KRIMI KIBERNETIK
HARMONIZIMI I LEGJISLACIONIT SHQIPTAR ME ATË EUROPIAN

Aldo Shkëmbi

Dorëzuar
Universitetit Europian të Tiranës
Shkollës Doktorale

Në përmbushje të detyrimeve të programit të Doktoratës në Shken`a Juridike, me profil e Drejtë Publike, për marrjen e gradës shkencore "Doktor"

Udhëheqës shkencor: Prof. Dr. Ilirjan Mandro

Numri i fjalëve: 59,323

Tiranë, Qershor 2015

DEKLARATA E AUTORËSISË

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.

ABSTRAKTI

Në vitet e fundit, shoqëritë në të gjithë botën kanë bërë përparime të mëdha në fushën e teknologjisë së informacionit dhe komunikimit. Teknologjia e informacionit dhe komunikimit tani përshkon pothuajse çdo aspekt të jetës së njerëzve e si rrjedhojë kjo e bën shoqërinë të ekspozuar ndaj kërcënimeve të tilla si krimi kibernetik, domethënë krimi i kryer kundër të dhënave dhe sistemeve kompjuterike ose nëpërmjet tyre.

Risitë që paraqet kjo fushë shtrojnë nevojën për ndërhyrje normative të vazhdueshme ndaj sjelljeve kriminale të ndodhura në hapësirën kibernetike, pasi format e konsumimit të veprave penale kibernetike ndryshojnë dukshëm nga format tradicionale të krimit dhe si rrjedhojë, aplikimi i mundshëm i normave ekzistuese penale ndaj sjelljeve të paligjshme të realizuara nëpërmjet sistemeve kompjuterike do të rrezikonte ndjeshëm zhvillimin shoqëror të vendit, sidomos në Shqipëri.

Shqipëria renditet ndër vendet ku zhvillimi i teknologjisë, qasja në internet dhe informatizimi i shoqërisë përparon shumë shpejt. Rritja e përdorimit të komunikimit përbën një vlerë të shtuar në zhvillimin shoqëror të vendit, por, në të njëjtën kohë, ajo e ekspozon atë ndaj rreziqeve të natyrës kibernetike me aktorë shtetërorë dhe jo shtetërorë.

Për të parandaluar dhe luftuar krimin kibernetik Shqipëria ka ratifikuar "Konventën e Budapestit mbi Krimin Kibernetik", dhe ka përfshirë në Kodin Penal disa veprava penale kibernetike me ligjin nr. 10023, datë 27.11.2008 për disa shtesa në ligjin nr. 7895 datë 27.01.1995 "Kodi Penal i Republikës së Shqipërisë", në kuadër të harmonizimit të legjislacionit të brendshëm me acqius-communitaries e veçanërisht me parashikimet e Konventës.

Pikërisht, qëllimi i këtij disertacioni është studimi i fenomenit të krimit kibernetik në dimensionet e ndryshme të evoluimit të tij në Europë dhe Shqipëri, duke analizuar parimet bazë të së drejtës dhe çdo dispozitë ligjore në kuadër të përcaktimeve dhe përmbajtjes së "Konventës së Budapestit mbi Krimin Kibernetik" duke theksuar nevojën e ndjekjes në mënyrë prioritare të një politike penale, që ka për qëllim mbrojtjen e shoqërisë nga krimi kibernetik, nëpërmjet hartimit të një legjislacioni të përshtatshëm dhe bashkëpunimit ndërkombëtar në luftën kundër këtij lloj krimi.

Fjalët kyçe: *Kompjuter; Sistem Kompjuterik; Krim kibernetik; Të dhëna kompjuterike; Harmonizim.*

ABSTRACT

In recent years, societies all over the world have made great progress towards being a society of information. The technology of information and communication (TIC) now permeates almost every aspect of human life, hence, this makes society exposed to such kind of crime, cybercrime, that means the crime committed against the data or against computer systems or through them.

The innovations that presents this area of technology create the neccessity of the continous normative interventions against these criminal behaviours that are happening in the cyberspace because the forms of the consumptions of these penal acts does visibly change from the traditional forms of crimes and applying the existing penal laws against these ilegal behaviours through the computering systems would considerably risk the social development of the country especially of Albania.

Albania is categorized as a country where the development of technology, internet access and the process of becoming informed have made a quick progress. The increased use of communication is an added value in the social development of the country, but at the same time, it exposses the country towards the risk of cyber nature, with governmental actors or non-governmental actors.

To prevent and fight cybercrime, Albania has ratified the "Budapest's Convention of Cybercrime " and has also included in the Penal Code some cyber penal acts, with the law no.10023, date 27.11.2008, and some other suplements in the law no.7895, date.27.01.1995 "Penal Code of the Albanian Republic", in the framework of harmonisation of the internal legislation with the acqius-communitaries ecpecially with the predictions of the convention.

The purpose of the dissertation, is exactly the study of the phenomenon of cybercrime, in his different dimensions of evolution in Europe and Albania, analyzing the basic principles of right and every legal provision in the framework of definitions and content of "Budapest convention on Cybercrime". Emphasizing the need to follow, a penal politic, a in a prior way, a politic that aims the protection of society from cyber crime, through the compilation of an adequate legislation and international cooperation in the fight against this crime.

Keywords: *Computer; Computer system; Cybercrime; Computer data; Harmonization.*

DEDIKIMI

Dedikuar familjes sime . . .

FALENDERIME

“Mos u mjafto me horizontin, kërko pafundësinë”, është një nga thëniet më të famshme të Jim Morrison, thënie e cila më ka shoqëruar në të gjithë periudhën e formimit tim akademik, duke më dhënë kurajo, forcë dhe ambicje për tu përballur me çdo sfidë dhe për të realizuar çdo ëndërr.

Përfundimi i këtij disertacioni ishte një endërr e cila do të kishte qenë e pamundur pa mbështetjen e familjes time, të cilën e falenderoj për kurajon dhe besimin që më ka dhënë duke më ndihmuar që ëndrrat dhe dëshirat ti bëj realitet.

Një falenderim i veçantë shkon edhe për Udhëheqësin tim shkencor, Prof.Dr. Ilirjan Mandro, i cili falë ekperiencës dhe profesionalizmit më ka mbështetur dhe më ka ndihmuar në realizimin e këtij disertacioni, duke më bëre që të kuptoj se të kesh ambicje dhe dëshira nuk mjafton, por që gjithashtu është e rëndësishme që për të arritur rezultatet e duhura duhet të dish edhe të zgjedhësh, dhe UET ishte ajo e duhura, jo vetëm për shërbimin dhe cilësinë që e diferencon, por edhe për stafin akademik të spikatur që ka dhe që e dallon në të gjithë spektrin e Arsimit të Lartë Shqiptar.

Mirënjohje gjithashtu shkon për të gjithë kolegët dhe miqtë që më kanë shoqëruar gjatë këtij udhëtimi të vështirë e të bukur dhe që me këshillat dhe mbështjetjen e tyre morale, kanë qenë një vlerë e shtuar dhe një ikonë frymëzimi për realizimin e këtij disertacioni.

PËRMBAJTJA E LËNDËS

KAPITULLI III: VENDIMARRJA E BASHKIMIT EUROPIAN NË LUFTËN KUNDËR KRIMIT KIBERNETIK, NJË DEKADË E ZHVILLIMEVE LIGJORE EUROPIANE

KAPITULLI IV: RREGULLIMI I KRIMIT KIBERNETIK NË SHQIPËRI NË KUADËR TË HARMONIZIMIT TË LEGJISLACIONIT TË BRENDSHËM ME ATË EUROPIAN

LISTA E SHKURTIMEVE

AKCE	Autoriteti Kombëtar i Certifikimit Elektronik
AKEP	Autoriteti i Komunikimeve Elektronike e Postare
AKSHI	Agjencia Kombëtare e Shoqërisë së Informacionit
ALCIRT	Agjencia Kombëtare për Sigurinë Kompjuterike
BE	Bashkimi Evropian
DSIK	Drejtoria e Sigurimit të Informacionit të Klasifikuar
ENISA	Agjencia e Bashkimit Europian për Sigurinë e Rrjeteve dhe Informacionit
EUROPOL	Zyra e Policisë Evropiane
EUROJUST	Njësia Gjyqësore e Bashkëpunimit Evropian
ISP	Ofruesit e Shërbimit të Internetit
SHISH	Shërbimi Informativ i Shtetit
NATO	Organizata e Traktatit të Atlantikut Verior
CERT	Ekipi i Përgjigjes ndaj Emergjencave Kompjuterike
TIK	Teknologjia e Informacionit dhe Komunikimit

PËRKUFIZIME

Sistem kompjuterik - konsiderohet një sistem i ndërlidhur kompjuterësh që ndajnë një sistem ruajtjeje qëndror dhe pajisje të ndryshme periferike.

Rrjet kompjuterik - konsiderohet një rrjet telekomunikimi që i lejon kompjuterat të shkëmbejnë të dhëna.

Të dhëna kompjuterike - konsiderohet çdo informacion i procesuar dhe/ose ruajtur në njëkompjuter.

Të dhëna personale- është çdo informacion për një person fizik, i cili është i identifikuar ose i identifikueshëm.

Hapësirë kibernetike - konsiderohet hapësira virtuale globale e të gjithë sistemeve të informacionit dhe të komunikimit të ndërlidhur në nivel të dhënash.

Harmonizimi i legjislacionit- nënkupton përafrimin e legjislacionit të brendshëm me *acquis-communitaries* nëpërmjet gjetjes se një metodike të përbashkët duke respektuar veçoritë legjislative kombëtare.

Kërcënim/sulm kibernetik – konsiderohet çdo përpjekje e drejtuar/e qëllimshme për të marrë akses, manipuluar, ndërhyrë ose dëmtuar integritetin, konfidencialitetin, sigurinë dhe/ose disponibilitetin e të dhënave, të një aplikimi ose të të dhënave të sistemit kompjuterik, pa patur autoritet ligjor për ta bërë këtë.

Krim kibernetik - konsiderohet ndërhyrje e paautorizuar drejt dhe/ose përmes përdorimit të TIK, penalizimi për të cilin rregullohet ngalegjislacioni penal.

Infrastruktura kritike – konsiderohen ato infrastruktura dhe/ose pjesë infrastrukturash që kanë rëndësi jetike për të siguruar funksione të rëndësishme sociale, cënimi apo shkatërrimi i të cilave do të kishte impakt serioz në shëndetin, sigurinë, dhe/ose mirëqënien ekonomike të qytetarëve.

Luftë kibernetike – konsiderohet çdo akt lufte në dhe/ose përreth hapësirës kibernetike që lidhet kryesisht me teknologjinë e informacionit.

Sabotazh kibernetik – konsiderohet sulmi kibernetik që ka si objekt të tij cënimin e integritetit dhe disponueshmërisë së një sistemi TIK**.**

Shënim: *Në këtë disertacion vetëm për efekt standartizimi në mënyrën e të shprehurit fjala 'kompjuterike' dhe 'kibernetike' do të konsiderohen ekuivalente.*

HIPOTEZAT E PUNIMIT

Hipoteza I:

Po evidentohet një progres i pjesshëm në luftën kundër krimit kibernetik dhe në transpozimin e standardeve ndërkombëtare në legjislacionin shqiptar, pasi Shqipëria nuk ka miratuar akoma një strategji dhe plan-veprimi për parandalimin dhe luftimin e krimit kibernetik.

Hipoteza II:

Kuadri ligjor dhe institucional shqiptar është i paplotë dhe ka nevojë për reformime në fushën e krimeve kibernetike për t'i bërë ballë nevojave dhe rreziqeve aktuale që paraqet ky fenomen.

PYETJET KËRKIMORE TË PUNIMIT

1. Pse duhet të shqetësohemi për krimin kibernetik?
2. Ç'është krimi kibernetik?
3. Çfarë e ndihmon të jetë kaq i përhapur?
4. Si mundemi ta parandalojmë dhe a jemi të përgatitur përballë këtij fenomeni?
5. Cilat janë sfidat për ligjvënësin shqiptar?
6. A është legjislacioni shqiptar në harmoni me standardet e BE?

Pyetje për trajtim:

1. A ka nevojë për reforma legjislative mbi krimin kibernetik në Shqipëri?
2. Cili është roli i prokurorëve në hetimin e krimit kibernetik?
3. Si e rregullon ligji procedural i vendit krimin kibernetik?
4. A i ka respektuar Shqipëria kriteret legjislative dhe masat procedurale të përcaktuara në Konventën e Budapestit mbi "Krimin Kibernetik"?
5. Çfarë veprash penale parashikohen nga legjisalcioni shqiptar për krimet kibernetike?

METODAT DHE METODOLOGJIA E KËRKIMIT

Në zhvillimin e këtij punimi shkencor kam përdorur disa metoda shkencore, të cilat konsistojnë në studimin e fenomenit të krimit kibernetik në dimensionet e evoluimit dhe shfaqjes së tij në një epokë, ku zhvillimi teknologjik ka arritur përmasa të mëdha, e parë kjo në perspektivën e rregullimit ligjor europian dhe vendas.

Metodat shkencore të përdorura në këtë studim janë: metoda historike, analtike, përshkruese, krahasuese dhe statistikore, të cilat janë gërshetuar në çështjet e trajtuara në këtë punim.

Metoda historike është përdorur për të pasqyruar zhvillimin evolutiv të krimit kibernetik, si dhe proceset evoluese të përqasjes së legjislacionit të brendshëm shqiptar me *acquis communitaries* në fushën e krimeve kibernetike.

Metoda analitike bazohet kryesisht në analizën e thellë ligjore të dispozitave e akteve komunitaredhe vendase në fushën kibernetike.

Metoda përshkruese e përdorur në këtë punim ka pasur si qëllim identifikimin e gjendjes aktuale të zhvillimit të krimit kibernetik dhe qasjes që ka vendi ynë kundrejt këtij fenomeni në kuadër të angazhimeve ndërkombëtare dhe europiane të ndërmarra, duke përshkruar më hollësi dhe duke bërë një trajtim të plotë dhe gjithëpërfshirës të kuadrit ligjor europian dhe vendas në lidhje me krimet kibernetike me qëllim evidentimin e problematikave që hasen në këtë fushë, si dhe zbatimin efektiv të praktikave më të mira në realitetin shqiptar.

Metoda krahasuese është përdorur për të vënë përballë sanksionimin e bërë nga legjislacioni europian në lidhje me parandalimin dhe luftimin e krimeve kibernetike dhe zbatimit në praktikë në shtete të ndryshme, e parë kjo në raport me rregullimin e bërë nga ligjvënësi shqiptar.

Metoda statistikore është përdorur në kreun IV kryesisht për të dhënë fakte e shifra në lidhje me realitetin e krimeve kibernetike në Shqipëri për periudhën 2010-2014.

HYRJE

Përdorimi i teknologjive të reja të informacionit dhe veçanërisht i internetit ka marrë një rëndësi të veçantë në jetën e përditshme. Ky fenomen prek, jo vetëm aktivitetet e organizmave shtetërore apo private, por mund të prekë dhe njeriun e thjeshtë në aktivitetin e tij të përditshëm, në sferën e tij private apo profesionale. Si çdo teknologji e re e vënë në dispozicion të një numri të madh përdoruesish, Interneti paraqet jo vetëm të mira dhe përfitime, por në të njëjtën kohë dhe një sërë problemesh që më përpara ishin të paimagjinueshme.

Keqpërdorimi i tekonologjisë nga elementë kriminalë njihet me emrin 'krim kibernetik' (*cybercrime*), i njohur si një nga format e krimit me një rrezikshmëri të lartë shoqërore, ku në thelb është veprimi i një personi mbi një sistem kompjuterik, që mund të shfaqet si mashtrim kompjuterik, falsifikim kompjuterik, thyerje e sistemeve të sigurisë apo në çfarëdo forme tjetër që përfshin si mjet sistemin kompjuterik të lidhur me një rrjet. Krimet kompjuterike janë përkufizuar si: "*Vepra penale që kryhen kundër individëve apo grupeve të individëve për qëllime të përfitimit monetar, dëmtimit të imazhit të viktimës apo shkaktimittë një dëmi fizik ose mendor drejtpërdrejt ose tërthorazi duke përdorur teknologjinë moderne*''. Në praktikën e përditshme konstatohen dy lloj sjelljesh përballë fenomenit të krimit kibernetik.

Në njërën anë kemi përdoruesin e përditshëm, i cili udhëhiqet shumë shpesh nga ideja që "*e keqja shkon gjithmonë tek të tjerët*". Në anën tjetër, kemi specialistët e fushës që udhëhiqen diametralisht nga e kundërta, domethënë që "*të tërë jemi të barabartë, të paktën në terma matematike, ndaj probabilitetittë të qënit objekt i një sulmi kriminal*". Ndryshe nga përdoruesi i zakonshëm, specialisti i kushton kohë analizës së fenomenit për të kuptuar funksionimin e tij.

