsiderohet "çdo veprim në lidhje me përdorimin e teknologjisë kompjuterike, me të cilën viktima përjeton ose mund të përjetojë humbje, ndërsa autori i krimit vepron me qëllim që t'i krijojë përfitim vetes" (Parker, 1973: 14). Ndërsa sipas autorëve të tjerë, Krimi kompjuterik është "çdo veprim ilegal, joetik dhe

sjellje të paautorizuara në përpunimin e të dhënave ose në bartjen e tyre në mënyrë automatike. Mohr, duke shtjelluar përmbajtjen e kriminalitetit kompjuterik, thotë se ai "…përmban mashtrimin kompjuterik, spiunazhin kompjuterik, si dhe keqpërdorimin kompjuterik". (Mohr.K, 1987: 41).

Krimet kibernetike janë lloje të ndërhyrjeve të paautorizuara në sisteme kompjuterike, përmes kompjuterëve, që kanë si synim ndërhyrjen në rrjete dhe në sisteme kompjuterike për marrjen e të dhënave personale dhe manipulimin me ato të dhëna; shfrytëzimin e resurseve kompjuterike për qëllime të terrorizmit; përgjimin dhe marrjen e të dhënave në sistemet kompjuterike për përfitime financiare, politike, të shantazhit; futja abuzive ose e kundërligjshme në një sistem informative; atentate kundër integritetit të të dhënave ose sistemeve informative etj.

Ekziston një numër i madh veprimesh që ndërlidhen me krimet kibernetike në aspektin social, si, për shembull, marrja dhe shpërndarja e materialeve të mbrojtura nga e drejta e autorit, si: botime shkencore, projekte muzikore - audio, videot dhe shumë veprimtari dhe krijime tjera akademike dhe të biznesit. Pjesë tjetër edhe më e rëndësishme e këtij krimi janë veprimet dhe qëllimet për ndërhyrje në organizatat shtetërore dhe qasja në informacionet e klasifikuara të shteteve të ndryshme, të cilat sot paraqesin një prej sfidave kryesore të sigurisë kombëtare në aspektin e komunikimeve elektronike dhe të dhënave.

Një pasojë tjetër e krimit kibernetikë është edhe viktimizimi dhe rrezikimi i të drejtave civile, siç janë dinjiteti njerëzor, e drejta e jetës private, e drejta e pronës etj. Kjo dikton nevojën në përkufizimin e krimit kibernetikë të zërë vend edhe aspekti i mbrojtjes së të drejtave themelore të njeriut të garantuara nga konventat ndërkombëtare dhe të shprehura drejtpërdrejt edhe në Kushtetutën e Republikës së Kosovës, që kanë

epërsi në rast konflikti ndaj të gjitha dispozitave ligjore dhe akteve të tjera të institucioneve publike (Čukalović, 2013: 83).

Janë një numër i madh mundësish, që shfrytëzohen për të arritur qëllimet me krime kompjuterike. Më të shpeshta janë përhapja e viruseve të ndryshme në rrjete të ndryshme të organizatave, shfrytëzimi i lëshimeve në sigurinë e sistemeve kompjuterike, marrja e fjalëkalimeve dhe të të dhënave tjera personale përmes mesazheve në e-mail, si dhe mosnjohja e mirë e rreziqeve nga e-mailet, që dërgohen nga burime të panjohura, të cilat kanë për qëllim qasjen e paautorizuar në e-mail dhe marrjen e të dhënave personale.

Sulmet në sistemet e informacioneve mund të ndahen duke u bazuar në kritere të ndryshme, varësisht nga shkalla e rrezikshmërisë së tyre, nga qëllimi i autorit që ndërmerr sulmin, nga vendi prej ku ndërmerret sulmi, nga metoda që përdoret për kryerjen e krimit (Dragiçevic, 2004: 49).

Krimet kibernetike, gjegjësisht, krimet kompjuterike kanë të bëjnë me ato vepra penale, që nuk mund të kryhen pa ndihmën e kompjuterit. Në këtë kontekst, "Delikti kompjuterik duhet të përmbajë operacione të larta në kompjuter, nën kushtet kur deri te shkelja nuk mund të vihet në ndonjë mënyrë tjetër " (Taber, 1979: 111). Në kuptimin e ngushtë, krimi kompjuterik përfshin çdo aktivitet kundërligjor përmes masave operative elektronike, të cilat cenojnë sigurinë e sistemeve kompjuterike dhe të dhënave të cilat procesohen, ndërsa në kuptimin e gjerë, krimet e ndërlidhura me kompjuterë përfshijnë çdo aktivitet kundërligjor përmes apo në lidhje me sistemin kompjuterik apo rrjetin kompjuterik, duke përfshirë veprat penale të posedimit, ofrimit, shpërndarjes së informatave përmes sistemit apo rrjetit kompjuterik.

Pra, krimet kibernetike janë krime që kryhen në internet ose duke përdorur internetin. Ekzekutuesi i krimit e kryen aktin kriminal dhe kryen aktivitet të gabueshëm në ueb-faqe në mënyra të ndryshme. (EC-Council Official Curriculum, "Computer Hacking Forensic Investigator", Courseware Manual 3.0 Volume 3, 2009).

Fakti që nuk ekziston një përkufizim tërësor dhe i pranuar botërisht për veprën penale të krimit kibernetik, i cili nuk paraqet një kategori të përbashkët fenomenologjike, lë hapësirë të konstatojmë se kemi të bëjmë me një formë të përgjithshme të paraqitjes së llojeve të ndryshme të veprave kriminale (Vula, 2010: 28). Një qasje e pranueshme haset në Konventën për Krimin Kibernetik, ku kemi një klasifikim në katër lloje të këtyre veprave: veprat penale kundër konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave të sistemeve kompjuterike, veprat penale të ndërlidhura me kompjuter, veprat penale me përmbajtje të kompjuterit dhe veprat penale të ndërlidhura me të drejtën e autorit (Gerceke, 2012: 12).

Ndërsa studiuesit Sun Tian Zhu dhe Cao Pei Zhong, nga Kina, e përcaktojnë krimin kibernetik si krim të kryer me kompjuter, si mjet, dhe si krim ndaj aseteve të kompjuterit, si objekt sulmi (Curtis, 2009: 2).

Autori Von Zur Muhlen e sqaron atë si "të gjitha sjelljet deliktuoze te të cilat kompjuteri ka qenë mjet ose cak i ekzekutimit". Kurse autori Vesel Latifi e quan si "një formë të veçantë të kriminalitetit, në të cilën kompjuteri paraqitet si mjet për kryerjen e veprimit ilegal (*modus operandi*) apo si objekt sulmi, drejtuar nga persona që posedojnë njohuri dhe prirje të veçanta për sistemet kompjuterike, me qëllim që vetes apo të tjerëve t'u sjellin përfitime" (Latifi, 2011: 459).

Kriminaliteti kompjuterik dallohet për nga niveli i lartë teknik dhe nga mundësia e veprimit në mjedise përkatëse. Veprimet e autorëve të këtyre veprave janë, kryesisht,

thyerja e sistemeve elektronike të sigurisë dhe vjedhja e të dhënave me interes, për t'i përdorur vetë ose për llogari të personave të tretë të interesuar, duke përfshirë vjedhjen e monedhave në banka apo në agjenci të kursimeve nëpërmjet deshifrimit të kodeve sekrete të kartave elektronike (Gjonçaj, 2013: 416). Pra, mund të themi se kriminaliteti kibernetikë krijon shqetësime edhe në fushën e financave, në nivel ndërkombëtar dhe kombëtar. Madje, ky shqetësim rritet edhe më shumë nga fakti se të gjitha këto aktivitete ilegale online në internet krijojnë mundësi edhe për pastrimi parash dhe për mbështetje financiare të aktiviteteve terroriste. Sidomos në këtë periudhë krimet kibernetike po marrin përmasa dramatike dhe serioze, përfshi rastet e kërcënimeve për sulme të tipit terrorizëm kibernetikë, pornografinë me fëmijë, shqetësimet online si formë e planifikimit, kryerjes apo koordinimit nëpërmjet rrjeteve kompjuterike, që njihen si hapësirë kibernetike. Një ndër rreziqet më serioze që mund të shkaktojë ky lloj aktiviteti është zhvillimi i luftës kibernetike për qëllime të motivuara politike, ushtarake, terroriste, për sabotim apo spiunazh dhe për sulm mbi sigurinë kombëtare të një shteti. Që nga viti 2006 deri në vitin 2011 janë shënuar një numër i konsiderueshëm incidentesh të dyshuara për krime kibernetike në nivel ndërkombëtar midis shteteve, siç janë rastet e sulmeve në Estoni dhe Gjeorgji (Cornish, 2010: 2).

Një formë me pasoja të rënda e krimeve kibernetike është terrorizmi kibernetikë, i cili kryhet duke përdorur kompjuterin dhe sulmet elektronike. Ky lloj terrorizmi është një ndërthurje e terrorizmit dhe e hapësirës kompjuterike. Kështu, terroristët kibernetikë mund të qasen në një sistem elektronik, por mund të kryejnë sulme edhe në të gjithë kompjuterët në tërë botën.

Terrorizmi kibernetikë është përkufizuar si një sulm i paramenduar, politik, i motivuar kundër informacionit, sistemeve a programeve kompjuterike, sulm që pasohen

me dhunë kundër shënjestrave nga grupeve ndërkombëtare apo agjentëve klandestinë, pra, sulme që shkaktojnë vdekje, dëmtime trupore, shpërthime, rënie avionësh, kontaminim uji apo humbje të ndryshme ekonomike. Edhe sulmet e rrezikshme që kryhen ndaj infrastrukturës mund të jenë krime kompjuterike, në varësi të impaktit të tyre.

Krimi kibernetikë është një prej sfidave më të rëndësishme edhe për institucionet e Republikës së Kosovës, në përgjithësi, dhe për Policinë e Kosovës, në veçanti. Republika e Kosovës ka ndërmarrë hapa konkretë në krijimin e infrastrukturës ligjore për parandalimin dhe luftimin e të gjitha formave të krimit kibernetikë, por ende mbetet shumë për të bërë, sidomos në kuptimin teknik të përballjes së suksesshme me këtë lloj krimi, që në Kosovë është fenomen relativisht i ri.

Rastet më të shpeshta të krimit kibernetikë në Kosovë janë: keqpërdorimi i fëmijëve përmes internetit (pornografia e fëmijëve në internet), hyrje e paautorizuar në sistemet kompjuterike (vjedhje e fjalëkalimeve, sulme në ueb-faqe qeveritare, të institucioneve të ndryshme publike, të kompanive të biznesit etj.), kërcënime dhe shantazhe përmes e-mail-it (përfshirë edhe ndaj personaliteteve të rëndësishme publike dhe institucioneve), lajmet e rrejshme (përmes e-mail-it të falsifikuar) etj. Një vepër penale e drejtuar kundër sistemeve kompjuterike me qëllim të shkatërrimit, modifikimit dhe përgjimit të sistemeve informatike dhe që meriton vëmendjen e duhur është edhe hakingu.

Hakingu

Me haking kuptohet mendja e njeriut kundër kompjuterit. Ai kryhet nga persona të specializuar, që quhen hakerë, dhe që merren me kryerjen e sulmeve kibernetike. Në përdorimin e tij më favorizues, hakingu me kompjuter nënkupton një programues kompulsiv, që eksploron, teston dhe shtyn kompjuterin në limitet e tij, pa marrë parasysh pasojat (Lyman, 2010: 605).

Të gjithë sulmuesit kibernetikë kanë karakteristika të caktuara. Ata nuk duan të zbulohen, prandaj përpiqen të fshehin veten e tyre, identitetin e tyre dhe vendndodhjen gjeografike të vërtetë. (Zwicky, 2000: 11-35).

Hakerët shpesh kanë bërë bujë në llogaritë imagjinare si njerëz që tinëzisht kanë manipuluar një labirint rrjetesh kompjuterike, sisteme dhe të dhëna, për të gjetur dhe për t'u qasur në informacione. Një haker shpesh shpenzon orë të tëra duke ekzaminuar llojet dhe strukturat e sistemeve në të cilat synon të depërtojë, duke përdorur aftësitë e tij për dredhi, mashtrime, si dhe duke anashkaluar kontrollet e vendosura rreth informacionit që është pronë e dikujt tjetër. Ata ndërtojnë programe softuerike dhe i shfrytëzojnë ato për të realizuar qëllimet e tyre. Hakeri ekspert është zakonisht zotërues dhe mjeshtër i disa gjuhëve të programimit, i protokolleve, rrjeteve dhe sistemeve operative. Gjithashtu, ai, me shkathtësi arrin të zotërojë tërësisht mjedisin teknik të sistemit kompjuterik që ka në shënjestër. Pasi zgjedh një sistem si objektiv, gjasat që hakeri ekspert të hyjë me sukses në atë sistem janë të larta. Në shkurt të vitit 2000, një haker i mitur, i quajtur 'Djali mafioz', ishte përgjegjës për një seri sulmesh ndaj ueb-faqeve të shquara. Ai u shpall fajtor për 56 akuza dhe u dënua me tetë muaj burgim për të mitur

(Rosencrance, Linda. "Teen Hacker 'Mafiaboy' Sentenced" Computer World Online. www.computerworld.com/security/story/0,10801,63823,00.html).

Krimin kibernetik të hakingut e karakterizon ndërhyrja e paautorizuar në sistemet e huaja kompjuterike, që në kuptimin klasik do të thotë ndërhyrje e dhunshme në objektet e huaja (Vula, 2010: 102). Në praktikë ekzistojnë dy mënyra për realizimin e kësaj vepre. E para, nënkupton marrjen e informacioneve të nevojshme, me metoda dhe teknika të ndryshme për ndërhyrje të suksesshme në sistemet e huaja kompjuterike, si në adresa të internetit, në numra telefonash, në parametrat identifikues, në porositë e shifruara, në sisteme operative etj. Informatat paraprake kanë të bëjnë me hulumtimin e postës elektronike apo asaj klasike, gazetave, përgjimet, prezantimet e rrejshme etj. (Petrovic, 2000: 118). Mënyra e dytë zhvillohet sipas parimit "provo, gabo, largoje gabimin". Me këtë mënyrë sulmuesi tenton ndërhyrjen në parametrat mbrojtës, për depërtim në sistemin e caktuar informativ. Bartësit e këtij veprimi janë hakerët. (Petrovic, 2000: 118). Nëse kompjuteri i sulmuar është në rrjetin lokal, hakeri mund të mund të mbikëqyrë rrjetin komunikativ dhe të ndajë porositë e shifruara që barten nëpërmjet këtij rrjeti

Krijimi dhe përhapja e viruseve

"Me termin virus kompjuterik, kuptohet programi që kryen disa veprime të qëllimshme dhe të padokumentuara, pa dijen e shfrytëzuesit dhe në dëm të tij" (Petroviç, 2000: 185). Karakteristikë themelore e kësaj vepre është krijimi dhe përhapja e këtyre

programeve destruktive, mundësitë e të cilave janë nxitja dhe bartja e formave të ndryshme të dëmtimeve në sistemet ku gjenden ato viruse (Vula, 2010: 105).

Një virus kompjuterik është një grup i udhëzimeve kompjuterike që riprodhon veten në programet kompjuterike kur, ata realizohen me programe të paautorizuara (Lyman, 2010: 605).

Ekzistojnë dy forma të kryerjes së kësaj vepre: krijimi dhe përhapja e viruseve. Dallimi kryesor ndërmjet këtyre formave është se krijimi i viruseve është veprim i bërë me vetëdije, ndërsa, për shkak të specifikës së përhapjes së infeksionit të viruseve, përhapja mund të jetë veprim me vetëdije apo edhe pa të (Petroviç, 2000: 218). Sipas të dhënave statistikore nga viti në vit, numri i viruseve është rritur dukshëm: nga 105 viruse që ishin në vitin 1990, në fund të vitit 1992, ky numër arriti në 3000 (Clough & Mungo, 1992: 113).

Infektimi me virus në numrin më të madh të rasteve ka të bëjë me kompjuterët privatë. Shumë autorë të kësaj vepre, si objektiv individual kishin infektimin e një numri sa më të madh kompjuterësh, duke dërguar e-maile një numri të madh të audiencës me përmbajtje të gjerë të përfshirë edhe shtojcave (attachmenteve) të bashkangjitura këtyre e-maileve (Rapport Annuel FEDPOL, 2014: 124).

Për të penguar përhapjen e viruseve programet softuerike duhen pajisur me antivirus. Antivirusi është zhvilluar për të zbuluar praninë e viruseve, pastaj për t'i eliminuar ata, si dhe për të mbrojtur programet nga infeksionet e ardhshme (Vacca, 2013:88).

Pirateria e softuerëve

Pirateria e softuerëve është dukuri që ka të bëjë me shkeljet e të drejtave, marrjen pa autorizim të krijimeve të ndryshme, si veprat muzikore, letrare, filmike, programeve kompjuterike, video-lojërave, bazave të të dhënave etj. Pirateria përfshin riprodhimin dhe shpërndarjen e kopjeve, të mbrojtura me të drejtën e autorit, apo komunikimin dhe vënien në dispozicion të tyre, pa autorizim paraprak nga titullari i së drejtës, kur autorizimi i tillë është i nevojshëm në bazë të ligjit (UNESCO, (2013) "Çfarë është pirateria", http://portal.unesco.org).

Piratët vjedhin softuerët për shkaqe të ndryshme, të cilat sillen nga injorimi i ligjeve e deri te krijimi i profitit. Ana e dobët e piraterisë është se ngulfat inovacionet, shkatërron shtytjet financiare për krijimin e programeve të reja dhe rrezikon rritjen e vazhdueshme të industrisë së softuerëve.

Pirateria e softuerëve paraqet formën më të përhapur të keqpërdorimeve në fushën e teknologjisë informatike (Dragiqevic, 1999: 141). Prandaj kjo veprimtari është sot një çështje serioze. Softuerët e paligjshëm jo vetëm prekin të drejtën e autorit, por mund të dëmtojnë seriozisht kompjuterë dhe sigurinë e tyre, duke shkaktuar bllokim të kompjuterëve, fshirje të skedarëve të rëndësishëm, mund të përmbajnë *spyware* që gjurmojnë të dhënat tuaja personale, si llogari bankare, karta krediti, fjalëkalime etj., dhe ua dërgojnë ato hakerëve. (http://albpchelp.blogspot.com/2012/11, parë më 10 prill 2015).

Fishingu

Fishingu (Phishing) është një prej krimeve më të vjetra kibernetike. Ideja e autorëve të kësaj vepre është të shtiren si subjekt i besueshëm në internet, duke u përpjekur të marrin informacione personale.

Kemi të bëjmë me një metodë mashtrimi me e-mail. Mashtruesi dërgon e-maile, që duken si zyrtare, në kërkim të viktimave të mundshme, për të mbledhur informacione personale dhe financiare. Gjithashtu, është e njohur se mashtrime të tilla bëhen edhe me qëllim vjedhjen e informacioneve të vlefshme, si fjalëkalime, numrat e kartave të kreditit, numrave të sigurimeve shoqërore, si dhe numrat e llogarive bankare. Gjatë këtij procesi, përdoruesve të tyre, pra, viktimave, u kërkohet të vizitojnë një faqe interneti për të rinovuar informacionin e tyre personal përmes postës elektronike.

Duket qartë se fishingu është çdo proces i projektuar për të nxjerrë të dhënat personale nga viktima e shënjestruar. Kjo shpesh bëhet me e-mail. "Një skenar i përbashkët mund të përfshijë autorin e veprës, që ka krijuar një ueb-faqe të rreme, të projektuar për t'u dukur si faqe legjitime e internetit, dhe një institucion financiar (Eastom &Taylor, 2011: 6).

Vjedhja e identitetit

Vjedhja e identitetit është procesi i marrjes së informacionit personal nga një person apo organizatë që paraqitet se është dikush tjetër. Kjo është bërë shpesh për të

marrë kredi në emër të viktimës, duke e vënë këtë në obligime financiare (Eastom &Taylor, 2011: 5).

Me anë të këtij krimi, një individ apo organizatë kriminale, zakonisht, qaset në informacionet dhe në të dhënat mbi llogarinë bankare apo kartën e kreditit të dikujt dhe, në mënyrë të paautorizuar, realizon transaksione monetare, duke shpenzuar paratë e atij personi (Ross, 2010: 23).

Pra, kemi të bëjmë me vjedhjen e identitetit të personit dhe pastaj ky identitet përdoret për të kryer mashtrim me të dhënat personale të viktimës, si: numrat e sigurimit, llogaritë bankare, numrat e kartës së kreditit. Vjedhësit e identitetit sigurojnë emrat, adresat, datat e lindjes të viktimave dhe mund të aplikojnë për kredi në emër të tyre.

Interneti është mënyra më e lehtë dhe më efektive për të kryer vjedhjet e identitetit. Është e thjeshtë për kriminelët të përdorin informacionin e kartave të kreditit të një personi tjetër, për të bërë blerje, pasi transaksionet nëpërmjet internetit bëhen shpejt dhe pa ndërveprimin paraprak personal. Ekzistojnë edhe metoda me të cilat një hajdut mund të shohë fjalëkalimin tuaj ose numrin personal identifikues, PIN-in. Gjithashtu, vjedhja e identitetit mund të bëhet duke u dërguar viktimave postë elektronike tërheqëse që përmbajnë viruse (Computer Hacking Forensic Investigator, 2009).

Është e rëndësishme të merren parasysh mjetet me të cilat kryhen vjedhjet e identitetit. Veprimi më i rëndësishëm për kryerësit është qasja në të dhënat personale, në mënyrë që ato të mund të përdoren në vjedhjen e identitetit. Ekzistojnë katër mënyra kryesore përmes të cilave personat qasen në të dhënat personale: fishingu, hakingu ose

spyware, qasja e paautorizuar e të dhënave dhe fshirja e informacioneve (Eastom &Taylor, 2011: 6).

Mashtrimet përmes internetit

Këto janë të shumta dhe të shumëllojshme, pasi interneti ka impakt të gjerë dhe shërben edhe si tregu më i mirë për promovimin e bizneseve dhe shërbimeve për klientët në mbarë botën. Nga mundësitë e ndryshme që gjenden në internet për veprime të tilla, është e vështirë për të dalluar shitësin ligjor dhe atë të rremë në internet. Këta të fundit mashtrojnë njerëzit, duke përdorur e-mailin, dhomat chat etj., që janë komponentë gjerësisht të përdorura të internetit. Një formë tjetër janë mashtrimet me kartë krediti. Sulmuesit, në mënyrë të paligjshme, përdorin kartë kreditin e tjetërkujt për të blerë mallra dhe shërbime të tjera në internet. Gjithashtu, duke përdorur teknika të ndryshme, ata mund të vjedhin të dhënat personale në transaksionet e një përdoruesi në internet ose thjesht nëpërmjet teknikave sociale të inxhinieringut (Computer Hacking Forensic Investigator, 2009).

Shkarkimet e paligjshme në internet

Shkarkimi nga një ueb-faqe e autorizuar, është i pranueshëm dhe i ligjshëm. Megjithatë, çdo produkt që është i mbrojtur me të drejtën e autorit nuk mund të shitet nga një organizatë apo individ i paautorizuar. Shkarkimi i paligjshëm ndikon në shitjet e

atij produkti. Shumica e krimeve bëhen për shkak të mjeteve të gatshme në dispozicion për kërkim të softuerit.

Ka shumë ngasje që të çojnë në shkarkime të paligjshme. Këto përfshijnë: marrjen e produkteve me kosto të ulët ose falas, nuk kërkohen informata personale, janë në dispozicion në të gjithë botën. Entitetet më të ndikuara të shkarkimeve më të paligjshme janë: produkte muzikore, filmike, programe, informacione konfidenciale dhe mbrojtëse, të dhënat në internet.

3.4. Veprat penale të ndërlidhura me sigurinë e informacionit të parashikuara me ligjin për parandalimin dhe luftimin e krimeve kibernetike

Në Kosovë ka pasur mangësi në infrastrukturën ligjore, sepse veprat penale që janë të ndërlidhura me sigurinë e informacionit, përfshirë edhe krimet kibernetike, nuk kanë qenë të parashikuara as në Kodin Penal të Kosovës dhe as me ndonjë ligj specifik. Me qëllim të avancimit të luftës kundër krimeve kibernetike, është bërë edhe modifikimi i pjesshëm i infrastrukturës ligjore. Në këtë kontekst, me qëllim që të rregullohet kjo çështje, veprat penale të cilat ndërlidhen me krimet kibernetike janë të parashkuara me një ligj të veçantë, Ligji për parandalimin dhe luftimin e krimeve kibernetike. 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 (Ligji për parandalimin dhe luftimin e krimeve kibernetike, neni 1).

Autoritetet dhe institucionet publike, në bashkëpunim me ofruesit e shërbimeve dhe organizatat joqeveritare, si dhe me përfaqësuesit e tjerë të shoqërisë civile,

zhvillojnë politikat, praktikat, masat, procedurat dhe standardet minimale për sigurinë e sistemeve kompjuterike (Ligji për parandalimin dhe luftimin e krimeve kibernetike, Neni 5).

Ky ligj parasheh pesëmbëdhjetë vepra penale:

- Qasja joligjore në sistemet kompjuterike,
- Interceptimi pa të drejtë,
- Interceptimi pa të drejtë i transmetimeve jopublike i të dhënave kompjuterike nga/për/ në ose brenda një sistemi kompjuterik,
- Interceptimi pa të drejtë i emetimeve elektromagnetike nga sistemet kompjuterike që mbajnë të dhëna jopublike kompjuterike,
- Transferimi i paautorizuar, ndryshimi, shlyerja, shkatërrimi i të dhënave kompjuterike apo kufizimi pa të drejtë,
- Transferimi i paautorizuar i të dhënave nga sistemet kompjuterike,
- Veprat penale kundër konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave të sistemeve kompjuterike;
- Transferi i paautorizuar;
- Pengimi i funksionimit të sistemeve kompjuterike;
- Prodhimi, posedimi dhe tentativa e paautorizuar;
- Shkaktimi i humbjes së pronës;
- Pornografia me fëmijë përmes sistemeve kompjuterike;
- Sekuestrimi, kopjimi dhe ruajtja e të dhënave dhe
- Qasja, nxënia ose incizimi i komunikimeve.

KAPITULLI 4. ANALIZË KRAHASUESE E LEGJISLACIONIT TË DISA VENDEVE NË FUSHËN E VEPRAVE PENALE TË NDËRLIDHURA ME SIGURINË E INFORMACIONIT

Lufta kundër veprave penale të ndërlidhura me sigurinë e informacionit në shumë vende të botës po merr përmasa të mëdha, prandaj shtetet duhet t'i kushtojnë vëmendje të veçantë legjislacionit që rregullon çështjen e luftimit të këtyre veprave penale.

Në nivel ndërkombëtar dhe atë europian janë bërë dhe po bëhen shumë përpjekje për të orientuar politikën penale të shteteve lidhur me veprat penale në fushën e sigurisë së informacionit, si dhe janë krijuar disa mekanizma policorë dhe organizata të veçanta, që merren me luftimin e këtyre veprave. Përafrimi i legjislacionit vendas me direktivat dhe strategjinë e BE-së kundër veprave penale të ndërlidhura me sigurinë e informacionit ndikon në rritjen e efektivitetit të bashkëpunimit të agjencive kombëtare të zbatimit të ligjit me institucionet evropiane dhe ndërkombëtare të angazhuara në parandalimin dhe luftimin e këtyre veprave.

Vështrimi i legjislacionit penal të shteteve të ndryshme na jep një pasqyrë të qartë mbi aspektet e përbashkëta dhe ndryshimet në këtë legjislacion. Analiza krahasuese mundëson, jo vetëm njohjen e tyre dhe, për rrjedhojë, lehtësimin e bashkëpunimit mes këtyre vendeve, por mundëson përmirësime të legjislacionit vendas, duke përfituar nga përvojat dhe modelet më të mira.

Në këtë kapitull të punimit analizohet legjislacioni i dy shteteve anëtare të BE-së, Sllovenisë dhe Kroacisë. Përzgjedhja e tyre është bërë nisur nga dy kritere: *së pari*, fqinjësia dhe nevoja për forcimin e bashkëpunimit rajonal në këtë fushë; *së dyti*, krijimi

i një tabloje sesi është hartuar legjislacioni i një shteti anëtar të BE-së, e cila ka një traditë në shtetndërtim dhe infrastrukturë ligjore të shkëlqyer. Përveç hartimit të një legjislacioni modern, këto dy shtete kanë krijuar edhe një proces praktik të kontrollit dhe të luftës kundër veprave penale të ndërlidhura me sigurinë e informacionit. Mendojmë se vështrimi krahasues i legjislacionit të Sllovenisë dhe Kroacisë, paraqet mundësi reale që të përvetësohen praktika ligjore sesi hartohet infrastruktura ligjore e një shteti.

4.1. Veprat penale të ndërlidhura me sigurinë e informacionit të parashikuara me Kodin Penal të Sllovenisë

Në legjislacionin slloven veprat penale të ndërlidhura me sigurinë e informacionit janë të parashikuara me Kodin Penal të Sllovenisë (KPS). Më poshtë po shtjellojmë disa prej tyre.

Përgjimi dhe regjistrimi i paligjshëm zërit -Neni 137

Paragrafi 1 dhe 2 i Nenit 137 të KPS e konsideron vepër penale kryerjen e njërit nga veprimet vijuese: përgjimin ose regjistrimin e kundërligjshëm të një bisede ose deklarate private, me përdorim të pajisjeve të veçanta, si dhe transmetimin e drejtpërdrejtë të një bisede a deklarate të tillë një personi të tretë ose lejimin e këtij personi për të mësuar bisedën ose deklaratën private.

Nëse vepra kryhet ose tentohet të kryhet nga një zyrtar, përmes shpërdorimit të detyrës ose autoritetit zyrtar, kjo paraqet rrethanë rënduese.

Regjistrimi vizual i paligjshëm - Neni 138

Neni 138 i KPS konsideron vepër penale veprimet me të cilat ndërhyhet në privatësinë e një personi tjetër, duke marrë në mënyrë të paautorizuar fotografi ose regjistrime të tjera vizuale të një personi ose të lokaleve të tij, pa pëlqimin e tij; transmetimi ose paraqitja e fotografive të tilla ose incizimeve te një person i tretë ose lejimi i një personi të tretë për të parë fotografi ose incizime të tilla.

Forma e kualifikuar e kësaj vepre penale themelore ekziston kur ajo kryhet nga një zyrtar nëpërmjet shpërdorimit të detyrës ose të autoritetit zyrtar.

Shkelja e fshehtësisë së mjeteve të komunikimit - Neni 139

Dispozita e nenit 139 të (KPS) konsideron vepër penale veprimet e kundërligjshme që ndërmerren me qëllim shkeljen e fshehtësisë së komunikimit, siç janë:

a) Hapja pa autorizim e letrës, telegramit ose ndonjë shkrese tjetër të vulosur apo dërgese që u përket personave të tjerë;

b) Përdorimi i instrumenteve teknike ose i agjentëve kimikë, me qëllim që, pa e hapur letrën, telegramin, ndonjë shkrese tjetër të vulosur apo dërgese, që u përkasin personave të tjerë, të mësojë përmbajtjen e tyre;

c) Përdorimi i instrumenteve teknike për të mësuar përmbajtjen e një mesazhi që transmetohet me anë të telefonit apo ndonjë mjeti tjetër të telekomunikacionit.

Te kjo vepër penale veprime të kundërligjshme që ndërmerren me qëllim shkeljen e fshehtësisë së komunikimit konsiderohen edhe veprimet:

a) Hapja e çdo objekti të mbyllur, në të cilin ka një mesazh, dhe në këtë mënyrë është informuar për përmbajtjen e mesazhit të tillë;
b) Veprimet me të cilat i lejohet një person i tretë të informohet për përmbajtjen e dërgesës ose të mesazhit;
c) Mbajtja, fshehja, asgjësimi ose dorëzimi i një letre të huaj, telegrami ose ndonjë dërgese tjetër personave të tretë dhe njoftimi i tyre me përmbajtjen e një letre të tillë, telegrami ose dërgese tjetër.
d) Vepra penale është me rrethanë të cilësuar, kur ajo kryhet nga një zyrtar përmes shpërdorimit të detyrës ose të autoritetit zyrtar, ose nga një punëtor apo zyrtar tjetër i autorizuar postar.

Publikimi i paligjshëm i shkrimeve private - Neni 140

Paragrafi 1 i Nenit 140 të KPS e konsideron vepër penale publikimin, pa leje zyrtare, të një ditari, letre apo ndonjë pjese tjetër private të të shkruarit që u përket personave të tjerë.

Zbulimi i paligjshëm i sekretit profesional - Neni 142

Dispozita e nenit 142 të KPS konsideron vepër penale veprimet e kundërligjshme që ndërmerren për zbulim sekreti, siç janë: zbulimi i kundërligjshëm i një sekreti *nga* avokati, mjeku, prifti, punonjësi social ose psikologu, që i kanë mësuar sekretet nga klienti i tyre (KPS, Neni 142, Paragrafi 1).

Në paragrafin 2 të këtij neni përcaktohet se nuk paraqet veprim inkriminues, nëse veprimi i zbulimit të sekretit është bërë për të mirën e përgjithshme.