Nga natyra, teknologjitë e reja janë në evolucion të vazhdueshëm dhe për rrjedhojë dhe rreziqet e lidhura me këtë teknologji evoluojnë në të njëjtën mënyrë. Scott Peck, një psikiatër i njohur amerikan dhe autor i suksesshëm librash shkruan: "*E vetmja mënyrë për të pasur siguri në jetë është të njohësh pasigurinë*". Prandaj njerëzimi duhet të përgatisë një mbrojtje dhe një luftë të fortë ndaj çdo lloj forme të krimit, qoftë atij tradicional të njohur edhe më parë, qoftë ndaj krimit kibernetik të ditëve të sotme.

Të ndodhur para problemeve që shkaktohen nga krimet kibernetike shumë vende po përpiqen të caktojnë kufijtë e tyre përmes mekanizmave filtrues dhe ndërtimit të pengesave elektronike. Por kohët e fundit ky lloj i ri krimi i ka thyer limitet e mëparshme të kohës dhe shtrirjes fizike duke kapërcyer kufinjtë shtetëror. Pra, nuk është më e mjaftueshme që një shtet të ketë masa parandaluese ndaj këtij fenomeni, por është i nevojshëm edhe bashkëpunimi i dy ose më shumë shteteve që të ketë rezultate në parandalimin dhe luftimin e këtij fenomeni.

Këshilli i Evropës ka dhënë një kontribut të rëndësishëm në këtë aspekt nëpërmjet rolit dhe kompetencave të tij, si institucioni më i rëndësishëm që ka për qëllim kryesor mbrojtjen e interesave të shteteve anëtare nëpërmjet bashkërendimit dhe bashkëpunimit më të gjerë midis tyre. Gjithashtu BE ka dhënë një kontributtë rëndësishëm për të luftuar fenomenin nëpërmjet përdorimit të instrumenteve komunitare (direktivat, vendimet, rekomandimet).

Në këtë mënyrë vendet që synojnë të anëtarësohen në BE duhet të transpozojnë në legjislacionin e tyre të gjithë *aquis communitaries*. Një ndër këto vënde është edhe Shqipëria, e cila në respektim të marrëveshjes së stabilizim - asocimit dhe përmbushjes së kritereve të përcaktuara nga BE duhet të nxisë hartimin dhe zbatimin e legjislacionit shqiptar në hetimin, ndjekjen penale, gjykimin dhe bashkëpunimin ndërkombëtar në luftën kundër krimit kibernetik.

Krimi kibernetik gjithnjë e më shumë po përhapet edhe në Shqipëri në forma nga më të ndryshmet. Por pavarësisht faktit se Shqipëria ka ratifikuar "Konventën e Budapestit mbi Krimet Kibernetike"dhe përfaqësohet në të ashtuquajturin Rrjeti i Lisbonës: **(***linket e institucioneve të trajnimit të gjyqësorit*), evidentohet nevoja për reforma legjislative të mëtejshme në këtë fushë.

KAPITULLI I: HISTORIKU DHE EVOLUCIONI I KRIMEVE KIBERNETIKE

1. Njohuri të përgjithshme mbi krimet kibernetike

Kriminaliteti si dukuri e dëmshme dhe e rrezikshme për njerëzimin, që nga kohërat më të lashta ka shfaqur tek njerëzit mendime dhe ide të ndryshme për mënyrën e parandalimit të tij në shoqëri. Zhvillimi i shoqërisë ka kaluar në etapa të ndryshme, të cilat kanë sjellë dhe konstatime të ndryshme për kriminalitetin. Me nocionin 'kriminalitet' kuptohet tërësia e të gjitha krimeve të kryera në një kohë, hapësirë dhe periudhë të caktuar. Ndryshimi i shoqërisë së sotme filloi me revolucionin agrar, u pasua nga revolucioni industrial dhe arriti deri në periudhën e sotme në epokën e revolucionit informatik[1].

Ndryshimi që solli revolucioni informatik ishte automatizimi i çdo proçesi duke e shnëdrruar çdo informacion në një kod binar, duke e përpunuar atë dhe duke gjeneruar informacion të ri. Revolucioni informatik solli sofistikimin e mëtejshëm të sjelljes kriminale, integrimin e sistemeve kompjuterike në veprat ekzistuese, ku çdo individi në saj të kësaj teknologjie mund t'i shkaktohet dëm masiv. Bazuar në format e ndryshme të kriminalitetit në shoqëritë e zhvilluara bashkohore evidentohet një formë e re krimi, ajo në fushën e kibernetikës[2].

Me arritjet e mëdha tekniko-teknologjike që ballafaqohet sot njerëzimi dallohet një lehtësim në automatizimet e proceseve të ndryshme nga njëra anë, ndërsa në anën tjetër një keqpërdorim i këtyre arritjeve që ka shfaqur një sërë problemesh dhe rreziqesh. Pra, revolucioni informatik përveç anëve të mira ka dhe anët e tij negative, që u kanë krijuar hapësirasjelljeve kriminale. Statistikat e para mbi krimin kibernetik janë mbajtur që prej vitit 1985, të dhëna këto që kanë ecur në rritje dhe zgjerim në shumë sfera të cilat nuk kanë ekzistuar më parë. Përdorimi i kompjuterit ka mundësuar kryerjen e shumë detyrave dhe funksioneve në fushën ekonomike, juridike, mjekësore, shkencore dhe fusha të tjera. Këto zhvillime kanë bërë që të shfaqen shumë sjellje anti shoqërore dhe kriminale për shkeljen e ligjit. Deri më tani nuk ekziston ndonjë përkufizim i pranueshëm botërisht për krimet kibernetike.

---

[1]Domenico V. (2007), "*La nuova criminalita informatica. Evoluzione del fenomeno e strategie di contrasto*", Rivista di Criminologia, Vittimologia e Sicurezza: 46–54.

[2] Halili R. (2008), *Kriminologjia*, Prishtinë, fq. 69.

Kjo vështirësi është pasojë e llojshmërisë së formave dheshpejtësisë së përhapjes të kësaj forme kriminaliteti. Në mes të viteve 50 një numër i madh biznesesh dhe agjencish shtetërore krijuan proceset e të dhënave kompjuterike, departamente të automatizuara, të cilat merreshin me hedhjen e të dhënave administrative. Rrisku kryesor që paraqitej në atë periudhë ishte avaria elektro-mekanike, si dhe programimet e dobëta kompjuterike[3].

Studimet e para lidhur me krimin kibernetik filluan në vitet 1960. Në këtë periudhë ky krim përfshinte abuzimin kompjuterik, sabotazhin kompjuterik, spiunazhin kompjuterik dhe përdorimin ilegal të sistemit kompjuterik. Në vitet 70 kostot e pajisjeve informatike u ulën në mënyrë dramatike, gjithashtu edhe programet komjuterike ishin me çmime të lira, pikërisht në këtë periudhë ishte shfaqja e fillimit të tregut për pavarësinë e programeve dhe furnizuesve të tyre[4].

Dështimi informatik vazhdonte të mbetej një rrisk për shkak se shumë individë kishin të drejtën e përdorimit të kompjuterave dhe të të dhënave, dhe mundësia e mashtrimit për të dy palët ishte më e madhe. Agjencitë dhe institucionet që siguronin burime të rëndësishme informatike kishin mundësi të merrnin një staf më të madh në numër. Gjatë viteve ‘70 dhe ‘80 vazhdoi trendi i zhvillimit dhe i përdorimit të kompjuterave. Të dhënat kompjuterike përdoreshin jo vetëm për raporte të përgjithshme, por edhe për analizat e nevojave të klientëve dhe për proceset e prodhimit dhe ruajtjen e të dhënave financiare. Bizneset arrinin të organizoheshin vetë brenda strukturës së tyre, duke e bërë të panevojshme punën e menaxherëve të mesëm dhe stafit administrativ. Kompjuterat e thjeshtësuan punën në biznese duke e bërë atë më efiçente[5]. Libri i parë mbi sigurinë e informacionit kompjuterik, libër si për profesionistët edhe për publikun në përgjithësi, u publikua në vitin 1970 dhe shënoi identifikimin e parë publik mbi problemin e sigurisë[6]. Në fund të viteve `80 ishte përhapur gjerësisht përdorimi i kompjuterave si në shtëpi ashtu edhe në kompanitë private, duke përdorur edhe aparatet modem për komunikimet e jashtme[7].

---

[3] www.oecd.org/dataoecd/3/42/46894657. pdf, fq.16.

[4] *Po Aty*, fq.15.

[5] *Po Aty*, fq.15

[6] *Po Aty*, fq.16.

[7] *Po Aty*, fq.16.

Në fillim të viteve `90 zhvillimi dhe përhapja e faqeve të internetit nëpër botë solli rritjen e përdoruesve, të cilët nuk ishin intelektual dhe akademik[8]. Ndërsa në periudhën midisviteve 1993 dhe 1995, interneti ishte plotësisht i hapur ndaj trafikut tregtar dhe në vitin 1996 funksiononin mbi 15 milion kompjutera[9].

Po të flasim në terma të rreziqeve dhe kërcënimeve, kjo teknologji e re e informacionit prodhoi një rrugë dhe drejtim të ri për aktivitetin kriminal, i cili mbulohej nga mundësia e anonimatit, duke bërë që shumë përdorues pa experience të shfrytëzoheshin dhe mashtroheshin. Trendi më i rëndësishëm lidhur me sigurinë e informacionit në biznese, aktualisht është lëvizja drejt infrastrukturave të dyshimta, jo të qarta. Një pjesë tjetër e siguruesve sa vjen e më shumë i sigurojnë klientëve të tyre burime informatike dhe kapacitete të ruajtjes së të dhënave, nëpërmjet shërbimeve të ndryshme si Google Docs dhe Gmail. Tregu për kryerjen e këtyre shërbimeve është vlerësuar me rreth 17 bilion dollarë në vitin 2009 dhe parashikohet të arrijë 54.2 bilion dollarë në vitin 2013[10].

2. Përkufizimi i krimit kibernetik

Kibernetika është degë shkencore e cila merret me krijimin e diagramave për sistemet e automatizuara. Klasifikohet si shkencë mbi qeverisjen dhe komunikimin mes qënieve të gjalla dhe makinerive. Fjala kibernetikë rrjedh nga fjala greke *kibernete* që do të thotë *timonier i anijes*, duke u nisur nga një analogji midis timonierit dhe qeverisësit apo drejtuesit. Ajo u njoh si shkencë me rastin e botimit të librit të Norbert Wenerit me titull "*Cybernetics*" dhe nëntitullin "*Qeverisja dhe komunikimi me organizmat e gjallë dhe makina*", libër i botuar në vitin 1948 në Paris.

Krimet kompjuterike janë përkufizuar si: "Vepra penale që kryhen kundër individëve apo grupeve të individëve me qëllim përfitimin e vlerës ekonomike, dëmin e imazhit të viktimës apo shkaktimin e një dëmi fizik ose mendor drejtëpërdrejt ose tërthorazi, duke përdorur teknologjinë moderne ose ndryshe përkufizohet si kryerja e veprimeve me anë të një sistemi të komanduar, ku qëllimi është përfitimi me anë të mashtrimit, thyerjes së sistemeve të sigurisë, shfrytëzimi etj.

[8] www.oecd.org/dataoecd/3/42/46894657. pdf, fq.17.

[9] *Po Aty*, fq.16.

[10] *Po Aty*, fq. 22.

Në dallim nga krimet e tjera të njohura, krimet kompjuterike dallojnë pasi ato janë të lehta për tu mësuar se si të përdoren, kërkojnë fare pak burime, por nga burimi i të cilave shkaktohen dëme të rënda dhe të mëdha, mund të kryhen në një juridiksion të caktuar pa qenë aty fizikisht, dhe ajo që është më e spikatur, paligjshmëria e tyre është jo dhe aq e kuptueshme[11]. Ndërsa sipas Konventës së Budapesttit mbi Krimet Kibernetike, termi krim kompjuterik është i ndarë në dy kategori:

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

(ii) Në një kuptim të gjerë, me krim kompjuterik do të kuptohet çdo sjellje e kryer nëpërmjet një kompjuteri apo sistemi kompjuterik, përfshirë krime të tilla si përpunimi i paligjshëm, ofrimi apo shpërndarja e informacionit nga një kompjuter apo rrjet, për të abuzuar dhe tërhequr me forma të tilla si ato për përkrahjen e grupeve terrorriste, pornografie dhe pedofilie[12].

Në ndryshim nga krimet tradicionale, krimet kibernetike kanë karakter global që kryhen përmes hapsirave dhe rrjeteve kompjuterike duke tejkaluar kufinjtë konvencional shtetërorë. Ato mund të përgatiten nga kudo dhe kundër një përdoruesi kompjuteri në një vend çfarëdo të globit[13]. Në praktikën e përditshme konstatohen dy lloj sjelljesh përballë fenomenit të krimit kibernetik: në njërën anë kemi përdoruesin e përditshëm, i cili udhëhiqet shumë shpesh nga ideja që "e keqja shkon gjithmonë tek të tjerët", në anën tjetër kemi specialistët e fushës që udhëhiqen diametralisht nga kundërta, domethënë që "të tërë jemi të barabartë, të paktën në terma matematikë ndaj probabilitetit të të qënit objekt i një sulmi kriminal"[14]. Ndryshe nga përdoruesi i zakonshëm, specialisti i kushton kohë analizës së fenomenit për të kuptuar funksionimin e tij.

---

[11]Masuda. (1980), "*The Information Society as Post-Industrial Society"*. New Delhi: Vikas. pp.16.

[12]McConnell International LLC. (2000). "*Cyber Crime…and Punishment? Archaic Laws Threaten Global Information"*. Available at:http://www.mcconnellinternational.com/services/CyberCrime.htm

[13]Amelie M. Weber. (2003), "*The Council of Europe's Convention on Cybercrime"*, 18 Berkeley Tech. L.J. pp. 22.

[14]Rosini L. (2007). "*Il computer crime e le strategie di constrasto*" Revista di Criminolgia, Vittimologia e Sicurezza: 12–17. http://www.vittimologia.it/rivista/rosini%202007-01-01.pdf.

Duhet theksuar fakti që në asnjë moment dhe në asnjë rrethanë nuk duhet të biem pre e idesë që një ditë këtë probabilitetin mund ta bëjmë zero. Ky pohim merr një rëndësi të madhe kur ka të bëjë me teknologjitë e reja dhe me sigurinë informatike[15].

3. Mënyrat e shfrytëzimit të internetit si mjet për kryerjen e krimit kibernetik

Në vitet e fundit shoqëritë në të gjithë botën, kanë bërë përparime të mëdha drejt kalimit në shoqërin e informacionit. Fakti që shoqëria po mbështetet gjithmonë e më shumë dhe si rrjedhojë po varet gjithmonë e më shumë nga teknologjia e informacionit dhe komunikimit, e bën atë të ekspozuar ndaj kërcënimeve të tilla si krimi kibernetik. Zhvillimi i teknologjisë kompjuterike ka përcaktuar rolin që kanë kompjuterat në zhvillimin dhe funksionimin e shoqërisë si dhe varësinë që individët kanë ndaj përparësive që ofron ky zhvillim teknologjik. Nëpërmjet aksesit në të dhënat e depozituara në sistemet kompjuterike, individ të ndryshëm për interesa dhe motive të ndryshme kanë shfrytëzuar kompjuterin si mjet për kryerjen e veprave penale kibernetike. Një veprimtari e caktuar kriminale nuk mund të kryhet pa ndihmën e kompjuterit. Përdorimi i kompjuterit si mjet për realizimin e veprimeve kriminale në fusha të caktuara, duke përdorur mekanizma të automatizuar, siç janë programet kompjuterike dhe të dhëna të tjera, i ka ndihmuar këta individë të realizojnë veprimin e tyre kriminal. Përdorimi i kompjuterit si mjet për kryerjen e krimit mund të bëhet kryesisht për këto forma të krimeve kibernetike si: keqpërdorimet financiare, krijimin dhe përhapjen e viruseve, vjedhjen e informatave nga sistemet kompjuterike, etj[16].

Duke marrë në konsideratë mundësitë e mëdha që ofron kompjuteri, ai mund të shfrytëzohet gjithashtu si mjet efikas për planifikimin, organizimin dhe udhëheqjen e veprimeve kriminale si nga ana e individit ashtu dhe nga organizatat kriminale. Në këtë këndvështrim, sot po luan rol gjithnjë e më të madh interneti me shërbimet e postës elektronike, që ofron mundësi të shpejtë komunikimi në çdo cep të botës. Kjo gjë lehtëson udhëheqjen dhe kontrollin e shpejtë të veprimeve të paligjshmetë autorëve të veprave penale në kibernetikë[17].

---

[15] Sieber U. (2005). "*The Threat of Cybercrime, Organised crime in Europe: the threat of Cybercrime"*. Situation report. Octopus Programme.pp19.

[16] Gordon S., Ford R. (2006). "*On the definition and classification of cybercrime*", in Journal in Computer Virology, n. 2, pp.13-20.

[17] Gercke M. (2009). "*Understanding Cybercrime. A Guide for Developing Countries",* available at:www.itu.int.

Përdorimi i kompjuterit ndeshet tepër edhe tek mashtrimet apo manipulimet e ndryshme për regjistrimin e gabuar të të dhënave, apo futjen e pasaktë të tyre në mënyrë të qëllimshme për përfitime pasurore ose dobi të tjera. Mashtrimet kompjuterike mund të bëhen në çdo sistem ekonomik apo në çdo sistem tjetër ku shrytëzohet sistemi informatik kompjuterik. Si rast praktik mjaft i ndeshur është ai i tregtisë elektronike E-bay që kryhet nëpërmjet internetit. Duhet të përmëndet se ky modernizim gjithnjë e më i madh i teknologjisë së informacionit ka bërë të mundur që kompjuteri me përparësitë e veta teknike që ka, të shfrytëzohet edhe si mjet i fortë për parandalimin, zbulimin, gjurmimin dhe provimin e veprave penale. Për këtë arsye organet e zbatimit të ligjit dhe agjencitë në mbarë botën janë të orientuara në ndërtimin dhe zhvillimin e sistemeve të automatizuara informatike. Rol të madh në këtë aspekt luan interneti, format i cili mundëson shkëmbim të informatave mes strukturave policore dhe agjencive të shteteve të ndryshme me qëllim identifikimin dhe ndalimin e autorëve tëveprave penale kibernetike.

Sistemet kompjuterike janë bërë pjesë vitale e mënyrës së jetesës. Për të kuptuar dhe analizuar më qartë fenomenin e krimit kibernetik është e rëndësishme të përcaktohet vendi, roli dhe mënyrat e shfrytëzimit të kompjuterit në këtë fushë. Lidhur me këtë, shikuar në mënyrë globale, autori A. Bequaj, në punimin e tij "*How to prevent computer crime*" thekson se shfrytëzimi i kompjuterit në fushën e krimeve kibernetike bëhet në pesë mënyra themelore. Lidhur me këtë autori i lartpërmendur paraqet këtë renditje: a). Kompjuteri si objekt sulmi; b). Kompjuteri si mjet i kryerjes (*modus operandi*); c). Kompjuteri si mjet për organizimin, planifikimin dhe udhëheqjen e kriminalitetit; d) Kompjuteri si simbol për mashtrim; f) Kompjuteri si mjet për ndalimin, zbardhjen dhe provimin e veprave penale[18]. Një ndarje përafërsisht të njëjtë nga aspekti kriminalistik e ka prezantuar edhe autori M. Boskoviq. Ky autor, shfrytëzimin e kompjuterit për qëllime kriminale e paraqet në katër forma themelore:

(i) Kompjuteri si mjet për kryerjen e veprës penale, ku autori përdor kompjuterin për të kryer veprën penale;

[18]Bequaj A . (1983). "*How to Prevent Computer Crime*", John Walley & Sons, Inc, pp. 1-14.

(ii) Kompjuteri si objekt sulmi, në të cilin kompjuteri dhe të dhënat e përmbledhura në të janë objekt i sulmit kriminal;

(iii) Kompjuteri si mjet për organizimin, planifikimin dhe udhëheqjen e veprimeve kriminale. Në këtë aspekt kompjuteri përdoret më shumë në fushën e krimit të organizuar, zakonisht në fazën e përgatitjes dhe planifikimit të veprimeve kriminale[19];

(iv) Kompjuteri si mjet të cilin e përdor policia për parandalimin, zbardhjen dhe provimin e veprave penale.

Në vijim do të trajtojmë më gjerësisht mënyrat e shfrytëzimit të kompjuterit dhe rolin e tij në kryerjen e veprave penale.

3.1. Kompjuteri si objekt sulmi

Zhvillimi i teknologjisë informatike ka përcaktuar rolin që kompjuteri ka në zhvillimin dhe funksionimin e shoqërisë bashkëkohore si dhe varësinë gjithnjë e më të madhe të shoqërisë ndaj teknologjisë informatike.

Në këtë këndvështim, sistemet kompjuterike dhe kompjuterat bëhen objekt i këtyre sulmeve kibernetike me qëllim ndryshimin e të dhënave apo asgjesimin e tyre. Gjithashtu rëndësia dhe vlera e hardwear-it dhe softwear- it si dhe llojet e ndryshme të të dhënave që gjenden në sistemet kompjuterike,tërheqin mjaftueshëm shumë individë dhe grupe të organizuara kriminale,të cilët tentojnë ti kompromentojnë ato në mënyrë ilegale[20].

3.2. Kompjuteri si mjet i kryerjes (modus operandi)

Një veprimtari e caktuar kriminale, nuk mund të kryhet pa ndihmën e kompjuterit. Përdorimi i tij si mjet për realizimin e veprimeve kriminale në fusha të caktuara, duke përdorur mekanizma të automatizuar për modifikim dhe manipulim të formave elektronike të vlerave shoqërore, siç janë programet kompjuterike dhe të dhënat të cilat prezantojnë të mirat dhe shërbimet, paratë ose informatat, mundëson ose lehtëson punën e autorit në realizimin e veprimeve të caktuara kriminale[21].

Në këtë kategori proceset kompjuterike konsiderohen si elemente kyçe dhe ato shërbejnë për të mundësuar, lehtësuar dhe shpejtuar realizimin e veprave të caktuara kriminale duke luajtur kështu një rol të rëndësishëm në këtë kontekst.

[20]Arthur J. Carter, IV & Audrey Perry. (2004). "*Computer Crimes"*. 41 AM. CRIM. L. REV. pp. 313-327.

[21]Wall D. (2001). "*Crime and the Internet"*. Routledge, London-New York, pp.184- 194.

Përdorimi i kompjuterit si mjet për kryerjen e krimit mund të bëhet kryesisht për realizimin e formave të krimit kibernetik si: keqpërdorimet financiare, krijimin dhe përhapjen e virusëve, vjedhjen e informatave nga sistemet kompjuterike, etj[22]

Është me rëndësi të përmendet edhe fakti se kompjuterinë të shumtën e rasteve dhe në të njëjtën kohë mund të shfaqet në role të dyfishta, si objekt dhe si subjektsulmi,pasi shumë veprime kriminale realizohen duke shfrytëzuar një kompjuter për të sulmuar kompjuterin tjetër. Nga sa u tha më sipër vlen të theksohet se kompjuteri dhe sistemet kompjuterike janë objekt i sulmeve të grupeve dhe individëve të ndryshëm, të cilët i sulmojnë ato me qëllim kompromentimin e të dhënave të ruajtura në ato sisteme, shkatërrimin e bazës së të dhënave apo modifikimin e tyre[23].

3.3. Kompjuteri si mjet për fshehje, planifikim, organizim dhe udhëheqje në realizimin e veprimit kriminal

Një nga zbulimet më të rëndësishme të zhvillimit dhe civilizimit tekniko-teknologjik është kompjuteri. Mirëpo, pavarësisht nga përparësitë dhe mundësitë që ka sjellë kompjuteri, ai është shfrytëzuar dhe keqpërdorur nga grupe dhe organizata të ndryshme kriminalepër të realizuar vepra penale kibernetike me qëllime fitimprurëse.

"Per shkak të mundësive të mëdha që ofron kompjuteri, ai mund të shfrytëzohet si mjet shumë i fortë dhe preçiz në planifikimin, organizimin dhe udhëheqjen e veprimeve kriminale, qoftë nga ana e individit ashtu edhe nga ana e grupeve apo organizatave kriminale".

Në këtë drejtim kompjuteri gjithnjë e më shumë shfrytëzohet në fushën e kriminalitetit të organizuar posaçërisht në fazën e përgatitjes dhe të planifikimit të veprimtarisë kriminale si dhe në procesin e kontrollit dhe të mbikqyrjes së realizimit të procesit të fundit, siç është realizimi i përfitimeve financiare[24]. Mund të thuhet se shfrytëzimi i kompjuterit për qëllime kriminale e u ka dhënë mundësinë individëve apo grupeve të ndryshme që të planifikojnë dhe organizojnë veprimet e tyre kriminale në mënyrë të shpejtë, preçize dhe cilësore.

---

[22]Carter D., & Bannister A. J. (2000). "*Computer crime: A forecast of emerging trends"*. Paper presented at the Academy of Criminal Justice Sciences Annual Meeting, New Louisiana.

[23]Brenner S.(2004). "*U.S. cybercrime law: Defining offenses"*. Information Systems Frontiers, pp.115- 132.

[24]Latifi V. (2004). "*Kriminalistika"*. Prishtinë, fq. 288.

Kompjuteri mund të ndihmojë që veprimet kriminale të kryhen shpejt dhe saktë, duke mundësuar përpunimin e një game të gjerë informacionesh dhe duke e bërë të vështirë identifikimin dhe zbulimin e këtyre veprimeve. Në këto veprime kriminale hyjnë: menaxhimi i librave të kontabilitetit (librat e dyfishtë), pastrimi i "*parave të pista*", veprimtritë e paligjshme bankare dhe veprime të tjera"[25].

Rol gjithnjë e më të madh në këtë kontekst po luan edhe interneti me shërbimin e postës elektronike (e-mail), i cili ofron mundësi të mëdha të komunikimit të shpejtë dhe të sigurt në çdo kënd të botës, duke u shftytëzuar nëkëtë mënyrë në masë të madhe ngakrimi i organizuar[26].

Pra, siç u tha më lart, shfrytëzimi i kompjuterit si mjet për fshehjen, planifikimin, organizimin dhe udhëheqjen e veprimeve kriminale, është i një rëndësie të veçantë. Me ndihmën dhe përdorimin e kompjuterit, individët apo grupet kriminale e kanë më të lehtë të menaxhojnë dhe kontrollojnë veprimtaritë e tyre ilegale, në kuptim të realizimit të qëllimeve të tyre kriminale në mënyrë të shpejtë dhe cilësore, siç është p.sh rasti i transaksioneve financiare ilegale miliona dollarëshe.

3.4. Kompjuteri si mjet për mashtrim

Njëra prej formave më të përhapura të keqpërdorimit të kompjuterit është përdorimi i kompjuterit për manipulime të ndryshme[27]. Këto manipulime konsistojnë në futjen dhe regjistrimin e të dhënave të pasakta ose në bllokimin për të futur të dhënat e sakta në kompjuter. Këto veprime sot përbëjnë numrin më të madh të keqpërdorimeve kompjuterike, si për nga numri ashtu edhe për nga lloji i formave nëpërmjet të cilave paraqiten.

Kompjuteri mund të krijojë një maskë ideale për kryerjen e disa veprimeve të caktuara kriminale, duke ju dhënë atyre një kualitet të veçantë. Mashtrimet kompjuterike janë të mundshme në çdo sistem ekonomik ose biznes tjetër në të cilin shfrytëzimi i sistemit kompjuterik mund të ndikojë në ecurinë e shpërndarjes së të mirave dhe vlerave monetare.

---

[25]Apruzzese, A. (2007). "*Dal computer crime al computer-related crime*". Rivista di Criminolgia, Vittimologia e Sicurezza: 55–60.

[26] Carter L.D (1995) . "*Computer Crime Categories:"How Techno-criminals Operate*". FBI Law Enforcement Bulletin Volume:64 Issue: 21-27.

[27] *Po Aty*.

Këto mashtrime janë të shumta në fushën e kontrollit të zhvillimeve të kapitalit financiar dhe zakonisht paraqiten në formë të mashtrimeve lidhur me sistemet e kontabilitetit dhe sistemet bankare, investimet, sigurimet, detyrimet tatimore, shpalljen e falimentimit, pastrimin e parave etj[28].

Sipas konstatimeve të shumë autorëve, mashtrimet kompjuterike zakonisht kryhen nëpërmjet internetit në rastet e "tregtisë elektronike ose ndryshe shit-blerjeve online". Sipas agjencisë APIS Security Consalting, thuhet se në një seminar të mbajtur në Sidney gjatë vitit 2003 nga ana e agjencive për mbrojtje të blerësve nëpërmjet internetit është provuar se: "në çdo 44 sekonda çdo njeri bëhet viktimë, pasi vendos të blejë mallin për të cilin informohet dhe njoftohet nëpërmjet internetit"[29].

3.5. Kompjuteri si mjet për parandalimin, sqarimin dhe provimin e veprimit kriminal

Modernizimi gjithnjë e më i madh i teknologjisë informatike ka bërë të mundur që kompjuteri me përparësitë teknike që ofron, të përdoret si mjeti dobishëm për parandalimin, zbulimin, sqarimin dhe provimin e veprave penale.

Integrimi i të dhënave në evidencat policore, shpejtësia, vërtetësia, kompletimi dhe llojshmëria e përpunimit të tyre, siç janë: seleksionimi sipas kritereve të ndryshme, përpunimi statistikor, krahasimi si dhe shfrytëzimi i tyre në kohën e duhur, rrit dhe forcon veprimtarinë preventive të organeve policore. Për këtë arsye, të gjitha policitë dhe agjencitë në mbarë botën janë të orientuara në ndërtimin, zhvillimin dhe modernizimin e sistemeve të automatizuara informative. Në këtë kontekst, rëndësi të veçantë sot luan interneti[30].

Interneti është shnëdrruar në një mjet të rëndësishëm për të gjurmuar dhe ndaluar kriminelët e shumë kërkuar, duke bërë që ata të mos gjejnë dhe të mos kenë strehim të sigurt në asnjë vend[31].

---

[28] Taylor R. W., & Loper D. K. (2003). "*Computer crime"*. In C. R. Swanson, N. C. pp. 32.

[29] Agency: APIS Security Consulting, 31.03.2004.

[30] Gordon/Hosmer/Siedsma/Rebovich. (2003). "*Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime"*. available at: http://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf.

[31] Carlesi C. (2003) "*Sicurezza informatica and 'computer crime*", Report, Istituto di Scienza e Tecnologie dell'Informazione. Alessandro Faedo, Pisa. pp. 18-22.

Me qëllim zbulimin e kriminelëve në çdo vend të botës, byrotë policore të shteteve të ndryshme, nëpërmjet internetit kryejnë shkëmbimin e informatave, paraqesin fletë-arreste me fotografitë e kriminelëve më të kërkuar si dhe kryejnë shumë veprime të tjera. Një kërkim të tillë e bën edhe Byroja Federale e Hetimeve (FBI) në SHBA, e cila nëpërmjet adresës së internetit: *http:/www.fbi.gov/mostwant/topten/tenlist.htm*, kërkon kriminelët më të kërkuar në SHBA[32].

Problematikën e kryerjes së veprave penale kibernetike e ka trajtuar edhe FBI *(Byroja Federale e Hetimeve)* e cila ka konstatuar se ekzistojnë tre grupe personash, të cilët paraqesin rrezikshmëri të lartë për kryerjen e veprave të tilla. Sipas tyre, grupi i parë dhe më i madhi përbëhet nga persona, të cilët ndërhyjnë në një kompjuter apo sistem kompjuterik vetëm që të binden nësekjo është e mundur, pa pasurndonjë qëllim për të vjedhur apo shkatërruar ndonjë të dhënë. Grupi i dytë i këtyre personave ndërhyjnë në sistemet kompjuterike me qëllim për të shkatërruar, ndryshuar apo penguar procesin e kompjuterit apo sistemit kompjuterik. Gjithsesi në të tre rastet bëhet fjalë për persona profesionistë dhe me aftësi të zhvilluara në fushën informatike[33].

Kriminaliteti kompjuterik përmban disa karakteristika që e dallojnë atë nga format e tjera të kriminalitetit. Një ndër karakteristikat është se, autorët e veprave penale të kriminalitetit kompjuterik nuk mund të krahasohen me autorët e formave klasike të kriminalitetit, pikërisht për shkak të specifikave të ndryshme të cilat i veçojnë ata në kryerjen e këtyre krimeve.

Personat që kryejnë vepra penale kibernetike kanë njohuri të zhvilluara në fushën e teknikës kompjuterike dhe informatikës kriminalistike. Këtu bëhet fjalë kryesisht për persona me inteligjencë të zhvilluar teknike, veprimtaria kriminale e të cilëve nuk është e lehtë të zbulohet dhe të provohet"[34].

---

[32]Rogers M. (1999). "*Organized Computer Crime and More Sophisticated Security Controls*: *Which Came First the Chicken or the Egg*". in Telematic Journal of Clinical Criminology, available at: www.criminologia.org.

[33]M. Chawki. (2005). "*A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy"*. DROIT-TIC. pp.14.

[34]Gordon S., Ford R. (2006). "*On the definition and classification of cybercrime*". in Journal inComputer Virology, n. 2, pp.13-20.