Shpërdorimi i të dhënave personale - Neni 143

Dispozita e nenit 143 të KPS konsideron vepër penale veprimet e kundërligjshme që ndërmerren për shpërdorimin e të dhënave personale, si:

1) Përdorimi në mënyrë të kundërligjshme i të dhënave personale, që mund të mbahen vetëm në bazë të ligjit ose në bazë të pëlqimit personal të individit, të cilit i të dhënat personale lidhen;
2) Depërtimi (thyerja) në bazën e të dhënave kompjuterike me qëllim marrjen e të dhënave personale të personit ose me qëllim që ato të dhëna t'i përdorë një person i tretë.
3) Publikimi në World Wide Web (rrjeti i hapur i internetit) ose mundësimi personit tjetër që të publikojë të dhënat personale të viktimave të veprave penale: shkelja e të drejtave dhe e lirive të viktimave, të dëshmitarëve të

mbrojtur, që përfshihen në të dhënat e procedurave gjyqësore të gjykatës, në të cilën prania e identifikimit të dëshmitarit publik ose dëshmitarëve të mbrojtur dëshmitarët dhe të dhënat personale të tyre kanë të bëjnë me procedurën gjyqësore nuk lejohet publikimi sipas ligjit apo vendimit të gjykatës, në bazë të të cilave këta persona mund të jenë identifikuar ose janë të identifikueshëm.

4) Marrja apo shfrytëzimi i identitetit të një personi tjetër dhe shfrytëzimi i të drejtave, fitimi e përfitimi pronësor në emër të një personi tjetër,
5) Forma e kualifikuar e kësaj vepre penale ekziston, kur ajo kryhet nga një zyrtar nëpërmjet shpërdorimit të detyrës ose autoritetit zyrtar.

Sulmi në sistemet e informacionit - Neni 221

Dispozita e nenit 221 të KPS konsideron vepër penale veprimet e kundërligjshme që ndërmerren me qëllim për sulme në sistemet e informacionit, si:

1) Sulmi apo depërtimi në një sistem informacioni, ose marrja në mënyrë të kundërligjshme e të dhënave nga sistemi informativ gjatë një transmetimi jopublik.
2) Përdorimi i kundërligjshëm i të dhënave në një sistem informacioni, ndryshimi, kopjimi, transmetimi, shkatërrimi, ose importimi ilegal i të dhënave në një sistem informacioni, ose pengimi i operimit të sistemit të transmetimit të dhënave ose informacioneve (KPS, Neni 221, Paragrafi 2).

3) Vepra penale është me rrethanë të cilësuar, nëse dëmet e shkaktuara nga kryerja e kësaj vepre janë të konsiderueshme.

Dhënia e informacioneve shpjeguese dhe blerja e paautorizuar e sekreteve tregtare - Neni 236

Neni 236 i KPS konsideron vepër penale veprimet e kundërligjshme vijuese:

1) Komunikimi ose përcjellja e paautorizuar e informacioneve të mbrojtura apo sekreteve tregtare një personi tjetër, duke i mundësuar qasje në informacion të tillë apo mbledhja e informacionit të tillë që ta përcjellë te një person i paautorizuar (KPS, Neni 236 , Paragrafi 1).
2) Prokurimi i paautorizuar i informacionit që është përcaktuar si sekret tregtar.
3) Vepra penale është me rrethanë të cilësuar, nëse informacioni është i rëndësisë së veçantë, ose nëse ai informacion i është dërguar një personi të tretë me qëllim transferimin e tij jashtë vendit, ose nëse vepra është kryer nga lakmia.
4) Nëse kjo vepër penale është kryer nga pakujdesia, kjo paraqet formë të lehtësuar të kryerjes së kësaj vepre.

Depërtimi (thyerja) në sistemet e informacionit tregtar (të biznesit) - Neni 237

Neni 237 i KPS konsideron si vepër penale veprimet vijuese:

1) Vendosja, ndryshimi, fshehja, fshirja ose shkatërrimi i paautorizuar i të dhënave ose i programeve kompjuterike; depërtimin e paautorizuar në një sistem kompjuterik me qëllim blerjen ose përfitimin e paligjshëm, për vete ose për një person të tretë, të pronës së tjetrit apo dëmtimin e pronës së tjetrit, gjatë kryerjes së veprimtarive të biznesit (KPS, Neni 237, Paragrafi 1).
2) Vepra penale është me rrethanë të cilësuar, nëse ajo ka rezultuar në një përfitim të madh të pronës ose me një humbje e madhe të pasurisë dhe nëse autori ka për qëllim të shkaktojë humbje të tillë të pronës ose për të fituar dobi pasurore juridike për vete.

Shpërdorimi i informacionit të brendshëm - Neni 238

Dispozita e nenit 238 të KPS konsideron vepër penale veprimet e kundërligjshme, që ndërmerren me qëllim shpërdorimin e informacionit të besueshëm, siç janë:

1) Marrja e informacionit të brendshëm me qëllim për të ndikuar në çmimin e letrave me vlerë apo të instrumenteve tjera financiare në tregun e organizuar në Republikën e Sllovenisë apo, të paktën, në një shtet anëtar të Bashkimit Europian.
2) Kushdo që komunikon informacion të brendshëm te një person i paautorizuar.
3) Kushdo që merr informacion të brendshëm pa autorizim dhe e përdor atë për blerje të drejtpërdrejtë ose të tërthortë.

4) Rrethanë rënduese paraqitet nëse vepra penale sipas paragrafëve të mësipërm ka të bëjë me letra me vlerë të lartë ose me instrumente financiare me vlerë.

Zbulimi i informacionit të klasifikuar - Neni 260

Paragrafi 1 i Nenit 260 të KPS konsideron vepër penale komunikimin dhe përcjelljen e informacionit të klasifikuar një personi tjetër, ose dhënien e qasjes në informacionin e klasifikuar një personi të paautorizuar.

Autor i kësaj vepre penale është zyrtari ose ndonjë person tjetër, që ka dështuar në marrjen e masave të mbrojtjes së informacionit të klasifikuar.

Vepra penale është me rrethanë të cilësuar, nëse ajo është kryer nga lakmia ose me qëllim publikimin ose duke përdorur të dhënat në fjalë jashtë vendit.

Shkelja e procedurës sekrete - Neni 287

Neni 287 i KPS konsideron vepër penale veprimet vijuese:

1.Zbulimi i pautorizuar të çfarëdo çështjeje për të cilat autori i veprës është vënë në dijeni para apo gjatë procedurave të mëparshme të gjykimit, gjatë gjykimit me gojë në procedurën administrative, ose gjatë gjykimit për kundërvajtje, ose në rrjedhën e një hetimi parlamentar, dhe publikimi i tyre është i ndaluar me vendim të lëshuar nga një gjykatë ose autoritet tjetër kompetent.

2) Publikimi i të dhënave personale të një fëmije, që është palë në një gjyqësor, administrative, ose procedura të tjera, ose publikimi i informacionit tjetër janë të rëndësishme për krijimin e identitetit të fëmijës.

3) Zbulimi i identitetit të një dëshmitari të mbrojtur, personit të rrezikuar ose një person me identitet të ndryshuar.

(4) Vepra penale është me rrethanë të cilësuar nëse ajo vepër është kryer nga një zyrtar.

Spiunazhi - Neni 358

Dispozita e nenit 358 të KPS konsideron vepër penale veprimet vijuese:

1) Shërbimi si agjent për një vend apo organizatë të huaj, duke mbledhur dokumente ushtarake, ekonomike ose informacion zyrtar; ose ofrimi i qasjes në informata ose në dokumente të tilla.
2) Themelimi ose drejtimi i një shërbimi të inteligjencës për një vend apo organizatë të huaj, në dëm të Republikës së Sllovenisë.
3) Bashkimi me një shërbim të zbulimit të huaj dhe mbështetja e operacioneve të tij.

4.2. Veprat penale të ndërlidhura me sigurinë e informacionit të parashikuara në Kodin Penal të Kroacisë

Në Legjislacionin kroat veprat penale të ndërlidhura me sigurinë e informacionit janë të parapara me Kodin Penal të Kroacisë (KPK).

Zbulimi i sekretit profesional - Neni 145

Neni 145 i KPK konsideron vepër penale të tillë:

1) Dhënien apo zbulimin e paautorizuar të informacionit që u është rrëfyer apo besuar atyre nga një person. Këtë vepër e kryen avokati, noteri publik, punëtori mjekësor, psikologu, institucionet e mirëqenies sociale.
2) Nëse sekreti është shpalosur për interes publik dhe kjo shpalosje tejkalon interesin e mbajtjes së sekretit, ky veprim nuk konsiderohet vepër penale.

Përdorimi i paautorizuar i të dhënave personale - Neni 146

Neni 146 i KPK konsideron vepër penale veprimet që ndërmerren me qëllim përdorimin e paautorizuar të të dhënave personale, siç janë:

1) Mbledhja, përpunimi apo përdorimi i të dhënave personale të personave fizikë, në kundërshtim me kushtet e përcaktuara në ligj.
2) Përpunimi i mëtejshëm i të dhënave personale kroate apo mundësimi një personi tjetër për t'u qasur te të dhënat e palës së tretë.
3) Mbledhja, përpunimi ose përdorimi i të dhënave personale të personave fizikë, në kundërshtim me kushtet e përcaktuara në ligj, të dhëna që kanë të bëjnë me origjinën racore, etnike, fetare apo bindjet politike; me anëtarësimin në sindikata, me shëndetin ose me jetën seksuale dhe personale, të dhënat e personave fizikë të procedurës penale ose kundërvajtëse.

4) Vepra penale është me rrethanë të cilësuar, nëse vepra penale kryhet nga një zyrtar gjatë kryerjes së detyrës.

Shpërdorimi i informacionit zyrtar- Neni 259

Neni 259 i KPK konsideron vepër penale veprimet që ndërmerren me qëllim shpërdorimin e informacionit zyrtar, siç janë:

1) Marrja ose disponimi i informacionit zyrtar nga një person për të apo për llogari të tjetrit, drejtpërdrejt ose tërthorazi,
2) Zbulimi, komunikimi, dorëzimi ose ndryshimi, si dhe vënia në dispozicion të personit tjetër të informacionit zyrtar,
3) Vepra penale është me rrethanë të cilësuar, nëse vepra penale kryhet nga personi zyrtar që ka qasje dhe zotëron informacionin përmes ushtrimit të punës ose detyrave dhe, nëse, si rezultat i shpërdorimit të informacionit zyrtar, realizohet fitim i konsiderueshëm financiar ose shkaktohet dëm i konsiderueshëm financiar.

Qasja e paautorizuar - Neni 266

Neni 266 i KPK konsideron vepër penale veprimet që ndërmerren me qëllim hyrjen apo qasjen e paautorizuar të personave në një sistem kompjuterik ose në të dhëna

kompjuterike, si dhe qasjen në një sistem kompjuterik ose në të dhënat elektronike të qeverisë, të organeve të pushtetit, të organeve lokale rajonale, të institucioneve publike apo të një kompanie me interes të veçantë publik.

Përgjimi i paautorizuar i të dhënave kompjuterike - Neni 269

Dispozitat e nenit 269 të KPK konsiderojnë vepër penale:

1) Përgjimin, regjistrimin, transmetimin e paautorizuar të të dhënave kompjuterike, përfshirë emisionet elektromagnetike nga një sistem kompjuterik ose mundësimi i marrjes së të dhënave.
2) Të dhënat e prodhuara nga kryerjen e një vepre do të shkatërrohen.

Zbulimi i të dhënave sekrete - Neni 347

Neni 347 i KPK konsideron vepër penale veprimet që kryhen për marrjen e paautorizuar dhe për zbulimin e të dhënave sekrete, me qëllim përdorimin e paautorizuar apo vënien në dispozicion të këtyre informacioneve personave të tjerë të paautorizuar.

Zbulimin i sekreteve shtetërore - Neni 144

Neni 144 i KPK konsideron vepër penale veprimet që ndërmerren për zbulimin e sekreteve shtetërore, siç janë:

1) Vënia në dispozicion e një sekreti shtetëror një personi të paautorizuar,
2) Nëse dikush, në mënyrë të paligjshme, ia vë në dispozicion një personi të paautorizuar sekretin të cilën ai e di.
3) Nëse një sekret shtetëror që i është besuar dikujt apo sekretin që ai e ka mësuar në mënyrë të paligjshme ia vë në dispozicion një personi të paautorizuar, në kohë lufte apo konflikti të armatosur.

Spiunazhi - Neni 348

Dispozitat e nenit 348 të KPK konsiderojnë vepër penale:

1) Vënien në dispozicion në mënyrë të paligjshme të informacionit konfidencial një shteti të huaj, një organizate të huaj, një personi të huaj juridik ose një personi që punon për ta.
2) Mbledhjen apo bërjen të arritshme të informacioneve sekrete një shteti të huaj, një organizate të huaj, një personi juridik të huaj ose një personi që punon për ta.

3) Bashkëpunimin me një organizatë të huaj në fushën e inteligjencës apo bashkimin ose dhënien e ndihmës një shërbimi të zbulimit të huaj që vepron kundër interesave të Kroacisë.

4) Vepra penale që është kryer në kohë lufte ose konflikti të armatosur, ku merr pjesë Republika e Kroacisë.

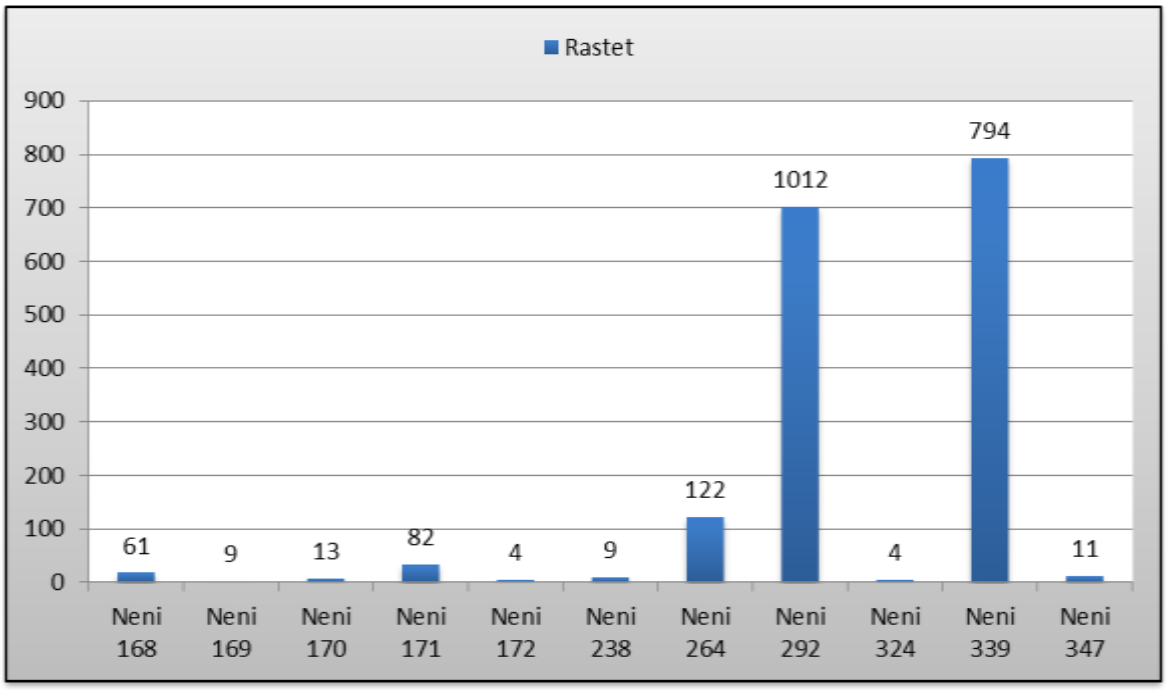
KAPITULLI 5: ANALIZA EMPIRIKE E TË DHËNAVE PËR VEPRAT PENALE TË NDËRLIDHURA ME SIGURINË E INFORMACIONIT NË KOSOVË NË PERIUDHËN 2007 – 2015

Ky kapitull përmban analizën e të dhënave empirike të Policisë dhe të Gjykatave për veprat penale të ndërlidhura me sigurinë e informacionit në Kosovë në periudhën 2007 – 2015. Pjesa e parë e kapitullit përmban analizën empirike të të dhënave të Policisë, ndërsa pjesa e dytë përmban analizën empirike të të dhënave të Këshillit Gjyqësor të Kosovës. Në analizën empirike të të dhënave jemi fokusuar në numrin e rasteve të ndodhura në periudhën 2007-2015, në numrin e personave të përfshirë në këto raste, gjininë, përkatësinë etnike, llojin e sanksionit penal të shqiptuar. Analiza e të dhënave është bërë për njëmbëdhjetë vepra penale të parashikuara në Kodin Penal të Kosovës.

5.1. Analiza empirike e të dhënave të Policisë

Bazuar në të dhënat e Sistemit Informativ të Policisë së Kosovës (SIPK), në territorin e Republikës së Kosovës gjatë periudhës 2007-2015, janë evidencuar gjithsej 2121 vepra penale të ndërlidhura me sigurinë e informacionit. Më pak raste të veprave penale të ndërlidhura me sigurinë e informacionit janë evidencuar për veprën penale "Shkelja e urdhrave për masat e fshehta ose teknike të vëzhgimit ose të hetimit" dhe për veprën penale "Asgjësimi apo fshehja e materialit arkivor", me gjithsej 4 raste të evidencuara. Ndërsa më shumë raste gjatë kësaj periudhe janë evidencuar për veprën

penale “Shpërdorim i pozitës zyrtare ose i autorizimit”, me gjithsej 1012 raste (Raport Statistikor i Policisë së Kosovës, datës, 2014:4).



***Burimi, Policia e Kosovës, SIPK**

Figura 2: Veprat penale në periudhën 2007 – 2015.

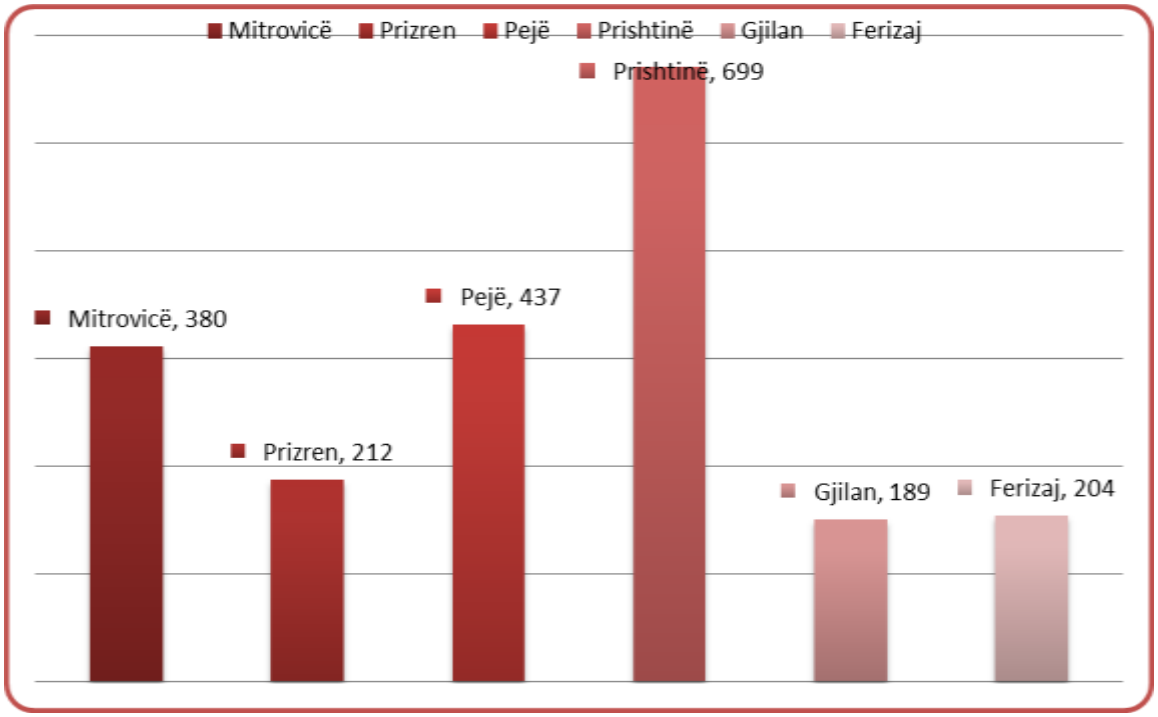
Analiza e të dhënave të veprave penale, sipas rajoneve policore të Kosovës

Në Kosovë, sipas ndarjes territoriale, deri në vitin 2013 kanë ekzistuar gjashtë rajone policore: Prishtina, Mitrovica, Peja, Prizreni, Ferizaj dhe Gjilani, ndërsa nga viti 2014, rajoni policor i Mitrovicës është ndarë në rajonin policor të Mitrovicës Veriore dhe rajonin policor të Mitrovicës Jugore, si dhe është krijuar rajoni policor i Gjakovës.

Nga 2121 vepra penale të evidencuara në periudhën nëntëvjeçare 2007-2015, në rajonin policor të Prishtinës janë evidencuar 699 raste, në rajonin policor të Mitrovicës

380 raste, në rajonin policor të Pejës 437 raste, në rajonin policor të Prizrenit 212 raste, në rajonin policor të Ferizajt 204 raste dhe në rajonin policor të Gjilanit 189 raste.

Siç shihet, në rajonin policor të Gjilanit janë evidencuar më pak vepra penale të ndërlidhura me sigurinë e informacionit, ndërsa më shumë vepra penale janë evidencuar në rajonin policor të Prishtinës.



***Burimi, Policia e Kosovës, SIPK-u**

Figura 3: Veprat penale sipas rajoneve policore në periudhën 2007 – 2015.

Në vijim po paraqesim analizën e të dhënave statistikore për secilën vepër penale të ndërlidhur me sigurinë e informacionit.

Cenimi i fshehtësisë së korrespondencës dhe i bazave të të dhënave kompjuterike - Neni 168

Gjatë periudhës 2007 - 2015 janë evidencuar 61 raste të veprës penale "Cenimi i fshehtësisë së korrespondencës dhe i bazave të të dhënave kompjuterike".

Në rajonin policor të Ferizajt nuk është evidencuar asnjë rast i kësaj vepre penale, në rajonin policor të Pejës janë evidencuar 15 raste, në rajonin policor të Mitrovicës 15 raste, në rajonin policor të Prishtinës 17 raste, në rajonin policor të Gjilanit 10 raste, në rajonin policor të Prizrenit 4 raste.

Në cilësinë e të dyshuarit kanë qenë të përfshirë 26 persona, nga të cilët 21 persona ishin të gjinisë mashkullore dhe 5 persona të gjinisë femërore.

Këta 26 persona të gjithë i përkasin nacionalitetit shqiptar.

Në cilësinë e viktimës kanë qenë të përfshirë 26 persona, nga të cilët, 9 persona të gjinisë mashkullore dhe 17 persona të gjinisë femërore.

Të kombësisë shqiptare ishin 25 persona, 1 person ishte boshnjak.

Zbulimi i paautorizuar i informacionit të besueshëm – Neni 169

Gjatë periudhës 2007 - 2015 janë evidencuar 9 raste të veprës penale "Zbulimi i paautorizuar i informacionit të besueshëm", nga të cilat 3 raste janë evidencuar në rajonin e policor të Pejës, 5 raste në rajonin policor të Prishtinës, 1 rast në rajonin policor të Mitrovicës, ndërsa në rajonet policor të Ferizajt, të Gjilanit dhe të Prizrenit nuk është evidencuar asnjë rast.

Në cilësinë e të dyshuarit kanë qenë të përfshirë 9 persona, të kombësisë shqiptare, nga të cilët, 8 persona ishin të gjinisë mashkullore dhe 1 person i gjinisë femërore.

Ndërsa në cilësinë e viktimës ka qenë i përfshirë 1 person, i gjinisë mashkullore, i kombësisë shqiptare.

Përgjimi dhe incizimi tonik i paautorizuar – Neni 170

Gjatë periudhës kohore 2007 - 2015 janë evidencuar 13 raste të veprës penale "Përgjimi dhe incizimi tonik i paautorizuar". Nga këto 3 raste janë evidencuar në rajonin policor të Prizrenit, 3 raste në rajonin policor të Ferizajt, 5 raste në rajonin policor të Prishtinës, 1 rast në rajonin policor të Mitrovicës dhe 1 rast në rajonin policor të Pejës.

Në cilësinë e të dyshuarit kanë qenë të përfshirë 31 persona, nga të cilët 29 persona ishin të gjinisë mashkullore dhe 2 persona të gjinisë femërore.

Nga këta, 24 persona ishin të kombësisë shqiptare, 5 persona ishin të kombësisë serbe, 1 person i kombësisë kroate dhe 1 person në kategorinë - të tjerë.

Në cilësinë e viktimës kanë qenë të përfshirë 23 persona, nga të cilët 20 ishin të gjinisë mashkullore, ndërsa 3 persona ishin të gjinisë femërore.

Të kombësisë shqiptare ishin 20 persona, ndërsa të kombësisë serbe ishin 3 persona.

Fotografimi dhe incizimet e tjera të paautorizuara – Neni 171

Gjatë periudhës 2007 - 2015 janë evidencuar 82 raste të veprës penale "Fotografimi dhe incizimet e tjera të paautorizuara". Nga këto janë evidencuar: 6 raste në rajonin policor të Prizrenit, 12 raste në rajonin policor të Pejës, 12 raste në rajonin policor të Mitrovicës, 13 raste në rajonin policor të Gjilanit, 16 raste në rajonin policor të Ferizajt dhe 23 raste në rajonin policor të Prishtinës.

Në cilësinë e të dyshuarit kanë qenë të përfshirë 68 persona, nga të cilët 61 ishin të gjinisë mashkullore dhe 7 të gjinisë femërore.

Nga këta persona të kombësisë shqiptare ishin 61 persona, 5 persona ishin serbë, 1 person ishte kroat dhe 1 person në kategorinë e etnive të tjera.

Në cilësinë e viktimës kanë qenë të përfshirë 38 persona, nga të cilat 23 ishin të gjinisë femërore, ndërsa 15 ishin të gjinisë mashkullore.

Të kombësisë shqiptare ishin 33 persona, të kombësisë serbe ishin 3 persona, ndërsa 2 persona ishin të kombësisë gorane.

Shkelja e urdhrave për masat e fshehura ose teknike të vëzhgimit ose të hetimit – Neni 172

Gjatë periudhës 2007-2015, janë evidencuar 4 raste të veprës penale "Shkelja e urdhrave për masat e fshehura ose teknike të vëzhgimit ose të hetimit".

Nga rastet e evidencuara, 1 rast ishte në rajonin policor të Prizrenit, 3 raste në rajonin policor të Prishtinës, ndërsa në rajonet policore të Pejës, të Mitrovicës, të Gjilanit dhe të Ferizajt nuk është evidencuar asnjë rast.

Në cilësinë e të dyshuarit kanë qenë të përfshirë 24 persona, të gjithë të gjinisë mashkullore.

Nga këta persona 11 ishin të kombësisë shqiptare, 1 person ishte serb dhe 12 në kategorinë – 'të tjerë'.

Në cilësinë e viktimës kanë qenë të përfshirë gjithsej 3 persona, të gjinisë mashkullore, të kombësisë shqiptare.

Kumtimi i paautorizuar i sekretit të punës – Neni 238

Gjatë periudhës 2007 – 2015 janë evidencuar 9 raste të veprës penale "Kumtimi i paautorizuar i sekretit të punës".

Nga rastet e evidencuara, 1 rast është evidencuar në rajonin policor të Prishtinës, 2 raste në rajonin policor të Prizrenit, 3 raste në rajonin policor të Mitrovicës dhe 3 raste në rajonin policor të Ferizajt. Në rajonin policor të Pejës dhe në atë të Gjilanit nuk është evidencuar asnjë rast.

Në cilësinë e të dyshuarit kanë qenë të përfshirë 62 persona, nga të cilët 55 ishin të gjinisë mashkullore dhe 7 të gjinisë femërore.

Nga këta persona, 57 ishin të kombësisë shqiptare, 1 person ishte serb dhe 4 persona në kategorinë 'të tjerë'.

Në cilësinë e viktimës kanë qenë të përfshirë 36 persona, nga të cilët 21 ishin të gjinisë mashkullore, ndërsa 15 të gjinisë femërore.

Të kombësisë shqiptare ishin 35 persona, ndërsa 1 person ishte serb.

Hyrja në sistemet kompjuterike - Neni 264

Gjatë periudhës kohor 2007 - 2015, janë evidencuar 122 raste të veprës penale "Hyrja në sistemet kompjuterike".

Nga rastet e evidencuara 1 rast ishte evidencuar në rajonin policor të Mitrovicës, 2 raste në rajonin policor të Prizrenit, 9 raste në rajonin policor të Ferizajt, 10 raste në rajonin policor të Gjilanit, 13 raste në rajonin policor të Pejës, ndërsa 87 raste në rajonin e Prishtinës.

Në cilësinë e të dyshuarit kanë qenë të përfshirë 150 persona, nga të cilët 148 ishin të gjinisë mashkullore dhe 2 persona të gjinisë femërore.

Nga këta, 140 persona ishin të kombësisë shqiptare, 6 persona ishin të kombësisë serbe dhe 4 persona në kategorinë 'të tjera'.

Në cilësinë e viktimës kanë qenë të përfshirë 75 persona, nga të cilët 67 ishin të gjinisë mashkullore, ndërsa 8 ishin të gjinisë femërore.

Të kombësisë shqiptare ishin 71 persona, të kombësisë boshnjake ishin 3 persona dhe një person ishte serb.

Asgjësimi, dëmtimi ose heqja e instalimeve publike – Neni 292

Gjatë periudhës 2007 – 2015, janë evidencuar 1012 raste të veprës penale "Asgjësimi, dëmtimi ose heqja e instalimeve publike".

Nga 1012 rastet e evidencuara, 71 raste janë evidentuar në rajonin policor të Gjilanit, 112 raste në rajonin policor të Ferizajt, 105 raste në rajonin policor të Prizrenit, 205 raste në rajonin policor të Pejës, 269 raste në rajonin policor të Prishtinës dhe 250 raste janë evidencuar në rajonin policor të Mitrovicës.

Në cilësinë e të dyshuarit kanë qenë të përfshirë 726 persona, prej tyre 725 janë të gjinisë mashkullore dhe 1 i gjinisë femërore.

Në cilësinë e viktimës kanë qenë të përfshirë 109 persona, nga të cilët, 99 ishin të gjinisë mashkullore, ndërsa 10 persona ishin të gjinisë femërore.

Të kombësisë shqiptare ishin 101 persona, 7 ishin të kombësisë serbe dhe 1 ishte boshnjak.

Asgjësimi apo fshehja e materialit arkivor – Neni 324

Gjatë periudhës 2007 – 2015 janë evidencuar 4 raste të veprës penale "Asgjësimi apo fshehja e materialit arkivor".

Nga 4 rastet e evidencuara, nga 1 rast është evidencuar në rajonet policore të Ferizajt, Prizrenit, Mitrovicës dhe të Prishtinës, ndërsa në rajonet policore të Gjilanit dhe të Pejës nuk është evidencuar asnjë rast.

Në cilësinë e të dyshuarit kanë qenë të përfshirë 9 persona; prej tyre 8 ishin të gjinisë mashkullore dhe 1 ishte i gjinisë femërore.

Nga këta, 8 persona ishin të kombësisë shqiptare dhe 1 person i kombësisë serbe.

Në cilësinë e viktimës ka qenë i përfshirë 1 person, i gjinisë mashkullore, i kombësisë shqiptare.

Shpërdorimi i pozitës zyrtare ose i autorizimit – Neni 339

Gjatë periudhës 2007–2015 janë evidencuar 1012 raste të veprës penale "Shpërdorim i pozitës zyrtare ose i autorizimit".

Nga 1012 rastet e evidencuara, 70 raste janë evidencuar në rajonin policor të Ferizajt, 95 në rajonin policor të Gjilanit, 98 në rajonin policor të Prizrenit, 114 në rajonin policor të Mitrovicës, 200 në rajonin policor të Pejës dhe 435 raste në rajonin policor të Prishtinës.

Në cilësinë e të dyshuarit kanë qenë të përfshirë 1762 persona, prej të cilëve 1571 ishin të gjinisë mashkullore dhe 191 ishin të gjinisë femërore.

Të kombësisë shqiptare ishin 1610, serbë 108, boshnjakë 19, romë 9, ukrainas 4, moldavë 2, dhe në kategorinë e nacionaliteteve 'të tjera' ishin 8 persona.

Në cilësinë e viktimës kanë qenë të përfshirë 103 persona, nga të cilët 65 ishin të gjinisë femërore, 38 ishin të gjinisë mashkullore.

Të kombësisë shqiptare ishin 98 persona, të kombësisë serbe ishin 4 persona dhe 1 në kategorinë e kombësive të tjera.

Zbulimi i fshehtësive zyrtare – Neni 347

Gjatë periudhës 2007–2015 janë evidencuar gjithsej 11 raste. Nga këto, 2 raste janë evidencuar në rajonin policor të Mitrovicës, 3 raste në rajonin policor të Pejës, 6 raste në rajonin policor të Prishtinës, ndërsa në rajonet policore të Ferizajt, të Gjilanit dhe të Pejës nuk është evidencuar asnjë rast.

Në cilësinë e të dyshuarit kanë qenë të përfshirë 20 persona, 15 të gjinisë mashkullore dhe 5 të gjinisë femërore.