"Për zbulimin e suksesshëm dhe sigurimin e provave të caktuara, përveç përcaktimit të nocionit të krimit kibernetik dhe të përpunimit të karakteristikave themelore të tij, rëndësi të veçantë ka kërkimi i formave të paraqitjes së tij dhe konkretizimi i tyre në vepra të caktuara penale"[35].

Zbulimi dhe të provuarit e krimeve kibernetike është detyrë e vështirë dhe e ndërlikuar. Ndërhyrjet e paautorizuara në sistemet kompjuterike mund të kryhen nga ana e autorit pa lënë gjurmë, duke qenë se veprimi mund të jetë kryer në një vend, ndërsa pasoja të jetë shkaktuar në një vend tjetër, në një largësi tejet të madhe. Për kryerjen e veprimeve kriminale shfrytëzohen metoda profesionale dhe teknike, të cilat vështirë zbulohen, dhe shpesh mund të provohen vetëm nëse zbulohen në çastin e kryerjes. Të gjitha studimet në këtë fushë tregojnë se numri i errët i kriminalitetit në këtë fushë është i lartë[36]. Asnjë instalim kompjuterik nuk është absolutisht rezistent ndaj veprimeve kriminale, kjo për shkak se nuk ekziston një mbrojtje absolute. Prandaj, numri i rasteve të regjistruara dhe të publikuara paraqesin arkivë të vërtetë për një kronikë kriminale. Ajo që e vështirëson problemin në tërësi është se autorët e këtij lloj kriminaliteti janë të "armatosur" mirë dhe jo vetëm që kanë intelekt të lartë, por njëkohësisht janë të përkrahur edhe ngateknologjiae lartë që u vjen në ndihmë. Shumë forma të kriminalitetit klasik, është vështirë të zbulohen, hetohen, provohen dhe autorët e tyre të dënohen, teknologjia informatike këtë e bën edhe më të vështirë. Ekzistojnë disa faktorë që vështirësojnë zbulimin dhe luftimin e krimit kibernetik, siç jane: *Së pari*, teknologjia e sofistikuar, kapaciteti shumë i madh për ruajtjen e të dhënave si dhe shpejtësia e funksionimit të kompjuterave. *Së dyti*, hetuesit dhe policia nuk posedojnë aftësi dhe njohuri të mjaftueshme dhe profesionale për t'u marrë me problemet në ambjentin kompleks të procesimit të të dhënave. *Së treti*, shumë prej viktimave nuk kanë njohuri dhe informacion që të planifikojnë raste të paparashikuara për tu ballafaquar me krime kibernetike, para se ato të zbulohen"[37].

[35]Gercke M. (2009). "*Understanding Cybercrime. A Guide for Developing Countries".* available at: www.itu.int.

[36]Hale Ch. (2002). *Cybercrime: Facts & Figures Concerning this Global Dilemma*, CJI, Vol. 18, available at: http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37.

[37]James A O'Brien.(1999). "*Management Information Systems".* (4th). New York: Irwin/McGraw-Hill.pp.8.

Duke trajtuar këtë çështje, vihet re, se e gjithë kjo tregon lindjen e një kategorie të re të kriminalitetit, në të cilin rolin kryesor e luan kompjuteri dhe për këtë shkak e ka marrë edhe emrin kriminaliteti kompjuterik[38]. Është konstatuar se kompjuteri nga aspekti juridiko-penal paraqitet si *modus operandi* për shumë vepra penale, por edhe si mjeti dobishëm për parandalimin, zbulimin, sqarimin dhe provimin e veprave penale[39].

4. Numri i errët i krimeve kibernetike

Krimet kibernetike kanë një numër të errët tepër të lartë që shpjegohet nga disa shkaqe si: karakteri global i këtyre veprave që s'kanë kufinjë,duke i dhënë mundësi autorëve të kryejnë veprën nga një anë tjetër e botës duke shfrytëzuar pajisjet themelore si kompjuteri, modemi, softueri etj; vështirësitë e zbulimit, ndjekjes dhe të provuarit e këtyre veprave; personaliteti i autorit të veprës penale; personaliteti apo sjellja e të dëmtuarit ndaj veprës së krimit kibernetik. Duke trajtuar këto probleme konstatohet se numri i veprave të pazbuluara të krimeve kibernetike është me të vërtetë i madh[40]. Kjo tregon se mungon një sistem mbrojtës për zbulimin e këtyre veprimeve kriminale dhe se mungon vullneti i të dëmtuarve për paraqitjen e rasteve në organet kompetente. Përveç një numri të madh veprash penale kundër teknologjisë së informacionit dhe komunikimit ose nëpërmjet saj, një numër gjithmonë e më i lartë i çështjeve të tjera që përfundojnë në gjykatë përfshijnë provat elektronike që janë memorizuar në një sistem kompjuterik. Kështu që gjyqtarët dhe prokurorët duhet të jenë të përgatitur të përballen me krimet kibernetike dhe provat elektronike. Rëndësia e teknologjisë së informacionit dhe komunikimit është aq e madhe në shoqërinë e sotme, saqë gjyqtarët dhe prokurorët duhet të kenë të paktën disa njohuri bazë të këtyre teknologjive dhe të problemeve që lidhen me to. Ndërsa në shumë vënde, organet e zbatimit të ligjit kanë arritur t'i fuqizojnë kapacitetet e tyre për të hetuar krimet kibernetike dhe për të siguruar provat elektronike, kjo duket se ka ndodhur p.sh. në Shqipëri në një shkallë më të ulët për gjyqtarët dhe prokurorët, të cilët megjithatë luajnë një rol kyç në proceset ligjore penale[41].

[38]Latifi V.(2009). "*Kriminalistika"*. Prishtinë, fq. 336-346.

[39]Sette R. (2000), *Criminalità informatica. Analisi del fenomeno tra teoria, percezione e comunicazione sociale"*. Clueb, Bologna, pg. 28.

[40]Wall D. (2001). "*Crime and the Internet".* Routledge, London-New York, pp. 1-17.

[41]Hale Ch. (2002). "*Cybercrime: Facts & Figures Concerning this Global Dilemma"*, CJI, Vol. 18.pp.19-31.

Gjyqtarët dhe prokurorët hasin vështirësi në përballjen me realitetet e reja të botës kibernetike. Për këtë arsye duhen bërë përpjekje të posaçme në drejtim të aftësimit të gjyqtarëve dhe prokurorëve për t'i ndjekur dhe gjykuar krimet kibernetike dhe për të përdorur provat elektronike nëpërmjet trajnimit, krijimit të rrjeteve dhe specializimit[42].

5. Masat për parandalimin dhe luftimin e krimit kibernetik

Krimi kibernetik, për shkak të karakterit të tij specifik, rrezikshmërisë së madhe shoqërore dhe shkallës së lartë të rritjes në masë të madhe, po bëhet problem i vërtetë shoqëror, madje jo vetëm në përmasa kombëtare, por edhe në përmasa ndërkombëtare. Kjo formë e kriminalitetit po zhvillohet me një shpejtësi aq të madhe, saqë praktikisht nuk ka precedent. Për këtë arsye vlen të përmendet konstatimi se kjo dukuri është një "industri", e cila p.sh disa vende siç është SHBA zhvillohet me ritme të shpejta. Vetëm në SHBA ka me miliona sisteme informatike e kompjuterike, të cilat janë të lidhura në rrjetin kompjuterik. Vetëm transaksionet financiare, që barten nëpërmjet katër sistemeve kryesore të rrjetit të bankave elektronike, si: Fedwire, Bankwire, Chips dhe SWIFT, së bashku përbëjnë afërsisht 300 miliardë dollarë qarkullim ditor brenda shtetit dhe afërsisht 600 miliardë dollarë qarkullim ditor në trafikun ndërkombëtar. Këto shuma dollarësh, duke i llogaritur edhe ato të shteteve të tjera në botë, të cilat janë në qarkullim monetar ditor nëpërmjet rrjeteve të ndryshme të sistemeve kompjuterike, me siguri që paraqesin një provokim të madh, të cilit shumica e krimineleve nuk mund t'i bëjnë ballë.

Për këto dhe shkaqe të tjera, është e pakontestueshme nevoja për një aksion adeguat, me qëllim parandalimin dhe luftimin e suksesshëm të këtij fenomeni të ri në shoqërinë bashkëkohore. Duke pasur parasysh vështirësitë e parandalimit, zbulimit, sqarimit dhe provimit të veprave të kriminalitetit kompjuterik, në luftën kundër këtij fenomeni shikuar në përgjithësi, në dispozicion janë tre lloje mekanizmsh, të cilët mund t'u përgjigjen me sukses këtyre provokimeve, dhe këto janë: pajisjet për mbrojtje, etika dhe ligjet. Këto mekanizma kanë karakter parandalues dhe represiv. Para së gjithash, në aplikimin e tyre përparësi duhet t'u jepet masave parandaluese në krahasim me ato represive[43].

[42]Wigert I. (2006). "*Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security"*. IIB-1.pp. 34-46.

[43]Bakewell, E. J., Koldaro, M., & Tija, J. M. (2001). "*Computer crime*". The American\ Criminal Law Review, 38, (3), 481-524.

Mbrojtja e suksesshme e sistemeve kompjuterike në aspektin global duhet shikuar si problem në tre nivele: ndërkombëtar, kombëtar dhe lokal. Sistemet globale kompjuterike dhe rrjedhja transnacionale e të dhënave dhe e informatave, praktikisht kanë "hequr" kufinjtë shtetërorë në kuptimin klasik, kështu që kriminelëve kompjuterike u mundësohet që veprat penale t'i kryejnë në një shtet, ndërsa pasojat t'i bartë shteti tjetër, edhe me mijëra kilometra larg atij shteti. Në këtë mënyrë, krimi kibernetik, praktikisht, bëhet problem ndërkombëtar, që imponon nevojën e mbrojtjes së sistemeve informatike jo vetëm të vendit, por në të njëjtën kohë edhe atyre të vendeve të huaja. Me këtë rast hapet edhe çështja e hetimeve ndërkombëtare, e ekstradimeve dhe ndëshkimit të kryerësve të kësaj kategorie të kriminalitetit[44].

Këto çështje shtrojnë nevojën e krijimit të një platforme të përbashkët në planin e mbrojtjes sësistemeve informatike, të mbështetur në standardet dhe orientimet ndërkombëtare, në njërën anë, dhe në anën tjetër, në bashkëpunimin e ngushtë dhe koordinimin e të gjithë anëtarëve të bashkësisë ndërkombëtare në drejtim të modernizimit, unifikimit dhe sinkronizimit të sistemeve të tyre juridike në fushën e kriminalitetit kompjuterik. Këto angazhime në nivelin ndërkombëtar do të mundësonin dhe do të lehtësonin luftimin dhe rregullimin e këtij problemi serioz dhe të ndërlikuar. Nëse parandalimi i kriminalitetit kompjuterik në nivelin ndërkombëtar nuk është i unifikuar dhe e i harmonizuar, ligjet nacionale do të paraqesin barriera për kapjen e kriminelëve kompjuterikë dhe e gjithë kjo do të çojë në krijimin e strehimorëve të kriminalitetit kompjuterik, në të cilët kriminelët kompjuterikë do të jenë mbi ligjet dhe imunë nga çdo ndëshkim[45].

Në planin nacional është e nevojshme që të përcaktohen bazat e përbashkëta të sigurisë në pajtim me standardet dhe rekomandimet ndërkombëtare dhe ato të BE-së, rishikimi i legjislacionit, futja e normave të reja apo modifikimi i atyre ekzistuese si dhe përshtatja e tyre me kërkesat e kohës[46].

---

[44]Me gjeresisht, shih: Vula V. vep. e. cit, fq. 150.

[45]Carlesi C. (2003). "*Sicurezza informatica and 'computer crime*", Report, Istituto di Scienza e Tecnologie dell'Informazione "Alessandro Faedo, Pisa. pg.17.

[46]Brenner S. W. (2001), "*Defining cybercrime: A review of State and federal law"*. In R. D.pp. 5-12.

Siguria kombëtare si koncept, në njëfarë mënyre konsiderohet si garantuese e ushtrimit të të drejtave të njeriut dhe pikërisht kjo është një nga detyrat më të rëndësishme të një shteti. Kjo garanci, sipas nenit 12 të Deklaratës Universale të të Drejtave të Njeriut, duhet të përmbushet nga një forcë publike, e cila në mënyrë të barabartë do të mbrojë interesat e gjera të të gjithë popullsisë dhe jo vetëm të atyre të cilëve ajo u është besuar.

Në këtë fillim të shekullit XXI, informacioni i trajtuar në të gjitha format e mundshme, elektronike apo tradicionale, përbën një pasuri të vërtetë, si për individët ashtu dhe për organizmat privatë apo shtetërorë dhe konsiderohet si një burim strategjik rreth të cilit zhvillohet ajo që sot quhet shoqëri e informacionit. Nuk është hera e parë që teknologjia dhe inovacionet qëlidhen me të janë një bazë e ndryshimeve të thella për shoqërinë; dje, inovacionet në fushat e energjisë, dhe sot, mënyrat e larmishme të komunikimit të njohurive dhe informacioneve nëpërmjet teknologjive të reja të telekomunikacionit.

Ky koncept i shoqërisë së informacionit, si një vazhdimësi e shoqërisë industriale të disa viteve më parë, në qendër të saj ka informacionin dhe njohuritë, si dhe mënyrën e përcjelljes së tyre pa limite gjeografike dhe kohore. Teknologjitë informatike, duke qënë të përdorura gjerësisht, janë një vektor shumë i rëndësishëm dhe i pashmangshëm për shumicën e aktiviteteve. Ky realitet ilustrohet me vendin gjithnjë e më të rëndësishëm që në jetën tonë të përditshme po zë ajo që quhet hapësirë virtuale (*cyberspace*), e cila gjithnjë e më shumë po ndryshon kufijtë tradicionalë, kohorë dhe gjeografikë dhe mënyrën e të jetuarit dhe të të menduarit në ditët e sotme. Nga ky këndvështrim, informacioni si një motor ekonomik i zhvillimit është një e mirë jomateriale që kërkon njëmbrojtje në lartësinë e vlerave dhe rëndësinë e tij, nga ana e individëve, organizmave dhe mbi të gjitha, të shtetit[47].

Krimet që synojnë manipulimin, fshirjen, modifikimin, mbikqyrjen, spiunazhin e informacioneve që qarkullojnë në rrjetet e komunikimit, mund të prekin drejtpërdrejt interesat e një individi, të një organizate, apo të një shteti. Kështu, siguria e informacionit është e lidhur ngushtësisht me sovranitetin e një shteti, që përbëhet nga mbrojtja e infrastrukturave kritike e sistemeve dhe e rrjeteve, e pasurive kulturore të kombit, e të

[47]Hayden E. (2006). "*Cybercrime's impact on Information security*, *Cybercrime and Security"*. IA-3, pp. 3.

mirave materiale dhe jomateriale, që do të thotë, e përmbledhur në një fjalë të vetme, nga mbrojtja e vlerave[48].

Në rrethet e ekspertëve të sigurisë, marrja në konsideratë e problematikës së sigurisë së informacionit, shpeshherë trajtohet si problem i lidhur tërësisht me një dimension teknik e shpesh edhe si një demagogji apo problematikë virtuale. Fatkeqësisht, faktet i kanë dhënë të drejtë, vetëm pjesërisht kësaj mënyre të të menduarit. Në të vërtetë, këto sulme virtuale kanë pasur rezultate mëse reale, me një bilanc shumë negativ për organizmat publikë apo privatë. Sa për ilustrim, mund tëpërmendim rastine Estonisë, një shtet sovran dhe anëtar i organizmave euro-atlantikë. Në rastin konkret në këtë shtet, pas rrënimit të përmendores së ushtarit sovjetik në një park të kryeqytetit të Estonisë, pasoi një sulm masiv mbi infrastrukturat e informacionit të institucioneve në Estoni dhe bëri që këto infrastraktura informatike të ndalonin së funksionuari për një kohë të gjatë, duke krijuar kështu një kaos të plotë në ekonominë e vendit. Duke përdorur një teknikë jo shumë të komplikuar përmbytjeje *(flooding),* sulmi u bë mbi infrastrukturën estoneze, nëpërmjet kompjuterave fantazmë *(boo triets),* gjë e cila mbingarkoi rrjetin kompjuterik në mënyrë të atillë, saqë ky nuk mundi ta përballonte ngarkesën dhe pushoi së funksionuari. Ministri i Mbrojtjes i Estonisë, Jaal Aavisko, do të deklaronte për gazetën *«The New York Times»:* "Kemi të bëjmë me një situatë që prek sigurinë kombëtare, të krahasueshme me një situatë kur portet tuaja bombardohen nga deti"[49]. Sot, në botën bashkëkohore, për sa i takon pikëpamjes së sigurisë së sistemeve kompjuterike dhe informatike, gjithnjë e më shumë dominon mendimi sipas të cilit sistemet e sigurisë nuk ekzistojnë, por vetëm ato të cilat kanë pak a shumë një shkallë të lartë të besueshmërisë[50]. Më qëllim të mbrojtjes së sistemeve kompjuterike dhe atyre informatike nga numri gjithnjë e më i madh i formave të ndryshme të kriminalitetit kompjuterik, është e nevojshme zhvillimi dhe zbatimi i një sistemi masash sigurie, për të garantuar mirëfunksionimin e sistemeve të komunikimit dhe të informacionit.

[48]Hale Ch. (2002). "*Cybercrime: Facts & Figures Concerning this Global Dilemma"*. CJI, Vol. 18, available at:http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37.

[49]Icove, D. & Seger, K. (1995). '*Computer crime: A crimefighter' s handbook"*. Sebastopol, CA: O'Reilly & Associates, Inc.pp.3-8.

[50]http://www.nytimes.com/2007/05/29/technology/29estonia.html.

Janë disa masa teknike që mund të ndiqen për të siguruar mbrojtjen e sistemeve nga sulmet kibernetike. Zbulimi i rrugëve dhe metodave të ndryshme për forcimin e infrastrukturës së komunikimit, është e nevojshme.

Një nga shembujt është zhvillimi i DNSSEC, i cili forcon serverat kryesor duke i siguruar vërtetimin e firmosur elektronik të informacionit DNS. Një punë e tillë kërkon forcimin e Protokollit të portave në kufi, të cilat kontrollojnë kursin e trafikuar ISP tek ISP. Vështirësia qëndron në faktin se këto ndryshime ndaj protokolleve të internetit ndodhin nga një proces i marrëveshjes dhe i pranimit, që përveç shqyrtimeve aktuale teknike, ka të bëjë me një debat ndërmjet lirisë dhe kontrollit[51].

Një propozim tjetër është detyrimi i individëve për të pasur një identitet të qëndrueshëm në internet. Disa politikbërës shpresojnë që kjo mund të arrihet nëpërmjet lëvizjes tek IP v 6, i cili është një proces i nevojshëm si procesi ekzistues i sistemit të adresës IP. Problemet që mund të lindin si rezultat i këtyre propozimeve janë të tilla si: procesi i regjistrimi, ky proces nëpërmjet të cilit personi fizik është i lidhur, është kompleks. Në këto kushte kemi rrethana të pranueshme kur individët dëshirojnë të veprojnë në mënyrë anonime pa u identifikuar në rrjetet e komunikimit kompjuterik[52].

Një nga masat teknike që është propozuar p.sh, në SHBA në Qershor të vitit 2010 i referohet një version të propozuar si internet i fikur (Internet Off- Switch). Vetë hapësira e informacionit në internet ka dimension pakufi dhe interneti nuk mund të fiket për një arsye të thjeshtë sepse nuk ka një qendër fikse. Në një rast urgjence është e mundur përballimi i situatës në nivel shtetëror dhe kombëtar, kur trafiku i informacionit i filtruar do të kalojë nëpërmjet kthesave kritike[53]. Çdo institucion publik duhet të investojë në sistemet e tij të teknologjisë. Kostoja është më e madhe kur këto sisteme dhe rrjete nuk përditësohen me filtra dhe programe të reja dhe mungesa e investimeve në këtë fushë sjellë kosto më të lartë kur vetë këto sisteme do të dalin jashtë përdorimit.

[51] OECD/IFP Project on "*Future Global Shocks*"-"*Reducing Systemic Cybersecurity Risk*" www.oecd.org/dataoecd/3/42/46894657. pdf .

[52] *Po Aty*: www.oecd.org/dataoecd/3/42/46894657.pdf .

[53] *Po Aty*: www.oecd.org/dataoecd/3/42/46894657. pdf.

Shteti duhet të garantojë sigurimin e sistemeve të teknologjisë së informacionit dhe komunikimit, me mjete dhe pajisje të standardeve ndërkombëtare, për të shmangur dhe evituar kërcënimet dhe sulmet me pasoja të shtrira në nivel kombëtar. Vetë ekspertët dhe specialistëtqë operojnë në këtë fushë, duhet të nxisin dhe të bashkëpunojnë me qeverinë dhe institucionet publike, për të siguruar mbështetjen në investime të mëtejshme, në mjete dhe paisje të sigurisë[54]. Institucionet publike dhe private kanë zhvilluar politikat e tyre për sigurimin e mjeteve dhe paisjeve për mbrojtjen e sistemeve dhe rrjeteve të tyre. Marrja e masave të koordinuara ndërmjet institucioneve publike dhe zhvillimi i politikave të partneritetit publik-privat është i rëndësishëm.

Mirëmbajtja e softeve duhet të kryhet nga personeli i çertifikuar i cili ka përgjegjësi jo vetëm për miratimin dhe zbatimin e ndryshimeve që mund ti bëhen softeve, por edhe për vazhdimësinë e sigurisë së rrjetit, pas zbatimit të ndryshimeve të bëra. Ky personel është përgjegjës për hartimin dhe zbatimin e proçedurave për menaxhimin dhe kontrollin e origjinës së softeve, prokurimin, instalimin dhe mënyrën e përdorimit të tyre[55].

6. Analiza e rrezikut

Është një proçedurë e cila përdoret për vlerësimin e besueshmërisë së kërcënimeve dhe humbjes potenciale, e cila mund të rezultojë nga ndjeshmëria e sistemit kompjuterik. Kjo masë i paraprin programit të sigurisë dhe ka për qëllim të ofrojë përgjigje për pesë pyetje themelore, si:

1. Cilat janë objektivat më të shpeshta të sulmeve kibernetike?

Duke iu përgjigjur kësaj pyetjeje, praktika na tregon se objektivat më të shpeshta të sulmeve janë kompjuterat dhe sistemet kompjuterike të shërbimeve informative dhe ato ushtarake, që janë objekt i spiunazhit; kompjuterat dhe sistemet kompjuterike të bizneseve,të cilat janë objekt i konkurrencës; kompjuterat dhe sistemet kompjuteriketë bankavedhe institucioneve të tjera financiare, të cilat në shumicën e rasteve janë objekt i kriminelëve profesionistë; kompjuterat dhe sistemet kompjuterike të organizatave të ndryshme, e veçanërisht të qeverive dhe shërbimeve publike, të cilat mund të jenë objekt i

[54] http://www.tradoc.mil.al/Standartizimi/Downloads/TEKSTI%20I%20PLOTE%20I%20MANUALIT%20TE%20STANDARDIZIMIT-SHTATOR%2009.pdf, Manuali i Standartizimit te FASH te RSH.

[55] www.nsaalbania.gov.al/vend922.html, VKM nr. 922, datë 19.12.2007 .

terroristëve; sistemet kompjuterike të ndërmarrjeve të cilat mund të jenëobjekt i të punësuarve apo i ish-punëtorëve dhe kompjuterat dhe sistemet kompjuterike të çdo organizate tjetër të cilat mund të jenë objekti hakerave, ndonjëherë nga provokimi intelektual, e ndonjëherë si rezultat i veprimeve të profesionistëve, të cilët punojnë për persona të tjerë. Dobësitë e një sistemi kompjuterik kanë të bëjnë me pikat vitale të cilat mund të jenë objekt i sulmeve. Është e nevojshme që ato më parë të identifikohen dhe ndërmjet tyre të përcaktohen prioritetet, në mënyrë që me programin e sigurisë të parashikohet mbrojtja e tyre. Numri më i madh i këtyre dobësive të sistemit kompjuterik rrjedh nga organizimi i dobët, mungesa e investimeve dhe mungesa e interesimit për mbrojtjen e sistemeve kompjuterike.

1. Cilat janë rreziqet ndaj të cilave ekspozohen sistemet kompjuterike?

Rreziqet të cilat u kanosen sistemeve kompjuterike kanë të bëjnë me objektet që u përmënden më lart, ato mund të jenë të provokuara me veprime të rastësishme apo të qëllimshme, të ndërmarra nga kryerësit e jashtëm *(eksterne*) apo të brendshëm *(interne),* por edhe nga forca të tjera të paparashikueshme *(vis major).*

2. Cilat janë kundërmasat e mundshme?

Qëllim i kundërmasave të mundshme është që ato të kenë veprim parandalues për të sprapsur kryerësin nga kryerja e veprave të tilla, pengojnë dhe ta ndërpresin atë,dhe nëse veprimi është ndërmarrë atëherë ta ndalojnë në përfundimin e veprimit të tij. Këto masa nuk përfshijnë vetëm masat e mbrojtjes teknike, ato përfshijnë të gjitha ato veprime dhe metoda me të cilat shmangen keqpërdorimet ose zvogëlohen pasojat e tyre negative.

5. *Cilët janë autorët e mundshëm?*

Të gjithë ata që marrin pjesë në sistemet kompjuterike ose në çfarëdo mënyre shfrytëzojnë resurset e tyre, duhet të informohen se cilët mund të jenëautorët e mundshëm të keqpërdorimeve të sistemeve kompjuterike, cilat janë motivet dhe si i realizojnëata synimet e tyre. Pas marrjes së përgjigjeve për pyetjet e përmendura, atëherë mund të merremi me vendosjen e programit të sigurisë, implementimin dhe testimin e mekanizmave mbrojtës, kontrollimin e punës së tyre dhe mbikqyrjen e vazhdueshme të punës për shfrytëzimin e sistemeve kompjuterike dhe resurseve të tyre[56].

[56]Wall D. (2001). "*Crime and the Internet".* Routledge, London-New York, pp. 1-17.

7. Vendosja e programit për siguri

Me programin për siguri duhet të dokumentohen veprimet dhe masat me të cilat do të arrihet njëshkallë e kënaqshme e mbrojtjes sëburimeve informatike si dhe do të përcaktohen të drejtat dhe detyrimet e të gjithë shfrytëzuesve të sistemit kompjuterik, të cilët në çfarëdo mënyre janë në lidhje me ato burime (bashkëpunëtorët e jashtëm, furnizuesit, kontraktuesit, etj.). Programi për siguri përbëhet prej katër komponentëve të cilët kanë të bëjnë me sigurinë fizike që përfshin të gjitha ato masa dhe veprime, qëllimi i të cilave është të pengohet hyrja e paautorizuar dhe dëmtimi i sistemeve kompjuterike.

Këto masa janë: sigurimi i sistemit kompjuterik nga vërshimet, zjarri, tërmeti, rryma elektrike, sigurimi fizik i objekteve etj. Për këtë qëllim përdoren masa të ndryshme siguruese, si: shërbimet e sigurisë, sistemi i alarmit, sistemi kundër zjarrit, kartat e ndryshme të identifikimit për akses në ndërtesën në të cilën janë të vendosura burimet e sistemeve kompjuterike, si dhe metodat e ndryshme biometrike të cilat bazohen në vetitë fizike apo në karakterin e ndonjë personi. Përveç kësaj, si komponent i dytë, këtu hyn edhe siguria njerëzore, e cila përfshin të gjitha veprimet dhe masat, qëllimi i të cilave është që të pengohen dëmet të cilat mund të shkaktohen me qëllim apo rastësisht nga të punësuarit, nga ish-të punësuarit apo nga persona të tjerë të mundshëm. Siguria e komunikimit, si komponent i tretë, përfshin masat, qëllmi i të cilave është që të sigurohet një komunikim i sigurt, i papenguar dhe sekret i shkëmbimit të të dhënave mes personave të autorizuar, që zhvillohet nëpërmjet aksesit nga largësia apo nëpërmjet rrjetit lokal. Këto masa para se gjithash kanë të bëjnë me kontrollin e hyrjes në sistemin kompjuterik (mbrojtja nga hakingu), kontrolli i kanaleve të komunikimit (mbrojtja nga përgjimi) etj[57].

Ndërkaq, si komponent i katërt është siguria operative, e cila ka të bëjë me mbrojtjen e hardwear-it dhe softwear-it për të ruajtur integritetin funksional të tyre. Nga të gjitha këto që u përmenden më lart, lidhur me mjetet dhe masat për parandalimin dhe luftimin e ndërhyrjeve dhe keqpërdorimeve të mundshme të sistemeve kompjuterike dhe informatike, arrihet në konstatimin se qëllim i vetëm, është mbrojtja e këtyre sistemeve me masat që sigurojnë mbrojtje në tre drejtime, si në: aspektin fizik, teknik dhe administrativ.

[57]Clifford R.D. (2011). "*Cybercrime: The investigation, prosecution, and defense of a computer-related crime"*. Durham, NC: Carolina Academic Press, pp. 11-68.

Me këto masa arrihet që deri diku të ruhet integriteti dhe mbrojtja e sistemeve kompjuterike[58].

8. Mbrojtja juridike sipërgjigje ndaj keqpërdorimeve të sistemeve kompjuterike

Ndërhyrjet e paligjshme kundër sistemeve kompjuterike, si në vendet e zhvilluara ashtu edhe në ato që pretendojnë zhvillim tekniko-teknologjik modern, çdo ditë e më shumë po bëhen problematike. Meqënëse sisteme kompjuterike plotësisht të sigurta sot nuk ka, paraqitet nevoja për një mbrojtje juridiko- penale, me të cilën do të mbroheshin të mirat më të rëndësishme të shoqërisë.

Detyrë e saj është që me kohë të gjejë përgjigje dhe në mënyrë gjithëpërfshirëse të ofrojë mbrojtje të të mirave më të rëndësishme dhe interesave të cilat janëkusht i funksionimit dhe shfrytëzimit të papenguar të sistemeve kompjuterike. Në rastin konkret, mbrojtja juridiko-penale do të kishte karakter parandalues, e drejtuar në parandalimin e kryerjes së veprave penale në fushën e krimeve kibernetike[59].

Për të arritur një mbrojtje efikase dhe gjithëpërfshirëse ndaj veprave penale kibernetike, është e nevojshme që të përcaktohen bazat themelore të mbrojtjes sipas standardeve dhe direktivave ndërkombëtare dhe europiane, të bëhen reforma ligjore nacionale, pastaj të futen norma të reja apo të modifikohen ato ekzistuese si dhe t'u përshtaten kërkesave të kohës[60].

[58]Clifford R.D. (2001), "*Cybercrime, the investigation, prosecution and defense of a Computer related crime"*. Carolina Academic Press, United States, pp.169.

[59]Wendy McAulif fe. (2001). "*Council of Europe Approves Cybercrime Treaty"*, ZDNET UK NEWS, at*:* http://new szdnet.co.uk/sto ry/0t269 -s209579600.html.

[60]Icove D. & Seger K. (1995). "*Computer crime: A crimefighter' s handbook"*. Sebastopol, CA: O'Reilly & Associates, Inc.pp.16-28.

KAPITULLI II: TRAJTIMI I PËRGJITHSHËM JURIDIKO-PENAL I KRIMEVE KIBERNETIKE

1. Rregullimi juridiko-penal në disa shtete të Europës

Rrezikshmëria e madhe shoqërore e krimeve kibernetike dhe rritja e përhershme e keqpërdorimit të komjuterave kërkojnë që kjo problematikë të rregullohet me dispozita të caktuara ligjore. Kështu nevojiten ndërhyrje të reja në kodet penale të cilat do të sanksionojnë këtë veprimtari kriminale. Për pengimin e kriminalitetit komjuterik, shumë shtete po bëjnë përpjekje për të gjetur mjete, metoda dhe masa sa më efikase në këtë drejtim. Në rradhë të parë duhet bërë pikërisht rregullimi juridiko-penal duke u parë si mbrojtje juridike nga ndërhyrjet e paautorizuara në sistemet komjuterike.

Me aprovimin e ligjeve që kanë të bëjnë me inkriminimin e veprës për ndërhyrje të paligjshme në sistemet komjuterike, ndërmjet ligjëvënësve ka patur diskutime të shumta lidhur me çastin kur kjo ndërhyrje fillon të trajtohet si vepër penale. Kështu shtete të ndryshme e trajtojnë si vepër penale që nga momenti i ndërhyrjes së parë të paautorizuar dhe disa të tjerë që prej momentit kur është shkaktuar dëmi më i vogël[61].

Mbrojtja juridike nga ndërhyrjet e pa autorizuara në sistemet komjuterike nuk ka mundur të sigurohet me normat ligjore penale tradicionale, për këtë arsye Bashkimi Europian dhe shumë shtete anëtare të tij kanë miratuar ligje të reja me qëllim krijimin e masave ndëshkimore për krimet kibernetike të ndodhura ndaj shoqërisë. Nga përmbajtja e ligjeve penale të Britanisë së Madhe del qartë se janë inkorporuar të gjitha format e paraqitjes së krimeve kibernetike, që prej rekomandimeve të Këshillit të Europës.

Britania e ka aprovuar ligjin mbi keqpërdorimin e komjuterave në vitin 1990 duke dhënë përcaktimin e veprave penale kompjuterike specifike. Në këtë ligj bëhet fjalë për vepra penale që mbulojnë rrethin më të gjerë të keqpërdorimeve komjuterike, ku përfshihen veprimet me dashje të autorit të veprës penale, siç janë mashtrimi komjuterik dhe sabotazhi kompjuterik, me qëllim shfrytëzimin e të dhënave, programeve komjuterike apo dhe të vetë sistemit komjuterik.