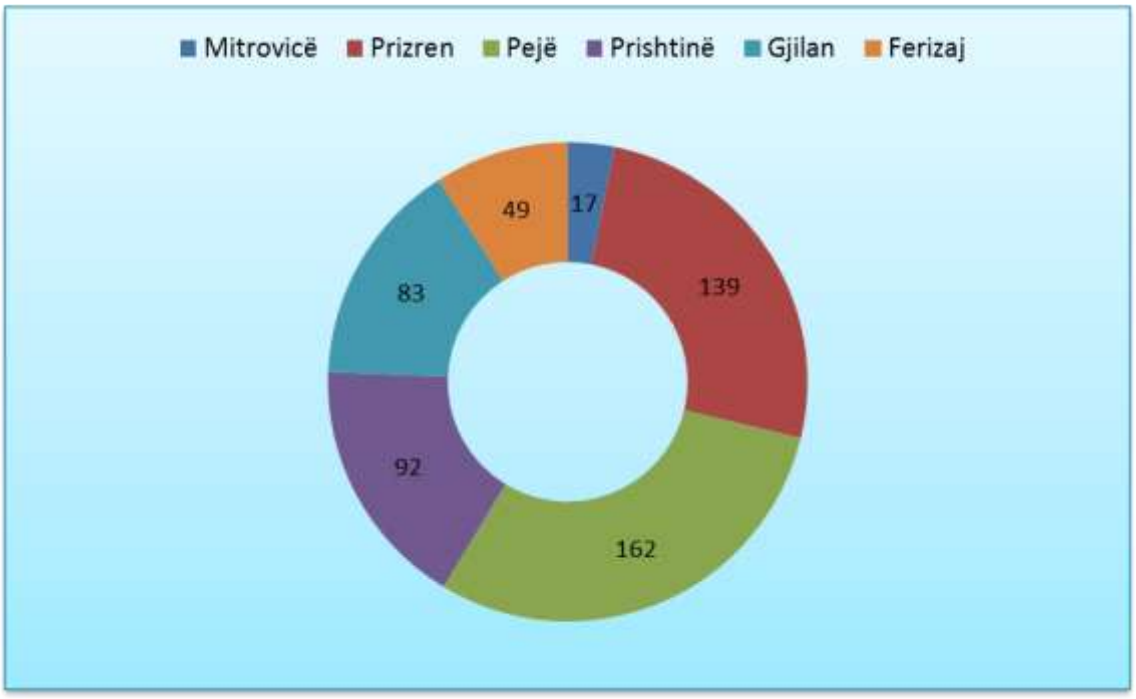
Nga këta persona, 19 janë të kombësisë shqiptare, 1 i kombësisë serbe.

Në cilësinë e viktimës kanë qenë të përfshirë 3 persona, të kombësisë shqiptare.

2 prej tyre ishin të gjinisë mashkullore, ndërsa 1 person ishte i gjinisë femërore.

5.2. Analiza empirike e të dhënave të sistemit gjyqësor

Bazuar në të dhënat e Këshillit Gjyqësor të Kosovës, nga Gjykatat e Kosovës në territorin e Kosovës gjatë periudhës 2007 – 2015, janë nxjerrë 542 vendime gjyqësore për 542 raste të veprave penale, në të cilat kanë qenë të përfshirë 622 persona.



***Burimi, Këshilli Gjyqësor i Kosovës.**

Figura 4: Çështje të gjykuara nga gjykatat për veprat penale lidhur me sigurinë e informacionit në periudhën 2007 – 201

Nga 542 çështje të gjykuara në periudhën 2007 – 2015

në rajonin policor të Prishtinës janë marrë 92 vendime gjyqësore;

në rajonin e Mitrovicës janë marrë 17 vendime gjyqësore;

në rajonin e Pejës janë marrë 162 vendime gjyqësore;

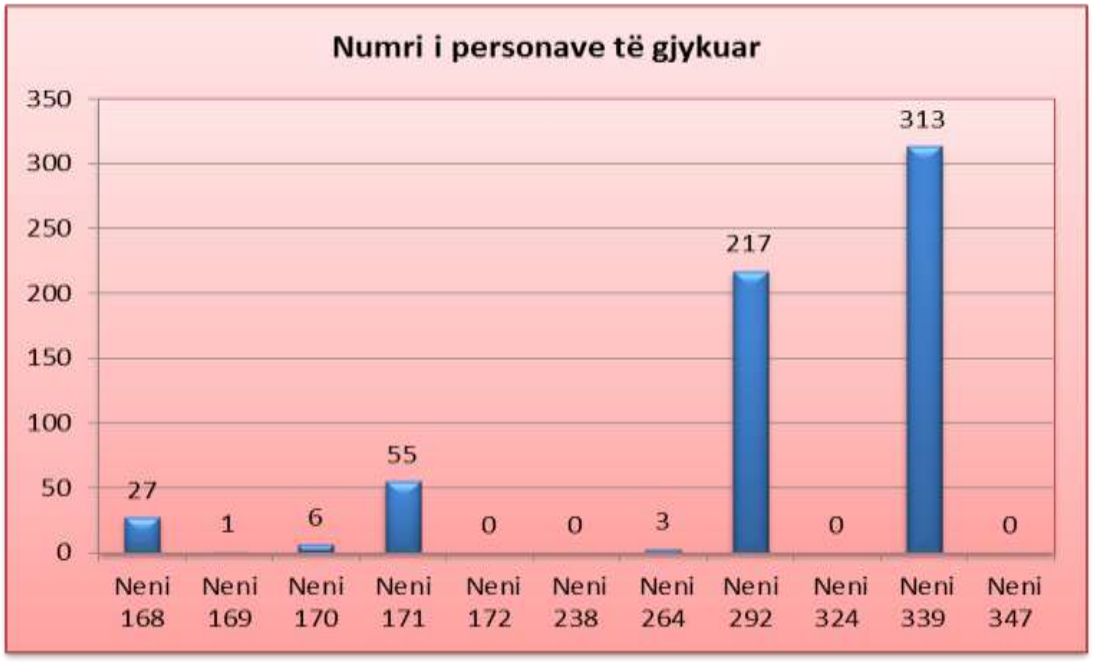
në rajonin e Prizrenit janë marrë 139 vendime gjyqësore;

në rajonin e Ferizajt janë marrë 49 vendime gjyqësore dhe

në rajonin e Gjilanit janë marrë 83 vendime gjyqësore.

Siç edhe shihet, më pak vendime gjyqësore për vepra penale të ndërlidhura me sigurinë e informacionit janë marrë në rajonin e Mitrovicës, gjithsej 17 vendime gjyqësore.

Ndërsa më shumë vendime gjyqësore për vepra penale të ndërlidhura me sigurinë e informacionit janë marrë në rajonin policor të Pejës, gjithsej 162 vendime gjyqësore.



***Burimi, Këshilli Gjyqësor i Kosovës.**

Figura 5: Numri i personave të gjykuar për veprat penale të ndërlidhura me sigurinë e informacionit

Nga shikimi i kujdesshëm që u kemi bërë të dhënave, na rezulton se nuk është evidencuar asnjë rast i vendimeve gjyqësore për këto vepra penale: "Kumtimi i paautorizuar i sekretit të punës", "Shkelja e urdhrave për masat e fshehura ose teknike të vëzhgimit apo të hetimit", "Asgjësimi apo fshehja e materialit arkivor", "Zbulimi i fshehtësive zyrtare".

Është evidencuar që për veprën penale "Zbulim i paautorizuar i informacionit të besueshëm" është marrë vetëm një vendim gjyqësor; dy raste për veprën penale "Hyrje në sistemet kompjuterike", janë marrë 2 vendime; dhe për veprën penale "Përgjimi dhe incizimi tonik i paautorizuar" janë marrë 7 vendime.

Për veprën penale "Cenimi i fshehtësisë së korrespondencës dhe i bazave të të dhënave kompjuterike" janë gjykuar 27 persona, prej të cilëve vetëm 1 person është dënuar me burg, 6 janë dënuar me kusht, 19 - me masa të tjera dhe 1 person është liruar nga akuza.

Për veprën penale "Zbulimi i paautorizuar i informacionit të besueshëm", nga 9 raste të evidencuara, është gjykuar vetëm 1 person, të cilit i është shqiptuar dënimi me masa tjera.

Për veprën penale "Përgjimi dhe incizimi tonik i paautorizuar" janë gjykuar 6 persona, prej të cilëve 3 janë dënuar me gjobë, 2 me masa tjera dhe për 1 person është vendosur me aktgjykim refuzues.

Për veprën penale "Fotografimi dhe incizimet e tjera të paautorizuara" janë gjykuar 55 persona. Dënimi me burg u është shqiptuar 8 personave, dënimi me gjobë u është shqiptuar 8 personave, dënimi me kusht u është shqiptuar 20 personave, dënimi me masa tjera u është shqiptuar 8 personave, për 9 persona është vendosur me aktgjykim refuzues dhe 2 raste janë parashkruar.

Për veprën penale “Hyrja në sistemet kompjuterike” janë gjykuar 3 persona, prej të cilëve vetëm njërit i është shqiptuar dënimi me burg; dënimi me gjobë i është shqiptuar 1 personi dhe për 1 person është vendosur me aktgjykim refuzues.

Për veprën penale “Asgjësimi, dëmtimi ose heqja e instalimeve publike” janë gjykuar 217 persona, prej të cilëve dënimi me burg u është shqiptuar vetëm 3 personave, dënimi me gjobë u është shqiptuar 106 personave, dënimi me kusht u është shqiptuar 47 personave, dënimi me masa tjera u është shqiptuar 23 personave, vërejtja e gjykatës u është shqiptuar 3 personave; për 16 persona është vendosur me aktgjykim refuzues, për 4 persona është vendosur me aktgjykim lirues, 7 raste janë parashkruar dhe 8 raste janë zgjidhur në mënyrë tjetër.

Për veprën penale “Shpërdorim i pozitës zyrtare ose i autorizimit” janë gjykuar 311 persona, prej të cilëve, dënimi me burg u është shqiptuar 31 personave, dënimi me gjobë 51 personave, dënimi me kusht 59 personave, dënimi me masa tjera u është shqiptuar 104 personave, vërejtja e gjykatës u është shqiptuar 2 personave, për 34 persona është vendosur me aktgjykim refuzues dhe për 30 persona është vendosur me aktgjykim lirues.

Në 53 raste veprat penale kundër sigurisë së informacionit janë kryer në bashkëveprim të grupeve nga dy e më tepër personave.

5.3. Analiza empirike e të dhënave të fituara me instrumentin e pyetësorit

Siç e kemi thënë më herët, një nga metodat që kemi ndjekur për grumbullimin e materialit për këtë punim, ka qenë edhe përdorimi i pyetësorit, i cili iu dërgua për

plotësim 400 zyrtarëve në Ministrinë e Punëve të Brendshme (MPB) dhe në Ministrinë e Financave, përkatësisht, në tri organizata të Sigurisë: në Policinë e Kosovës, në Inspektoratin Policor të Kosovës dhe në Doganën e Kosovës. Prej tyre kemi mundur të grumbullojmë mjaft të dhëna empirike, të nxjerra nga përgjigjet e dhëna në pyetësorët, të cilat i kemi gjykuar interesante, të vlefshme për qëllimin e punimit tonë dhe që, faktikisht, na kanë shërbyer për njohjen reale të mjaft problematikave që lidhen me temën e studimit tonë, si dhe për të nxjerrë disa përfundime dhe rekomandime.

Pyetësori është përbërë nga 24 pyetje; rezultatet e përgjigjeve nga 400 të anketuarit u evidencuan dhe u analizuan. Në vijim po sjellim disa konstatime dhe problematika.

Struktura gjinore e pjesëtarëve të organizatave të sigurisë, të anketuar, që i kanë plotësuar pyetësorët është 360 meshkuj dhe 40 femra.

Përgatitja arsimore e të anketuarve është:

shkollimin e mesëm e kanë 114 veta apo 28.5%,

nivelin bachelor të shkollimit e kanë 208 veta apo 52%,

nivelin master e kanë 76 veta apo 19 %,

ndërsa 2 veta apo 0.5% janë duke vijuar studimet e doktoratës (PhD Candidate).

Marrë në tërësi 324 të anketuar apo 71.5 % janë me përgatitje shkollore superior, fakt ky që ka rëndësi të madhe, sepse si rezultat i këtij hulumtimi del se 71.5 % të zyrtarëve të organizatave të sigurisë në Kosovë kanë përfunduar shkollimin universitar.

Detyrat (pozitat) të cilat aktualisht të anketuarit i kryejnë në organizatat e tyre:

Nga 400 të anketuarit që plotësuan pyetësorin, 100 persona apo 25% i përkasin nivelit administrativ dhe teknik të menaxhimit; 134 të anketuar apo 35.5% e tyre i përkasin nivelit të parë të menaxhimit, respektivisht, janë mbikëqyrës të nivelit të parë,

120 të anketuar apo 30 % e tyre janë mbikëqyrës të nivelit të mesëm dhe 46 të anketuar apo 11.5 % e tyre janë mbikëqyrës të nivelit të lartë të menaxhimit.

Pyetjes *"Cila është përvoja juaj në shkëmbim të informacioneve?"*, i janë përgjigjur 400 të anketuar. Nga përgjigjet e tyre rezulton se: 80 të anketuar apo 20 % kanë përvojë nga 1 deri 3 vjet; 38 të anketuar apo 9.5% kanë përvojë nga 3 deri 5 vjet; 100 të anketuar apo 25% kanë përvojë nga mbi 5 vjet dhe 182 të anketuar apo 45.5% kanë përvojë nga mbi 10 vjet.

Pyetjes *"A keni njohuri për veprat penale të ndërlidhura me sigurinë e informacionit?",* i janë përgjigjur 399 të anketuar, nga përgjigjet e të cilëve rezulton se: 41 të anketuar apo 10.3 % nuk kanë njohuri; 112 të anketuar apo 28% kanë njohuri elementare; 196 të anketuar apo 49% kanë njohuri të mira; 50 të anketuar apo 12.5% kanë njohuri të shkëlqyeshme.

Për pyetjen *"A keni vijuar ndonjë trajnim në fushën e sigurisë së informacioneve?",* janë përgjigjur 400 të anketuar, nga përgjigjet e të cilëve rezulton se: 257 të anketuar apo 64.3 % nuk kanë vijuar asnjë trajnim; 93 të anketuar apo 23.3 % kanë vijuar tri trajnime; 36 të anketuar apo 9% kanë vijuar më shumë se tri trajnime; 14 të anketuar apo 3.5% kanë vijuar më shumë se 5 trajnime.

Pyetjes *"A keni marrë pjesë në ndonjë konferencë, seminar apo punëtori të përbashkët me organizatat tjera të sigurisë, ku ka qenë temë informacioni, siguria e informacionit apo shkëmbimi i informacioneve?"* i janë përgjigjur 400 të anketuar, nga përgjigjet e të cilëve rezulton se: 259 të anketuar apo 64.8 % nuk marrë pjesë në ndonjë konferencë, seminar apo punëtori të përbashkët me organizatat tjera; 100 të anketuar apo 25 % kanë marrë pjesë në një konferencë, seminar apo punëtori të përbashkët: 36 të anketuar apo 9%, kanë marrë pjesë në një konferencë, seminar apo punëtori të

përbashkët dhe 5 të anketuar apo 1 % kanë marrë pjesë në mbi 5 konferenca, seminare apo punëtori të përbashkëta.

Pyetjes *"Cili është niveli i komunikimit dhe shkëmbimit të informacioneve mes të anketuarve?"*, iu përgjigjën të 400 personat dhe nga përgjigjet rezulton se: 106 të anketuar apo 26.5 % kanë deklaruar se niveli është i ulët; 212 të anketuar apo 53 % kanë deklaruar se është niveli i mesëm, 56 të anketuar apo 14% kanë deklaruar se është niveli i lartë, ndërsa 22 të anketuar apo 5.5% kanë deklaruar se nuk shkëmbejnë informacione.

Për pyetjen *"Si u shpërndahen informacionet njësive tjera?",* përgjigjet e 400 të anketuarve, ndahen kështu: 165 të anketuar apo 41.3% deklarojnë se shpërndarja bëhet përmes rrjetit të brendshëm; 129 të anketuar apo 32.3% deklarojnë se bëhet përmes intranetit; 99 të anketuar apo 24.8% deklarojnë se bëhet përmes formave tjera.

Në 73.5% të rasteve rezulton se shpërndarja e informacioneve bëhet përmes rrjetit të brendshëm dhe intranetit, pasi këto rrjete ofrojnë standarde të larta të sigurisë në shkëmbimin e informacioneve.

Pyetjes *"A shkëmbeni informacione të klasifikuara me organizatat e sigurisë?"* i janë përgjigjur 400 të anketuar dhe: 305 të anketuar apo 76.3% deklarojnë se shkëmbejnë bazuar në ligjet e aplikueshme dhe në Procedurat Standarde të Operimit (PSO), ndërsa 94 të anketuar apo 23.5% deklarojnë se nuk kanë shkëmbyer asnjëherë informacione të klasifikuara.

Nga analiza e përgjigjeve të pranuara rezulton se 76.3% e të anketuarve shkëmbejnë informacione të klasifikuara dhe se shpërndarja e tyre bëhet duke u bazuar në ligjet edhe PSO-të e aplikueshme.

Pyetjes *"A keni njohuri për ndonjë marrëveshje të bashkëpunimit për shkëmbim të informacioneve mes organeve të sigurisë?",* i janë përgjigjur 400 të anketuar. Nga përgjigjet rezulton se: 117 të anketuar apo 29.3 % nuk kanë njohuri; 192 të anketuar apo 48 % kanë njohuri elementare; 85 të anketuar apo 21.3 % kanë njohuri të mira; 5 të anketuar apo 1.3 % kanë njohuri të shkëlqyeshme.

Bazuar në faktin se mbi 77.3 % e të anketuarve të organeve të sigurisë nuk kanë njohuri apo se kanë vetëm njohuri elementare për marrëveshje të bashkëpunimit për shkëmbim të informacioneve mes organeve të sigurisë, del e domosdoshme që të punohet sistematikisht që ata të njoftohen në mënyrë të hollësishme për të gjitha marrëveshjet e bashkëpunimit për shkëmbim të informacioneve mes organeve të sigurisë.

Pyetjes *"A keni pasur shkëmbim të informatave me agjencionet policore të shteteve tjera?",* i janë përgjigjur 400 të anketuar. Nga përgjigjet rezulton: 219 të anketuar apo 54.8% kanë deklaruar se bëhet shkëmbim; 104 të anketuar apo 26% kanë deklaruar se bazuar në pozitën aktuale ata nuk shkëmbejnë informacione; 212 të anketuar apo 53% kanë deklaruar se është nivel i mesëm; 56 të anketuar apo 14% kanë deklaruar se është nivel i lartë, dhe 76 të anketuar apo 19 % kanë deklaruar se asnjëherë nuk shkëmbejnë informacione.

Pyetjes *"A është vërejtur trend i zvogëlimit të krimit në Republikën e Kosovës pas bashkëpunimit ndërkombëtar?",* i janë përgjigjur 398 të anketuar, nga të cilët 326 apo 81.5 % deklarojnë se është vërejtur trend i zvogëlimit të krimit; 71 të anketuar apo 17.8% deklarojnë se nuk është vërejtur trend i zvogëlimit të krimit.

Që bashkëpunimi ndërkombëtar ndikon pozitivisht në luftimin, parandalimin dhe pakësimin e krimeve shihet edhe në faktin se 81.5 % të anketuarve e kanë konstatuar

dhe pohojnë se si rezultat i bashkëpunimit ndërkombëtar ka pasur ulje të numrit të krimeve.

Pyetjes *"A paraqet pengesë për shkëmbim të informatave me organizatat ndërkombëtare policore, mosanëtarësimi i Republikës së Kosovës?",* i janë përgjigjur 400 të anketuar, nga të cilët: 281 apo 70.3% thonë se paraqet pengesë; 27 të anketuar apo 6.8 % deklarojnë se nuk paraqet pengesë; 46 të anketuar apo 11.5 % deklarojnë se bashkëpunimi është i kufizuar; ndërsa 44 të anketuar apo 11% deklarojnë se ka shumë barriera në bashkëpunim.

Pyetjes *"Cilat janë sfidat e organizatës suaj për sigurinë e informacioneve?",* i janë përgjigjur 400 të anketuar, nga të cilët: 195 apo 48.8 % deklarojnë se sfida kryesore është mungesa e memorandumeve të bashkëpunimit; 107 të anketuar apo 26.8% deklarojnë se është mungesa e kapaciteteve teknike; dhe 88 të anketuar apo 22% deklarojnë se zbrazëtitë në legjislacion paraqesin sfidën kryesore për sigurinë e informacioneve.

Pyetjes *"A mendoni se duhet hartuar një strategji nacionale në fushën e sigurisë së informacionit",* i janë përgjigjur 400 të anketuar, nga të cilët: 301 të anketuar apo 75.3 % deklarojnë se hartimi i një strategjie të tillë duhet të jetë prioritet kombëtar; 95 të anketuar apo 23.8% thonë se është e nevojshme; 4 të anketuar apo 1.% deklarojnë se nuk është e nevojshme.

Pyetjes *"Në cilat fusha janë shënuar rezultate konkrete në bashkëpunim me institucionet e tjera?",* i janë përgjigjur 312 të anketuar, nga të cilët: 77 të anketuar apo 19.3 % deklarohen pozitivisht, janë shënuar në parandalimin dhe luftimin e krimit; 20 të anketuar apo 5.6% deklarojnë se janë shënuar në parandalimin dhe luftimin e narkotikëve, të trafikimit të qenieve njerëzore dhe të kontrabandimit me emigrantë; 23

të anketuar apo 5.8 % pohojnë se janë shënuar në luftimin e krimit të organizuar dhe terrorizmit; 18 të anketuar apo 4.5% deklarojnë se janë shënuar rezultate në bashkëpunim mes INTERPOL-it, EUROPOL-it dhe Policisë së Kosovës (PK); 22 të anketuar apo 5.6 % pohojnë se janë shënuar rezultate në shkëmbimin e informacioneve me INETRPOL-in; 16 të anketuar apo 4.1 % deklarojnë se janë shënuar rezultate në parandalimin dhe luftimin e terrorizmit; 22 të anketuar apo 5.6% deklarojnë se janë shënuar rezultate në parandalimin e krimit të organizuar; 4 të anketuar apo 1.1 % deklarojnë se janë shënuar rezultate në arrestimin e personave të kërkuar, 14 të anketuar apo 3.9 deklarojnë se janë shënuar rezultate në hetimin e krimit; 15 të anketuar apo 5.8 deklarojnë se kanë shkëmbyer të dhëna në lidhje me verifikimin dhe identifikimin e personave; 7 të anketuar apo 2.3 se janë shënuar rezultate në bashkëpunim me ILECU-n, 5 të anketuar apo 1.3 deklarojnë se nuk kanë shkëmbyer informacione asnjëherë, 2 të anketuar apo 0.6 % deklarojnë se janë shënuar rezultate në bashkëpunim në mes të PK-së dhe AKI-së në luftimin e krimit, 2 të anketuar apo 0.6% deklarojnë se shkëmbimi është bërë në përgjigje të kërkesave të shteteve të huaja, 2 të anketuar apo 0.6 % deklarojnë se janë shënuar rezultate në luftimin e krimeve ekonomike dhe terrorizmit, 4 të anketuar apo 1.1% deklarojnë se janë shënuar rezultate në fushën e sigurisë, 3 të anketuar apo 0.8 deklarojnë se janë shënuar rezultate në fushën e luftimit të krimeve kibernetike dhe 21 të anketuar apo 5.4% deklarojnë se nuk kanë informata apo ‘nuk e dinë’.

Pyetjes *“Sipas përvojës tuaj, ku ka më së shumti ngecje në fushën e shkëmbimit të informacioneve?”,* i janë përgjigjur 310 të anketuar, nga të cilët, 51 të anketuar apo 13.4% pohojnë se në fushën e shkëmbimit të informacioneve mungojnë informatat kthyese apo fidbeku; 22 të anketuar apo 5.6 % pohojnë se ngecjet vijnë nga

mosanëtarësimi i PK-së në organizata ndërkombëtare, 47 të anketuar apo 11.6 si shkak të ngecjeve japin mungesën e komunikimit, të bashkëpunimit dhe të besimit të ndërsjellë; 19 të anketuar apo 3.8% deklarojnë se ka ngecje te klasifikimi i informacioneve dhe në ruajtjen e informacioneve konfidenciale dhe sekrete; 15 të anketuar apo 3.5 % deklarojnë se ngecjet vijnë nga mosimplementimi i Strategjisë Policimi i Udhëhequr nga Inteligjenca dhe PSO-të; 18 të anketuar apo 3.6% pohojnë se ka ngecje në shkëmbim të informacioneve mes njësive, drejtorive në kuadër të organizatave të sigurisë; 9 të anketuar apo 2.4 % deklarojnë si ngecje kryesore vonesat në përgjigje dhe në trajtimin e informative; 6 të anketuar apo 1.7% i gjejnë ngecjet te burokracia në menaxhimin e mesëm dhe të lartë; dhe 4 të anketuar apo 1% e tyre deklarojnë se ngecjet vijnë ngaqë shteti i Kosovës ende nuk konsiderohet palë plotësisht e barabartë.

Pyetjes *"Çka do të duhej të ndryshonte që shkëmbimi i informacioneve në organizatën tuaj të jetë më efikas?",* nga 400 të anketuar, i janë përgjigjur 314, nga të cilët: 111 të anketuar apo 28.6 % e tyre deklarojnë se duhet të avancohen bashkëpunimi dhe besimi reciprok brenda organizatës së sigurisë dhe ai ndërinstitucional; 49 apo 12.7 % deklarojnë se duhet funksionalizuar sistemi i informatës kthyese; 29 të anketuar apo 8.5 % e tyre kërkojnë të avancohet bashkëpunimi në fushën e implementimit të legjislacionit në praktikë, bazuar në faktin se në aspektin teorik ekziston një infrastrukturë e mirë ligjore, por sfidë mbetet implementimi i saj në praktikë; 18 të anketuar apo 4.8 % deklarojnë se duhen avancuar kapacitetet teknike dhe profesionale në fushën e sigurisë së informacioneve dhe të shkëmbimit të informacioneve; 13 të anketuar apo 3.6 % deklarojnë se duhen shtuar kapacitetet me trajnime të ndryshme në fushën e sigurisë së informacioneve dhe të shkëmbimit të informacioneve; 10 të

anketuar apo 2.6 % deklarojnë se duhet të anëtarësohet Kosova në organizata rajonale dhe ndërkombëtare (Inerpol, Europol, Frontex etj.), 6 të anketuar apo 1.4% deklarojnë se duhet të organizohen takime më të shpeshta.

Pyetjes *"Me cilat organizata të sigurisë keni pasur shkëmbim të informacioneve?",* nga 400 të anketuar i janë përgjigjur 375; nga të cilët 161 apo 43.3 % deklarojnë se kanë pasur me drejtori të ndryshme në kuadër të PK-së dhe kryesisht me Drejtorinë për Inteligjencë dhe Analiza; 67 të anketuar apo 17 % deklarojnë se shkëmbimin e bëjnë me CIA-n, FB-në, AKI-në dhe PK-në; 52 të anketuar apo 14.6 % deklarojnë se shkëmbimin e bëjnë me FSK-në, EULEX-in, KFOR-in, OSBE-në; 15 të anketuar apo 4.2 % deklarojnë se kanë shkëmbime me PK-në dhe Doganën e Kosovës; 14 të anketuar apo 3.7% deklarojnë shkëmbime me INTERPOL-in dhe EUROPOL-in; 13 të anketuar apo 3.3% deklarojnë se e bëjnë shkëmbimin me IPK-në; 7 të anketuar apo 1.8 % deklarojnë se kanë shkëmbime me AKI-në dhe NJIF-in; 4 të anketuar apo 1.1% deklarojnë se bëjnë shkëmbime me Prokurori dhe Gjykata, 6 të anketuar apo 1.5% deklarojnë se shkëmbimin e informacioneve e bëjnë me AKI-në dhe FSK-në.

KAPITULLI 6: ASPEKTE FENOMENOLOGJIKE DHE ETIOLOGJIKE TË VEPRAVE PENALE TË NDËRLIDHURA ME SIGURINË E INFORMACIONIT

6.1. Aspekte të përgjithshme fenomenologjike të veprave penale të ndërlidhura me sigurinë e informacionit

Ecuria dhe dinamika e kryerjes së këtyre veprave penale

Kryerja e veprave penale të ndërlidhura me sigurinë e informacionit, si pjesë e kriminalitetit të përgjithshëm, ka shkaktuar dhe vazhdon të shkaktojë pasoja të rënda jo vetëm për individët, për institucionet afariste, për ato shtetërore, por edhe për sigurinë kombëtare. Rrezikshmëria e lartë shoqërore nga pasojat e këtyre veprave penale reflektohet në mënyrat e kryerjes së këtyre veprave, pasi autorët nuk kanë nevojë të rrezikojnë dhe të dërgohen afër vendeve ku do të realizohen sulmet kundër sistemeve ku ruhen informacionet e klasifikuara.

Për trajtimin e këtij fenomeni, kontribut të veçantë japin shkencat juridiko-penale përmes studimit të fenomenologjisë kriminale, të ecurisë dhe dinamikës së këtij kriminaliteti.

Fenomenologjia kriminale është pjesë e kriminologjisë dhe merret me studimin e formave të paraqitjes së kriminalitetit, me strukturën dhe dinamikën e tij (Halili, 2005: 115).

Kjo formë e krimit nuk njeh kufi territorialë dhe viktimë potenciale e tij mund të jetë çdo person a organizatë. Prandaj për ta luftuar dhe parandaluar atë kërkohet

angazhim i përditshëm i strukturave të specializuara, por edhe studime që ofrojnë zgjidhje afatgjata. Këtij qëllimi do t'i shërbente edhe ndërmarrja e një studimi të mirëfilltë në bashkëpunim me institucionet qeveritare dhe joqeveritare, duke u ndalur jo vetëm në aspektin sasior të përhapjes dhe të pranisë së këtij krimi, por edhe në aspektin e përcaktimit të masave dhe metodave për përballimin e këtij krimi që ka marrë dimensione ndërkombëtare. Pikërisht ky dimension e bën edhe më të vështirë luftën kundër tij.

Në vendet e zhvilluara janë bërë studime për format, për shtrirjen dhe dinamikën e krimeve të ndërlidhura me sigurinë e informacionit. Megjithë specifikat e ndryshme që ato, strukturat tona duhet të njihen me to dhe të nxjerrin prej tyre konkluzione për të pasuruar përvojën lidhur me njohjen e formave të këtij krimi dhe të metodave që ndjekin autorët e tij.

Në vendin tonë, megjithë përpjekjet e mira që po bëhen në këtë fushë, ka mjaft probleme dhe mangësi. Gjatë hulumtimit të kësaj teme, na ka dalë se në institucione të ndryshme të Kosovës ekzistojnë rreth 25 baza të dhënash, por mungon një strukturë e mirëfilltë e të dhënave të unifikuara, që do të ndihmonte njohjen reale të shtrirjes së këtij krimi në vend dhe që do të lehtësonte kryerjen e një studimi rreth tij. Mungesa e kësaj strukture unike të të dhënave dëmton shumë punën e institucioneve të sigurisë, të cilat, vërtet, kanë bazën e tyre të të dhënave, por kjo nuk mjafton, nëse nuk unifikohen në një strukturë të vetme, që bën të mundur shfrytëzimin e tyre në nivel kombëtar. Por duhet thënë se dhe në secilin institucion nuk ekziston një bazë unike e të dhënave, çka e bën edhe më të vështirë njohjen e këtij kriminaliteti, shtrirjen dhe përmasat e tij. Puna e bërë deri tani, bazuar në të dhënat e mbledhura në këto institucione, ka ndihmuar për të konstatuar se kjo formë e kriminalitetit ka shënuar rritje gjatë viteve të fundit, krahasuar

me vitet paraprake, gjë që rezulton nga rastet e evidencuara dhe të shqyrtuara nga institucionet vendore (Statistikat e Policisë së Kosovës, 2014), megjithatë nuk është e mjaftueshme për zbulimin në shkallën e duhur të mënyrave të kryerjes së këtij krimi, të metodave që përdorin autorët e tij, me qëllim arritjen e standardeve që kërkon lufta ndaj kriminalitetit.

Mënyrat e kryerjes së këtyre veprave penale

Mënyrat e kryerjes së veprave penale të ndërlidhura me sigurinë e informacionit janë të lloj-llojshme, ato prekin interesa shoqërore të ndryshme. Si autorë të këtyre veprave janë persona kryesisht me aftësi profesionale në fushën e teknologjisë informatike, por edhe persona me njohuri të limituara në këtë fushë. Zhvillimi i teknologjisë dhe i softuerëve kompjuterikë në qasje apo në interceptim të sistemeve kompjuterike, në një mënyrë apo në një tjetër, ka mundësuar rritjen e vëllimit dhe të dinamikës së veprave penale të ndërlidhura me sigurinë e informacionit, në veçanti të krimeve kibernetike. Varësisht prej mënyrës së kryerjes, në rastet kur krimi ndërlidhet me kompjuter, veprat penale kur krimi lidhet me përmbajtjen e paligjshme dhe veprat penale ku kompjuteri përdoret si objekt për kryerjen e veprës penale, në të shumtën e rasteve kemi të bëjmë me tipa të autorëve me aftësi profesionale dhe, varësisht prej motiveve dhe qëllimit, mund t'i veçojmë si: kryerës amatorë, profesionalë dhe hakerë (Vula, 2010: 120).

Në rastet e amatorëve, kemi të bëjmë me subjekte të profesioneve të ndryshme jo doemos të lidhur me fushën e teknologjisë informatike, por që, për shkaqe dhe rrethana

personale, social-ekonomike, shndërrohen në autorë potencialë të krimeve të ndërlidhura me sigurinë e informacionit dhe, në të shumtën e rasteve, veprojnë si bashkëpunëtorë të kriminelëve profesionistë apo hakerëve, të cilët i shfrytëzojnë më shpesh në përdorimin kartash të klonuara në bankomate. Në këto raste, mundësitë e kapjes së autorëve janë më të mëdha, ngaqë ata nuk arrijnë t'i mbulojnë gjurmët.

Sa u përket autorëve profesionistë të veprave penale të ndërlidhura me sigurinë e informacionit, mund të themi se ata dallojnë nga ata amatorë, pasi, si profesionistë, ata kryejnë rregullisht vepra të tilla, duke i realizuar me veprime dhe mënyra të sofistikuara. Këtë aktivitet ata e kanë kthyer në profesion dhe në mjeshtëri të përhershme e tyre, për të siguruar të ardhura kryesore apo suplementare për jetesën e tyre; ata karakterizohen nga qëndrueshmëria e mjeshtërisë kriminale apo specializimi, domosdoshmëria e dijeve dhe shprehive praktike apo të kualifikimit (Vula, 2010: 120).

Në saje të aftësive të avancuara dhe të mundësive për të lëvizur nëpër rajone të ndryshme, autorët profesionistë shfrytëzojnë të gjitha mjetet dhe mënyrat që ofron komunikimi bashkëkohor për kryerjen e veprave penale, përfshirë edhe përcjelljen dhe bartjen e informatave përmes internetit dhe komunikimeve të tjera elektronike. Ata janë në gjendje që përmes hapësirës kibernetike, të kryejnë aktivitete ilegale, si falsifikim dokumentesh, mashtrime të viktimave përmes internetit, mbulim të aktiviteteve financiare të bizneseve, shpërndarje materialesh online si dhe komunikime për të organizuar veprimtari të tilla. "Së fundi, hakerët njihen si persona me njohuri të veçanta për sistemet kompjuterike dhe me aftësi për manipulime të programeve të ndryshme, por, për nga mënyra e kryerjes, ata mund të klasifikohen në hakerë kopjues, vjedhës kompjuterikë, trafikantë, sabotues, hakmarrës dhe spiunë (Vula, 2010: 125).

Veprimtaria e këtyre autorëve profesionistë dhe amatorë ka çuar në rritjen e numrit të veprave penale të ndërlidhura me sigurinë e informacionit dhe e ka bërë më të vështirë zbulimin dhe kapjen e tyre.

Format e kryerjes së këtyre veprave penale

Në saje të zhvillimit të teknologjisë informatike dhe të përdorimit të sistemeve kompjuterike, shfaqen edhe forma të reja të veprave penale të ndërlidhura me sigurinë e informacionit përmes krimit kibernetik.

Sipas autorit Bequai A., ekzistojnë pesë faza që konsiderohen si pika kritike për keqpërdorim të sistemeve kompjuterike: hyrja, dalja, programimi, përdorimi dhe bartja (Vula, 2010: 126).

Në fazën e hyrjes, autorët mund të kryejnë plotësim, ndryshim, ndërrim apo fshirje të dhënash. Të tilla vepra ilegale ndodhin kryesisht në biznese apo vende pune, duke bërë modifikime rrogash, shtim të numrave fiktivë të të punësuarve, rritje honorari, falsifikim dokumentesh për shërbime bankare, transferim pagesash në llogari të ndryshme etj.

Në fazën e daljes autorët mund të marrin në mënyrë të paautorizuar të dhëna konfidenciale biznesi, të dhëna të klientëve, me qëllim përfitimi, duke ua prezantuar ato konkurrentëve apo agjentëve që kanë interes për lista të punonjësve apo të dhëna për zhvillime të softuerëve, të programeve, me qëllim sabotimi apo shantazhi.

Në fazën e programimit nevojitet një qasje më profesionale, për shkak se kemi të bëjmë me ndërrim, fshirje, modifikim apo sabotim të programeve. Në këto raste autorët

përdorin softuerë dhe programe destruktive, siç janë viruset, karremat dhe forma të tjera, duke shkaktuar dëme të mëdha.

Në fazën e përdorimit, nga përdorues zyrtarë apo privatë, ndodh shfrytëzimi i paautorizuar i sistemeve kompjuterike, por edhe gjë që ndodh edhe nga pakujdesia në rastin e hapjes së ueb-faqeve, linqeve dhe shkarkimit të të dhënave nga burime të panjohura, që mund të hapin dyert për sulm kompjuterik.

Së fundi, faza e bartjes konsiderohet si faza më e ndjeshme, ngaqë kemi të bëjmë me cenimin e lidhjeve të komunikimit përmes prezantimit të rrejshëm, mbulimit të kanaleve, infiltrimit aktiv dhe përgjimit.

Në të gjitha rastet është shqetësues fakti se në mënyrë të paautorizuar bëhet përcjellja e informatave dhe keqpërdorimi i tyre, duke u cenuar kështu fshehtësia e të dhënave që shkakton shqetësim për përdoruesit, afarizmin, shërbimet bankare dhe institucionet shtetërore.

Vendi i kryerjes së këtyre veprave penale

Karakteristikë kryesore e veprave penale të ndërlidhura me sigurinë e informacionit është efekti i tyre global dhe, për këtë arsye, kërkon një fokusim ndërkombëtar, mbasi, ndër tjera, autorët shfrytëzojnë metoda nga më të ndryshmet, që nuk kufizohen në një tërësi territorial. Kryerja e këtyre veprave penale mund të ndodhë larg vendit të ngjarjes. Kjo i bën provat më të paqëndrueshme dhe krijon vështirësi në sigurimin e tyre për kapjen dhe dënimin e autorëve, siç ka ndodhur me rastet e njohura të mashtrimit me e-mail “419 scams”, autorë të të cilave në rastet më të shpeshta janë

nga SHBA, Anglia, Nigeria, Ishujt Ivory, Togoja, Afrika e Jugut, Norvegjia dhe Spanja (Brenner, 2010: 83).

Meqenëse kjo formë e krimit ka efekt transnacional, është më specifike dhe nuk mund të analizohet me veçori si veprat e tjera penale, siç janë: mobiliteti shoqëror, veçoritë rajonale, kohore apo sezonale, mund të konstatojmë se vetë hapësira e internetit dhe qasja në sisteme kompjuterike kudo në botë përbën në vete një zonë kibernetike kriminale", po qe se fillimisht mungojnë: legjislacioni adekuat që i penalizon këto veprime kriminale, mekanizmat implementues dhe mbrojtja e duhur nga vetë përdoruesit dhe nga kompanitë përkatëse për sigurinë.

6.2. Aspekte konkrete fenomenologjike të autorëve të veprave penale të ndërlidhura me sigurinë e informacionit

Për parandalimin dhe luftimin e veprave penale të ndërlidhura me sigurinë e informacionit nevojitet një studim i veçorive individuale të personave që merren me këtë formë të krimit, në mënyrë që të përcaktohen profilet e autorëve të tyre.

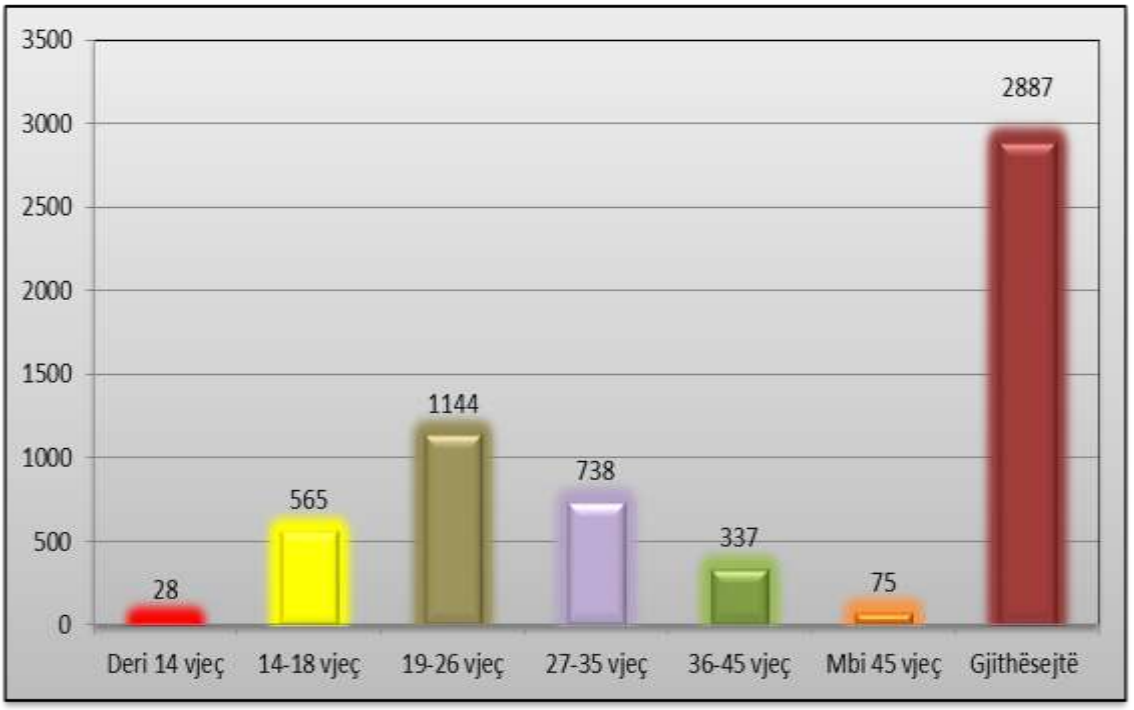
Duke pasur parasysh aspektet e përgjithshme të këtyre veprave, në aspektin konkret jemi fokusuar te veçoritë individuale të autorëve të veprave penale të ndërlidhura me sigurinë e informacionit në Kosovë, siç janë: mosha, gjinia, niveli arsimor dhe përkatësia sociale dhe etnike.

Të gjitha këto, si një tërësi e veçorive individuale, studiohen për trajtimin dhe format e paraqitjes së krimit, në përgjithësi, dhe të strukturës së autorëve, në veçanti.

Mosha e personave të dyshuar të këtyre veprave penale

Mosha është një karakteristikë e veçantë kur bëhet fjalë për fenomenin kriminal. Sipas studimeve empirike, praktikës gjyqësore, statistikës kombëtare apo të autorit D. Parker, mbështetur edhe nga autori A. Bequai, autorët e veprave penale të ndërlidhura me sigurinë e informacionit dhe, në veçanti, autorët e veprave penale të krimit kibernetik i takojnë moshës midis 15 deri 45 vjeç (Vula, 2010: 118). Bazuar në të dhënat statistikore dhe në kërkimet empirike kriminologjike në botë, shihet se mosha më e pranishme në veprimet kriminale është ajo prej 25 deri 30 vjeç, pastaj grupi i moshës 30 deri 50 vjeç dhe më pak grupi i moshës përtej 60 vjeç (Halili, 2008: 131).

Bazuar në të dhënat e Policisë së Kosovës, rezulton se në periudhën 2007 – 2015, numri i personave të dyshuar për veprat penale të ndërlidhura me sigurinë e informacionit është 2887. Nga ky numër, 1144 persona të dyshuar i takojnë grupmoshës 19-26 vjeç; 738 persona të dyshuar i takojnë grupmoshës 27-35 vjeç; 565 persona të dyshuar i takojnë grupmoshës 14-18 vjeç; 337 persona të dyshuar i takojnë grupmoshës 36-45 vjeç; 75 persona të dyshuar i takojnë grupmoshës mbi 45 vjeç dhe 28 persona i të dyshuar i takojnë grupmoshës deri në 14 vjeç.

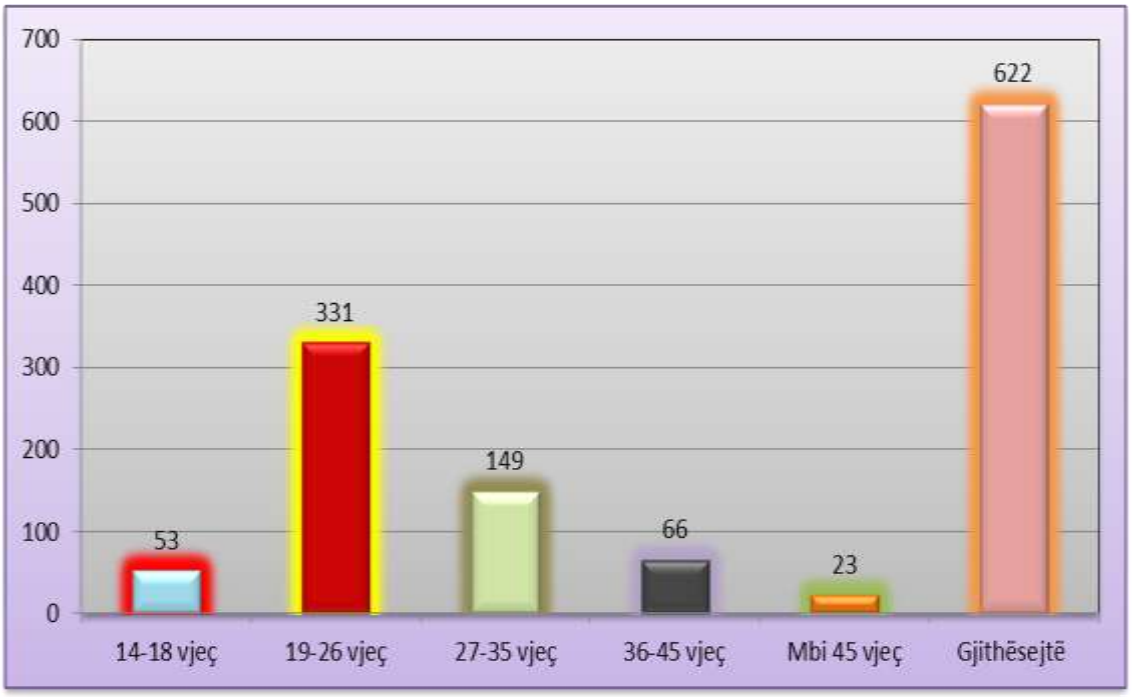


***Burimi: Policia e Kosovës 2007 – 2015.**

Figura 6: Mosha e të dyshuarve për veprat penale të ndërlidhura me sigurinë e informacionit gjatë periudhës 2007 – 2015.

Mosha e personave të dënuar (autorëve) të këtyre veprave penale

Bazuar në të dhënat e Këshillit Gjyqësor të Kosovës, nga 622 personat për të cilët është marrë vendim gjyqësor, rezulton se 331 prej tyre i takojnë grupmoshës 19-26 vjeç; 149 persona takojnë grupmoshës 27-35 vjeç; 53 persona i takojnë grupmoshës 14-18 vjeç; 66 persona i takojnë grupmoshës 36-45 vjeç dhe 23 persona i takojnë grupmoshës mbi 45 vjeç.



***Burimi: Këshilli Gjyqësor i Kosovës, 2007 – 2015**

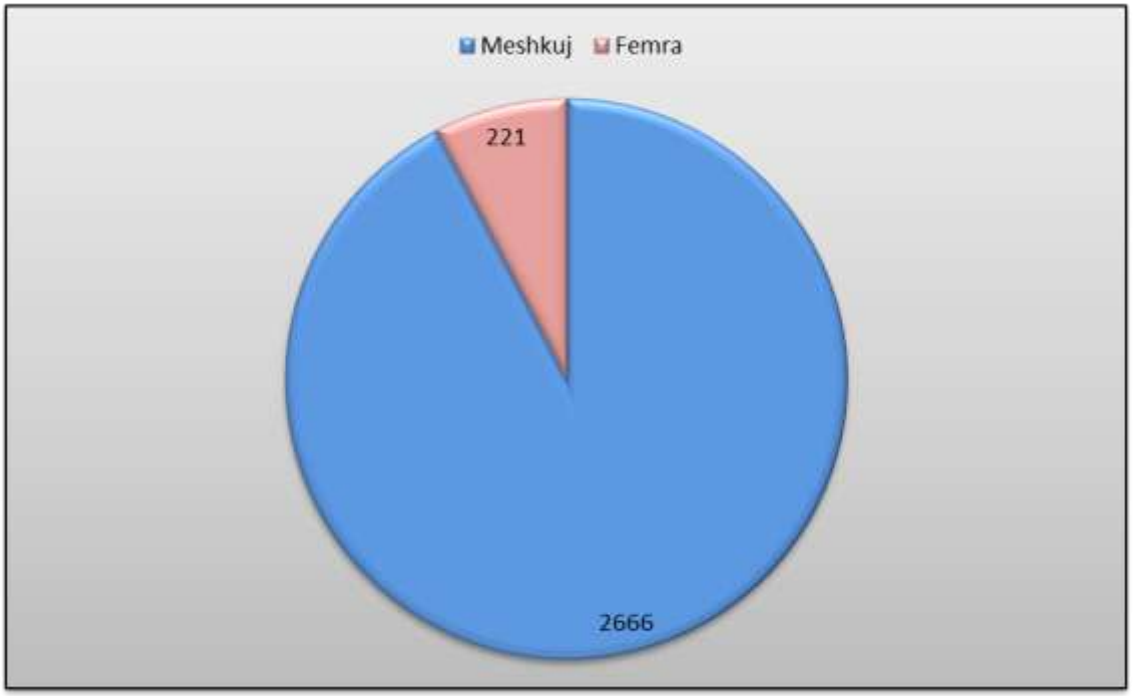
Figura 7: Mosha e të dënuarve për vepra penale të ndërlidhura me sigurinë e informacionit, në periudhën 2007 – 2015

Gjinia e personave të dyshuar, e viktimave dhe e autorëve të këtyre veprave penale

Studimet e deritanishme empirike dhe statistikore mbi veçoritë individuale të autorëve, sidomos të gjinisë së tyre, vetëm sa e mbështesin faktin se kriminaliteti në këtë fushë është dukuri tipike e gjinisë mashkullore, por nuk përjashtohet mundësia e kryerjes së veprave penale të ndërlidhura me sigurinë e informacionit edhe nga femra. Kjo është dëshmuar edhe nga të dhënat e mbledhura nga statistikat vendore në prokurori dhe gjykata, ku janë identifikuar raste të që vepra të tilla kanë kryer femra. Ajo që e karakterizon autoret e gjinisë femërore të këtyre veprave është fakti se ato më shumë

janë të përfshira si bashkautorë, në kuptimin se kanë ofruar ndihmë apo shtytje dhe, më pak, si organizatore apo në rolin e personit që kryen veprën.

Gjinia e të dyshuarve. Bazuar në të dhënat e Policisë së Kosovës, rezulton se nga 2887 persona të dyshuar të veprave penale të ndërlidhura me sigurinë e informacionit, 2666 janë të gjinisë mashkullore, ndërsa 221 persona janë të gjinisë femërore.



***Burimi: Policia e Kosovës 2007 – 2015**

Figura 8: Gjinia e të dyshuarve për vepra penale të ndërlidhura me sigurinë e informacionit, në periudhën 2007 – 2015

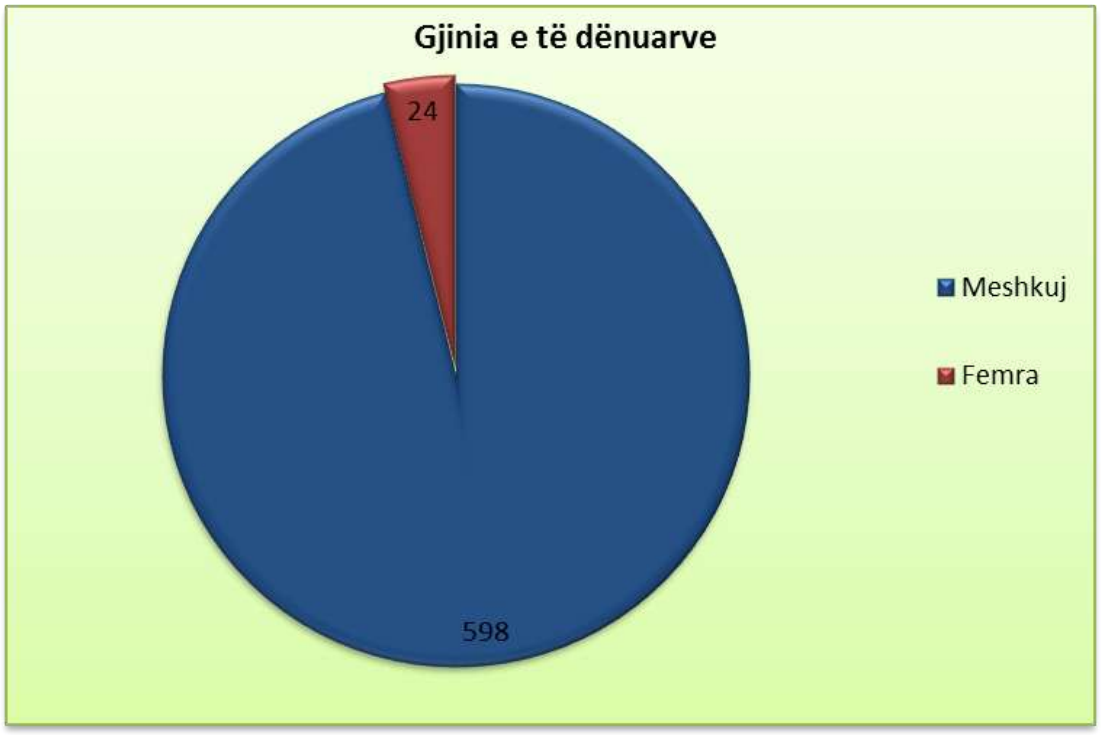
Gjinia e viktimave. Bazuar në të dhënat e Policisë së Kosovës, rezulton se nga 418 persona që ishin viktima të veprave penale të ndërlidhura me sigurinë e

informacionit gjatë kësaj periudhe, 284 janë të gjinisë mashkullore, ndërsa 134 persona janë të gjinisë femërore.

***Burimi: Policia e Kosovës 2007 – 2015**

Figura 9: Gjinia e viktimave të veprave penale të ndërlidhura me sigurinë e informacionit në periudhën 2007 – 2015.

Gjinia e të dënuarve. Bazuar në të dhënat e Këshillit Gjyqësor të Kosovës, rezulton se nga 622 persona të dënuar për vepra penale të ndërlidhura me sigurinë e informacionit, 598 persona janë të gjinisë mashkullore, ndërsa 24 persona janë të gjinisë femërore.



***Burimi: Këshilli Gjyqësor i Kosovës 2007 – 2015**

Figura 10: Gjinia e të dënuarve për vepra penale të ndërlidhura me sigurinë e informacionit 2007 – 2015.

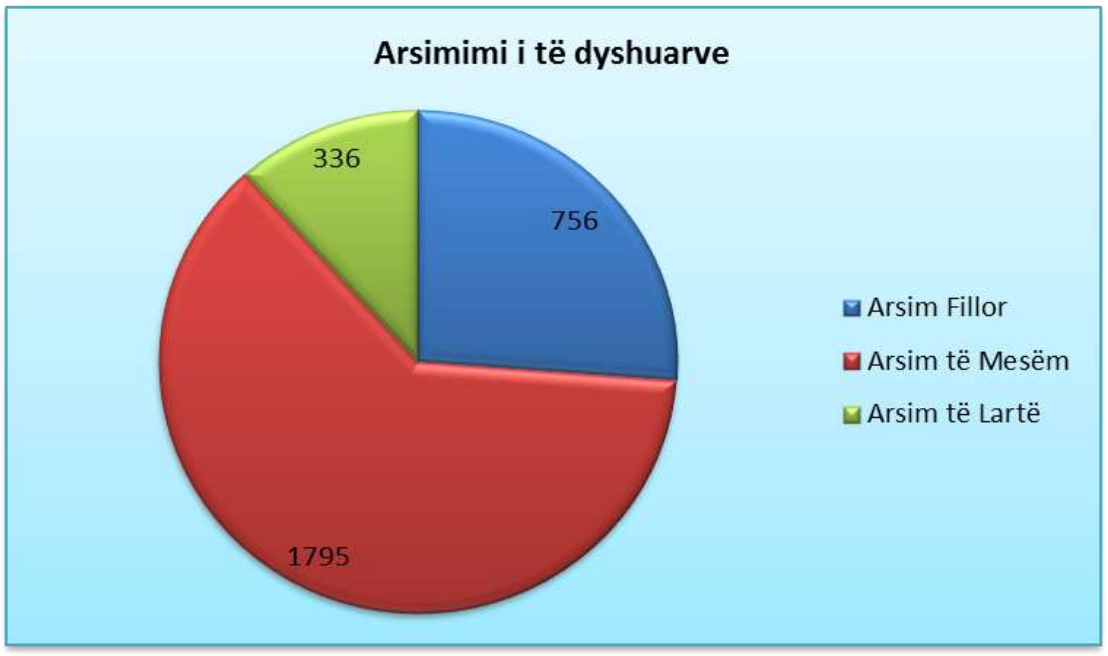
Niveli arsimor i të dyshuarve dhe i autorëve të këtyre veprave penale

Ngritja kulturo-arsimore është një faktor me rëndësi në formimin dhe aftësimin e njeriut për të pasur një jetë të sigurt dhe më të suksesshme (Halili, 2008: 260).

Sikurse u tha edhe më sipër, te mënyra e kryerjes së veprave penale të ndërlidhura me sigurinë e informacionit, për kryerjen e tyre kërkohet, por jo me çdo kusht, aftësi profesionale në fushën e teknologjisë informatike. Praktika tregon se autorët e këtyre veprave që lidhen me teknologjinë informatike, në shumicën e rasteve, janë me nivel arsimor të lartë në këtë fushë. Ky nivel arsimor i autorëve, si veçori individuale, ka më shumë rëndësi në rastet kur kompjuteri përdoret si mjet apo si objekt

për kryerjen e veprave penale të ndërlidhura me sigurinë e informacionit. Për shkak të zhvillimit të hovshëm të shkencës së informatikës, autorët me njohje të ulët të kësaj teknologjie nuk arrijnë të kryejnë vepra penale kundër sigurisë së informacionit aty ku kërkohet përdorimi i softuerëve të avancuar.

Niveli arsimor i të dyshuarve. Bazuar në të dhënat e Policisë së Kosovës, rezulton se nga 2887 persona të dyshuar për veprat penale të ndërlidhura me sigurinë e informacionit, 756 kanë arsimim fillor, 1795 kanë arsimim të mesëm dhe 336 kanë arsimim të lartë.



***Burimi: Policia e Kosovës 2007 – 2015**

Figura 11: Arsimimi i të dyshuarve për veprat penale të ndërlidhura me sigurinë e informacionit, në periudhën 2007 – 2015.

Niveli arsimor i të dënuarve. Bazuar në të dhënat e Këshillit Gjyqësor të Kosovës rezulton se nga 622 persona të dënuar për veprat penale të ndërlidhura me sigurinë e informacionit kanë 116 arsimim fillor, 399 kanë arsimim të mesëm dhe 107 kanë arsimim të lartë.

***Burimi: Këshilli Gjyqësor i Kosovës, 2007 – 2015**

Figura 12: Arsimimi i të dënuarve për veprat penale të ndërlidhura me sigurinë e informacionit në periudhën 2007 – 2015

Përkatësia etnike e të dyshuarve, e autorëve dhe e viktimave të këtyre veprave penale

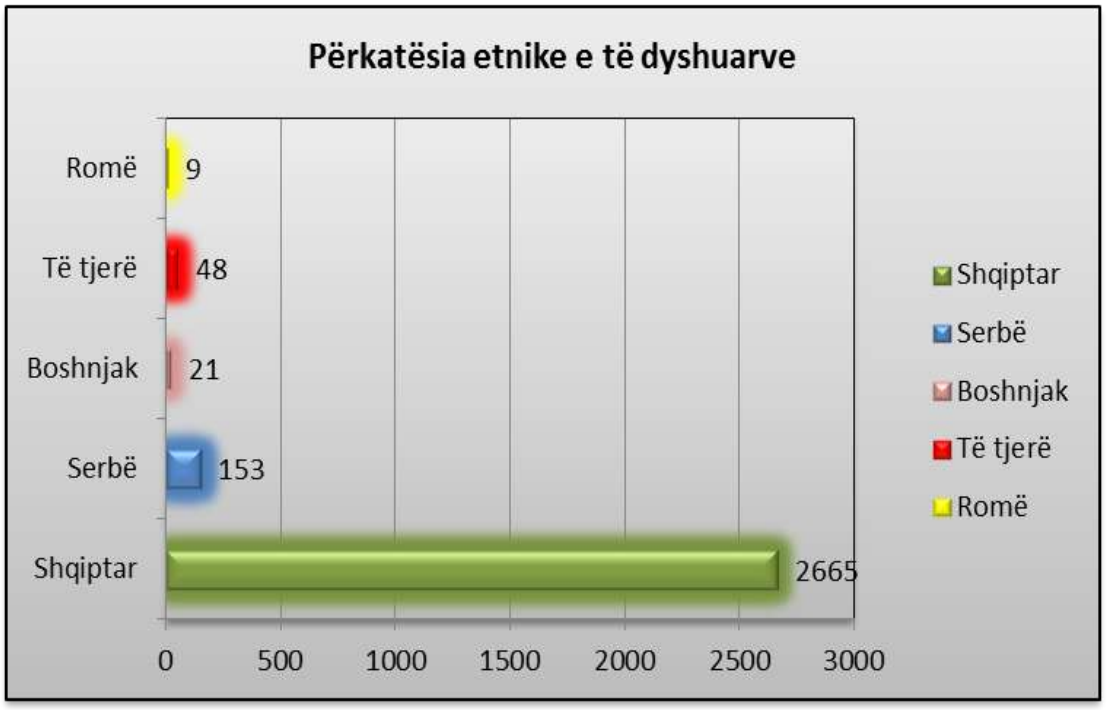
Nisur nga fakti se kemi të bëjmë me një formë të kriminalitetit që është i pranishëm në të gjitha shtetet ku teknologjia informatike ka arritur një nivel të caktuar

zhvillimi, ku aplikohet në masë përdorimi i sistemeve kompjuterike për komunikim apo për ruajtje të të dhënave, përkatësia etnike apo kombëtare është më karakteristike si veçori rajonale.

Struktura etnike e të dyshuarve dhe autorëve të veprave penale të ndërlidhura me sigurinë e informacionit reflekton me strukturën e popullit të Kosovës, ku mbi 90 % e popullatës është e kombësisë shqiptare.

Prandaj, gjatë hulumtimit të rasteve dhe, bazuar në të dhënat e nxjerra, në Kosovë, në periudhën 2007 – 2015, është vërejtur se në numër më të madh janë evidencuar autorë të kombësisë shqiptare, që përbën pjesën dërrmuese të popullsisë në Kosovë. Por nuk ka munguar edhe prania e autorëve nga etni të tjera, si serbë, boshnjakë dhe turq, por në numër më të vogël.

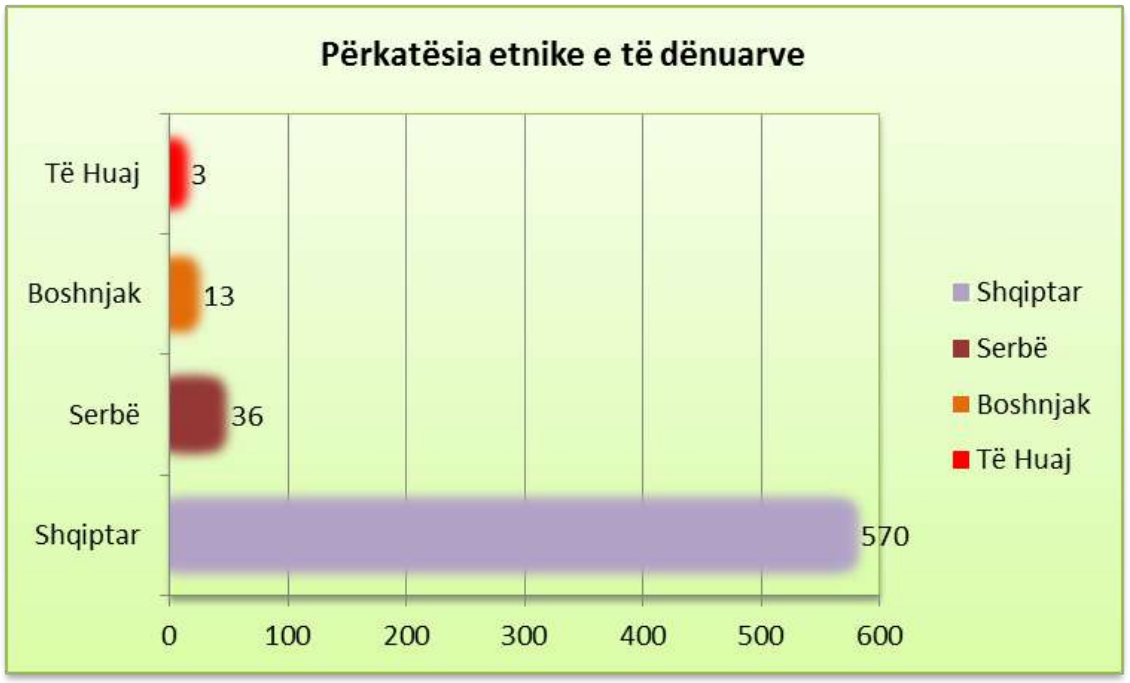
Përkatësia etnike e të dyshuarve. Bazuar në të dhënat e Policisë së Kosovës, rezulton se nga 2887 persona të dyshuar të veprave penale të ndërlidhura me sigurinë e informacionit, 2665 janë të kombësisë shqiptare; 153 persona janë të pakicës serbe; 48 persona janë të kategorive etnike "të tjerë"; 21 persona janë të përkatësisë etnike boshnjake dhe 9 persona janë të përkatësisë etnike rome.