[61]GORDON/FORD. (2006). "*On the Definition and Classification of Cybercrime".* Journal in ComputerVirology, Vol. 2, No. 1. pp 13-20.

Legjislacioni penal i Austrisë nuk ka pasur ndonjë normë të posaçme deri në vitin 1987 mbi sanksionimin e veprës penale të krimeve kibernetike. Lidhur me trajtimet e bëra nga ligji është përkrahur konstatimi i autorit Dragievic, i cili konstaton se "me rastin e kryerjes së reformave në Ligjin Penal të Austrisë, duhet të zgjerohen përgjegjësitë penale dhe në vepra të tjera, siç është hakingu, për një mjedis shoqëror të zhvilluar". Për vepra të kësaj fushe janë parashikuar dënime me burg deri në 2 vjet ose me gjobë dhe po kjo vepër kur kryhet në rrethana cilësuese sanksionohet dënimi me burgim nga 6 muaj deri ne 5 vjet[62].

Zhvillimi i rregullimit të normave juridike-penale të zhvilluara në fushën e krimeve kibernetike, sikurse në shumë shtete të zhvilluara edhe në Gjermani ka shkuar në drejtim të njëjtë me kryerjen e ndryshimeve në Kodin Penal ekzistues për disa pjesë të reja që kanë të bëjnë me veprat penale në fushën e krimeve komjuterike. Në vitin 1986 është aprovuar ligji mbi ndalimin e kriminalitetit ekonomik në të cilin janë inkorporuar veprat nga fusha e kriminalitetit kompjuterik siç janë: vjedhja e të dhënave, mashtrimi kompjuterik, falsifikimi kompjuterik i të dhënave me rëndësi të veçantë për procesin e të provuarit dhe sabotazhi kompjuterik. Për këto vepra penale të përmendura janë parashikuar sanksione penale të cilat janë nga 1 deri në 5 vite, si dhe dënimi me të holla[63].

Në Kodin Penal të Kanadasë, në nenin 342/1 është sanksionuar vepra penale për krime kibernetike me një dënim i cili nuk kalon 10 vjet[64]. Kodi Penal Francez i vitit 1993, i cili është në fuqi aktualisht parashikon respektivisht në nenet 182, 323/1 dhe 323/4, veprat penale kibernetike si: marrje e paautorizuar e të dhënave,mashtrimi komjuterik, falsifikimi i të dhënave komjuterike dhe pengimin e funksionimit të sistemit kompjuterik. Lidhur me këto vepra penale parashikohen dënimi me gjobë dhe dënimi me burgim nga 1 deri ne 3 vjet. Ligji Penal i Polonisë bën një trajtim të veprave penale në fushën e kibernetikës sipas rekomandimeve të Këshillit të Europës, duke parashikuar dënime me burgim në më shumë se 8 vjet për qasjen e paautorizuar në sistemin komjuterik, për përgjim kompjuterik, pengimin e të dhënave dhe sabotazhin kompjuterik. Përhapjen e informacioneve të marra në mënyrë të paligjshme e dënon autorin e veprës penale me 2 vjet burg.

[62]Ligji penal i Austrise, Viene 1991, fq. 141.

[63]Ligji penal Gjerman, neni 202/a vjedhja e te dhenave, fragmente nga 6. Gragiqeviq, fq. 174-175.

[64]Handbook of Legislative Procedures of computer Netework Missue in EU countries (CSIRT) , pp. 47.

2. Struktura dhe prezenca e krimeve kibernetike

Kriminaliteti kompjuterik është produkt i zhvillimit të pandërprerë të teknologjisë kompjuterike. Ndikimi i teknologjisë kompjuterike në të gjitha sferat e jetës ka bërë qëkrimet kibernetike të përhapen ndërkombëtarisht. Krimet kibernetike për shkak të rrezikshmërisë së lartë që kanë dhe karakterit global shfaqen në hapësirën kibernetike me shumëllojshmëri formash, ku më të përhapurat janë:

2.1. Hyrja e paautorizuar kompjuterike në sistemet kompjuterike

Me ***"hyrje"*** në një sistem kompjuterik do të kuptojmë hyrjen në tërësi ose në një pjesë të tij në njësitë kryesore përbërëse, në të dhënat e ruajtura në dosje, në të dhënat e trafikut ose të përmbajtjes me qëllim sigurimin e aksesit në memorien e brendshme të sistemit, duke pasur kështu mundësinë për të pasur kontaktme të dhënatdheprogramet e regjistruara në të ose që përmbaheneventualisht në pajisje të tjera të jashtme, që janë të lidhura me sistemin komjuterik pa qenë e nevojshme në këtë rast që të kalohen pengesa të tjera. Duke nisur nga ky moment, veprimet mbartin rrezikshmëri për fshehtësinë e të dhënave dhe programeve të pranishme në sistem dhe për këtë arsye justifikohet ndërhyrja nëpërmjet sanksionit penal. Nga pikëpamja teknike, aksesi në një sistem kompjuterik mund të konsumohet me realizimin e lidhjes së thjeshtë elektronike midis dy kompjuterave nëpërmjet modemit ose me anë të aksesit fizik nga afër me aparatin dhe do të konsiderohet se është kryer në momentin kur vërtetohet se përdoruesi ka pasur mundësinë reale për të 'komunikuar' me pajisjen në të cilën ka kryer aksesin fizik. Si rrjedhim, në këndvështrimin juridik vepra penale do të konsiderohet e kryer në rastin kur përveç fazës fizike, autori ka kaluar edhe në atë logjike[65]. Hyrja në sistemin kompjuterik që të cilësohet si abuzive duhet të kryhet nëpërmjet cënimit të masave të sigurisë. Masat e sigurisë mund të jenë fjalëkalime alfabetike ose numerike të cilat shkruhen nëpërmjet tastierës ose fjalëkalime të memorizuara në shiritin magnetik të një tesere, e cila më pas vendoset në një pajisje lexuese të posaçme, ose të dhëna antropometrike – gjurmët e gishtave ose të retinës së syrit – të dallueshme nëpërmjet sensorëve përkatës ose të tipit fizik si psh. një çelës metalik për ndezjen e kompjuterit[66].

[65]Pica, G. (1999). "*Diritto penale delle tecnologie informatiche"*, Torino: UTET, pg. 40.
[66]D'Aietti, G. (1994). "*Accesso abusivo a sistemi informatici"*, në Borruso, R., Buonome, G., Corasaniti, G, dhe D'Aietti, *G. Profili Penali del Informatica. Milano:* Botimet Giuffre, pg. 73.

Gjithashtu, si veprime që cënojnë masat e sigurisë duhet të konsiderohen edhe rastet kur abuzuesi ka arritur të hyjë në sistem, jo duke thyer fjalëkalimet apo mjetet e tjera të sigurisë, por duke përdorur në mënyrë mashtruese dhe abuzive të dhënat identifikuese për hyrjen në sistem, të cilat mund t'i ketë siguruar nga subjekte që janë të autorizuar për përdorimin e tyre.

Në gjuhën e përgjithshme për ndërhyrjet e pautorizuara në sistemet kompjuterike përdoret termi Hacking, përkthimi i së cilës është pirateria kompjuterike. Ajo konsiston në kopjimin, ndryshimin dhe/ose fshirjen e të dhënave të ruajtura në një kompjuter ose sistem kompjuterash. Termi i referohet hyrjes në një sistem kompjuterik, i cili është i lidhur me një rrjet telekomunikimi publik ose në një sistem kompjuterik brenda të njëjtit rrjet, siç është rasti i një rrjeti me veprim lokal LAN (local area network), ose nëpërmjet internetit në rastin e kompjuterave të një ndërmarrjeje[67].

Ky term përfshin çdo aktivitet të qëllimshëm dhe të planifikuar, ku pas përcaktimit të sistemit objekt sulmi, studiohen karakeristikat e tij të sigurisë dhe përgatiten mjete (fjalëkalime ose programe) për të siguruar akses të paautorizuar ose për të penguar funksionimin normal të sistemit[68].

Në fillim të viteve 90, doli në pah ndarja e këtij aktiviteti në *Hacking* dhe *Cracking*,e cila bazohej në qëllimin e ndjekur nga subjektet që kryejnë një ndërhyrje të paautorizuar kompjuterike.

Kështu, termi *haker* përdoret për të treguar një ekspert në fushën kompjuterike, i cili shkel masat e sigurisë së një sistemi kompjuterik i shtyrë nga kurioziteti dhe dëshira e tij për të marrë njohuri mbi ndërtimin e sistemit kompjuterik dhe mënyrën e tij të funksionimit. Ai nuk hyn në një sistem kompjuterik me qëllim që të kryejë një vepër penale, siç mund të jetë manipulimi i të dhënave kompjuterike apo pengimi i funksionimit normal të sistemit. Ndërkohë, termi *cracker* përdoret për të treguar ata specialistë që hyjnë në mënyrë të paautorizuar në një sistem kompjuterik me qëllim kryerjen e një vepre penale.

---

[67]Raport shpjegues i Konventës së Këshillit të Evropës "*Mbi Krimin Kompjuterik*", koment nr. 46.

[68]Sharma, V. (2011). "*Information Technology Law - Law and Practice",* (3 Edition), New Delhi: Universal Law Publishing, pp. 172.

Pra në thelb, ndryshimi midis *hackerave* dhe *crackerave* qëndron në faktin se *hackerat* i identifikojnë veprimet e tyre të ndërhyrjeve kompjuterike, si veprime të kryera brënda rregullave etike, ndërsa *crackerat* nuk i përmbahen kornizave etike[69].

Duhet theksuar se arsyeja kryesore e ndëshkimit të veprimeve të hyrjes së thjeshtë në mënyrë të paautorizuar në një sistem kompjuterik, sanksionuar në legjislacione të ndryshme të vendeve të BE-së, lidhet me rrezikshmërinë që paraqet veprimi në fjalë si një veprim, i cili zakonisht i paraprin kosumimit të krimeve të tjera kompjuterike.

2.1.1. Struktura e krimit dhe e mira juridike e mbrojtur

Parashikimi i veprimeve të hyrjes së paautorizuar në një sistem kompjuterik si vepër penale e veçantë e gjen pikënisjen në një sjellje tjetër të paligjshme të dënueshme vazhdimisht sipas ligjit penal që është ajo e dhunimit të banesës.

Pra, hyrja e paautorizuar kompjuterike vlerësohet në pamje të parë si një shtrirje në planin ideal të mbrojtjes juridiko-penale të padhunueshmërisë së banesës drejt një trajte të re që ky koncept merr nën dritën e zhvillimeve teknologjike dhe që njihet si '*banesa kompjuterike*'[70].

Sigurisht që një interpretim i tillë vlen për sa kohë që hyrja e paautorizuar është kryer në kompjuterin personal të një përdoruesi privat pasi nëse veprimet e hyrjes abuzive kryhen ndaj një sistemi kompjuterik të zotëruar nga një entitet juridik privat ose publik, lidhja me konceptin e padhunueshmërisë së banesës, qoftë edhe virtuale, nuk është më e pranishme. Kjo për arsye se koncepti i padhunueshmërisë së banesës është i lidhur ngushtë me të drejtën që ka çdo person për respektimin e jetës së tij private dhe gëzimi i kësaj të drejte është i lidhur në mënyrë të pashmangshme me personat fizikë dhe jo me personat juridikë, si krijesa artificiale të ligjit.

Dispozita mbi hyrjen e paautorizuar kompjuterike gjen zbatim në këto raste:

1. Kur realizohet një hyrje e paautorizuar në distancë në një sistem kompjuteriknë sajë të cënimit të masave të sigurisë;

[69] *Po aty*.

[70] Në doktrinën dhe praktikën gjyqësore italiane ky koncept ka ardhur duke u konsoliduar gjithnjë e më shumë dhe njihet si '*domicilio informatico'*.

2. Kur realizohet një hyrje e paautorizuar në një sistem kompjuterik[71] në sajë të cënimit të masave të sigurisë dhe nëpërmjet kontaktit nga afër, të drejtëpërdrejtë fizik me sistemin;
3. Kur një person, i cili ka qenë i autorizuar për të hyrë dhe përdorur sistemin, ka tejkaluar këtë autorizim duke kryer veprime të cilat shkojnë jashtë kufinjve të lejuar të përdorimit të sistemit nga ana e tij, si psh. aksesi në dokumente ose programe të ruajtura në pjesë të veçanta të memories së brendshme të sistemit.

Për inkriminimin e veprimeve në fjalë nuk kërkohet ardhja e ndonjë pasoje të veçantë pasi bëhet fjalë për një vepër penale formale. Vepra konsiderohet e kryer që në momentin që kryhet hyrja në mënyrë të paautorizuar apo në tejkalim të autorizimit në një sistem kompjuterik. Ky qëndrim shkon në të njëjtën linjë arsyetimi që ndiqet për aplikimin e përgjegjësisë penale në rastin e dhunimit të banesës. Edhe për këtë vepër nuk kërkohet që veprimi i hyrjes në banesën e tjetrit kundër vullnetit të tij të shoqërohet nga ndonjë pasojë e caktuar. Sjellja në fjalë, konsiderohet e rrezikshme që nga ky moment pasi dhunon të drejtën e privatësisë.

Studiuesit e të drejtës evropiane në fushën e teknologjisë së informacionit pranojnë gjithashtu konceptin e banesës virtuale.Si pikë referimi për këtë qëndrim merret përqasja e bërë nga ligjvënësi evropian në Direktivën 2002/58 mbi E-Privatësinë. Në pikën 24 të Direktivës thuhet se "*pajisjet fundore të përdoruesve janë pjesë e sferës private të tyre dhe gëzojnë mbrojtje sipas Konventës Evropiane të të Drejtave të Njeriut. Përdorimi i programeve kompjuterike përgjuese (spyware), pajisjevemonitoruesetë aktivitetitonline (web bugs), pajisjeve tëtjeratë ngjashme gjurmuese, padijeninë e përdoruesve me qëllim sigurimin e aksesit në informacionin e ruajtur në kompjuterin e tyre, ruajtjen e informacioneve të caktuara në të, ose gjurmimin e aktiviteteve të kryera, mund të cënojë seriozisht privatësinë e përdoruesve".* Kështu, ndërhyrja në '*banesën elektronike*' nëpërmjet programeve kompjuterike përgjuese duhet të konsiderohet si dhunim i hapësirës elektronike private apo i banesës virtuale[71].

[71]Në Konventën "*Mbi Krimin Kibernetik*", thuhet se *"Sistem kompjuterik"* do të thotë çdolloj pajisje apo grup i ndërlidhur ose pajisje të lidhura, një ose më shumë prej të cilave, vazhduese të një programi kryejnë procesime automatike të të dhënave.

Identifikimi i të mirës juridike të prekur me konceptin e 'banesës kompjuterike' mbetet koherent për sa kohë që hyrja e paautorizuar kompjuterike kryhet në një kompjuter personal. Megjithatë, duke iu referuar legjislacionit shqiptar mund të themi se mbrojtja që ofron neni 192/b shtrihet edhe ndaj sistemeve kompjuterike që përdoren në sektorin industrial, tregtar, si dhe atë publik, të cilët po ashtu janë të mbrojtur zakonisht nëpërmjet masave të veçanta të sigurisë[72].

Po të kemi parasysh rëndësinë dhe natyrën e rezervuar të të dhënave që përmbahen në to është e rëndësishme të theksohet se nuk kërkohet që personi, i cili ka bërë hyrjen e paautorizuar në sistemin kompjuterik të ketë pasur një qëllim të caktuar të padrejtë apo të pandershëm. Në këtë kontekst, elementi i vetëm i mjaftueshëm për ta konsideruar veprën të konsumuar është vërtetimi i faktit se ndërhyrja ka ndodhur për shkak të cënimit të vullnetshëm të masave të sigurisë së sistemit. Nëpërmjet një formulimi të tillë, ligjvënësi i ka dhënë një aplikim mjaft të gjerë dispozitës duke dënuar edhe ato forma të hyrjeve të paautorizuara (hacking), të cilat nuk kanë një synim të keq në vetvete dhe që kryhen thjesht nga kureshtja për të testuar aftësitë në fushën kompjuterike. Përqasja e cila e identifikon interesin e mbrojtur me interesin personal të padhunueshmërisë së banesës fizike nuk mund të justifikojë faktin që, në rastin e hyrjes së paautorizuar kompjuterike kërkohet që sistemi kompjuterik të jetë i mbrojtur nga masa të caktuara sigurie, ndërkohë që vepra penale e dhunimit të banesës konsiderohet e konsumuar me vërtetimin e rrethanës së hyrjes në banesën e tjetrit kundër vullnetit të tij, pavarësisht faktit nëse dera e shtëpisë ka qenë e hapur ose jo. Në fakt në këtë perspektivë, zgjidhja e dhënë nga ana e ligjvënësit shqiptar për mbrojtjen juridiko-penale vetëm të atyre sistemeve që kanë qenë të pajisur me masa sigurie, duket jo shumë e qartë pasi në pranimin si të mirëqënë të faktit të ekzistencës së një mjedisi të padhunueshëm të privatësisë informatike, do të lindte detyrimi për mbrojtjen në mënyrë jo të diferencuar të të gjithë poseduesve të një sistemi kompjuterik, si të atyre që kanë adaptuar masa sigurie, ashtu edhe të atyre të cilët në çfarëdolloj mënyre tjetër, ua kanë bërë të qartë të tretëve mospajtimin me veprime të ndërhyrjes në sistemin e administruar prej tyre[73].