***Burimi: Policia e Kosovës, 2007 – 2015**

Figura 13: Përkatësia etnike e të dyshuarve për vepra penale të ndërlidhura me sigurinë e informacionit, në periudhën 2007 – 2015

Përkatësia etnike e të dënuarve. Bazuar në të dhënat e Këshillit Gjyqësor të Kosovës rezulton se nga 622 persona të dyshuar të veprave penale të ndërlidhura me sigurinë e informacionit, 570 persona janë të kombësisë shqiptare, 36 persona janë të përkatësisë etnike serbe, 13 persona janë të përkatësisë etnike boshnjake dhe 3 persona janë shtetas të huaj.



***Burimi: Këshilli Gjyqësor i Kosovës 2007 – 2015**

Figura 14: Përkatësia etnike e të dënuarve për vepra penale të ndërlidhura me sigurinë e informacionit 2007 – 2015

Përkatësia etnike e viktimave. Bazuar në të dhënat e Policisë së Kosovës, rezulton se nga 418 persona në cilësi të viktimave të veprave penale të ndërlidhura me sigurinë e informacionit, 391 janë të kombësisë shqiptare; 19 persona janë të pakicës serbe; 5 persona janë të përkatësisë etnike boshnjake dhe 3 të përkatësive etnike të tjera.

***Burimi: Policia e Kosovës 2007 – 2015**

Figura 15: Përkatësia etnike e viktimave të veprave penale të ndërlidhura me sigurinë e informacionit, në periudhën 2007 – 2015

6.3. Aspekte të përgjithshme etiologjike të veprave penale të ndërlidhura me sigurinë e informacionit

Faktorët subjektivë që ndikojnë në kryerjen e këtyre veprave penale

Në kuptimin e ngushtë, faktorët që ndikojnë tek autorët potencialë të këtyre veprave dhe, njëherësh, në nxitjen, përhapjen dhe vëllimin e tyre, janë faktorët subjektivë apo endogjenë, që kanë të bëjnë me personalitetin e autorit. Faktorët subjektivë janë të shumtë dhe, sipas autorit Petroviç, ata ndahen në: *motive, gatishmëri*

dhe *mundësi* për të kryer veprën, si parakusht për t'u realizuar kryerja e krimit (Vula, 2010: 144).

Në këtë drejtim, vetitë psikike dhe biologjike luajnë një rol të rëndësishëm në jetën e njeriut, prandaj, si të tilla, ato influencojnë në sjelljet e tij, në ndikimet e faktorëve të jashtëm dhe në rezistencën ndaj tyre.

Vetitë psikike dhe biologjike të autorëve.

Siç u theksua më sipër, personaliteti i njeriut përbëhet prej vetive biologjike dhe psikike. Këto veti janë të pranishme dhe kanë ndikim në funksionimin e përditshëm të njeriut, prandaj kur kemi të bëjmë me veprime që bien ndesh me normat morale e ligjore, duhet të analizohen personaliteti dhe struktura psikike e autorit, me qëllim që të përcaktohet se sjellja devijante apo e kundërligjshme vjen si pasojë e vetë personalitetit të autorit dhe jo nga ndikimet e faktorëve të jashtëm.

Si veti dhe cilësi psikike, që mund të analizohen, janë: motivet, karakteri, temperamenti, emocionet, shprehitë, inteligjenca, aftësitë, qëndrimet, kujtesa, të menduarit dhe të tjera.

Tek autorët e krimeve kibernetike, varësisht llojit të veprës, kemi të bëjmë me personalitete me karakter të dobët, që u nënshtrohen motiveve dhe interesave të ulëta, lakmisë materiale, që mund të jetë si pasojë e kushteve sociale, ekonomike, familjare dhe kulturore (Halili, 2007: 339).

Në vijim do të shqyrtohen disa nga cilësitë më të theksuara të kësaj forme të krimit.

Motivet e autorëve të veprave penale të ndërlidhura me sigurinë e informacionit.

Me motive, "në vështrimin penalo-juridik kuptohen shtytjet a cytjet e brendshme, që bëjnë që personi të kryejë vepra penale. Ato lindin te personi që është nën ndikimin e ngacmimeve të jashtme, për shembull, nga fyerjet ose nga veprimet e paligjshme e të pamoralshme të një tjetri etj." (Elezi, Kaçupi & Haxhia, 2006: 117). Ato paraqesin "fuqitë nxitëse që e shtyjnë një individ të jetë aktiv, e orientojnë dhe e udhëheqin veprimtarinë e tij në jetë" (Halili, 2005: 352) dhe "në zgjidhjen e problemeve ose të situatave konkrete" (Hysi, 2005: 238).

Motivet, si faktorë subjektivë psikologjikë, kanë një rol përcaktues në nxitjen e autorëve për kryerjen e veprës penale. Ndër motivet e rrezikshme të sjelljes së njeriut shquajmë motivin i agresivitetit, që në shumë raste është me pasoja shumë të rënda. Ndërsa motivet më të theksuara në raport me kriminalitetin në fushën, që po trajtojmë në këtë punim, janë: motivi financiar (material), social (shoqërim, vetëpohim, agresivitet, siguri) dhe politik (ideologjik).

Shumica e veprave penale të këtij krimi ka të bëjë me motivin *financiar*, pasi autori shtyhet nga dëshira e madhe për pasurim, për të qenë i afirmuar dhe për të siguruar mirëqenien e vet. Këto motive shfaqen në formën e lakmisë dhe të pangopësisë materiale; për rrjedhojë, themi që tek ai person normat morale dhe ligjore këtu nuk paraqesin ndonjë pengesë. Rastet më tipike të kësaj natyre janë veprimet individuale të autorëve ndaj llogarive personale të viktimave, ata kërkojnë para në shkëmbim të e-mailit të tyre personal, apo të llogarisë në rrjetet sociale, që, më së shumti, përmbajnë të dhëna private. Kjo bëhet me kërcënime për asgjësimin apo abuzimin me llogaritë e tyre.

Motivet materiale shfaqen në konkurrencën ekonomike, kur autori motivohet për transferim të paautorizuar të informatave konfidenciale, me qëllim pasurimin e vet.

Në rastin e motiveve sociale, personit i lind nevoja për të qenë pjesë e shoqërisë apo e kolektivit; kur e tepron në këtë, paraqiten devijime, prirje për të imituar, për t'u identifikuar me ndonjë person apo grup. Rastet më tipike të veprave penale janë bashkimi në grupe kriminale të organizuara për të kryer mashtrime, distribuime të materialit pornografik me fëmijë, sulme të sistemeve bankare etj.

Te motivet e *vetëpohimit*, autori, zakonisht, identifikohet si haker, i cili ka dëshirën e afirmimit në shoqëri, të dallohet për aftësitë e tij nga të tjerët, duke u identifikuar me nofkë anonime për publikun, ndërsa në rrethin e hakerëve njihet për veprimet e tij në ndërhyrje të sistemeve kompjuterike.

Te motivet e *agresivitetit*, autorët veprojnë me qëllim që t'u shkaktojnë viktimave humbje, dëme dhe dhimbje të caktuara. Agresiviteti paraqitet si burim i problemeve dhe i konfliktit të autorit me shoqërinë, që rezultojnë me kryerje edhe të krimeve kibernetike, si: ndërhyrje në sisteme kompjuterike, përdorim i internetit për shpërndarjen e materialeve raciste ose ksenofobe nëpërmjet sistemit kompjuterik; fyerja me motive raciste ose ksenofobie nëpërmjet sistemit kompjuterik etj.

Te rastet me motivet e *sigurisë*, autorët veprojnë me qëllim që t'i sigurojnë vetes një gjendje stabile në plotësimin e nevojave dhe dëshirave të tyre. Në këto raste, i kapluar nga frika dhe nga pasiguria dhe në pamundësi të sigurimit të një jetese të dëshiruar, autori vepron duke ndryshuar, duke fshirë apo duke dëmtuar të dhënat në sistemin kompjuterik, të cilat do të cenonin sigurinë e tij, për shembull, pozitën e tij në ndonjë kompani, duke i dëmtuar të tjerët apo edhe për të mbuluar veprimet e mëparshme ilegale.

Rastet me motive *politike* shkaktojnë ndërhyrje në sisteme kompjuterike përmes qasjes së agjentëve për sprapsjen e kundërshtarëve politikë të një vendi, kërkimin e të dhënave konfidenciale për dëmtimin e vlerave politike dhe ekonomike të vendit tjetër. Sidomos në aspektin e ideologjisë, për ekstremistët politikë dhe terroristët kompjuterët paraqesin një nga simbolet e klasës udhëheqëse ose shtetin që duhet shkatërruar (Vula, 2010: 147).

Faktorët objektivë që ndikojnë në kryerjen e këtyre veprave penale

Bazuar në etiologjinë kriminale, faktorë objektivë apo ekzogjenë, që ndikojnë në vëllimin e kriminalitetit në përgjithësi, por edhe te veprat penale të ndërlidhura me sigurinë e informacionit, në veçanti, konsiderohen të gjitha ato shkaqe, kushte apo rrethana, që ndikojnë në krijimin, në zgjerimin dhe në intensitetin e këtyre veprave. Në literaturën e kriminologjisë, si përcaktuese në këto sjellje kriminale, krahas vetive psikike të personalitetit, konsiderohet edhe baza biologjike, pra vetitë anatomike dhe biologjike të individit. Këta faktorë mund t'i kërkojmë, si në specifikat e teknologjisë informatike, te varësia e shoqërisë ndaj kësaj arritjeje për komunikim dhe zhvillim të veprimtarive, ashtu edhe te faktorët ekonomiko-shoqërorë, ideo-politikë dhe socio-patologjikë. Zhvillimi i teknologjisë informatike, siç e kemi vënë në dukje, mundëson përdorimin e saj edhe për vepra kriminale më të sofistikuara, duke ndikuar, kështu, në rritjen e vëllimit të krimit kibernetik.

Megjithëse kjo formë e sofistikuar e krimit karakterizon vendet e zhvilluara, për arsye të përdorimit shumë të gjerë të teknologjisë mjaft të përparuar informatike, prania e autorëve të veprave penale të ndërlidhura me sigurinë e informacionit vihet re edhe në

vendet e varfra, ku, për shkak të faktorëve ekonomiko-socialë, të papunësisë dhe të motivit për pasurim, autorët përpiqen dhe shfrytëzojnë edhe ato mundësi të pakta që kanë për të përdorur shërbimet që ofrojnë qasje në internet (internet-kafetë) dhe për të kryer mashtrime online, duke i kaluar kufijtë rajonalë dhe ndërkombëtarë, sidomos në vendet ku legjislacioni nuk i penalizon veprimet e tilla. Po ashtu, si pasojë e mangësive teknike dhe njerëzore për mbrojtjen e tyre, është vështirë që ato të luftohen dhe të parandalohen. Më të drejtë edhe autori Petroviç ndan faktorët në kuptimin e gjerë dhe të ngushtë të tyre, duke i klasifikuar faktorët e gjerë si pjesë të faktorëve kriminogjenë që i përshtaten kësaj veprimtarie kriminale dhe faktorët kriminogjenë të ngushtë që ndikojnë te kryerësi i veprës së kriminalitetit kompjuterik (Vula, 2010: 147).

Megjithatë, faktorët objektivë nuk duhet të absolutizohen dhe, për të arritur te një përgjigje e saktë ndaj ndikimeve të këtyre vetive në kriminalitet, duhen marrë në konsideratë varësia dhe ndërlidhja e këtyre rrethanave me rrethanat shoqërore, ekonomike, familjare, kulturore. Këtu ndikon edhe fakti që shkaku i kryerjes së krimit është shprehje sociale e cilësive negative të personalitetit, kur veçoritë jo të favorshme të proceseve të veçanta psikike dhe prania e kushteve dhe e cilësive biologjike mund ta favorizojnë vetëm veprimin e këtyre shkaqeve, prandaj duhet vlerësuar tërësia e ndikimit dhe ndërthurja reciproke me faktorët objektivë socialë (Gjonçaj, 2013: 216). Po ashtu, defektet mentale dhe çrregullimet biologjike e psikike të pranishme në jetën e përditshme mund të kenë ndikim në kryerjen e veprave penale të këtij lloji, siç është rasti i dëmtimeve të pajisjeve kompjuterike nga autorët me probleme mendore.

Faktorët ekonomiko-shoqërorë që ndikojnë në kryerjen e këtyre veprave penale.

Në literaturën e kriminologjisë, faktorët ekonomikë dhe shoqërorë konsiderohen ndër faktorët e jashtëm me ndikim në paraqitjen e kriminalitetit, gjë të cilën e ka vërtetuar edhe praktika: kur kriminaliteti është në nivele të larta, ka edhe kriza ekonomike, industrializim dhe urbanizim. Arritjet dhe transformimet e mëdha në shoqëri prekin, në njërën anë, një numër të konsiderueshëm të popullsisë, që vuan nga varfëria dhe nga papunësia që kanë ndikim të caktuar në sjellje kriminale. Edhe krizat ekonomike trajtohen si faktorë me ndikim të dukshëm në shtimin e disa formave të kriminalitetit, edhe në dinamikën e krimit kibernetikë. Rënia e prodhimit, ulja e standardit të një shteti sjell me vete varfërinë dhe mungesën e kushteve për mbijetesë, gjë që çon në lindjen e rrethanave që ndihmojnë kryerjen e veprimeve kriminale, si vjedhjet, mashtrimet, tregtia e palejuar, bursa e zezë, bixhozi, prostitucioni etj. (Halili, 2008: 241).

Pra, faktorët ekonomikë dhe shoqërorë kanë ndikim në shfaqjen e veprave penale të ndërlidhura me sigurinë e informacionit dhe kjo varet edhe nga motivi i autorit, por, për shkak të specifikave të tij, në të shumtën e rasteve kategorizohet krim i organizuar apo krim i "jakave të bardha" për shkak të aftësive dhe qasjes në sisteme kompjuterike.

Faktorët ideopolitikë që ndikojnë në kryerjen e këtyre veprave penale.

Faktorët ideopolitikë përfshijnë shkaqe, rrethana dhe kushte shoqërore, që ndikojnë në shfaqjen e sjelljeve kriminale, siç janë: konfliktet ideopolitike, kulturore;

luftërat, religjioni etj. Në çdo shoqëri, në momente të caktuara mund të shpërthejnë rrethana të konfliktit ideor dhe politik, kur përmes mjeteve të komunikimeve apo rrjeteve sociale, individë a grupe individësh mund të ndikohen dhe të mbështesin botëkuptime të ndryshme ideologjike, religjioze etj. Si rezultat i ndikimeve të tilla, krijohen gjendje që shkaktojnë rrezikshmëri dhe nxisin konflikte politike, qoftë nën ndikimin e aspiratave nacionaliste, qoftë në mbështetje të ndonjë ideologjie dhe e gjitha kjo mund të rezultojë në luftë, në propagandë armiqësore, në organizim të rrjetit të agjentëve dhe të informatorëve, në spiunazh dhe në tradhti.

Mbizotërimi i rrethanave të konflikteve ideore dhe politike shkakton edhe rritjen e aktiviteteve të kriminalitetit politik, të aktiviteteve terroriste, të sabotimeve etj. Krahas këtyre ndikimeve, që ndodhin midis shteteve, paraqiten edhe konflikte të brendshme, kur regjimet në pushtet përdorin masa për të penguar aktivitetin e lirë politik, për të cenuar sigurinë e qytetarëve, pronën, të drejtat dhe liritë qytetare etj.

Nga ana tjetër, konfliktet kulturore paraqiten te shtetet me përbërje të ndryshme kombëtare, etnike, religjioze, ku bëjnë pjesë kultura, religjione e raca të ndryshme (Halili, 2008: 241). Në literaturë dhe në rastet e studiuara në praktikë, te këto lloje konfliktesh vërehet shfrytëzimi i sistemeve kompjuterike dhe i internetit për qëllime ideopolitike (Gerecke, 2012: 112).

Vlen të përmenden rastet e veprave penale të ndërlidhura me sigurinë e informacionit, e veçanërisht sulmet kibernetike mes shteteve, kur shkaktohen pengesa në funksionimin e infrastrukturës dhe ueb-faqeve qeveritare, kur organizohen aktivitete terroriste të motivuara politikisht për të shkaktuar pasoja të rënda dhe dëm ekonomik, duke sulmuar në rastet më ekstreme kompjuterë, rrjete dhe të dhënat në sistemet kompjuterike ushtarake, sistemet e administratës shtetërore, kontrollin ajror, sistemin e

gazit, të ujit, të energjisë elektrike, ku bëjnë pjesë edhe keqpërdorimi i sistemeve kompjuterike për qëllime përgjimi të kundërshtarëve politikë nga regjimet në pushtet, shpërndarja kompjuterike e materialeve pro gjenocidit ose krimeve kundër njerëzimit, kanosja për motive racizimi dhe ksenofobie nëpërmjet sistemit kompjuterik etj.

Në krahasim me faktorët e tjerë objektivë, mund të themi se faktorët ideo-politikë kanë një rëndësi më të madhe, për shkak të seriozitetit të veprave dhe rrezikimit të madh të shoqërisë në rast të kryerjes së këtyre veprave, që, si kundërpërgjigje, shkaktojnë efektin zinxhir për mbrojtje nga agresiviteti i jashtëm apo dhe mbrojtje të ideologjive dhe të drejtave të cenuara, që garantohen me konventa ndërkombëtare.

Faktorët sociopatologjikë që ndikojnë në kryerjen e këtyre veprave penale.

Prania e dukurive sociopatologjike në shoqëri ndikon në praninë e kriminalitetit në përgjithësi. Ato prekin vlerat morale, njerëzore dhe sociale në ambientin shoqëror dhe rëndom paraqiten si shkak i çrregullimeve sociale-ekonomike.

Në literaturën e kriminologjisë, veprimtaritë që mund të kryhen përmes veprave penale kundër sigurisë së informacionit, si dukuri sociopatologjike, mund t'i veçojmë si vepra penale të mundësimit ose detyrimit në prostitucion, pornografia me fëmijët dhe bixhozi online. Meqenëse rekrutimi dhe organizimi i prostitucionit penalizohet nga kodi penal, ligjvënësit në të ardhmen, si masë shtesë preventive, mund ta përcaktojnë këtë vepër edhe si krim kibernetikë, në rast se rekrutimi dhe organizmi bëhet nëpërmjet sistemeve kompjuterike.

Krahas prostitucionit, si dukuri sociopatologjike që kanë lidhje me forma të ndryshme të kriminalitetit përmenden edhe devijimet dhe çrregullimet e ndryshme

seksuale, të njohura si patologji seksuale, si faktorë kriminogjenë, që karakterizojnë autorët e njohur si pedofilë (Halili, 2008: 288).

Me qëllim mbrojtjen nga këta faktorë kriminogjenë, në nivel ndërkombëtar dhe në Konventë i është dhënë prioritet parandalimit dhe luftimit të pornografisë, në veçanti, veprave penale të pornografisë me fëmijë, duke kërkuar nga autoritetet të nxjerrin ligje dhe të ndërmarrin masa për ta sanksionuar atë si vepër penale në ligjet vendore; po ashtu, veprave penale të ofrimit të materialeve me përmbajtje pornografike ndaj të miturve, prodhimit të materialeve me pornografi me qëllim shpërndarjen e tyre përmes sistemit kompjuterik, prodhimit të një materiali të tillë për vete apo për të tjerët dhe zotërimit të tyre në sistemin kompjuterik.

KAPITULLI 7: ASPEKTI KRAHASUES I KLASIFIKIMIT TË INFORMACIONEVE, TË SHËRBIMEVE TË INTELIGJENCËS DHE I ROLIT TË TYRE PËR SIGURINË E INFORMACIONIT

7.1 Klasifikimi i informacioneve dhe rëndësia e klasifikimit

Klasifikimi i informacioneve është një komponent shumë i rëndësishëm për sigurinë e informacionit, sepse mundëson themelimin e një sistemi unik për klasifikimin dhe ruajtjen e informacioneve që kanë të bëjnë me interesat kombëtare të sigurisë, si dhe për verifikimin e sigurisë së personave që kanë qasje në këto informacione.

Një aspekt i rëndësishëm i sigurisë së informacionit është njohja e vlerës së informacionit dhe përcaktimi i procedurave të mbrojtjes së informacioneve. Të gjitha informacionet nuk kanë vlerën e barabartë, kështu që nuk kërkohet e njëjta shkallë mbrojtjeje. Prandaj kërkohet që të bëhet klasifikimi i informacioneve. Disa faktorë që ndikojnë në klasifikimin e informacionit kanë të bëjnë me vlerësimin e vlerës që informacioni ka për organizatën, me kohëzgjatjen e klasifikimit të informacionit. Klasifikimi i një aktivi të veçantë të informacionit duhet të rishikohet periodikisht, për të siguruar klasifikimin e informacioneve dhe për të siguruar se janë duke u ndjekur kontrollet e sigurisë të kërkuara për klasifikim.

Nëse një e dhënë apo informacion klasifikohet si kërcënim, pa i plotësuar kriteret e përcaktuara me ligj, atëherë ai mund të ndikojë negativisht për sigurinë kombëtare, ashtu si mund të rrezikojë sigurinë kombëtare edhe mos klasifikimi i një të dhëne apo informacioni si kërcënim, i cili i plotëson kriteret e parapara me ligj, sepse ai

mund të dobësojë mundësinë e ndërmarrjes së hapave të nevojshëm dhe të përgatitjeve për çrregullimet e mundshme (Abazoviq, 2006: 84).

Klasifikimi i informacioneve paraqet aktin apo procesin përmes të cilit ato përcaktohen si informacione të klasifikuara (Ligji për Klasifikimin e Informacioneve, neni 3). Qeveria e secilit vend klasifikon asetet e informacionit, për të siguruar se ato janë të mbrojtura në mënyrë të përshtatshme për të mbështetur jo vetëm parandalimin dhe luftimin e rreziqeve të sigurisë kombëtare, por edhe biznesin e sektorit publik me shfrytëzimin efektiv të informacionit, si dhe për të përmbushur kërkesat e legjislacionit përkatës, marrëveshjet dhe detyrimet ndërkombëtare (Government Security Classifications, USA, 2014, f. 3).

Kjo vlen për të gjitha informacionet që qeveria mbledh, duke filluar nga informacionet që përmbajnë të dhëna për sigurinë kombëtare, informacionet për të gjitha llojet e krimit, informacionet që ndërlidhen me sigurinë publike, por edhe informacione të tjera. Secili zyrtar që punon në institucionet publike e ka për detyrë të respektojë fshehtësinë dhe integritetin e çdo informacioni dhe këto informacione duhen shfrytëzuar vetëm për nevoja zyrtare të institucioneve të cilat punojnë në përputhje të plotë me ligjet e aplikueshme të vendit.

Klasifikimet e informacioneve tregojnë ndjeshmërinë e tyre në aspektin e ndikimit të mundshëm që rezulton nga humbja apo nga keqpërdorimi dhe nevojën për t‘u mbrojtur nga një profil i gjerë kërcënimesh. Klasifikimi i informacioneve zbatohet nga të gjitha institucionet publike që ushtrojnë kompetenca ekzekutive, legjislative dhe gjyqësore.

Ruajtja e informacioneve të klasifikuara është proces kompleks që kërkon formim profesional, edukim dhe përgjegjësi. Një kuadër i lartë i niveleve të kontrollit mundëson që të gjitha informatat e klasifikuara të trajtohen me kujdes, në përputhje me

detyrimet ligjore dhe për të reduktuar rrezikun e humbjes ose të qasjeve të paautorizuara në informacionet e klasifikuara.

Organizatat e sigurisë aplikojnë sisteme rigoroze kontrolli të të gjitha informacioneve të klasifikuara, me qëllim që ato të analizohen dhe të përdoren në përputhje me interesat kombëtare të vendit, duke u mundësuar vendimmarrësve që të marrin vendime në interes të vendit dhe duke parandaluar me kohë kërcënimet dhe rreziqet që i kanosen vendit.

Nivelet e klasifikimit të informacioneve

Varësisht nga përmbajtja, nga ndjeshmëria e informacionit dhe nga niveli i rrezikut dhe i pasojave për interesat e sigurisë së vendeve nga publikimi i paautorizuar i informacioneve, ekzistojnë nivele të ndryshme të klasifikimit të informacioneve.

Në disa vende ekzistojnë tri nivele të klasifikimit të sigurisë së informacioneve: niveli zyrtar, niveli sekret dhe tepër sekret; ndërsa në vende të tjera ekzistojnë katër nivele të klasifikimit të informacioneve: niveli i kufizuar, konfidencial, sekret dhe tepër sekret.

Në NATO ekzistojnë katër nivele të klasifikimit të informacioneve: niveli top sekret, sekret, konfidencial dhe të kufizuara. Edhe informacionet e paklasifikuara, megjithëse janë të tilla, ato nuk mund të bëhen publike pa lejen e NATO-s.

Me qëllim të qartësimin e aspektit krahasues të klasifikimit të informacioneve, në vazhdim do të paraqesim procesin e klasifikimit të informacioneve në Republikën e Kosovës, Republikën e Sllovenisë dhe Republikën e Kroacisë.

7.2. Klasifikimi i informacioneve në Republikën e Kosovës

Informacion i klasifikuar është çdo informacion dhe material, publikimi i paautorizuar i të cilave do të cenonte në shkallë të ndryshme interesat e sigurisë së Republikës së Kosovës, ndërsa autoritet i klasifikimit të informacioneve është çdo person i përcaktuar që ka kompetencë origjinale apo të deleguar për të klasifikuar informacione (Ligji për Klasifikimin e Informacioneve, neni 3).

Në Republikën e Kosovës, klasifikimi i informacioneve zbatohet në të gjitha institucionet publike që ushtrojnë kompetenca ekzekutive, legjislative, gjyqësore, dhe në Presidencën e Kosovës.

Bartës i autorizuar i informacioneve të klasifikuara është secili person i cili ka në posedim informacionin e klasifikuar, ka leje të vlefshme të sigurisë dhe i plotëson kushtet tjera që lejojnë qasjen në informacionin e klasifikuar, përveç nëse përcaktohet ndryshe me ligj (Ligji për Klasifikimin e Informacioneve, neni 3).

Se në cilat informacione të klasifikuara do të ketë qasje personeli i autorizuar varet nga parimi "Nevoja për njohuri". Në bazë të këtij parimi, vendimi i marrë nga një bartës i autorizuar i informacionit të klasifikuar se pranuesit të ardhshëm i duhet qasje në informacionin specifik të klasifikuar, për të punuar ose për të ndihmuar në një funksion të ligjshëm dhe të autorizuar qeveritar, detyrë zyrtare ose funksion publik.

Kriteret e klasifikimit të informacioneve në Kosovë

Informacionet klasifikohen vetëm nëse është e nevojshme dhe nëse klasifikimi bëhet nga autoriteti kompetent i klasifikimit, informacionet zotërohen, prodhohen nga

Republika e Kosovës apo për të, ose janë nën kontroll të Republikës së Kosovës, por edhe informacionet që bien brenda një apo më shumë prej këtyre kategorive:

- siguri publike;
- mbrojtje, plane ushtarake, sisteme armësh apo operacione;
- informacione për marrëdhëniet me jashtë dhe qeveritë e jashtme, përfshirë burimet konfidenciale;
- veprimtari zbulimi dhe të zbatimit të ligjit, përfshirë metoda dhe burime të zbulimit;
- sisteme, instalime, infrastruktura, projekte, plane apo shërbime të mbrojtjes, që lidhen me interesat e sigurisë të Republikës së Kosovës dhe
- veprimtari shkencore, teknologjike, ekonomike, financiare që lidhen me interesat thelbësore të sigurisë së Republikës së Kosovës (Ligji për Klasifikimin e Informacioneve, neni 3).

Kompetencën për klasifikim të informacioneve e ka vetëm institucioni publik që e ka prodhuar informacionin. Nëse informacionin e ka prodhuar Policia, atëherë Policia është autoriteti i vetëm që mund të bëjë klasifikimin e informacionit.

Nivelet e klasifikimit të informacioneve në Kosovë

Në secilin institucion publik në Kosovë, autoriteti i klasifikimit vendos nëse informacioni duhet klasifikuar dhe përcakton nivelin e klasifikimit të informacionit që në momentin kur prodhohet informacioni. Vendimi nëse duhet klasifikuar informacioni

dhe përcaktimi i nivelit të klasifikimit bazohet në një vlerësim të pasojave të dëmshme që mund të rezultojnë për interesat e sigurisë së Republikës së Kosovës nga hapja e paautorizuar e informacionit të tillë (Ligji për Klasifikimin e Informacioneve, neni 8).

Niveli i klasifikimit të informacionit bëhet varësisht prej shkallës së dëmit që do të shkaktonte publikimi i paautorizuar i tij në interesat e sigurisë në Republikën e Kosovës. Në Kosovë ekzistojnë katër nivele të klasifikimit të informacioneve: niveli tepër sekret, sekret, konfidencial dhe niveli i kufizuar.

Niveli "Tepër Sekret" zbatohet për informacionet, hapja e paautorizuar e të cilave, sipas vlerësimit të arsyeshëm, do të shkaktonte dëm jashtëzakonisht të rëndë për interesat e sigurisë së Republikës së Kosovës (Ligji për Klasifikimin e Informacioneve, neni 6).

Informacione të klasifikuara si tepër sekret, mund të jenë informacionet që përmbajnë plane mbrojtjeje, plane ushtarake, sisteme armësh apo operacione. Një shembull i informacioneve sekrete kanë qenë informacionet për planin e ndërhyrjes në pjesën veriore të Kosovës. Një plan të tillë institucionet e sigurisë së Kosovës e realizuan më datën 15.07.2012. Po ashtu, informacione tepër sekrete mund të jenë ato informacione që përmbajnë veprimtari shkencore, teknologjike, ekonomike, financiare që lidhen me interesat thelbësore të sigurisë së Republikës së Kosovës.

Niveli "Sekret" zbatohet për informacionet, hapja e paautorizuar e të cilave do t'i dëmtonte seriozisht interesat e sigurisë së Republikës së Kosovës (Ligji për Klasifikimin e Informacioneve, neni 8).

Informacione sekrete mund të jenë ato informacione që përmbajnë të dhëna për sigurinë publike, të dhëna për individët, për grupet kriminale që merren me krim të organizuar.

Niveli “Konfidenciale”, zbatohet për informacionet, hapja e paautorizuar e të cilave do të mund t’i dëmtonte interesat e sigurisë së Republikës së Kosovës (Ligji për Klasifikimin e Informacioneve, neni 3). Të nivelit konfidencial mund të konsiderohen procedurat standarde të operimit, rregulloret e brendshme, raportet e punës etj.

Niveli “I Kufizuar”, zbatohet për informacionet, hapja e paautorizuar e të cilave do të ishte e pafavorshme për interesat e sigurisë së Republikës së Kosovës (Ligji për Klasifikimin e Informacioneve, neni 3).

Kompetencën origjinale për klasifikim në nivelin “Tepër Sekret” e kanë: Presidenti i Kosovës, Kryetari i Kuvendit të Kosovës, Kryeministri, Kryesuesi i Këshillit të Sigurisë së Kosovës; Drejtori i Agjencisë së Kosovës për Inteligjencë, Drejtori i Përgjithshëm i Policisë së Kosovës dhe Komandanti i Forcës së Sigurisë së Kosovës. Kompetencën origjinale të klasifikimit në nivelin “Sekret”, “Konfidenciale” dhe “I Kufizuar” e kanë sekretarët e përhershëm, krye shefat ekzekutivë apo drejtorët ekzekutivë të institucioneve publike dhe pozicionet e barasvlershme me ta, përveç nëse ata ia delegojnë këtë kompetencë zyrtarëve të lartë vartës (Ligji për Klasifikimin e Informacioneve, neni 7).

Dokumentet të cilat përmbajnë informacione të klasifikuara i shpërndahen vetëm personave që kanë leje përkatëse të sigurisë dhe kanë nevojë për njohuri rreth atyre informacioneve. Shpërndarja fillestare e informacioneve të klasifikuara specifikohet nga institucioni që e ka krijuar informacionin.

Për të pasur qasje në informacione të klasifikuara, është rregull i përgjithshëm që për qasjen në informacione të klasifikuara çdo person duhet të ketë leje të vlefshme mbi sigurinë, të ketë nevojë për të qenë në dijeni të këtyre informacioneve që ta kryejë misionin apo detyrën e tij zyrtare dhe të ketë nënshkruar deklaratën e konfidencialitetit.

Përjashtim bëhet vetëm për Presidentin e Republikës së Kosovës, Kryetarin e Kuvendit të Kosovës dhe Kryeministrin, të cilët janë të autorizuar të kenë qasje në informacionet e klasifikuara, me qëllim të kryerjes së detyrave zyrtare të tyre pa i përmbushur këto kërkesa, me kusht që të kenë nevojë për të qenë në dijeni të këtyre informacioneve (Ligji për Klasifikimin e Informacioneve, neni 22).

7.3. Mbrojtja e informacioneve të klasifikuara në Republikën e Kosovës

Mbrojtja e informacionit luan një rol të rëndësishëm për sigurinë kombëtare të vendit dhe çdo rrezikim i informacioneve të klasifikuara duhet konsideruar problem kombëtar. Mbrojtja dhe siguria e informacionit lidhet me detyrimet kombëtare ligjore, në kuadrin e qenies vend anëtar ose të bashkëpunimit me Organizatën e Kombeve të Bashkuara, Këshillin e Evropës, Bashkimin Evropian, NATO-n, INTERPOL-in, OSBE-në, EUROPOL-in, etj. Fakti që Kosova nuk është pjesë e këtyre organizatave ndërkombëtare, paraqet një barrierë që e vështirëson punën e organizatave të sigurisë, veçanërisht në shkëmbimin e të dhënave dhe në krijimin e një infrastrukture të përbashkët të sigurisë së informacionit. Harmonizimi dhe përshtatja e kuadrit ligjor kombëtar me atë të strukturave të mësipërme, mbetet një fushë ku institucionet shtetërore duhet të bëjnë më shumë.

Mbrojtja e hapësirës së informacionit kërkon një vizion të fortë dhe lidership. Në këtë aspekt, kërkohen ndryshime në politika, teknologji, edukim, por edhe në infrastrukturën ligjore. Duke evidencuar angazhimin në çështjet e sigurisë së informacionit në nivele të larta të qeverisjes, të industrisë dhe të shoqërisë civile, kjo do

të lejojë që Kosova të vazhdojë përpjekjet për futjen e teknologjive të reja dhe për përmirësimin e politikave të sigurisë kombëtare.

Siguria e informacionit mund të kërcënohet dhe të rrezikohet nga sulme të vazhdueshme, si ndërhyrjet ilegale në telekomunikim, terrorizmi kibernetikë, vjedhja me anë të telemarketimit, pastrimi i parave etj. Me përparësi duhen parë sidomos siguria dhe mbrojtja e informacioneve të klasifikuara ndaj sistemeve depërtuese të disa vendeve fqinje, si Republika e Serbisë, Republika e Maqedonisë, që janë të interesuara për arsye historike në zotërimin e informacionit të klasifikuar të Kosovës.

Fusha e teknologjisë së hapësirës së informacionit është një fushë ku përfshin jo vetëm internetin dhe kompjuterët, por edhe lloje të tjera rrjetesh, siç janë rrjetet telefonike dhe satelitore. Një një pjesë të hapësirës së informacionit e zë interneti, por studiuesit e sotëm priren t'i pranojnë si të barabarta, si internetin, ashtu edhe hapësirën e informacionit. Përdorimi i internetit ka krijuar lehtësira të mëdha. Ai është zhvilluar nga një numër i vogël i universiteteve dhe agjencive qeveritare në një rrjet të gjerë të më shumë se dy bilionë shfrytëzuesve.(Kim & Solomon, 2014: 2).

Mbrojtja e hapësirës kibernetike të Kosovës

Transformimi i efekteve të pushtetit kibernetike në objektiva dhe politika është arti dhe shkenca e secilës strategjisë . (Dolman, 2005:6).

Siguria kibernetike është krijuar për të mbështetur arritjen e objektivave të mëdha, qëllimet strategjike të gjithë elementeve të nevojave dhe interesave të Strategjisë së Sigurisë Kombëtare. Kontributi kryesor i një strategjie kombëtare për hapësirën kibernetike do të jetë në mënyrë të qartë të demonstrojnë se si ajo e bën të mundur

arritjen e objektivave të të gjitha strategjive të tjera, veçanërisht Strategjisë Kombëtare të Sigurisë. (Schreier, 2015:18).

Rritja e konsiderueshme e numrit të shfrytëzuesve të Internetit në vitet e fundit në Kosovë ka sjellë me vete rrezikimin e hapësirës kibernetike të Kosovës nga sulmet kibernetike. Disa veprimtari kriminale që kanë ndodhur te ne janë të mjaftueshme për të theksuar dobësinë e rrjeteve kompjuterike në vend, që ende konsiderohen së janë në fazën e zhvillimit. Sidomos hapësira e informacionit, ku përfshihet edhe interneti, është një mundësi për shkatërrim, për krime elektronike, veçanërisht kur fuqia e informacionit përdoret si mënyrë për kryerjen e këtyre krimeve.

Edhe në Republikën e Kosovës, referuar në analizën e rishikimit strategjik të sektorit të sigurisë, krimi kibernetikë si krim jokonvencional është identifikuar si një prej rreziqeve, sfidave apo kërcënimeve globale që mund të cenojnë edhe sigurinë e vendit. Për të garantuar sigurinë kibernetike kërkohet jo vetëm angazhim i të gjitha strukturave përkatëse, por edhe një koordinim dhe bashkëpunim tyre me struktura homologe të vendeve të tjera në ndërkombëtar, pasi hapësira kibernetike tashmë është bërë një hapësirë globale dhe pa kufij. Megjithëse Kosova është pjesë aktive e shumë aktiviteteve dhe programeve në fushën e sigurisë kibernetike, pengesë serioze paraqet fakti që Kosova nuk është pjesë e shumë organizatave ndërkombëtare për arsye të pamundësisë së saj për t'u anëtarësuar në OKB, NATO, BE, por edhe në organizatat ndërkombëtare policore.

Besimi i shtuar në sistemet komunikuese dhe informative i ka bërë shtetet të cenueshme ndaj sulmeve kibernetike, që mund të shkaktojnë dëme të mëdha në sistemet kombëtare, në rrjetet kompjuterike dhe në infrastrukturën e informimit, të ekonomisë, bankave, bizneseve dhe të trafikut ajror dhe tokësor. Nëse i referohemi Strategjisë për

Siguri Kibernetike të Bashkimit Europian dhe dokumenteve të tjera ndërkombëtare, kriminaliteti kibernetikë, përgjithësisht, përfshin një spektër të gjerë veprimtarish kriminale të ndryshme, ku kompjuterët dhe sistemet informatike angazhohen ose si vegël primare ose si shënjestër primare.

Qindra mijëra sulme kibernetike ndodhin në ditë në mbarë botën dhe po bëhen më të ashpra gjithnjë e më tepër. Madje, në kushtet e sotme, kur terrorizmi ndërkombëtar është bërë një rrezik serioz për çdo vend, pritet që kërcënimi i këtyre sulmeve të shtohet dita-ditës, duke shkaktuar mjaft dëme ekstreme. Këto prekin shumë vende, shumë sektorë dhe prej tyre nuk përjashtohet as vendi ynë. Madje, ato janë të pranishme në Kosovë, si një kërcënim për administratën publike, për ekonominë dhe për fusha të tjera. Ky aktivitet kriminal kibernetikë inkurajohet edhe nga axhenda të ndryshme politike. Siç theksohet edhe në Analizën e rishikimit strategjik të sektorit të sigurisë së Republikës së Kosovës, 2014, fq.19, krimet kibernetike paraqesin një rrezik ndaj sigurisë, stabilitetit dhe funksionimit të shtetit.

Për avancimin e standardeve të mbrojtjes së sigurisë së informacionit në Kosovë, qeveria dhe të gjitha institucionet tona, aktualisht aplikojnë standarde të larta të mbrojtjes kibernetike të informacioneve të klasifikuara. Tashmë, te ne është krijuar një bazë e mirë për ruajtjen e sigurisë së informacioneve të klasifikuara, e cila bazohet në infrastrukturën ligjore të kësaj fushe, siç janë Kodi Penal i Kosovës, Ligji për Parandalimin dhe Luftimin e Krimit Kibernetikë, Ligji për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë. Këto ligje u kanë mundësuar pjesërisht institucioneve të sigurisë krijimin e mekanizmave institucionalë për parandalimin dhe luftimin e krimit kibernetikë me masa konkrete, parandalimin, zbulimin dhe

sanksionimin e shkeljeve përmes sistemeve kompjuterike, si garanci për respektimin e të drejtave të njeriut dhe për mbrojtjen e të dhënave personale.

Megjithatë, puna në këtë drejtim duhet avancuar në vazhdimësi, pasi shohim që sistemet mbrojtëse kibernetike në Kosovë janë shumë vulnerabile ndaj depërtimeve të organizatave dhe të individëve me veprim kriminal. Kjo dikton avancimin e standardeve të sigurisë së hapësirës kibernetike.

Mendoj që për këtë del nevoja urgjente që Kosova të hartojë Strategjinë Kombëtare të Sigurisë Kibernetike. Vlerësojmë se me nxjerrjen e këtij dokumenti madhor dhe me zbatimin e tij, niveli i sigurisë kibernetike, mbrojtja nga sulmet kibernetike do të rriten shumë, pasi nënkuptohet që kjo strategji do të përcaktojë masa konkrete dhe efikase edhe për një hapësirë kibernetike të sigurt, sidomos ndaj sistemeve depërtuese të disa vendeve që janë të interesuara në zotërimin e informacionit të klasifikuar të Kosovës, siç janë Rusia, Serbia, Maqedonia etj.

Po në këtë kuadër shtrohet edhe detyra për të modifikuar, pasuruar dhe avancuar tërë infrastrukturën aktuale ligjore, me synimin që legjislacioni aktual i kësaj fushe në Kosovë të ketë një bazament sa më të qëndrueshëm të sigurisë së informacioneve dhe mekanizma sa më efikase të mbrojtjes së informacioneve të klasifikuara. Kjo dhe hartimi i Strategjisë Kombëtare për Sigurinë e Informacionit do të ndikojnë së tepërmi në krijimin e një hapësire të sigurisë kibernetike të standardeve të larta. Institucionet përkatëse do të obligoheshin të përmbushnin brenda afateve të caktuara aktivitetet e tyre të caktuara në planin e veprimit, si dhe realizimin në vazhdimësi të detyrave dhe të përgjegjësive që rrjedhin nga ky plan veprimi.

Mbrojtja e informacioneve të klasifikuara të Kosovës nga kërcënimet e jashtme

Pranohet që sistemet mbrojtëse kibernetike të Kosovës janë mjaft vulnerabile sidomos ndaj kërcënimeve të disa shteteve dhe organizatave me veprim jo demokratik. Kjo vjen edhe ngaqë në Kosovë veprojnë shumë organizata vendore dhe ndërkombëtare qeveritare dhe joqeveritare, disa nga të cilat janë të interesuara në zotërimin e informacioneve të klasifikuara të Kosovës.

Nga ana tjetër problemi bëhet edhe më i mprehtë për shkak se disa vende fqinje, si Serbia dhe Maqedonia, por edhe shtete të tjera, si Rusia, në vazhdimësi janë përpjekur dhe përpiqen të sigurojnë informacione të klasifikuara që lidhen me veprimtarinë e Institucioneve të Kosovës e, në veçanti, me veprimtarinë e Agjencive të Sigurisë.

Qëllimi i tyre është i qartë. Përmes zotërimit të këtyre informacioneve ata synojnë të hartojnë plane dhe të ndërmarrin veprime të fshehta, me qëllim kërcënimin e sigurisë kombëtare të Kosovës, në mënyrë që vendi ynë të mbetet edhe në të ardhmen një vend me siguri të paqëndrueshme, të jetë një shtet i dështuar dhe i destabilizuar, për ta përdorur këtë si pretekst për të rrezikuar paqen dhe sigurinë jo vetëm të Kosovës, por edhe të rajonit të Ballkanit Perëndimor.

Mbrojtja e informacioneve të klasifikuara të Kosovës ndaj sistemeve depërtuese të Republikës së Serbisë

Ky problem është bërë edhe më i pranishëm për faktin se edhe pas përfundimit të luftës, në qershor 1999, në Kosovë kanë vazhduar veprimtarinë e tyre disa struktura joligjore të Serbisë, siç janë: Shërbimi Sekret i Serbisë (BIA), Ministria e Punëve të

Brendshme (MUP), Mbrojtja Civile dhe struktura të tjera. Operatorët joligjorë të Postës dhe Telekomit të Serbisë, që kanë vepruar në disa pjesë të territorit të Kosovës, paraqitnin një mundësi dhe rrezik potencial për qasje dhe depërtim në informacionet e klasifikuara të Kosovës. Këto struktura joligjore, të dirigjuara nga qeveria e Serbisë, në bashkëpunim të ngushtë me grupe të organizuara kriminale në pjesët e territorit të Kosovës ku jeton minoriteti serb, veçanërisht në Rajonin e Mitrovicës Veriore, duke përfituar nga situata e paqëndrueshme politike pas shpalljes së pavarësisë, kanë luajtur rol të madh në organizimin e jetës në të gjitha fushat, duke u fuqizuar si faktorë vendimmarrës dhe duke iu imponuar popullatës së gjerë. Veriu i Republikës së Kosovës ishte bërë parajsë edhe për të gjitha format e krimit të organizuar. Këto struktura joligjore dhe grupe të organizuara kriminale e kishin zgjeruar fushën e veprimtarisë së tyre, duke depërtuar edhe në zonat e brendshme të territorit të Republikës së Kosovës, në bashkëpunim të ngushtë me grupet e organizuara kriminale lokale dhe rajonale. Gjatë kësaj kohe, Serbia ka pasur 2200 agjentë në Ballkan, që kanë punuar për Shërbimin e Sigurimit Shtetëror Serb, dhe vetëm në territorin e Kosovës kishte 700 agjentë, pra, një rrjet të gjerë agjentësh të Shërbimeve të saj Sekrete, në veçanti, Shërbimit Sekret Serb (BIA). Përveç BIA-s, në Kosovë ka edhe 400 bashkëpunëtorë publikë dhe të fshehtë të MUP-it. (http://www.albaniadiaspora.com/ gazeta e diasporës shqiptare, 25.12.2015).

Shërbimet serbe po punojnë intensivisht për zbehjen e imazhit të kosovarëve në sytë e ndërkombëtarëve, duke tentuar që gradualisht Kosova nga viktimë të marrë tiparet e viktimizuesit (http://www.albaniadiaspora.com/ gazeta e diasporës shqiptare, 25.12.2015).

Agjentët e BIA-s që kanë vepruar në veri të Mitrovicës, të gjitha informacionet i kanë dërguar të shkruara në letër, në CD apo në USB në qytetin e Kralevës, në Serbi,

duke ua dorëzuar udhëheqësve të BIA-s.(http://www.telegrafi.com/lajme/ja-si-ka-vepruar-sherbimi-sekret-serb-kunder-kosoves-vitet-e-fundit-2-68433.htmlSpublikuar 10.08.2015).

Veprimtaria e strukturave joligjore të Serbisë në pjesën veriore të vendit tone është ndërprerë pas aksionit të Institucioneve të Sigurisë së Kosovës, të realizuar më 15 korrik 2012, por nuk duhet neglizhuar fakti që ende në Kosovë janë infiltruar dhe veprojnë shumë agjentë të fshehtë, që gjithsesi përbëjnë kërcënim për sigurinë kombëtare.

7.4. Klasifikimi i informacioneve në Republikën e Sllovenisë

Në Republikën e Sllovenisë, klasifikimi i informacioneve zbatohet në të gjitha institucionet publike, që ushtrojnë kompetenca ekzekutive, legjislative, gjyqësore, si dhe në Presidencën e Republikës së Sllovenisë.

Atje konsiderohet informacion i klasifikuar çdo informacion dhe material, publikimi i paautorizuar i të cilëve do të cenonte në shkallë të ndryshme interesat e sigurisë së Republikës së Sllovenisë. Ndërsa autoritet i klasifikimit të informacioneve është çdo person i përcaktuar që ka Kompetencë origjinale apo të deleguar për të klasifikuar informacione (Akti mbi Informacionin e Klasifikuar - Gazeta Zyrtare e Republikës së Sllovenisë, nr.: 50/06).

Bartës i autorizuar i informacioneve të klasifikuara është çdo personi që ka në posedim informacionin e klasifikuar, që ka leje të vlefshme të sigurisë dhe i plotëson kushtet tjera që lejojnë qasjen në informacionin e klasifikuar, përveç nëse përcaktohet ndryshe me ligj.

Informacioni mund të përkufizohet si ‘i klasifikuar’, nëse është brenda një apo më shumë prej këtyre kategorive:

- siguri publike;
- mbrojtje;
- Punë të Jashtme;
- inteligjencë dhe aktivitetet e sigurisë së Agjencive Shtetërore të Republikës së Sllovenisë;
- sisteme, projekte, plane apo shërbime të mbrojtjes, që lidhen me interesat thelbësore të sigurisë, të inteligjencës dhe të aktiviteteve të Agjencive Shtetërore të Republikës së Sllovenisë;
- veprimtari hulumtuese shkencore, teknologjike, ekonomike, financiare, që lidhen me interesat thelbësore të sigurisë, të inteligjencës dhe të aktiviteteve të Agjencive Shtetërore të Republikës së Sllovenisë.

Nivelet e klasifikimit të informacioneve në Slloveni

Në secilin institucion publik në Slloveni, autoriteti i klasifikimit vendos nëse informacioni duhet klasifikuar dhe përcakton nivelin e klasifikimit të informacionit qysh në momentin kur prodhohet informacioni. Vendimi nëse duhet klasifikuar informacioni dhe përcaktimi i nivelit të klasifikimit bazohet në vlerësimin e pasojave të dëmshme, që mund të rezultojnë për interesat e sigurisë së Republikës së Sllovenisë nga hapja e paautorizuar e një informacioni (Akti mbi Informacionin e Klasifikuar - Gazeta Zyrtare e Republikës së Sllovenisë, Nr. 50/06).

Niveli i klasifikimit të informacionit bëhet varësisht nga shkalla e dëmit, që do të shkaktonte në interesat e sigurisë në Republikën e Sllovenisë publikimi i paautorizuar i tij.

Në Slloveni ekzistojnë katër nivele të klasifikimit të informacioneve, ato janë: niveli tepër sekret, sekret, konfidencial dhe niveli i kufizuar.

Niveli "Tepër Sekret" zbatohet për informacionet, hapja e paautorizuar e të cilave, sipas vlerësimit të arsyeshëm, do të shkaktonte dëm jashtëzakonisht të rëndë për interesat e sigurisë së Republikës së Sllovenisë.

Informacione të klasifikuara si tepër sekret, mund të jenë informacionet që përmbajnë plane mbrojtjeje, plane ushtarake, sisteme armësh apo operacione.

Niveli "Sekret" zbatohet për informacionet, hapja e paautorizuar e të cilave do t'i dëmtonte seriozisht interesat e sigurisë së Republikës së Sllovenisë (Akti mbi Informacionin e Klasifikuar - Gazeta Zyrtare e Republikës së Sllovenisë, nr. 50/06).

Informacione sekrete mund të jenë ato informacione që përmbajnë të dhëna për sigurinë publike, të dhëna për individët, për grupet kriminale që merren me krim të organizuar.

Niveli "Konfidencial" zbatohet për informacionet, hapja e paautorizuar e të cilave do t'i dëmtonte interesat e sigurisë së Republikës së Sllovenisë. Të nivelit konfidencial mund të konsiderohen procedurat standarde të operimit, rregulloret e brendshme, raportet e punës etj.

Niveli "I Kufizuar" zbatohet për informacionet, hapja e paautorizuar e të cilave mund të dëmtojë veprimtarinë ose kryerjen e detyrave të një agjencie.

Kompetencën origjinale për klasifikim në nivelin "Tepër Sekret" e kanë: Presidenti i Sllovenisë, Kryetari i Kuvendit të Sllovenisë, Kryeministri, Kryesuesi i Këshillit të Sigurisë së Sllovenisë; Drejtori i Agjencisë së Sllovenisë për Inteligjencë; Drejtori i Përgjithshëm i Policisë së Sllovenisë dhe Komandanti i Forcave të Armatosura të Sllovenisë.

Për të pasur qasje në informacione të klasifikuara është rregull i përgjithshëm që, për qasje në informacione të klasifikuara, çdo person duhet të ketë lejen e vlefshme të sigurisë, të ketë nevojë për të qenë në dijeni të këtyre informacioneve, për të kryer misionin apo detyrën e tij zyrtare, dhe të ketë nënshkruar deklaratën e konfidencialitetit. Përjashtim bëhet vetëm për Presidentin e Republikës së Sllovenisë, për Kryetarin e Kuvendit të Sllovenisë dhe për kryeministrin, të cilët janë të autorizuar të kenë qasje në informacionet e klasifikuara në funksion të kryerjes së detyrave zyrtare të tyre pa i përmbushur këto kërkesa, me kusht që të kenë nevojë për të qenë në dijeni të këtyre informacioneve.

7.5. Klasifikimi i informacioneve në Republikën e Kroacisë

Siguria e Informacionit në këtë vend është një zonë e sigurisë, për të cilën janë të përcaktuara dhe zbatohen në praktikë masa dhe standard, si: masat e përgjithshme të sigurisë për parandalimin, zbulimin dhe eliminimin e dëmeve të shkaktuara nga humbja apo nga zbulimi i paautorizuar i informacionit të klasifikuar ose të paklasifikuar.

Organet dhe personat juridikë që i përdorin informacionet e klasifikuara dhe ato të paklasifikuara brenda sferës së tyre të aktiviteteve, aplikojnë procedurat për trajtimin

e informacioneve të klasifikuara dhe atyre të paklasifikuara, si dhe standardet dhe masat për mbikëqyrjen e sigurisë së informacioneve.

Nivelet e klasifikimit të informacioneve janë: tepër sekret, sekret, konfidencial dhe i kufizuar.

Niveli i klasifikimit të informacionit bëhet varësisht prej shkallës së dëmit që do të shkaktonte publikimi i paautorizuar i tij në interesat e sigurisë në Republikën e Kroacisë. Në Kroaci ekzistojnë katër nivele të klasifikimit të informacioneve, ato janë: niveli tepër sekret, sekret, konfidencial dhe niveli i kufizuar.

Niveli "Tepër Sekret", zbatohet për informacionet, hapja e paautorizuar e të cilave sipas vlerësimit të arsyeshëm do të shkaktonte dëm jashtëzakonisht të rëndë për interesat e sigurisë së Republikës së Kroacisë.

Niveli "Sekret", zbatohet për informacionet, hapja e paautorizuar e të cilave do t'i dëmtonte seriozisht interesat e sigurisë së Republikës së Kroacisë.

Niveli "Konfidenciale", zbatohet për informacionet, hapja e paautorizuar e të cilave do të mund t'i dëmtonte interesat e sigurisë së Republikës së Kroacisë.

Niveli "E Kufizuar", zbatohet për informacionet, hapja e paautorizuar e të mund të dëmtojë veprimtarinë ose kryerjen e detyrave të Agjencioneve.

7.6. Vështrim i përgjithshëm krahasues mbi shërbimet e inteligjencës dhe rolin e tyre për sigurinë e informacionit

Termi inteligjencë i referohet shkallës së ndërgjegjësimit dhe të kuptuarit që ka një shtet për mjedisin e tij strategjik, duke u bazuar në mbledhjen dhe në analizën e të

dhënave sekrete dhe publike. Në këto të dhëna përfshihen edhe informacionet e ndryshme rreth shteteve, grupeve, individëve ose aktiviteteve potencialisht të rrezikshme, përfshirë edhe terrorizmin.

Mbledhja e informacioneve, analiza, përpunimi dhe shpërndarja e tyre apo, siç quhet ndryshe, inteligjenca, është një detyrë tejet e rëndësishme. Kjo është dhe arsyeja pse shumë vende u kushtojnë rëndësi të madhe agjencive të inteligjencës.

Shërbimet e inteligjencës kanë ekzistuar në një formë apo një tjetër për shekuj me radhë, roli i tyre ka qenë gjithmonë për të spiunuar njëri-tjetrin (Vilasi, 2013: 1).

Shërbimet e inteligjencës luajnë një rol të rëndësishëm në mbrojtjen e sigurisë nacionale dhe zbatueshmërinë e sundimit të ligjit. Qëllimi kryesor i tyre është mbledhja, analizimi dhe shpërndarja e informacionit që ndihmon politikëbërësit dhe subjektet tjera publike të ndërmarrin masa në mbrojtjen e sigurisë kombëtare. Kjo ka të bëjë edhe me mbrojtjen e të drejtave të njeriut (DCAF, Pako Udhëzimesh, 2011: 10).

Agjencitë e inteligjencës janë pjesa më vitale dhe më e ndjeshme e një shteti, ato janë stabilizuesit, por edhe alarmuesit e parë të shtetit, nëse ai kërcënohet. Sa më e fortë të jetë inteligjenca e një shteti, aq më të fortë janë edhe sektorët tjerë, si: diplomacia, siguria, ekonomia dhe energjia. Shërbimet e inteligjencës luajnë një rol krucial në mbrojtjen e shtetit dhe të popullsisë kundër kërcënimeve ndaj sigurisë kombëtare, përfshirë edhe terrorizmin (DCAF, 2011: 14). Këtë e themi, sepse, aktualisht, bota moderne ka hyrë në epokën e informacionit. Lufta për informacion është lufta për njohjen e situatës së vërtetë. Nëse nuk posedojmë informacione dhe nuk e njohim situatën e vërtetë, atëherë nuk jemi në gjendje të marrim vendime të drejta. Rëndësia e shërbimeve të inteligjencës në shoqëri është mjaft e madhe, ato prodhojnë analiza në fusha të rëndësishme që lidhen me sigurinë kombëtare, bëjnë mbledhjen e

informacioneve dhe qasjen në të dhëna. Kjo nënkupton përdorimin e burimeve të hapura dhe të burimeve të fshehta, siç janë spiunët, agjentët, informatorët e ndryshëm, bashkëpunëtorët etj.

Shërbimet e inteligjencës janë një ndër shtyllat më të forta dhe më të rëndësishme të një shteti, sepse luajnë një rol jetik në mbrojtjen e sigurisë kombëtare. Meqë burimet e tyre janë të kufizuara, është me rëndësi që këto burime të përdoren në mënyrë efektive dhe efikase.

Shërbimet e inteligjencës së një shteti, në pajtim me kompetencat dhe me përgjegjësitë ligjore të tyre, bëjnë mbledhjen, sistematizimin, analizën, përcaktimin dhe pasimin e informatave dhe të të dhënave; zbulojnë, hulumtojnë dhe pamundësojnë qëllimet e shërbimeve të huaja informative ndaj shtetit të vet duke përdorur metoda dhe mjete të posaçme në parandalimin, zbulimin dhe hulumtimin e të gjitha dukurive dhe të ngjarjeve që përbëjnë kërcënim të sigurisë së një shoqërie (Maslesha, 2006: 81).

Në shoqëritë demokratike, shërbimet e inteligjencës mbledhin informacionet që u nevojiten për të përmbushur mandatin e tyre nga burimet publike, siç janë artikujt e mediave, raportet nga organizatat qeveritare dhe joqeveritare, si dhe botimet akademike. Shërbimet e inteligjencës, gjithashtu, mbledhin informacione nga personat dhe anëtarët e grupit, që me veprimet e tyre terroriste kërcënojnë sigurinë kombëtare, duke përdorur edhe persona me identitete false për t'u infiltruar në organizata dhe për të dhënë informacione për aktivitetet e tyre.

Në aspektin e sigurisë kombëtare, shërbimet e inteligjencës janë ajka e shtetit, janë organi më i rëndësishëm dhe më efikas në identifikimin dhe parandalimin e rreziqeve të sigurisë kombëtare. Nëse shteti posedon shërbime të inteligjencës që janë me nivel të lartë profesional, efikase, efektive dhe që në aspektin kombëtar i kushtojnë

vëmendje të lartë sigurisë së informacionit dhe janë të përgatitura për çdo situate, atëherë shteti ka të ardhme të sigurt, e ka sigurinë kombëtare të sigurt, sepse ka informacione të sakta.

Këto arrihen duke pasur informacione, informatorë të besueshëm dhe profesionistë në sjelljen e informatës së saktë, po ashtu, edhe duke përdorur të gjitha burimet njerëzore dhe teknologjike për të ofruar standardet më të larta të informacioneve të klasifikuara dhe të sigurisë së tyre, sepse këto paraqesin aset kombëtar dhe janë shumë të vlefshme për sigurinë kombëtare.

Mungesa e profesionalizmit dhe mungesa e informacioneve reflektohet edhe në efikasitetin e dobët të shërbimeve të inteligjencës dhe ky fakt bën që një shtet nuk do të mund të kishte zhvillime progresive dhe frytdhënëse për mbarëvajtjen e sigurisë së tij.

Për t'i eliminuar këto dobësi nevojitet edhe një mbikëqyrje efektive. Në demokracitë e reja, mbikëqyrja efektive e komunitetit të inteligjencës është e rëndësishme, për shkak të tensionit që ekziston mes punës së inteligjencës dhe vlerave demokratike të caktuara, të tilla, si hapja dhe transparenca (Born & Wills, 2012: 75).

Sot, pothuajse të gjitha shtetet e botës, në strukturat e tyre institucionale dhe shoqërore kanë shërbime të inteligjencës, sepse për të pasur një shërbim sa më efikas për shtetin kërkohet mbledhja, vlerësimi, analizimi i informacioneve dhe siguria e informacioneve. Këto mundësojnë analizimin e kërcënimeve të mundshme ndaj sigurisë kombëtare dhe ndihmojnë në parandalimin e krizave eventuale, mundësojnë mbarëvajtjen e zhvillimeve si dhe sigurojnë stabilitetin e situatës së sigurisë në territorin e vendit, ku ato veprojnë.

Institucionet për mbikëqyrjen e shërbimeve të inteligjencës gjatë punës së tyre kanë qasje në informacionin e klasifikuar dhe të ndjeshëm. Prandaj një sërë

mekanizmash janë të vendosura për të siguruar institucionet mbikëqyrëse dhe pjesëtarët e tyre që të mos shpalosin informacionin e tillë në mënyrë të qëllimshme apo të paqëllimshme (DCAF, Pako Udhëzimesh, 2011: 18).

Në lidhje me rëndësinë e shërbimeve të inteligjencës theksohet se: "Pa një shërbim të fuqishëm, të mençur dhe të mprehtë të inteligjencës, si presidentët, ashtu edhe gjeneralët mbesin të verbër dhe të paaftë për të vepruar" (Weiner, 2011: 8).

Në Republikën e Kosovës, Agjencia e Kosovës për Inteligjencë është Shërbimi Kombëtar i Inteligjencës, ndërsa si shërbime të inteligjencës me ndikim, si në përfshirje në territorin e tyre, por edhe në aspekte rajonale ndërkombëtare, janë: Shërbimet e Inteligjencës Amerikane, Shërbimet e Inteligjencës Gjermane, Shërbimet e Inteligjencës Ruse, Shërbimet Britanike të Inteligjencës, Shërbimi i Inteligjencës së Izraelit, por edhe shërbime tjera të inteligjencës.

7.7. Agjencia e Kosovës për Inteligjencë - AKI

Në kuadër të institucioneve të sigurisë së Republikës së Kosovës, vepron edhe Agjencia e Kosovës për Inteligjencë, e cila në fokus të veprimtarisë së saj ka mbledhjen, vlerësimin, analizimin dhe shpërndarjen e informacioneve, me qëllim luftimin e kërcënimeve të brendshme dhe të jashtme, përfshirë edhe terrorizmin, si njërin nga kërcënimet më serioze. Në nivel kombëtar, Agjencia e Kosovës për Inteligjencë është e vetmja Agjenci e Inteligjencës.

AKI është themeluar në mesin e vitit 2008, pas shpalljes së Pavarësisë së Kosovës, si shtet i pavarur dhe sovran.

AKI është themeluar për të mbledhë informata në lidhje me kërcënimet dhe rreziqet ndaj sigurisë në Kosovë (Qehaja, 2012: 117). Duke marrë parasysh që AKI nuk ka faqe zyrtare të internetit (ueb-faqe), ky fakt e bën atë më të mbyllur nga agjencitë tjera të inteligjencës.

Puna e AKI-së bazohet në Kushtetutën e Republikës së Kosovës dhe në ligjin për AKI-në. Sipas Kushtetutës së Republikës së Kosovës, mandati i AKI-së është të zbulojë, të hetojë dhe të mbikëqyrë kërcënimet ndaj sigurisë së Kosovës (Kushtetuta e Kosovës, Neni 129).

Po ashtu, Kushtetuta sanksionon që AKI-ja të jetë një institucion profesional, politikisht i paanshëm, me përbërje shumetnike dhe që i nënshtrohet kontrollit apo mbikëqyrjes nga ana e Parlamentit (Kushtetuta e Kosovës, Neni 129).

AKI ka mandat të veprojë në tërë territorin e Kosovës, ajo ka rolin primar në luftimin e kërcënimeve ndaj sigurisë dhe, në këtë kontekst, edhe të luftimit të kërcënimeve ndaj sigurisë së informacionit. Ajo është themeluar si domosdoshmëri e nevojës për informacion me kohë dhe të saktë për inteligjencë, kundër-inteligjencë, kërcënime nga brenda dhe jashtë, terrorizmin ndërkombëtar apo vendor, prodhimin dhe trafikimin e narkotikëve, krimin e organizuar, krimin ekonomik, sabotazhin dhe të gjitha çështjet tjera të inteligjencës të lidhura me sigurinë e Kosovës është esenciale për popullin e Kosovës (Kushtetuta e Kosovës, Neni 169).

Ashtu sikurse institucionet tjera të sigurisë, edhe AKI është ballafaquar me shumë sfida, njëra prej të cilave ka qenë bashkëpunimi me qytetarët e Kosovës. Megjithëse barrierat e të kaluarës për mosbashkëpunim me institucionet e sigurisë janë eliminuar (më parë akti i bashkëpunimit me këto institucione është konsideruar si veprim tradhtie), tani, përkundrazi, bashkëpunimi me institucionet e sigurisë paraqet

çelësin e sigurisë për parandalimin dhe luftimin e veprimeve kriminale e, në këtë kontekst, edhe të veprave penale të ndërlidhura me sigurinë e informacionit.

AKI ka hapësirë veprimi vetëm brenda territorit të Kosovës. Kjo, po ashtu, paraqet një sfidë për AKI-në, sepse kufizimi i veprimit të saj vetëm brenda territorit të Kosovës e kufizon edhe fushëveprimin e saj për të dërguar dhe për të infiltruar agjentët e saj në territorin e shteteve tjera.