[72]Neni 192/b i Kodit Penal.

[73]Büllesbach A. (2010). "*Concise European IT Law",* Kluwer Law International, pp. 196.

Një shpjegim të plotë të termit banesë kompjuterike gjejmë në një vendim të kohëve të fundit të Gjykatës Italiane të Kasacionit[74]. Sipas gjykatës: "me parashikimin në Kodin Penal të veprës penale të hyrjes së paautorizuar kompjuterike, ligjvënësi ka siguruar mbrojtjen e *'banesës informatike'*, të asaj hapësire ideale (por edhe fizike në të cilën ruhen të dhënat kompjuterike) që i përket personit… për më tepër, mbrojtja që ofron dispozita penale në fjalë, nuk shtrihet vetëm ndaj të dhënave me përmbajtje shumë personale të mbledhura në sistemet kompjuterike të mbrojtura, por shtrihet edhe më tej duke u konkretizuar në atë që quhet *'jus excludendi alios'*, pavarësisht faktit se çfarë përmbajtjeje kanë të dhënat e mbyllura në këto sisteme, të dhëna që i përkasin sferës së mendimit personal apo aktivitetit të punës. Si rrjedhim, kjo mbrojtje që ofron ligji shtrihet edhe në aspektet ekonomike-pasurore të të dhënave, pavarësisht nëse titullari i *'ius exclundendi'* është person fizik, person juridik, privat, publik ose çfarëdo enti tjetër". Nga një interpretim i tillë, është e qartë se e mira juridike e mbrojtur është '*ius excludendi'* e titullarit të sistemit kompjuterik, pavarësisht natyrës së të dhënave që përmbahen në sistem, '*Ius excludendi'* nënkupton të drejtën e titullarit të një sendi për të kundërshtuar çdo ndërhyrje nga ana e të tretëve ndaj të mirës që është objekt i së drejtës.

2.1.2. Hyrja abuzive nga një person i autorizuar për të pasur akses në sistem.

Deri më tani kemi analizuar rastet kur hyrja e paautorizuar në një sistem kompjuterik kryhet nga një subjekt i jashtëm, i cili nuk ka të drejta aksesi në sistem, në saj të cënimit të masave përkatëse të sigurisë. Megjithatë, vlen të theksohet se në një pjesë të mirë të rasteve, akoma edhe më të rrezikshme paraqiten këto praktika të hyrjes abuzive, kur ato ndërmerren nga persona, që për arsye të punës që kryejnë, janë në kontakt direkt me sistemin. Praktika të tilla, njihen ndryshe si *'insider hacking'* që do të thotë pirateri kompjuterike e kryer nga brenda sistemit (pra, kur subjekti ka një autorizim për të hyrë në sistem, por tejkalon kufinjtë e autorizimit dhe hyn edhe në pjesë të sistemit në të cilat nuk i lejohet të hyjë). Parashikimi nga ana e ligjvënësit i përgjegjësisë penale edhe në rastin e përdorimit të sistemit kompjuterik në tejkalim të autorizimit nga ana e subjektit që ka pasur akses të ligjshëm në të ka rëndësi të madhe praktike.

[74]Vendim nr. 42021, dt. 26.10.2012 i Gjykatës Italiane të Kasacionit.

Në disa raste, pasojat e dëmshme që mund të vijnë nga veprimet e paautorizuara të një përdoruesi të brendshëm të sistemit kompjuterik mund të jenë shumë herë më të mëdha se sa ato që do të vinin nga ndonjë sulm i jashtëm. Gjithashtu, mund të ndodhë që subjekti i cili kryen veprime në tejkalim të autorizimit, nga mungesa e njohurive të sakta apo të specializuara në lidhje me veprimet që kryen, të shkaktojë dëmtime serioze në funksionimin e sistemit sikurse edhe humbje të të dhënave të administruara prej tij.

Vepra penale do të konsiderohet e kryer në këtë formë, kur personi i autorizuar, tejkalon kufinjtë e lejuar të përdorimit të sistemit, dhe hyn në një zonë të memories së brendshme të tij, e cila jo vetëm është e ndryshme nga pjesët e tjera në të cilat punonjësit i lejohet të hyjë, por është edhe e mbrojtur nëpërmjet masave të tjera të sigurisë.

Një praktikë e tillë mund të ndodhë p.sh. kur një punonjës policie tejkalon autorizimin që ai ka për përdorimin e kompjuterave të vënë në dispozicion të forcave të policisë për marrjen e informacioneve për qëllime private. Në vijim, prezantohet një rast i gjykuar nga Gjykata e Apelit në Ohio, USA në lidhje me përdorimin në tejkalim të autorizimit të një sistemi kompjuterik:

Në çështjen *State v Morning,* Mathew Moning, një punonjës policie në Cincinnati, Ohio u dënua pasi kishte tejkaluar autorizimin për të pasur akses në një bazë të dhënash elektronike të forcave të policisë. Mroning ishte caktuar që të kryente shërbimin e tij si punonjës policie pranë një pike të grumbullimit të makinave që ishin të sekuestruara nga punonjësit e policisë. Në zyrën e tij, në pikën e grumbullimit në fjalë, ndodhej një kompjuter që përdorej nga punonjësit e policisë për qëllime të ligjshme gjatë veprimtarisë së tyre ligj zbatuese, si psh. për të kontrolluar pronarin e një automjeti. Edhe pse Moning kishte dijeni mbi faktin që ai ishte i autorizuar të përdorte kompjuterin vetëm për qëllime që lidheshin me zbatimin e detyrave të tij si punonjës në pikën përkatëse të grumbullimit të automjeteve, në Shtator të vitit 2000, ai përdori kompjuterin e zyrës për të marrë akses në bazën e të dhënave të Qendrës Rajonale të Informacioneve Kriminale (RCIC).

Kjo bazë të dhënash, përbënte një nga tre burimet e vëna në dispozicion të forcave policore për të hetuar mbi të kaluarën kriminale të një personi. Pas sigurimit të aksesit në këtë bazë të dhënash, punonjësi i policisë Moning, i nxitur nga kureshtja si dhe dëshira për të vënë eventualisht në pozitë shtetasin J.H, nisi një kërkim për të kaluarën e tij kriminale.

Nga kërkimi, Moning zbuloi se J.H ishte i dënuar për shkelje të dispozitave mbi substancat narkotike. Në vijim, ai kishte bërë një kopje të informacionit dhe pasi e kishte printuar ia kishte treguar këtë fakt shtetasit J.H. Ky i fundit, pasi mori dijeni mbi veprimet e punonjësit Moning kërkoi informacion në autoritetet lokale të policisë se përse ishte marrë ky informacion. Autoritetet policore u shprehën se ky kërkim ishte i pabazuar në ligj. Si rrjedhim, gjykata amerikane dënoi Moning për tejkalim të autorizimit për përdorimin e sistemit komjuterik.

2.1.3. Vendi i konsumimit të veprës penale të hyrjes së paautorizuar kompjuterike

Në doktrinë shfaqet mendimi se vepra penale e hyrjes së paautorizuar kompjuterike duhet të konsiderohet formalisht e konsumuar në vendin në të cilin ndodhet sistemi kompjuterik që pëson sulmin dhe jo në vendin ku ndodhet fizikisht shkelësi në momentin që kryen veprimin e paligjshëm[75].

Në terma të përgjithshme, për shkak të ndërlidhjes së gjerë të rrjeteve kompjuterike dhe fluksit ndërkufitar të të dhënave, konstatohen probleme të konsiderueshme në lidhje me individualizimin e vendit të kryerjes së veprës dhe të përcaktimit të juridiksionit kompetent. Për të dhënë një përgjigje më të plotë në këtë drejtim është e rëndësishme të vëmë në dukje edhe parashkimet që përmban Vendimi Kuadër i BE-së "Mbi sulmet kundër sistemeve të informacionit"[76].

Në nenin 10 të këtij vendimi parashtrohen rregullat që duhet të ndiqen për përcaktimin e juridiksionit, në rastet e kryerjes së veprave penale të tilla si: hyrja e paautorizuar kompjuterike apo ndërhyrja në sistemet ose të dhënat kompjuterike. Sipas pikës 1 këtij neni, çdo shtet anëtar zbaton juridiksionin e tij nëse vepra është kryer:a) tërësisht ose pjesërisht brenda territorit të tij; b) nga një shtetas i tij; ose c) në dobi të një personi juridik, i cili e ka selinë kryesore në territorin e atij shteti.

Gjithashtu, thuhet se në përcaktimin e juridiksionit në përputhje me këto rregulla, secili shtet duhet të sigurojë që të përfshijë brenda juridiksionit rastet kur: a) vepra është kryer nga një person i cili ndodhet fizikisht në territorin e atij shteti, pavarësisht nëse vepra është

[75] *Vepër e cit.,* Pica, G. (1999). "*Diritto penale delle tecnologie informatiche".*

[76] Vendim Kuadër 2005/222/JHA, dt. 24 shkurt 2005 "*Mbi sulmet ndaj sistemeve të informacionit*".

kryer ose jo kundër një sistemi informatik të ndodhur në territorin e atij shteti; ose b) vepra është kryer kundër një sistemi informatik të ndodhur në territorin e atij shteti, pavarësisht faktit nëse personi i cili kryen veprën ndodhet apo jo fizikisht brenda territorit të tij[77].

Më tej, shpjegohet se në rastin kur vepra hyn në juridiksionin e më shumë se një shteti anëtar, dhe secili prej shteteve në fjalë mundet në mënyrë të vlefshme të fillojë ndjekjen penale mbi bazën e të njëjtave fakte, ato duhet të bashkëpunojnë midis tyre në mënyrë që të vendosin se cili prej tyre do të procedojë penalisht shkelësin/shkelësit, me synimin kur është e mundur, të përqëndrimit të procedurave në një shtet të vetëm[78]. Gjatë këtij procesi, mund të merren në konsideratë faktorët në vijim:

a. shteti në territorin e të cilit është kryer vepra;
b. shteti, shtetësinë e të cilit mban autori i veprës penale;
c. shteti në të cilin është gjetur autori i veprës penale.

2.1.4. Vënia në dispozicion ose dhënia në përdorim e mjeteve të aksesit

Me shprehjen *'dhënie në përdorim'* do të identifikohet çdo lloj forme e paligjshme e qarkullimit të mjeteve të përshtatshme për kryerjen e veprave penale kundër integritetit të të dhënave dhe sistemeve kompjuterike[79].

Me *'veprime për vënien në dispozicion të mjeteve të aksesit'* do të kuptohen ato veprime që i paraprijnë mbajtjes apo shpërndarjes dhe që mund të konsistojnë në përpjekjet e bëra personalisht për gjetjen e këtyre mjeteve ose përpjekjeve për ta marrë paisjen apo kodin nga një person i tretë.

Kjo lloj sjelljeje e paligjshme nuk duhet të interpretohet në një kuptim ngushtësisht teknik, atë të kryerjes së veprimeve mbi një kompjuter apo nëpërmjet një kompjuteri me qëllim vënien në dispozicion (sigurimin) e mjeteve të aksesit, por në kuptimin funksional që përfshin çdo lloj mënyre tjetër nëpërmjet së cilës mund të arrihet të sigurohen këto mjete[80].

---

[77]Vendim Kuadër 2005/222/JHA, dt. 24 shkurt 2005 "*Mbi sulmet ndaj sistemeve të informacionit*".

[78] Neni 10, pika 2 i Vendimit Kuadër 2005/222/JHA.

[79] Neni 10, pika 4 i Vendimit Kuadër 2005/222/JHA.

[80] Antolisei, F. (1994). "*Diritto Penale, parte speciale",* Milano: Giuffre, pg. 80-82.

Mënyra të tjera mund të jenë marrja dijeni nëpërmjet dokumenteve në letër në të cilat janë pasqyruar të dhënat, duke marrë nëpërmjet mashtrimit të dhënat e thëna verbalisht, ose duke vëzhguar proçesin e të shkruarit të tyre në tastierë nga personi i autorizuar[81]. Për sa i përket prodhimit të mjeteve të aksesit, vepra mund të konsiderohet e kryer në të gjitha ato forma që janë të përshtatshme për të siguruar një ose më shumë kopje të këtyre mjeteve.

2.2. Qëndrimi i paautorizuar në një sistem kompjuterik

Këtu është fjala për ato raste kur hyrja në sistem ka ndodhur në mënyrë të rregullt apo aksidentale, por gjithmonë pa cënuar masat e sigurisë dhe më pas qëndrimi i mëtejshëm në sistem kryhet kundër vullnetit të shprehur ose të heshtur të subjektit që ka të drejtën të refuzojë veprimin.

Do të ishim përpara një situate të tillë p.sh. kur hyrja në sistemin kompjuterik ka ndodhur si rezultat i një gabimi në shkrimin e adresës së një faqeje në internet apo kur një person vendoset në mënyrë të rastësishme në mes të një komunikimi të zhvilluar midis personave të tretë. Në këto situata, subjekti duhet të gjejë mënyrën për të dalë nga sistemi apo nga komunikimi që nga momenti që ai konstaton se bëhet fjalë për një sistem apo komunikim tëmbyllur, në të cilin ai nuk është i autorizuar për të qenë i pranishëm. Pas këtij momenti, qëndrimi i mëtejshëm në sistem do të konsiderohet si qëndrim i paautorizuar. Sigurisht që edhe këtu vlen të theksohet se të tilla veprime do të përmbanin rrezikshmëri shoqërore për sa kohë që sistemi në të cilin qëndrohet është i mbrojtur nga masa të veçanta sigurie sepse vetëm në këtë rast shfaqet rreziku i përhapjes së mundshme të të dhënave që përmbahen në sistem apo kryerjes së operacioneve të caktuara të cilat i lejohen vetem përdoruesit të ligjshëm.

Parashikimi i veçantë në ligj i rasteve të tilla do të paraqiste rëndësi edhe në ato situata kur personi i autorizuar për të hyrë në një pjesë të sistemit kompjuterik në mënyrë të rastësishme ose për shkak të mosfunksionimit të masave të veçanta të sigurisë të pjesëve të veçanta të sistemit, arrin të hyjë në këto pjesë tëtjera, ku nuk është i autorizuar të hyjë.

[81]Parodi C. (1998). "*La tutela penale dei sistemi informatici e telematici: le fattispecie penali",* in Relazione presentata al Convegno Nazionale su "Informatica e riservatezza" del CNUCE, Pisa. I aksesueshëm në faqen www.privacy.it/cpisaparod.html.

Ndërkohë që ligjvënësi shqiptar në nenin 192/b nuk parashikohen si të dënueshme rastet e qëndrimit në mënyrë të paautorizuar në një sistem kompjuterik të mbrojtur. Në këtë rast, neni 192/b nuk do të mund të zbatohej duke qenë se për të hyrë në mënyrë të paautorizuar në pjesët e tjera të sistemit punonjësi nuk ka cënuar ndonjë masë sigurie dhe si rrjedhim situata të tilla mbeten ende të pambuluara në ligjin penal.

Gjithashtu, vlen të përmendet se dispozita e Kodit Penal shqiptar mbi hyrjen e paautorizuar kompjuterike, në kushtet e formulimit aktual, nuk do të gjente zbatim në rastin kur personi i autorizuar për të hyrë në mënyrë të përkohshme në sistem për kryerjen e një veprimi të caktuar, të kërkuar nga zotëruesi i sistemit, vazhdon të qëndrojë brenda tij edhe pasi ka përfunduar veprimin dhe qëndrimi i mëtejshëm në sistem nuk është i nevojshëm. Si p.sh. kur një tekniku i kërkohet që të hyjë në sistem për zgjidhjen e një problemi të caktuar apo një programuesi kompjuterik i autorizohet hyrja në sistem me qëllim instalimin e një programi të ri. Në situata të tilla, mund të themi se jemi përpara qëndrimit në mënyrë të paautorizuar nga momenti që subjekti vazhdon të qëndrojë në brendësi të sistemit edhe pse ka përfunduar kryerjen e veprimit të ngarkuar ndaj tij.