Informata më specifike na ofron Ligji për Agjencinë e Kosovës për Inteligjencë, i miratuar nga Kuvendi i Republikës së Kosovës në qershor 2008. Sipas këtij ligji, AKI është agjenci për siguri dhe inteligjencë në Kosovë, që nuk ka fuqi ekzekutive, në këtë mënyrë eliminon mundësinë që AKI të përdorë forcë në mënyrë direkte apo indirekte, arrestimin e qytetarëve apo inicimin e procedurave penale (Ligji për AKI-në, Neni 2).

Ligji për Agjencinë e Kosovës për Inteligjencë nuk i jep AKI-së autorizim që të detyrojë persona apo kompani të bashkëpunojnë për aktivitetet e saj, përveçse kur bashkëpunimi i tyre është në baza vullnetare. AKI është agjenci e pavarur që i raporton direkt Kryeministrit dhe Presidentit të Republikës. Agjencia nuk është pjesë e strukturës së ndonjë ministrie dhe as pjesë e zyrës së Kryeministrit. Ajo është agjenci për siguri dhe inteligjencë në Kosovë, që mbledh informacione në lidhje me kërcënimet ndaj sigurisë së Kosovës.

Si rast kërcënimi ndaj sigurisë së Kosovës konsiderohen: kërcënimi ndaj integritetit territorial, ndaj integritetit të institucioneve, ndaj rendit kushtetues, stabilitetit dhe zhvillimit ekonomik, si dhe kërcënimet ndaj sigurisë globale në dëm të Kosovës, përfshirë:

- Terrorizmin;
- nxitjen, ndihmën dhe shtytjen ose përkrahjen e terrorizmit,

- spiunazhin kundër Kosovës apo në dëm të sigurisë së Kosovës;
- sabotazhin drejtuar kundër infrastrukturës vitale të Kosovës;
- krimin e organizuar kundër Kosovës apo në dëm të sigurisë së Kosovës në cilëndo mënyrë, përfshirë larjen e parave;
- nxitjen e pakënaqësisë në strukturat e sigurisë;
- trafikimin e substancave ilegale, armëve apo qenieve njerëzore;
- prodhimin ilegal apo transportin e armëve të shkatërrimit në masë, ose të komponentëve të tyre, si dhe të materialeve dhe pajisjeve të nevojshme për prodhimin e tyre;
- trafikimin ilegal të prodhimeve dhe të teknologjive nën Kontrollin Ndërkombëtar;
- aktivitetet që bien ndesh me të drejtën humanitare ndërkombëtare;
- aktet e dhunës së organizuar apo të frikësimit kundër grupeve etnike apo fetare në Kosovë,
- çështjet që kanë të bëjnë me kërcënime serioze ndaj shëndetit apo sigurisë publike (Ligji për AKI-në, Neni 3).

Për të realizuar aktivitetet e saj, AKI-ja ka mundësitë e veta për mbledhjen e informacionit, që përfshijnë:

përgjimin mobil dhe statik;

personelin e fshehtë për mbledhjen e informacioneve;

përgjimin teknik, siç janë pajisjet për dëgjim, përgjim dhe përcjellje;

agjentët e fshehtë dhe mbledhjen e të dhënave konfidenciale, si nga bankat, portet dhe telefonin.

Prioritetet strategjike të AKI-së parashtrohen në Platformën Vjetore të Politikës së Inteligjencës dhe Sigurisë, e cila përmban udhëzimet e përgjithshme për punën e AKI-së (Ligji për AKI-në, Neni 2).

AKI-ja respekton parimet e Deklaratës Universale për të Drejtat e Njeriut, të Konventës Ndërkombëtare për të Drejtat Civile dhe Politike, të Konventës Europiane për Mbrojtjen e të Drejtave të Njeriut dhe të Lirive Themelore, dhe parime të tjera relevante, të pasqyruara në instrumentet ligjore të njohura ndërkombëtarisht, dhe kryen aktivitetet e veta në pajtueshmëri me to.

AKI-ja, organet dhe institucionet tjera në Kosovë janë të obliguara të bashkëpunojnë dhe të ndihmojnë njëra-tjetrën në kryerjen e detyrave të tyre dhe të koordinojnë aktivitetet brenda kompetencave të veta, në harmoni me ligjet dhe me rregulloret në fuqi në lidhje me mbrojtjen e burimeve, të metodave dhe të informacionit tjetër të klasifikuar (Ligji për AKI-në, Neni 8).

Mbledhja, ruajtja dhe trajtimi i informacionit dhe i sigurisë së informacioneve të klasifikuara nga AKI

AKI është e autorizuar të mbledhë, të mbajë dhe të shpërndajë informacione për qëllime të ligjshme qeveritare. Këto aktivitete rregullohen me procedura strikte, në pajtueshmëri me parimin e ligjshmërisë, të proporcionalitetit, të nevojës për të ditur dhe vetëm për avancim të sigurisë kombëtare. I gjithë informacioni i mbledhur klasifikohet në një mënyrë, që përcaktohet si e përshtatshme nga drejtori i AKI-së dhe në

pajtueshmëri me legjislacionin përkatës në fuqi për mbrojtjen dhe klasifikimin e informacionit (Ligji për AKI-në, Neni 23).

Punonjësit e AKI-së duhet të mbrojnë informacionin e klasifikuar dhe, si kusht punësimi, nënshkruajnë një marrëveshje për ruajtjen e fshehtësisë. Obligimi për të mbrojtur këto fshehtësi nuk pushon, kur punonjësi nuk është më i punësuar në AKI. Procedura e përmendur më lart lejon mbledhjen e informacionit i cili përfshin, por nuk kufizohet në informacionin e mbledhur gjatë aktivitetit të ligjshëm të inteligjencës, informacionin që del nga hetimi i ligjshëm i personelit ose sigurimit fizik, ose informacionin që ka të bëjë me personat për të cilët ka arsye të besohet se janë burime apo kontakte potenciale me qëllimin e vetëm të përcaktimit të përshtatshmërisë ose të besueshmërisë të tyre (Ligji për AKI-në, Neni 23).

Në kryerjen e detyrave dhe të përgjegjësive të veta, AKI-ja mund të mbledhë informacione duke i fshehur arsyet për mbledhjen e tij, për shkak të natyrës sekrete të tyre; mund të krijojë kontakte të fshehta me individë private; mund të krijojë dhe mund të përdorë sisteme informacioni për avancimin e mbledhjes së inteligjencës; mund të përdorë forma të mashtrimit operativ që nuk shkaktojnë lëndime fizike apo që dëmtojnë shëndetin; mund të përgatisë dhe të përdorë dokumente mbulesë për mbrojtjen e punonjësve të AKI-së dhe të personave fizikë që bashkëpunojnë me ta, si dhe fshehjen e qëllimit të sigurisë së tyre; mund të krijojë dhe të mbajë organizata të përkohshme për qëllime të mbledhjes së fshehtë të të dhënave, si dhe mund të caktojë punonjës të AKI-së të punojnë në fshehtësi në institucione apo organe të Kosovës (Ligji për AKI-në, Neni 23).

AKI ndërmerr masat përkatëse të sigurisë për mbrojtjen e informacioneve, të ruajtura në skeda të automatizuara të të dhënave, nga shkatërrimi aksidental apo i

paautorizuar, nga humbja aksidentale, si dhe nga qasja, nga ndryshimi dhe nga shpërndarja aksidentale (Ligji për AKI-në, Neni 31).

Mbikëqyrja e AKI-së kryhet nga Komisioni Mbikëqyrës Parlamentar. Gjatë mbikëqyrjes parlamentare të ushtruar nga ky Komision do të vihet në dispozicion informacion i klasifikuar, përveçse kur shpalosja e tij do të kërcënonte interesat vitale të sigurisë kombëtare të lidhura me mbrojtjen e burimeve dhe të metodave në një rast specifik. Anëtarët e Komisionit Mbikëqyrës Parlamentar janë të detyruar të ruajnë fshehtësinë lidhur me informacionin që ka të bëjë me sekretet zyrtare në të cilat kanë pasur qasje dhe ky obligim i ruajtjes së sekretit do të mbetet në fuqi pas përfundimit të këtij mandati (Ligji për AKI-në, Neni 38). Komisioni mbikëqyrës parlamentar krijon procedura me shkrim për të mbrojtur sigurinë e informacioneve të klasifikuara nga zbulimi dhe qasja e paautorizuar. (Ligji për AKI-në, Neni 35). Në mënyrë që të kryejnë funksionet e tyre mbikëqyrëse, anëtarëve të komisionit u duhet qasje në informacionet e klasifikuara.

Ligji për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë, me përjashtim të Presidentit, Kryeministrit dhe Kryetarit të Kuvendit, kërkon nga secili, përfshirë dhe deputetët e Kuvendit të Kosovës, t`i nënshtrohen verifikimit të sigurisë para se të kenë qasje në informacionet e klasifikuara. Kjo e lë të hapur mundësinë që deputetit mund t`i refuzohet kërkesa për qasje në informacion të klasifikuar.

Që nga themelimi i saj e deri më sot AKI, ka arritur të performojë detyrat e saj me profesionalizëm. Deri më tani, asnjë rast i shkeljes së të drejtave të njeriut nga ana e AKI-së nuk është evidencuar nga Avokati i Popullit.

AKI ka arritur të identifikojë me kohë disa celula terroriste në Kosovë, madje ka ngritur dyshime se “disa organizata joqeveritare ishin të përfshira në disa aktivitete të

dyshimta për pastrimin e parave, në funksion të akteve të ardhshme terroriste në Lindjen e Mesme. Bazuar në këto suksese, Departamenti Amerikan i Shtetit ka përshëndetur performancën e AKI-së (Raporti i Shteteve për Terrorizmin" 2009).

7.8. Agjencia për Siguri dhe Inteligjencë e Republikës së Sllovenisë – SOVA

Agjencia për Siguri dhe Inteligjencë e Sllovenisë (SOVA) është themeluar si agjenci e pavarur informative dhe e sigurisë menjëherë pas njohjes së pavarësisë së Republikës së Sllovenisë. Integrimi i Sllovenisë në NATO, BE dhe në mekanizmat e tjerë ndërkombëtarë ka krijuar lehtësira edhe në fushën e sigurisë. Bazuar në parimin se vendi ka nevojë për një organizatë profesionale dhe efektive, SOVA, si shërbim i pavarur ofron mbështetje në marrjen e vendimeve për sigurinë kombëtare të Republikës.

Bazë ligjore për veprimtarinë e saj është Akti, i miratuar fillimisht në vitin 1999 e, më pas, i ndryshuar në nëntor të vitit 2003. Neni 2 i Aktit i përcakton tri detyra themelore të agjencisë: mbledhja e të dhënave; vlerësimi i të dhënave dhe transmetimi i të dhënave nga jashtë ose në lidhje me vendet tjera të botës.

Meqenëse Republika e Sllovenisë ka sistem shtetëror demokratik, puna e institucioneve të sigurisë e, në veçanti, e atyre inteligjente, ka disa institucione mbikëqyrëse. Në rastin konkret, Agjencia për Siguri dhe Inteligjencë mbikëqyret nga qeveria, përmes Komisionit Parlamentar, nga gjykata përkatëse, nga Avokati i Popullit, nga gjykata e auditimit të buxhetit dhe nga zyra e mbikëqyrjes pranë Ministrisë së Financave. Gjithashtu, SOVA ka edhe mekanizmat e brendshëm të kontrollit.

7.9. Agjencia e Sigurisë dhe Inteligjencës së Kroacisë - SOA

Agjencia e Sigurisë dhe Inteligjencës është Shërbimi Kroat i Sigurisë dhe Inteligjencës, i themeluar në vitin 2006, me miratimin e Aktit të Sistemit të Sigurisë dhe Inteligjencës së Republikës së Kroacisë.

Sistemi i Sigurisë dhe Inteligjencës në Kroaci është reformuar në vitin 2006, me miratimin e Ligjit për Sigurinë dhe Sistemin e Inteligjencës (Zakon o sigurnosno-obavještajnom sustavu). Me këtë ligj janë krijuar dy shërbime të sigurisë, që janë ende aktive sot:

Agjencia e Sigurisë dhe Inteligjencës.

Agjencia e Sigurisë dhe Inteligjencës Ushtarake.

Agjencia e Sigurisë dhe Inteligjencës është përqendruar në parandalimin e veprimtarive apo veprimeve të ndërmarra që rrezikojnë rendin kushtetues, sigurinë e organeve shtetërore, të qytetarëve dhe interesat kombëtare, si në vijim:

- terrorizmi dhe format e tjera të dhunës së organizuar,
- aktivitetet e inteligjencës të agjencive të huaja të inteligjencës, të organizatave dhe individëve,
- organizatat ekstremiste dhe aktivitetet e grupeve dhe të individëve,
- rrezikimi i sigurisë së zyrtarëve më të lartë shtetërorë dhe i hapësirave dhe i objekteve të mbrojtura,
- krimi i organizuar dhe krimi ekonomik,
- qasja e paautorizuar në sistemet e informacionit dhe të komunikimit të mbrojtura të organeve qeveritare,

- zbulimi i informacionit të klasifikuar nga drejtuesit dhe punonjësit e organeve shtetërore, të institucioneve shkencore dhe personat juridikë me autorizime publike,
- aktivitetet e tjera, që synojnë të kërcënojnë sigurinë kombëtare.

SOA mbledh, analizon, përpunon dhe vlerëson të dhënat ekonomike, politike, shkencore-teknologjike, të sigurisë dhe të dhëna tjera që kanë të bëjnë me shtetin, me organizatat, me aleancat politike dhe ekonomike, me grupe dhe njerëz, veçanërisht ato që tregojnë qëllimet, aftësitë, planet dhe aktivitetet sekrete, me të cilat kërcënohen siguria kombëtare ose të dhënat që cilat janë me rëndësi për sigurinë kombëtare të Republikës së Kroacisë.

KAPITULLI 8: PËRFUNDIME DHE REKOMANDIME

Nga studimi dhe analiza komplekse e sigurisë së informacionit, në përgjithësi, dhe veprave penale të ndërlidhura me sigurinë e informacionit, në veçanti, në Kosovë për periudhën 2007-2015, si dhe nga shtjellimi i hipotezave bazë të këtij punimi nëpërmjet metodologjive shkencore të prezantuara në pjesën e hyrjes, kemi arritur në disa përfundime dhe rekomandime që sipas mendimit tonë janë të dobishme dhe që janë pasqyruar në vijim.

8.1. PËRFUNDIME

- Informacioni dhe siguria e tij janë bashkudhëtarë, që e kanë përcjellë zhvillimin e shoqërisë.

- Shoqëria bashkëkohore sot ballafaqohet me arritjet më të mëdha të zhvillimit tekniko- teknologjik. Rritja e përdorimit të teknologjisë informative, në përgjithësi, dhe e internetit, në veçanti, dhe tendenca për një shoqëri gjithnjë e më të ndërlidhur rrit edhe rreziqet me të cilat përballemi, sepse zhvillimi i teknologjisë informative dhe përdorimi i internetit në shoqërinë bashkëkohore ka sjellë një numër të madh lehtësish, në njërën anë, dhe, në anën tjetër, njëkohësisht ka krijuar lehtësira edhe për keqpërdorim të paramenduar të këtyre arritjeve teknologjike, ka krijuar mundësi shumë të lehta për kryerje të veprave penale kundër sigurisë së informacionit.

- Hapësira e informacionit dhe e sigurisë së informacionit kërkon bashkëpunim

dhe koordinim kombëtar dhe ndërkombëtar, për të garantuar sigurinë e informacioneve. Siguria e informacionit është problem që preokupon të gjithë përdoruesit e teknologjisë informative në një shoqëri. Në veçanti, siguria e informacionit është çështje prioritare për sigurinë kombëtare.

- Siguria e informacionit është detyrë e gjithë shoqërisë e kjo në Kosovë dhe në vendet tjera mund të arrihet duke ndërtuar ura të bashkëpunimit kombëtar dhe ndërkombëtar në harmonizimin e rregullave juridike dhe veprim të përbashkët në sigurimin e sistemeve globale informatike, zhvillimin e mëtejshëm të politikave dhe të procedurave për luftimin e krimeve kompjuterike.

- Problemi i sigurisë së informacionit dhe i veprave penale të ndërlidhura me sigurinë e informacionit vazhdon të mbetet shqetësim i madh edhe për shoqërinë kosovare, pasi kryerja e këtyre veprave përbën formën më të rrezikshme të shkeljes së të drejtave të njeriut, si dhe rrezik për sigurinë kombëtare.

- Klasifikimi i informacioneve është një komponentë shumë e rëndësishme për sigurinë e informacionit, sepse kjo mundëson themelimin e një sistemi unik për klasifikimin dhe ruajtjen e informacioneve që kanë të bëjnë me interesat nacionale të sigurisë si dhe për verifikimin e sigurisë së personave që kanë qasje në këto informacione.

- Në Kosovë, sipas kërkimeve tona, referuar burimeve dhe autorëve të ndryshëm, nuk rezulton që disa vepra penale të ndërlidhura me sigurinë e informacionit, siç janë

krimet kibernetike, të kenë ekzistuar më parë. Faktet flasin se këto vepra paraqesin një fenomen krejt të ri, që u shfaq pas vitit 1999, pas çlirimit të Kosovës, kohë pas të cilës morën përmasa dramatike.

- Veprat penale kundër sigurisë së informacionit kërkojnë reagim të specializuar të institucioneve të drejtësisë penale, të agjencive të zbatimit të ligjit dhe të prokurorisë, prandaj këto institucione duhet të avancojnë kapacitetet e tyre për rritjen e efikasitetit dhe të efektivitetit të hetimeve, të sigurimit të dëshmive elektronike të ndërlidhura me këto vepra penale.

- Relevancat nëpërmjet trajtimit të figurave të veprave penale të ndërlidhura me sigurinë e informacionit, përkufizimi juridik i qasur me Kodin Penal dhe disa ligje tjera që cilat janë pjesë përbërëse e kuadrit ligjor në Kosovë, identifikimi i figurave dhe i elementeve kryesore juridike të veprave penale dhe i veprimeve dhe elementëve të tjera, rrethanat e cilësuara etj., përbëjnë një ndihmesë për studentin e drejtësisë dhe për juristin, që të bëjnë dallimin e qartë ndërmjet veprave të tjera dhe të përcaktojnë saktë dispozitën konkrete të pjesës së posaçme të Kodit Penal, ku cilësohet juridikisht vepra penale dhe mbi bazën e së cilës do të akuzohet autori i saj.

- Trajtimi i dallimit të qartë midis veprave penale të ndërlidhura me sigurinë e informacionit do të ndihmojë sado pak punonjësit e policisë, të prokurorisë dhe të gjykatave në kualifikimin e saktë të veprës. Po ashtu, edhe dallimi midis figurave të këtyre veprave penale është me interes praktik.

- Reformat e kryera në fushën e legjislacionit, në kuadrin e integrimit Europian të Kosovës, harmonizimi i tij me konventat ndërkombëtare dhe me standardet e BE-së, kanë përfshirë hartimin e amendamenteve për një pjesë të konsiderueshme të kuadrit ligjor, siç janë Kodi Penal dhe Kodi i Procedurës Penale, si dhe hartimin e disa ligjeve të reja në fushën e sigurisë së informacioneve, si Ligji për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë, Ligji për Parandalimin dhe Luftimin e Krimeve Kibernetike, Ligji për Mbrojtjen e të Dhënave Personale, si dhe shumë ligje tjera.

- Kuadri ligjor i Kosovës në fushën e sigurisë së informacioneve ka ngjashmëri esenciale me legjislacionin e BE-së, në përgjithësi, dhe me legjislacionin e Sllovenisë, në veçanti.

- Kosova, megjithëse ka investuar shumë për kompletimin e kuadrit ligjor në fushën e sigurisë së informacionit, ende në nivel kombëtar nuk ka një strategji kombëtare në fushën e sigurisë së informacionit. Është nevojë urgjente hartimi i një Strategjie Kombëtare të Sigurisë së Informacionit, e cila brenda saj do të duhet të përmbajë edhe një strategji sektoriale në fushën e sigurisë kibernetike.

Këtë konkluzion e argumentoj duke u bazuar edhe në hulumtimin tim, të bazuar në analizën e pyetësorëve, që janë realizuar me tri Agjenci të Sigurisë, ku 99.1 % e të anketuarve deklarojnë se hartimi i një strategji nacionale në fushën e sigurisë së informacionit është i nevojshëm dhe duhet të jetë prioritet kombëtar.

Kjo strategji do të na orientojë të reflektojmë mbi natyrën e vlerave që ne dëshirojmë dhe gjykojmë se duhen mbrojtur. Ajo do t'u mundësojë Agjencive të Sigurisë të kuptojnë se në cilin segment gjenden hallkat e dobëta që rrezikojnë gjithë

sistemin e informacionit dhe sigurisë së tij.

- Punimi trajton edhe rreziqet strategjike që sjellin veprat penale kundër sigurisë së informacionit, në përgjithësi, dhe krimet kibernetike, në veçanti; rritjen dhe zgjerimin e krimit të organizuar; shkeljen e të drejtës së privatësisë; destabilizimin ekonomik përmes rasteve të mashtrimeve kompjuterike, ndërhyrjeve në sistemet bankare, shtimit të pastrimit të parave etj.

- Rasti i Kosovës përbën një shembull ekzemplar të *modus operandit* të veprave penale kundër sigurisë së informacionit. Ai duket shumë inovativ, krahasuar me grupet kriminale të vendeve të tjera të rajonit. Fillimisht, mënyra e veprimit të grupeve kriminale kosovare ka qenë në forma të thjeshta, si hyrje e paautorizuar në sistem kompjuterik, kërcënime dhe shantazhe përmes e-mail-it, por, më pas, u kalua në forma më të ashpra, duke iu bashkuar edhe grupeve më të organizuara kriminale dhe duke arritur që, në mënyrë të paautorizuar, të marrin të dhëna sekrete.

- Fakti që veprat penale kundër sigurisë së informacionit rrezikojnë çdo përdorues potencial të mjeteve të teknologjisë informatike dhe shfrytëzues të internetit, sugjeron forma më të gjithanshme të informimit, trajnimit, edukimit apo të të mësuarit, sidomos të të rinjve dhe të institucioneve të shoqërisë: familja, shkolla, shoqëria civile, institucionet e shtetit.

- Të dhënat tregojnë se suksesi lidhur me parandalimin e veprave penale të ndërlidhura me sigurinë e informacionit varet shumë nga shkalla e njohjes dhe e

informimit të të rinjve për mundësitë e rrezikut nga krimet që kryhen përmes shfrytëzimit të paautorizuar të teknologjisë dhe të rrjeteve të komunikimit.

- Marrja e informacionit për veprat penale të ndërlidhura me sigurinë e informacionit, përmes përfshirjes në programet shkollore apo përdorimit të formave të tjera që përdor shkolla, organizimi i punëtorive të përbashkëta të përfaqësuesve të shoqërisë civile, mediave dhe zyrtarëve të agjencive të sigurisë, organizimi i fushatave ndërgjegjësuese për shfrytëzimin e drejtë të internetit janë forma më e mirë për institucionalizimin e një informimi të kualifikuar për shoqërinë, në përgjithësi, dhe për rininë shkollore, në veçanti.

- Profili socio-demografik i autorëve të veprave penale kundër sigurisë së informacionit evidencon faktin se këto vepra kryhen kryesisht nga autorë të krimit, që janë të gjinisë mashkullore. Nga 622 personat për të cilët janë marrë vendime gjyqësore, 598 persona janë të gjinisë mashkullore, ndërsa 24 janë të gjinisë femërore.

- Autorë të krimeve kibernetike, kryesisht, janë persona që posedojnë njohuri të avancuara për sistemet kompjuterike dhe që kryjnë vepra kriminale, kryesisht, përmes teknologjisë kompjuterike.

- Bazuar në të dhënat e Sistemit Informativ të Policisë së Kosovës, në territorin e Republikës së Kosovës gjatë periudhës nëntëvjeçare 2007–2015, janë evidencuar gjithsej 2121 raste të veprave penale të ndërlidhura me sigurinë e informacionit.

- Në Kosovë gjatë periudhës nëntëvjeçare 2007-2015, janë nxjerrë vendime gjyqësore për 542 raste të gjykuara të veprave penale të ndërlidhura me sigurinë e informacionit, në të cilat kanë qenë të përfshirë 622 persona. Nga 542 çështje të gjykuara, janë marrë më pak vendime për vepra penale të ndërlidhura me sigurinë e informacionit në rajonin e Mitrovicës, gjithsej 17 vendime gjyqësore, ndërsa rajoni në të cilin janë marrë më shumë vendime gjyqësore për vepra penale të ndërlidhura me sigurinë e informacionit është rajoni i Pejës, gjithsej 162 vendime gjyqësore.

- Analizimi i profilit arsimor i autorëve të veprave penale kundër sigurisë së informacionit evidencon faktin se nga 622 persona të dënuar për veprat penale të ndërlidhura me sigurinë e informacionit 116 kanë arsimim 8-vjeçar, 399 kanë arsimim të mesëm dhe 107 kanë arsimim të lartë.

- Agjencitë e inteligjencës kanë rëndësi të madhe për sigurinë e informacionit. Ato janë pjesë e rëndësishme e sigurisë kombëtare. Funksioni i tyre është grumbullimi dhe analizimi i informatave për kërcënimet ndaj shtetit dhe popullsisë së tij. Sa më e fortë që është inteligjenca e një shteti aq më të fortë janë edhe sektorët tjerë si: diplomacia, siguria, ekonomia dhe energjia. Agjencitë e inteligjencës janë pjesa më vitale dhe më e ndjeshme e një shteti, ato janë stabilizuesit, por edhe alarmuesit e parë të shtetit nëse ai kërcënohet. Shërbimet e inteligjencës luajnë një rol kritik në mbrojtjen e shtetit dhe popullsinë e saj kundër kërcënimeve ndaj sigurisë kombëtare, duke përfshirë edhe terrorizmin.

- Gjatë hulumtimit të kësaj teme, është vënë re se, megjithëse në institucione të ndryshme në Kosovë ekzistojnë rreth 25 baza të të dhënave, megjithatë, mungon një strukturë e mirëfilltë e të dhënave të unifikuara, që do të lehtësonte një studim lidhur me shtrirjen e këtij fenomeni. Mungesa e një strukture unike të të dhënave nuk është vetëm problem i mungesës së një baze unike të të dhënave të institucioneve të sigurisë në nivel kombëtar, por është problem i pranishëm pothuajse në të gjitha institucionet e sigurisë, sepse as në këto institucione nuk ekziston një bazë unike e të dhënave, por baza të veçanta të të dhënave.

Përfundime për hipotezat e punimit të doktoraturës

Hipoteza e parë: Në Republikën e Kosovës nuk ekziston një infrastrukturë ligjore e strukturuar, që rregullon sigurinë e informacionit.

Kjo hipotezë është vërtetuar. Si rezultat i hulumtimit të bërë, rezulton se nuk ekziston një infrastrukturë ligjore e strukturuar, që rregullon sigurinë e informacionit.

Në Republikën e Kosovës, veprat penale të ndërlidhura me sigurinë e informacionit nuk janë të parashikuara me një kod apo ligj të vetëm, por me disa ligje. Disa vepra penale janë të parashikuara me Kodin Penal të Kosovës, disa me Ligjin për Parandalimin dhe Luftimin e Krimeve Kibernetike, ndërsa vepra penale "Zbulimi i informacioneve të klasifikuara dhe mosruajtja e informacioneve të klasifikuara" është e parashikuar, edhe me Kodin Penal, edhe me Ligjin për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë. Për këtë vepër penale me Kodin Penal nuk është

parashikuar dënimi që mund të shqiptohet, por përcaktohet se për këtë vepër, autori dënohet sipas Ligjit për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë. Kjo paraqet një paqartësi juridike, sepse, parimisht, një vepër penale nuk mund të parashihet me dy ligje të aplikueshme, siç ndodh me këtë vepër penale. Prandaj kjo vepër penale nuk duhet të figurojë fare në Ligjin për Klasifikim të Informacioneve dhe Verifikimin e Sigurisë, por të figurojë te Kodi Penal, ngaqë, sipas kritereve elementare për ndërtimin e ligjeve, në përgjithësi, si dhe të ligjeve penale, në veçanti, nuk rekomandohet që e njëjta vepër penale të parashihet në dy apo më shumë ligje.

Hipoteza e dytë*: *Në Kosovë, në aspektin formal ekzistojnë disa ligje të cilat rregullojnë sigurinë e informacionit, por sfidues mbetet implementimi i këtyre ligjeve në praktikë.

Kjo hipotezë është vërtetuar. Sfidë kryesore është implementimi i plotë në praktikë i ligjit për klasifikimin e informacioneve dhe verifikimin e sigurisë. Me këtë ligj parashihet që të gjithë zyrtarëve të cilët kanë qasje në informacionet e klasifikuara duhet t‘u bëhet verifikimi i sigurisë, me qëllim që ata të marrin certifikatën e sigurisë dhe se mosmarrja e kësaj rezulton me transferimin e personit apo të zyrtarit në një pozitë tjetër të barasvlershme, për të cilën nuk nevojitet verifikimi i sigurisë apo, nëse kjo nuk është e mundur, atëherë mosmarrja e lejes së sigurisë rezulton me largim nga puna. Në disa institucione të sigurisë një numër i konsiderueshëm i zyrtarëve që kanë qasje në informacionet e klasifikuara kanë dështuar në procesin e verifikimit të sigurisë, sepse ata, sipas Agjencisë së Kosovës për Inteligjencë, kanë paraqitur rrezik të papranueshëm për sigurinë, megjithatë, këta zyrtarë nuk janë larguar nga vendet e tyre

të punës, por vazhdojnë të qëndrojnë aty dhe të kenë autorizime të plota për qasje dhe për trajtim të informacioneve të klasifikuara.

Hipoteza e tretë: Në institucionet e sigurisë së Republikës së Kosovës, siguria fizike e informacionit i plotëson të gjitha standardet e kërkuara.

Kjo hipotezë është vërtetuar. Në të gjitha institucionet e sigurisë në Kosovë aplikohen standarde të larta të sigurisë fizike të informacioneve. Këto standarde janë në përputhje të plotë me ligjin për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë.

Institucionet e sigurisë së Republikës së Kosovës posedojnë dhoma të të dhënave, që i plotësojnë standardet më të larta ndërkombëtare të ruajtjes së informacioneve.

Hipoteza e katërt: Në Kosovë janë shënuar pak raste të veprave penale të ndërlidhura me sigurinë e informacionit. Në këto raste autorë të veprave penale kryesisht janë personat e gjinisë mashkullore.

Kjo hipotezë është vërtetuar. Nga Gjykatat e Kosovës në territorin e Kosovës gjatë periudhës 2007 – 2015, janë nxjerrë 542 vendime gjyqësore për 542 raste të veprave penale, në të cilat kanë qenë të përfshirë 622 persona.

8.2. REKOMANDIME

Në përgjithësi, studimi ka identifikuar fushat ku nevojiten përmirësime dhe ka identifikuar sfidat dhe çështjet që kërkojnë vëmendje më të madhe, në mënyrë që të parandalohen dhe të luftohen veprat penale të ndërlidhura me sigurinë e informacionit.

Në vijim janë rekomandimet e dala nga punimi i doktoraturës:

- Të hartohet Strategjia Kombëtare e Sigurisë së Informacioneve. Autoritet për miratimin e kësaj strategjie duhet të jetë Qeveria e Republikës së Kosovës.

Kjo strategji do të plotësojë kuadrin ligjor në fushën e sigurisë së informacionit dhe do të lehtësojë luftën kundër veprave penale të ndërlidhura me sigurinë e informacionit. Vlerësojmë se, me nxjerrjen e këtij dokumenti dhe me zbatimin e tij, siguria e informacionit do të përcaktohet si prioritet kombëtar, duke siguruar prioritetet afatshkurtëra, afatmesme dhe afatgjata të sigurisë informacionit.

Hartimi dhe zbatimi i kësaj strategjie do të mundësojë avancimin e standardeve të sigurisë së informacionit dhe kjo do të mundësojë edhe mbrojtjen e informacioneve të klasifikuara ndaj sistemeve depërtuese të disa vendeve që janë të interesuara në zotërimin e informacionit të klasifikuar të Kosovës

- Të hartohet Strategjia për Sigurinë Kibernetike. Autoritet për miratimin e kësaj strategjie duhet të jetë Ministria e Punëve të Brendshme e Republikës së Kosovës.

Hartimi i Strategjisë për Sigurinë Kibernetike do të mundësojë avancimin e standardeve të sigurisë së hapësirës kibernetike të Kosovës dhe mbrojtjen nga sulmet kibernetike, sepse me këtë strategji do të përcaktoheshin masat konkrete për krijimin e një hapësire kibernetike të sigurt.

-Të bëhet plotësimi i Kodit Penal të Kosovës. Në Kodin Penal të Kosovës të parashihet një Kapitull i veçantë që të emërtohet Veprat Penale kundër Sigurisë së Informacionit, sepse inkorporomi i këtyre veprave në një kapitull të veçantë mundëson procedim penal më të lehtë.

- Ligji për Parandalimin dhe Luftimin e Krimeve Kibernetike të shfuqizohet dhe të gjitha veprat penale që i parashikon ky ligj të inkorporohen në Kodin Penal të Kosovës.

- Vepra penale "Zbulimi i informacioneve të klasifikuara dhe mosruajtja e informacioneve të klasifikuara", e cila, aktualisht është e parashikuar me dy ligje të aplikueshme: me Kodin Penal të Kosovës dhe me Ligjin për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë, nuk duhet të figurojë fare në Ligjin për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë, por vetëm në Kodin Penal të Kosovës.

Për këtë vepër penale në nenin 133 të Kodit Penal nuk është parashikuar fare dënimi që mund t'i shqiptohet autorit të krimit, por përcaktohet se, për këtë vepër, autori dënohet sipas Ligjit për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë. Kjo vepër penale nuk duhet të figurojë fare në Ligjin për Klasifikim të Informacioneve dhe

Verifikimin e Sigurisë, sepse, sipas kritereve elementare për ndërtimin e ligjeve, në përgjithësi, si dhe të ligjeve penale, në veçanti, nuk rekomandohet që e njëjta vepër penale të parashihet në dy apo më shumë ligje.

-Në nivel kombëtar të ndërtohen dhe të avancohen standarde unifikuese të të gjitha bazave të të dhënave.

Në Këshillin Prokurorial të Kosovës të ndërtohet një Sistem elektronik për menaxhimin e rasteve. Në Prokurorinë e Kosovës të bëhet regjistrimi i të dhënave në bazat e të dhënave për veprat penale dhe këto të dhëna të pasqyrohen në raporte statistikore, të cilat duhet të jenë transparente për publikun.

- Të avancohen më tutje kapacitetet e agjencive të zbatimit të ligjit në luftimin e krimit kibernetikë.

Të rriten kapacitetet e Policisë së Kosovës për luftimin e krimeve kibernetike. Sektori për Luftimin e Krimeve Kibernetike të ngrihet në nivel Drejtorie për luftimin e Krimeve Kibernetike.

- Të zbatohen sistemet e zbulimit të ndërhyrjeve, duke përdorur sensorë pasivë për të identifikuar rastet kur përdoruesit e paautorizuar përpiqen për t'u qasur në rrjetet dhe në sistemet e TI-së.

Të bëhet mbikëqyrja dhe filtrimi i informacionit të shpërndarë për parandalimin e rreziqeve që mund të sjellë informacioni nga interneti.

- Të punohet më shumë në ndërgjegjësimin e publikut, me qëllim ngritjen e vetëdijes së publikut për shfrytëzimin e drejtë të resurseve të teknologjisë informative

dhe ngritjen e vetëdijes për shfrytëzimin e drejtë dhe të sinqertë të resurseve të teknologjisë informative në lidhje me veprat penale të ndërlidhura me sigurinë e informacionit.

Të organizohet mbajtja e ligjëratave, e punëtorive dhe e seminareve me organizatat e sigurisë, me institucionet arsimore, me shoqërinë civile dhe me të tjerë, me qëllim senzibilizimin në njohjen me mënyrat dhe me mjetet e keqpërdorimit të kompjuterëve, për mënyrat dhe masat për parandalimin dhe luftimin e veprave penale të ndërlidhura me sigurinë e informacionit.

- Të investohet më shumë në trajnimin e vazhdueshëm të zyrtarëve.

Bazuar në analizën e përgjigjeve nga pyetësorët rezulton se mbi 64% e zyrtarëve të organeve të sigurisë nuk kanë vijuar asnjë trajnim në fushën e sigurisë së informacioneve. Është e domosdoshme që atyre t'u ofrohen rregullisht trajnime në fushën e sigurisë së informacioneve.

- Të organizohen konferenca, seminare apo punëtori të përbashkëta me organizatat e sigurisë, në mënyrë që te zyrtarët e organeve të sigurisë të ngrihet niveli i vetëdijes dhe i profesionalizmit për informacionin dhe për rëndësinë e sigurisë së informacionit; të rritet fryma e bashkëpunimit dhe besimit reciprok, e cila do të rezultonte në ngritjen e "urave të bashkëpunimit" mes organizatave të sigurisë dhe në avancimin e profesionalizmit, të efikasitetit dhe të efektivitetit në fushën e shkëmbimit të informacioneve.

Ky rekomandim argumentohet bazuar në faktin se mbi 64% e të anketuarve punonjës të organeve të sigurisë nuk kishin marrë pjesë në ndonjë konferencë, seminar

apo punëtori të përbashkët me organizatat tjera të sigurisë, ku ka qenë temë informacioni, siguria e informacionit apo shkëmbimi i informacioneve, del është e domosdoshme që të organizohen konferenca, seminare apo punëtori të përbashkëta me organizatat tjera të sigurisë, në mënyrë që tek ata të rritet fryma e bashkëpunimit dhe e besimit reciprok, e cila do të rezultonte në ngritjen e "urave të bashkëpunimit" mes organizatave të sigurisë dhe ngritje të profesionalizmit, të efikasitetit dhe të efektivitetit në fushën e shkëmbimit të informacioneve.

- ***Të punohet për ngritjen e nivelit të bashkëpunimit me organizatat vendore dhe ato ndërkombëtare në luftën kundër veprave penale të ndërlidhura me sigurinë e informacionit.***

Të punohet më shumë në lobimin me qëllim anëtarësimin e Policisë së Kosovës në organizatat ndërkombëtare: EUROPOL, INTERPOL, FRONTEX, SELECO etj. Anëtarësimi i Policisë së Kosovës në këto organizata do ta avanconte bashkëpunimin dhe do ta ngrinte nivelin e punës me shkëmbimin e informacioneve në luftën e përbashkët kundër krimit të organizuar, terrorizmit dhe korrupsionit.

- Të shtohen hetimet proaktive, si mënyra më efektive me të cilën mund të arrihet ndjekja e suksesshme penale e autorëve të veprave penale të ndërlidhura me sigurinë e informacionit.

- Të zhvillohen nga organet e zbatimit të ligjit më shumë operacione të përbashkëta hetimore ndërkombëtare, të cilat, siç tregon përvoja e deritanishme, janë mënyra më e mirë e luftës kundër veprave penale të ndërlidhura me sigurinë e informacionit, kur autorët e krimeve janë nga disa shtete. Numri i këtyre operacione të përbashkëta në të ardhmen duhet të rritet.

Rekomandime për hipotezat e punimit të doktoraturës

Rekomandime për hipotezën e parë: *Në Republikën e Kosovës nuk ekziston një infrastrukturë ligjore e strukturuar, që rregullon sigurinë e informacionit.*

Të bëhet plotësimi dhe amendimi i mëtejmë i kuadrit ligjor që rregullon sigurinë e informacionit në Kosovë.

Veprat penale që ndërlidhen me sigurinë e informacionit dhe që janë të parashikuara me ligjin për parandalimin dhe luftimin e krimeve kibernetike duhet të inkorporohen në Kodin Penal të Kosovës. Në Kodin Penal të Kosovës, veprat penale kundër sigurisë së informacionit të përfshihen në një kapitull të veçantë të veprave penale dhe ky kapitull të emërtohet: Veprat penale kundër sigurisë së informacionit.

Rekomandime për hipotezën e dytë: *Në Kosovë, në aspektin formal ekzistojnë disa ligje të cilat rregullojnë sigurinë e informacionit, por sfidues mbetet implementimi i këtyre ligjeve në praktikë.*

Të bëhet implementimi i plotë ligjit për klasifikimin e informacioneve dhe verifikimin e sigurisë për të gjithë zyrtarët që kanë qasje në informacionet e klasifikuara.

Në të gjitha institucionet e sigurisë së Kosovës dhe në institucionet e tjera, të gjithë zyrtarëve që kanë qasje në informacionet e klasifikuara dhe që kanë dështuar në procesin e verifikimit të sigurisë t'u ndalohet menjëherë qasja në informacionet e klasifikuara dhe ata të transferohen në pozita pune të barasvlefshme me pozitat aktuale dhe kur kjo nuk është e mundur, ata të largohen nga vendet e tyre të punës.

Të krijohet një Agjenci për verifikimin e sigurisë.

Rekomandimet për hipotezën e tretë: *Në institucionet e sigurisë së Republikës së Kosovës, siguria fizike e informacionit i plotëson të gjitha standardet e kërkuara*.

Megjithëse institucionet e sigurisë së Republikës së Kosovës posedojnë dhoma të të dhënave, numri i këtyre dhomave duhet të rritet, ashtu siç parashihet me standardet më të larta ndërkombëtare. Secila agjenci sigurie në nivel vendi, duhet të ketë, së paku, dy Dhoma të të Dhënave, të cilat duhet të jenë të lokalizuara në distancë dyzet kilometra larg nga njëra-tjetra, me qëllim që, në raste të rrezikut eventual të shkatërrimit të Dhomës së të Dhënave nga ndonjë sulm kriminal, sulm terrorist apo nga forca madhore, shfrytëzohet Dhoma tjetër e të Dhënave.

Rekomandimet për hipotezën e katërt: *Në Kosovë janë shënuar pak raste të veprave penale të ndërlidhura me sigurinë e informacionit. Në këto raste autorë të veprave penale kryesisht janë personat e gjinisë mashkullore.*

Megjithëse në Kosovë janë shënuar pak raste të veprave penale të ndërlidhura me sigurinë e informacionit, duhen rritur kapacitetet dhe masat për parandalimin dhe zbulimin e këtyre veprave penale, me qëllim që në vazhdimësi të aplikohen masat e mbikëqyrjes dhe të paralajmërimit të hershëm.

Duhet të rritet numri i zyrtarëve të agjencive të zbatimit të ligjit në kuadër të njësive të specializuara, që merren me luftimin e veprave penale të ndërlidhura me sigurinë e informacionit.

Të gjitha këto rekomandime të theksuara më lart janë të nevojshme për t'u realizuar, me qëllim luftimin me efikasitet më të madh të veprave penale të ndërlidhura me sigurinë e informacionit, ngaqë teknologjia informatike gjithnjë po shënon përparime të shpejta, të cilat në mënyrë permanente duhet të përcillen.

Kjo është e nevojshme edhe për të realizuar avancimin e standardeve të sigurisë së informacioneve dhe të rritjes së efikasitetit të Agjencive të Sigurisë në parandalimin dhe zbulimin e veprave penale të ndërlidhura me sigurinë e informacionit, sepse këto Agjenci gjithnjë duhet të jenë të përgatitura për të ecur një hap para autorëve të këtyre veprave penale.

LISTA E REFERENCAVE / BIBLIOGRAFIA

A. LITERATURA

Abazoviç, D., M. (2006), *Siguria Nacionale*, Sarajevë/Prishtinë (përkthim U.N AAB, f. 44 – 84;

Adamski, A. (2001). *Computer Crime in Poland,* three years experience in enforcing law, Warshava, f. 102;

Bagad V.S &. Dhotre I.A (2009). *"Information Security*" published by Technical Publications Pune, 2009, f. 1;

Bacic, F. & Pavlovic S, *Komentar Krivicnog Zakona*, f. 543;

Bacic, F. & Sheparovic Z., (1997) *Komentar Krivicno Pravo, Posebni dio*, Zagreb, f. 26;

Blyth, A. & Kovacich, L., G. (2007). *Information Assurance-Security in the Information Environment*, USA, published by Springer Science , f. 3;

Blank G., B., (2004), *Technology Fundamentals for IT Success, Sybex*, USA, f.3*;*

Bequaj A. (1983), *How to prevent Computer Crime*, John Walley & Sons, Inc, f. 16;

Brenner, S., (2010) *Cybercrime: Criminal Threats from Cyberspace*, California, f.83;

Broadhurst, R. and P. Grabosky, (2005). *Cyber-crime: The challenge in Asia*. 2005, Hong Kong University Press: Hong Kong, f.37;

Borko, H., (1968). *Information Science: What is it?* American Documentation, f 3-5;

Born H., & Wills Aidan, (2012),Pako e Instrumenteve. *"Mbikëqyrja e Shërbimeve të Inteligjencës*". DCAF. f. 75;

Bishop Mat, (2004), *Introduction to Computer Security*, printet by Pearson Education, Inc., USA, f. 3-4;

Buckland B.& Schreier F., & Winkler Th.,(2015), *"Democratic Governannce Challenges of Cyber Security"* DCAF, f.18*;*

Casey E., (2002) *Handbook of Computer Crime Investigation,* Great Britain, printed by Elsevier Academic;

Cornish, P., (2010), *Cyberwafare, The Royal Institute of International Affairs*, London, f.2;

Cookridge, E.H., (2005), *Spiuni i Shekullit*, përkthyer nga Piro Koçi, Shtëpia Botuese

"Bota Shqiptare", Tiranë; f. 8;

Clough B. & Mungo P., (1992), *Aproaching Zero:Data Crime and the Computer Underworld*, faber, London, f. 113;

Collins A & Sten A., (2006), *Studime bashkëkohore të sigurisë*, botuar nga UET PRESS, Tiranë, përkthim nga Enri Hide, f. 313-318;

Cuellar, M. F. (2001). *The transnational dimension of cyber crime and terrorism*. A. D. Sofaer, & S. E. Goodman (Eds.). Hoover Institution Press; f 1;

Curtis G., (2009), *Cybercrime*: An Annotated Bibliography of Select Foreign-Language Academic Literature, Washington, f. 2;

Cornish, P., (2010) *Cyberwafare*, the Royal Institute of International Affairs, London, f. 2;

Chuck E., & Det-Jeff T., (2011), *Computer Crime, Investigation, and the Law*, USA, f. XVI-12;

Çukalović, I., (2013) *Komentar i Kushtetutës së Republikës së Kosovës*, Prishtinë, f. 83;

David Kim&Michael Solomon, (2014) "*Fundamentals of Information Systems Security*", USA, f. 2;

Dragiqeviq, A. D. (1999), *"Leksikon Ekonomije i informatike"* Zagreb, f. 10-141;

Dragiqeviq, D., (2004) "*Komjuterski Kriminalitet i Informacijski Sustavi*", Zagreb, printed by IBS, f.10.-4141;

Dolman E., & (2005), " *Power and Principle in the Space and Information Age*" London, Frank Cass, DCAF, f. 6;

Dulles Allaen *"Asetet e Spiunazhit"(2003), Onufri "* Tiranë, f. 3;

Dragutin, Ll., (1982), *Savremena Spiunazha*, Beograd, f. 78;

Elezi I., (2009), " *E Drejta Penale"*, Pjesa e posaçme, Tiranë, f. 180-369;

Elezi, I., & Kaçupi, S., & Haxhia, R. M., (2006). *Komentari i Kodit Penal të Republikës së Shqipërisë*, Pjesa e përgjithshme, Tiranë, f. 117;

Easttom, C. (2011), *Computer crime, investigation, and the law*. Cengage Learning, USA, f. XVI;

Franjo Bacic, Sime Pavlovic, *Komentar Krivicnog Zakona*, f. 543;

Glick, L.,(1995), *Kriminology*, Boston-London-Tokyo, p. 2012;

Gerecke, M.,(2012), *Understanding Cybercrime: Phonema, Challenges and Legal Response*, Geneva, f. 12- 112;

Glick, L., (1995), *Kriminology*, Boston, f.212;

Gjonçaj, L., & Gjonçaj, G., (2013), *Kriminologjia*,Tiranë, f.133 – 416;

Hampson F., O., & Malone M., D., *From Reaction to Conflict Prevention*, LYNNE RIENNER Publishers, London, f. 44;

Halili. R., (2005), Kriminologjia, Prishtinë, f. 352,

Halili. R., (2005), Penologjia, shtypur nga shtypshkronja "MultiGraphics", Prishtinë, f. 29;

Halili, R., (2007), *Viktimologjia*, Prishtinë, f. 133-339;

Halili. R., (2008) *Kriminologjia*, Prishtinë, f. 115-352;

Heather L.,W., (2007) *The Central Intelligence Agency*,f. 19;

Hysi, V., (2005*), Kriminologjia,* Kristalina-KH, Tiranë, f. 238;

Jonathan H., *E Drejta Penale*, (2013),Teori, Kazuse dhe Materiale, Tiranë, f. 30;

Jeffery K.,(2010), *The History of the Secret Intelligence Service 1909-1949*, Bloomsbury Publishing, London, 2010, f. Xix;

Korajlic. N,. & Muharremi D,.(2009) *Kriminalistika*, Prishtine;

Katyal, N. K. (2001),*Criminal Law in Cyberspace*, University of Pennsylvania Law Review, vol. 149, 1003 2001, R. M. Couch, A Suggested Legislative Approach to the Problem of Computer Crime, 38 Washington and Lee Law Review, 1194, 1981;

Lyman, D. M.(2010). *Criminal investigation, The art and the science*, 6th edition, Prentice Hall., f. 605-607;

Latifi, V., 2011, *Kriminalistika*, Prishtinë, f. 459;

Lessig, L. (2013). "*Remix:Making Art and CommerceThrive in the Hybrid Economy"*, f.181;

Llukiq D., (1982*), Savremena Spiunazha*, Beograd, f. 78;

Matthews B., & Ross L., (2010), *Metodat e Hulumtimit - Udhëzues praktik për shkencat sociale dhe humane*, Botuar nga Qendra për Arsim Demokratik (CDE),

Tiranë, f. 51-201;

Maslesha, R., (2006), *Teoritë dhe Sistemet e Sigurisë*, Sarajevë, f. 81;

Mendel, T., Puddephatt, A., Wagner, B (2012*). "Global Survey on Internet Privacy and Freedom of Expression",* f.102;

Musci A., & Minicangeli M., (2005), *Të Fshehtat e Mosadit*, përkthyer nga Vladimir Bregu, Shtëpia Botuese "Bota Shqiptare", Tiranë, f. 39-40;

Matthieu Bloch M., & Barrosh, J., (2011)" *Physical-Layer Security from Information Theory to Security Engineering"*, Cambridge University Press, f.3;

Mohr. K, (1987)*Polizeilisches Lagebild Der Compter Kriminalita*t, Die Policai no. 2 Bremen, f.41;

Mohrenschlager, M., (1993), *Comuter Crime and and other Crimes against Information Technologies in Germany*, Review of Penal Law, Preparatory Coloquium, Wuzburg, ERES, Toulouse, f. 332;

Petrovic S. (2000), *Komjuterski Kriminal*, Beograd, f. 118-218;

Petrovic S., (2000) *Komjuterski Kriminal*, Beograd, f. 118-218;

Peltier, R., Th., *(*2001), *Information Security Policies, Procedures and Standards*, CRC PressTaylor &Francis Group, USA, f. xiii;

Parker, Don (1973), *Comuter Abuse*, Springfield, f.14;

Qehaja F., & Vrajolli M., (2012), *Alamak për Mbikëqyrjen e Sektorit të Sigurisë në Ballkanin Perëndimor*,Toena, Tiranë, f. 117;

Ross, Jeffry Ian (2010), *Criminal Investigations Cybercrime*; New York, published by Chelsea House Publishers, f.19-24;

Roscini, M. (2014).*Cyber operations and the use of force in international law*. Oxford University Press; f.1;

Russell L. R., (2007), *Sharpening Strategic Intelligence*-, Why the CIA get is wrong what need to be done to get it right", New York, Cambridge University Press, f.1-9,

Ronald K., *(*1992), *Inside the CIA*, Printed in the USA, f. 3;

Rifkin, J. (2001). *"The Age of Access: How the Shift fromOwnership to Access is Transforming Modern Life",* f. 221;

Roscini, M. (2014),*Cyber operations and the use of force in international law*. Oxford

University Press, f.1;

Ross, J.I., (2010), *Criminal Investigations Cybercrime*, New York, published by Chelsea House Publishers, f. 23-24;

Samuel C. Quade, S., C., (2009), III, Encyclopedia of Cybercrime, Greenwood press Westport, connecticut , London, f. 7;

Schneier B., (2000), *Secrets and Lies: Digital Security in a Networked World*, John Wiley Sons: first edition;

Strebe, Matthew.(2004) *Foundations Network Security*, f.1;.

Salihu I., (2008), *E Drejta Penale, Pjesa e Përgjithshme*, Fama, Prishtinë, f. 183-275,

Salihu I., (2009) *E drejta Penale, Pjesa e posaçme*, Fama, Prishtine; f. 169;

Salihu I., & Zhitia H., & Hasani F,. (2014) & *Komentar i Kodit Penal të Republikës së Kosovës*, Botimi 1, "GIZ", Prishtinë; f. 381 – 1224,

Sieber U., & Willey J., (1986)"*The International Handbook in Comuter Crime*, f.111;

Schreier, F., (2015) On Cyberwarfare, DCAF, f.18;

Strebe, M.,(2004), *Foundations Network Security*, f.1;

Samuel C. Mc Quade, (2009), *Encyclopedia of Cybercrime*, , Greenwood press Westport, connecticut , London, f.7;

Stamp, M,. & Willey, J., (2011),"*Information Security, Principles and Practice*", Canada, Wiley, f. 11;

Strebe, M.,(2004), *Foundations Network Security*, f.1;.

Samuel C. Mc Quade, (2009), *Encyclopedia of Cybercrime*, , Greenwood press Westport, connecticut , London, f.7;

Tzu, S., (1988), *The Art of War*, translated by Samuel B. Griffith.Oxford: Oxford Univeristy Press, f. 84.

Taber, J.K.,(1979) *On Computer Crime*, computer and law jurnal, nr. 517, f. 111;

Thomas, R., P., (2001) "*Information Security Policies, Procedures and Standards*" published by CRC Press Taylor &Francis Group, USA, f. Xiiii;

Vesel Latifi, (2011*), Kriminalistika*,Prishtinë, f. 459;

Vacca R., J.,(2013), *Computer and Information Security*, Published by Elesvier Inc.Canada, f.88;

Vilasi C., A., (2013), *The History of MI6-The Intelligence and Espionage Agency of the British Government*, published by Author House UK Ltd, USA 2013, f. 1;

Vilasi C., A., (2013), *The History of MOSSAD*, published by Author House UK Ltd,USA, f.33;

Vula V., (2010), *Kriminaliteti kompjuterik*, Shtypshkronja "Koha" Prishtinë", f. 26.-120,

Vasik, M.(1991), *Crime and Computer*, Oxford, f. 24;

Whitman, E.,M., & Mattord,H., J., (2011) *Principles of Information Secyrity,* Course Technologu; Fourth edition, f. 4-44;

Weiner T., (2011),*Trashëgimi prej Hiri, Historia e CIA-s*, Prishtinë, f. 8;

William B., (2005), *CIA dhe Ushtria Amerikane, Ndërhyrjet në vendet e ndryshme të botës që prej luftës II Botërore*, Tiranë, f .22- 604;

Wylder John, *(2003),Strategic Security Information,* CRC Press, USA, f.4*;*

Wieczorek, M., Vos, D., & Bons, H. (2014). Motivation and Introduction in *Systems and Software Quality*, f. 1-29;

Zwicky, D., E., & Cooper S., Chapman, B., D, (2000), Building Internet Firewalls, published by O'relly & Associates, USA, f. 11-35;

B. BURIME PARËSORE:

LEGJISLACIONI KOMBËTAR

- Kushtetuta e Republikës së Kosovës;
- Kodi Penal i Përkohshëm i Kosovës, Prishtinë, 2004,
- Kodi i Përkohshëm i Procedurës Penale të Kosovës, Prishtinë, 2004,
- Kodi Penal i Kosovës, Prishtinë, 2013;
- Kodi i Procedurës Penale i Kosovës, Prishtinë, 2013;
- Ligji nr. 03/L-063- Ligji për Agjencinë e Kosovës për Inteligjencë;
- Ligji nr. 03/L-178 - Ligji për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë;
- Ligji nr. Nr. 8457 - Ligji për Informacionin e Klasifikuar "Sekret Shtetëror";
- Ligji nr. 2004/34, Ligji Kundër Korrupsionit;

- Ligji mbi qasjen në dokumentet publike;
- Ligji Nr. 03/L-172, për Mbrojtjen e të Dhënave Personale, Prishtinë, 2010;
- Ligji 03/L-166 për Parandalimin dhe Luftimin e Krimit Kibernetik, Prishtinë, 2010
- Strategjia - Policimi i Udhëhequr nga Inteligjenca, 2013 - 2017;
- Strategjia Kombëtare e Republikës së Kosovës kundër Krimit të Organizuar, 2009-2012,
- Buletini i Praktikës Gjyqësore,(2004-2005),Gjykata Supreme e Kosovës, Prishtinë;
- Buletini i Praktikës Gjyqësore,(Korrik-Shtator, 2005), Gjykata Supreme e Kosovës, Prishtinë;
- Buletini i Praktikës Gjyqësore (2009-2010), Gjykata Kushtetuese e Kosovës, Prishtinë;
- Buletini i Praktikës Gjyqësore (2011), Gjykatat e Qarkut të Kosovës, Prishtinë;
- Buletini i Praktikës Gjyqësore (2011), Gjykata Kushtetuese e Kosovës, Prishtinë;
- Buletini i Praktikës Gjyqësore, (2011),Gjykata Supreme e Kosovës, Prishtinë;
- Buletini i Praktikës Gjyqësore, (2012), Gjykata Kushtetuese e Kosovës, Prishtinë;
- Buletini i Praktikës Gjyqësore,(2014),Gjykata Kushtetuese e Kosovës, Prishtinë;
- Buletini i Praktikës Gjyqësore,(Tetor, 2015),Gjykata e Apelit të Kosovës, Prishtinë;

LEGJISLACIONI NDËRKOMBËTAR

- Kodi Penal i Sllovenisë, Lublanë, 2008;
- Kodi Penal i Kroacisë, Zagreb, 2013;
- Deklarata Universale për të Drejtat dhe Liritë e Njeriut e Kombeve të Bashkuara, 1948.
- Konventa Evropiane për Mbrojtjen e të Drejtave të Njeriut, 1950.

- Konventa mbi Krimin Kibernetikë, nënshkruar më 23.11.2001, ratifikuar më 20.06.2002 dhe në fuqi nga 01.07.2004.
- Direktiva 95/46/EC e Parlamentit Evropian dhe e Këshillit për Mbrojtjen e Individëve në lidhje me Procesimin e të Dhënave Personale dhe Lëvizjen e të Dhënave të tilla, tetor 1995;
- Direktiva 95/46/EC e Parlamentit Evropian dhe e Këshillit për Procesimin e të Dhënave Personale dhe Mbrojtjen e Privatësisë në Sektorin e Telekomunikimeve, 15 dhjetor 1997;
- Direktiva DoD 5200,1, "*Sigurimit të Informacionit*, SHBA, 28 prill 1997;
- Classified Information Act (Official Gazette of the Republic of Slovenia, No.: 50/06);
- Information Security Act, (2007), Republic of Croatia.
- Zakon o dostopu do informacij javnega značaja, UPB2, Official - Akti mbi Informacionin e Klasifikuar - Gazeta Zyrtare e Republikës së Sllovenisë , Nr .: 50/06.
- Vendimi Nr. 121, i datës 15.03.2001, *për rregullat e sigurimit fizik të informacionit të klasifikuar*, Republika e Shqipërisë;
- Vendimi kornizë 2005/222/JHA i Këshillit të BE-së, për *Sulmet kundër Sistemeve të Informacionit*, 24 shkurt 2005.
- Vendimi nr. i datës 19.07.2001, *për sigurinë e informacionit të klasifikuar sekret shtetëror në rrjetet informatike, mjetet dhe pajisjet e transmetimit*;
- Vendim nr. 478, *për sigurimin e informacionit të klasifikuar "sekret shtetëror*" në rrjetet informatike, mjetet dhe pajisjet e transmetimit, datë 19.07.2001,
- *Rregullat e sigurimit fizik të informacionit të klasifikuar*, Republika e Shqipërisë, Këshilli i Ministrave, vendim nr. 121, datë 15.3.2001.

VENDIME NGA PRAKTIKA GJYQËSORE

- Rasti Cotlet kundër Rumanisë kërkresa numër 38565/95, faqe 467;
- Rasti Lavents kundër Letonisë, kërkesa 58442/00, faqe 229);

- Rasti Copland kundër Mbretërisë së Bashkuar, kërkesa nr. 62617/00).
- Rasti Peck kundër Mbretërisë së Bashkuar, këërkesa numër 44647/98, faqe:508).
- Rasti *Uzun kundër Gjermanisë*, aplikacioni numër 35623/05;
- Rasti Godelli kundër Italisë, aplikimi nr: 33783/09;
- Rasti Mitkus kundër Letonisë, aplikimi numër 7259/03;
- Aktgjykimi i Gjykatës së Qarkut në Pejë, Ap.nr.100/2010, datë 31.10.2011 dhe aktgjykimi i Gjykatës Supreme Pkl. Nr. 5/2012, datë 21.2.2012,
- Aktgjykimi i Gjykatës së Qarkut në Bjellovar KZ.nr. 328/91, dt. 29.05.1991,

C. BURIMET DYTËSORE:

Analizë e rishikimit Strategjik të Sektorit të Sigurisë së Republikës së Kosovës, (2014) Kapitulli IV, Seksioni 5.2, f.19,

DCAF. (2011). *Përmbledhje e praktikave të mira mbi Agjencitë e Inteligjencës dhe mbikëqyrja* e tyre, 2011, Pako udhëzimesh- Ligjbërja për Sektorin e Sigurisë, Gjenevë, f. 10-18;

EC-Council. (2009). Official Curriculum, "*Computer Hacking Forensic Investigator*", Courseware Manual 3.0 Volume 3.

EUROPOL, TE-SAT (2013*). EU Terrorism Situation and Trend Raport*, European Police Office, f.12.

EUROPOL. (2012). *Making Europe Safer*, Publications Office of the Europian Union, Luxembourg, f. 46.

EUROPOL EU Terrorism Situation and Trend Raport 2013,

FEDPOL. (2014). *Rapport Annuel, Office federal de la Police fedpol*, Confederation Suisse, p. 124;

FSSH (1980) Fjalori i gjuhës së sotme shqipe, Tiranë, f. 721.

Government Security Classifications, USA, 2014, f. 3.

J.K. Taber, "*On Computer Crime*", Computer and law jurnal nr. 517, 1979.

KIPRED. (2014). *Kosova në kontekstin e sigurisë dhe të mbrojtjes të Ballkanit Perëndimor*, Instituti Kosovar për Hulumtim dhe Zhvillim të Politikave , Nr. 3/14, f. 11.

Raporti i Shteteve për Terrorizmin i Departamentit Amerikan të Shtetit për vitin 2009.

Raport monitorimi mbi veprimtarinë e komisionit parlamentar të sigurisë kombëtare i Institutit për Demokraci dhe Ndërmjetësim Çështje të Sigurisë, 2012. Prishtinë, Nr. 5, f. 102.

Raportet vjetore të punës së Policisë së Kosovës për vitet : 2007 – 2015.

Raporti analitik statistikor i Policisë së Kosovës, Prishtinë, 2014.

Raportet Statistikore të Këshillit Gjyqësor të Kosovës për vitet 2007 – 2015.

Raport Statistikor, Policia e Kosovës, Prishtinë 2014.

Statistikat e Jurisprudencës për vitet 2007-2015, Enti i Statistikave të Kosovës;

BURIME NGA UEB FAQE

Internet Usage Statistics, World Internet Users and 2015 Population Stats, marrë nga www.internetworldstas.com/stats.htm; parë më 20.06.2015.

Denning E.D. "Crime and Crypto on the Information Superhigway", Georgetown University, Dec.13.1994, adresa në internet:htp://www.cosc.georgtown.edu.

Rosencrance, L. "Teen Hacker 'Mafiaboy' Sentenced "Computer World Online. www.computerworld.com/security/story/0,10801,63823,00.html, parë më 15 prill 2014.

UNESCO, (2013). "Çka është pirateria. (http://portal.unesco.org/culture/en/ev.php), parë më 20.04.2013,

Wieczorek, M., Vos, D., & Bons, H. (2014). Motivation and Introduction. In *Systems and Software Quality*(pp. 1-29). Springer Berlin, Heidelberg.<http://www.tcf.ua.edu/AZ/ITHistoryOutline.htm> parë më 10 shtator 2014.

Whitehead, Jennifer (13 October 2005). http://www.brandrepublic.com/news/5219 , parë më 13 dhjetor 2014.

Ueb-faqja zyrtare e De La Salle University. "*Military Intelligence*, e qasshme në: http://www.dlsu.edu.ph/offices/osa/rotc/pdf/ms1/military-intelligence.pdf parë më 23 gusht 2014;

Ueb-faqja zyrtare e Qendrës së Përbashkët për Inteligjencë e NATO-s (NIFC). Historia e NIFC-it. E qasshme në: http://web.ifc.bices.org/about.htm, parë më 4 tetor 2014.

Grant Gross (2006) **"***Government CIO survey*" e qasshme në: http://www.networkworld.com/article/2309399/lan-wan/gov, parë më 22 shtator 2014;

Wieczorek, M., Vos, D., & Bons, H. (2014). Motivation and Introduction. In *Systems and Software Quality* (pp. 1-29).

Springer Berlin Heidelberg.<http://www.tcf.ua.edu/AZ/ITHistoryOutline.htm > parë më 10 shtator 2013;

http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

http://albpchelp.blogspot.com/2012/11/si-te-mbani-kompjuterin-tuaj.dpuf.

http://albpchelp.blogspot.com/2012/11, parë më 10 prill 2015,

http://sq.swewe.net/word_show.htm/?383573_1&Shoq%C3%ABria_feudale

http://kallxo.com/?s, parë më 10.12.2015,

http://www.sova.gov.si/si/delovno_podrocje, parë më 03.12.2015.

http://www.albaniadiaspora.com/gazeta e diasporës shqiptare, 25.12.2015.

http://www.telegrafi.com/lajme/,ja-si-ka-vepruar-sherbimi-sekret-serb-kunder-kosoves-vitet-e-fundit-2-68433.htmlSpublikuar 10.08.2015,

http://www.tcpipguide.com/free/t_History of the OSI, Reference Model.htm)