Së fundmi, në një perspektivë krahasuese, përmendim faktin se në kodin penal italian sjellje të tilla mbulohen nga vepra penale mbi *'hyrjen e paautorizuar në një sistem kompjuterik ose telematik'*. Përgjegjësia penale për këtë vepër aplikohet *ndaj cilitdo që hyn në mënyrë abuzive në një sistem kompjuterik ose telematik të mbrojtur nga masa sigurie ose qëndron në të kundër vullnetit të shprehur apo të heshur të subjektit që ka të drejtën e përjashtimit nga qëndrimi*[82].

Me shprehjen *'vullnet i heshur jo miratues'* nga ana e titullarit të sistemit do të kuptohen të gjitha ato raste kur nga tërësia e rrethanave është e kuptueshme që veprimi në fjalë nuk ka qenë i autorizuar për t'u kryer. Si p.sh. kur një punonjës, i cili, për shkak të detyrës ka akses vetëm në një pjesë të sistemit kompjuterik, hyn edhe në pjesë të tjera, hapja dhe përdorimi i të cilave nuk lidhen me detyrën e ushtruar prej tij, atëherë edhe nëse këto pjesë të veçanta të sistemit nuk janë të mbrojtura nga masa specifike sigurie, është e kuptueshme që ekziston një vullnet i heshtur i titullarit për refuzimin veprimeve që mund të rezultojë qartë edhe nga detyrimi i punëmarrësit për t'iu përmbajtur vetëm atyre veprimeve

[82] Neni 615 *ter*, i Kodit Penal Italian.

që lidhen me detyrën e tij në punë dhe për të mos u përfshirë në veprime të tjera që tejkalojnë kufijtë e detyrës së tij. Si përfundim, themi që vepra konsiderohet e kryer në të gjitha rastet e hyrjes apo qëndrimit me dashje në memorien e brëndshme të kompjuterit, pa miratimin e zotëruesit të ligjshëm të tij dhe me vetëdijen që ky i fundit ka zbatuar masa të caktuara sigurie për të dhënat e ruajtura në memorie.

2.3. Përdorimi i pajisjeve memorizuese të tastierës

Një çështje që paraqet hapësirë për diskutim ka të bëjë me mënyrën se si do të cilësohen rastet e përdorimit abuziv të pajisjeve memorizuese të tastierës. Memorizuesi i tastierës (*keylogger*) është një program apo pjesë fizike kompjuterike që përdoret për të monitoruar dhe regjistruar cilindo prej tasteve që një përdorues shtyp në tastierën e kompjuterit të tij personal. Personi i cili ka instaluar programin apo pajisjen në fjalë mundet në këtë mënyrë të monitorojë të gjitha tastet e përdorura nga përdoruesi i kompjuterit dhe si rrjedhim mund të gjejë lehtësisht fjalëkalime ose informacione të tjera me natyrë konfidenciale[83].

Në rastin kur këto pajisje janë instaluar dhe përdorur në mënyrë të suksesshme në një sistem kompjuterik atëherë mund të themi se nëpërmjet tyre është arritur të realizohet një hyrje abuzive në sistem. Megjithatë duke iu referuar legjislacionit shqiptar,kujtojmë se në mënyrë që të kemi një hyrje të paautorizuar kompjuterike në kuptim të nenit 192/b duhet që hyrja të jetë realizuar nëpërmjet cënimit të masave të sigurisë.

Në rastin në fjalë, mekanizmi nëpërmjet të cilit kryhen veprimet që mundësojnë hyrjen në sistem kompjuterik është i tillë që nuk shoqërohet me cënim të masave të sigurisë pasi bëhet fjalë për një ndërhyrje më pak të avancuar, e cila kufizohet thjesht në memorizimin e funksioneve të tastierës së përdorur nga subjektet që përdorin rregullisht sistemin. Cënimi i masave të sigurisë ndodh në një fazë të mëvonshme, kur pasi këto pajisje janë vënë në funksionim dhe është mbledhur informacioni konfidencial i synuar, fjalëkalimet e sigurura janë përdorur për të realizuar hyrjen e suksesshmenë memorien e brendshme të kompjuterit.

[83]Poonia, A.S., Bhardwaj, A. dhe Dangayach, G.S. (2011). *Cyber Crime: Practices and Policies for its Prevention.* The First International Conference on Interdisciplinary Research and Development, Tajlandë.pp.22.

Në këto kushte do të ishte e vështirë që veprimet e përdorimit abuziv të pajisjeve (*keylogger*) dhe të memorizimit të serisë së tasteve të shtypura nga përdoruesi i kompjuterit të cilësoheshin si hyrje e paautorizuar kompjuterike. Në situatën aktuale duket se veprimet bien në hapësirën e veprimit të nenit 293/ç që parashikon veprën penale të keqpërdorimit të pajisjeve edhe pse duhet theksuar se kjo dispozitë është projektuar për të parandaluar apo ndëshkuar një fazë përgatitore dhe më pak të avancuar të veprimeve kriminale në fushën kompjuterike.

Nga ana tjetër theksojmë që është e qartë se veprimet e mbajtjes apo vënies në dispozicion të këtyre programeve do të cilësohen sipas nenit 293/ç pasi kemi të bëjmë thjesht me sigurim mjetesh që shërbejnë për sigurimin e një fjalëkalimi me qëllimin final kryerjen e veprës penale të hyrjes të paautorizuar në kompjuterin e një personi, kompanie private apo enti publik. Pra, veprimet në fjalë, janë veprime të mirëfillta përgatitore dhe si të tilla, nuk shoqërohen nga marrja e ndonjë veprimi të drejtëpërdrejtë për të realizuar në mënyrë konkrete hyrjen e paautorizuar në një sistem kompjuterik të caktuar.

2.4. Ndërhyrja në të dhënat dhe sistemet kompjuterike

Në realitetin e sotëm të shoqërisë së informacionit, ku një pjesë e mirë e të dhënave ruhen ose përpunohen në trajtë dixhitale është shumë e rëndësishme që të merren masat e nevojshme ligjore dhe operative për mbrojtjen e integritetit dhe vërtetësisë së këtyre të dhënave. Ndërhyrja në të dhënat kompjuterike mund të realizohet nëpërmjet fshirjes së të dhënave kompjuterike që është ekuivalente me shkatërrimin që mund të kryhet ndaj objekteve që kanë një ekzistencë materiale, *Suprimimit* që nënkupton çdo veprim që ndalon ose i jep fund disponueshmërisë ndaj të dhënave për subjektin i cili ka të drejtë aksesi në kompjuterin ose mbajtësin e të dhënave në të cilin ato janë ruajtur.

Instalimi i programeve të dëmshme si viruset ose *Trojan-horset* do të cilësohet sipas kësaj forme të ndërhyrjes në të dhënat kompjuterike duke qenë se çon në një modifikim të të dhënave. Megjithatë duhen dalluar format e ndërhyrjeve të paligjshme nga veprimet e kryera normalisht për projektimin ose funksionimin e rrjeteve të komunikimit si p.sh vënia në provë ose mbrojtja e sigurisë së një sistemi kompjuterik të autorizuara nga pronari ose operatori i tij, ose rikonfigurimi i sistemit operativ të kompjuterit që kryhet në rastet kur operatori i sistemit siguron një program kompjuterik të ri.

Modifikimi i të dhënave të trafikut të komunikimit me qëllim lehtësimin e komunikimeve anonime (si p.sh aktivitetet e sistemeve anonime remailer) në parim duhet të konsiderohen si veprime legjitime për mbrojtjen e privatësisë së komunikimeve dhe si rrjedhim të cilësohen si veprime të autorizuara. Megjithatë, në raportin shpjegues të "Konventës mbi Krimin Kibernetik" shpjegohet qartë se shtetet palë mund të shfaqin vullnetin për të kriminalizuar abuzime të caktuara të lidhura me komunikimet anonime, si psh. kur paketa me të dhënat e kokës së email janë modifikuar me qëllim fshehjen e identitetit të autorit të një vepre penale.

Krahas ndërhyrjes në të dhënat kompjuterike një figurë tjetër penale është dhe ndërhyrja në sistemet kompjuterikee njohur ndryshe si sabotazhi kompjuterik. Termi *sabotazh kompjuterik* përdoret për të treguar të gjitha veprimet e paligjshme të përdorimit të kompjuterave dhe rrjeteve të komunikimit si mjete për realizimin e qëllimeve kriminale. Këtu bëhet fjalë për veprimtari që synojnë të nxjerrin jashtë funksionimit apo të manipulojnë sistemet e komandimit, kontrollit dhe të komunikimit, të cilat përbëjnë objekt sulmi, në saj të përdorimit në mënyrë të përqëndruar të ndërveprimit të një numri të madh kompjuterash të vënë nën kontroll në mënyrë të paligjshme nga ana e keqbërësve.

Praktikat e sabotazhit kompjuterik njihen ndryshe edhe me termin *cyberwar*, që do të thotë luftë kompjuterike. Dërgimi i mesazheve email të padëshiruara (spamming), për qëllime tregtare ose jo, shihet si një aktivitet i cili mund të dënohet në bazë të kësaj dispozite vetëm nëse aftësia për të komunikuar pengohet në mënyrë serioze dhe të qëllimshme, si rezultat i dërgimit të mesazheve *spam* në sasi të madhe dhe me shpeshtësi të lartë[84].

Sanksionimi i kësaj vepre merr në mbrojtje interesin e ligjshëm të operatorëve dhe përdoruesve të sistemeve kompjuterike dhe të telekomunikacionit për të mundësuar funksionimin e tyre në mënyrën e duhur.Për efekt cilësimi juridik të veprës, kërkohet që pengesat e krijuara të jenë serioze. Interpretimi i shprehjes mund të bëhet duke marrë për bazë orientimin e dhënë nga hartuesit e Konventës sipas të cilëve, "*do të konsiderohet si krijim i pengesës serioze, dërgimi i të dhënave në drejtim të një sistemi të veçantë kompjuterik në një mënyrë, përmasa dhe shpeshtësi të tillë që sjell një efekt dëmtues të*

[84]Koment nr. 69 i Konventës "*Mbi Krimin Kibernetik*".

konsiderueshëm në aftësinë e zotëruesit ose operatorit të sistemit për të përdorur sistemin ose për të komunikuar me sisteme të tjera"[85].

Në terma të përgjithshëm mund të themi se me sistem kompjuterik do të kuptohet kombinimi i një tërësie aparaturash që bën të mundur transmetimin në distancë të të dhënave dhe informacioneve, nëpërmjet përdorimit të teknologjive të komunikimit[86].

Ndër formate ndërhyrjeve në sistemet kompjuterike mund të përfshihen praktika të tilla si:

a. përdorimi i programeve që bëjnë të mundur veprimin e sulmeve të refuzimit të shërbimit (denial of service attacks) .
b. instalimi i kodeve dëmtuese siç mund të jenë viruset të cilat ndalojnë ose ngadalësojnë në mënyrë domethënëse funksionimin e sistemit.
c. zbatimi i programeve të cilat dërgojnë sasi shumë të mëdha e-mailesh ndaj një marrësi të caktuar në mënyrë që të bllokojnë funksionet komunikuese të sistemit të përdorur prej tij.

2.5. Vjedhja e identitetit dhe impersonifikimi online

Vjedhja e identitetit është përkufizuar si mbajtja, transferimi i paligjshëm ose keqpërdorimi i informacionit personal me qëllim kryerjen e një krimi tjetër. Identiteti në botën virtuale mund të kuptohet si një maskë që i korrespondon një subjekti të caktuar në jetën reale. I njëjti person mund të ketë maska të ndryshme në botën virtuale, që janë identitetet e ndryshme me të cilat ai paraqitet dhe nga ana tjetër nën të njëjtën maskë (identitet virtual) mund të fshihen persona të ndryshëm, të cilët paraqesin të dhëna të njëjta identifikimi.

Përpjekja për të dhënë një përkufizim për konceptin e identitetit është një sipërmarrje pothuajse e pamundur duke pasur parasysh kompleksitetin dhe evoluimin e vazhdueshëm të kësaj çështjeje. Aplikacionet e reja teknologjike të bazuara në krijimin e profileve virtuale mund të ndikojnë në ndryshimin në mënyrë radikale të konceptit të identitetit duke ekspozuar disa nga anët e fshehura të jetës së një personi duke analizuar gjurmët dixhitale

[85]Koment nr. 67 i Konventës "Mbi Krimin Kibernetik".

[86]Calice A. (2006), "*I computer crimes nell'ordinamento giuridico italiano: inquadramento sistematico ed efficacia della risposta sanzionatoria"*, kursi 'Criminalità informatica e protocolli investigativi, Romë, fq.24, sikurse është cituar nga Scognamilio P. (2008), "*Criminalita informatica: Commento organico alla legge 18 marzo 2008, n.48",* Napoli: Botimet Simone, fq. 20.

që njerëzit lënë gjatë veprimeve që kryejnë, ose duke shfrytëzuar apo grupuar bashkë përmbajtjen e bazave të mëdha të të dhënave[87]. Në shoqërinë dixhitale, dhe në veçanti në rrjetet sociale (të cilat aplikojnë vizionin e të konsideruarit të internetit si një hapësirë sociale e cila inkurajon dhe mbështet pjesëmarrjen e individëve), vihet në dispozicion një masë shumë e madhe informacioni me natyrë personale. Njerëzit mund të përshkruajnë në mënyrë të detajuar identitetin e tyre duke përdorur profile që mundësohen nga shërbimet e rrjeteve sociale[88]. Identitetet në mjediset virtuale janë komplekse dhe përfshijnë si identitetet personale (të vërteta ose fiktive) që administrohen nëpërmjet sistemeve të menaxhimit të identitetit dixhital ashtu edhe ato që krijohen në sajë materialeve të deklaruara nga vetë njerëzit kur ata krijojnë një profil. Të dyja këto këndvështrime duhet të shihen si plotësuese të njëra-tjetrës në kuptimin që të marra së bashku, ato japin kuptimin e plotë të asaj çka do të konsiderohet identitet i personit. Në studimin e konceptit të identitetit nga pikëpamja strukturore merr rëndësi kuptimi i tipareve të një personi si dhe shpalosja e këtyre tipareve në kontekste të ndryshme. Kështu, termi identitet përdoret për t'iu referuar një grupi veçorish (të përhershme ose të përkohshme) të cilat përshkruajnë karakteristikat e individit në kontekstin e aktiviteteve të ndryshme praktike në të cilat ai përfshihet. Ndërkohë në kuptimin proçedural, rëndësi thelbësore për përcaktimin e identitetit marrin elementët që mund të përdoren për të identifikuar një person, siç mund të jenë emri i personit, një fjalëkalim i caktuar etj. Ky lloj identiteti mund të përdoret për të siguruar akses një sistem të caktuar informacioni ose bazë të dhënash ashtu sikurse dhe për të siguruar të drejtën për të përmbushur një transaksion të caktuar në rrugë elektronike[89]. Faqet e rrjeteve sociale janë shndërruar tashmë në një pjesë integrale të ndërveprimit të përditshëm social. Zhvillimi i vrullshëm i këtyre metodave të shoqërizimit online është shoqëruar edhe me shfaqjen e fenomenit të përvetësimit online të identitetit të një personi tjetër[90].

[87]Anrig, B., Benoist, E., etj. (2006), "*Virtual Persons Applied to Authorization, Individual Authentication and Identification*. *At Identity in a Networked Society"*. FIDIS consortium, pp.6.

[88]Nabeth, T. Identity of Identity. Në Rannenberg, K., Royer, D., & Deuker, A. (2009), "*The Future of Identity in the Information Society. Challenges and Opportunities"*. Berlin, pp. 21-22.

[89]*Po aty*. pp. 36.

[90]Kjo praktikë është e njohur gjerësisht me termin online impersonation.

Vjedhja e identitetit të një personi në rrjete sociale mund të kryhet nëpërmjet dy mënyrave të ndryshme:

(i) duke vjedhur të dhënat identifikuese të llogarisë së tij në rrjetin social (adresën e emailit dhe fjalëkalimin);

(ii) duke krijuar një profil të ri me të dhëna tërësisht të rreme dhe duke u shtirur si një person tjetër[91].

Në këtë kontekst, kur flasim për vjedhje të identitetit virtual i referohemi më tepër veprimeve të huazimit të paligjshëm të identitetit në kuptimin procedural, ndërsa kur rastet e përvetësimit të një identiteti fiktiv virtual lidhen me kuptimin strukturor të identitetit, veprimet e paligjshme të përvetësimit të një identiteti fiktiv virtual nuk identifikohen me konceptin e '*vjedhjes së identitetit'* (identity theft).

Termi '*vjedhje e identitetit*' ka gjetur përhapje të gjerë në praktikën juridike amerikane dhe i referohet një prej formave të konsumimit të veprës penale të mashtrimit kompjuterik. Konkretisht, sipas kësaj përqasjeje vjedhja e identitetit konsiston në vjedhjen e të dhënave të tilla personale si: emri, numri i sigurimeve shoqërore, datëlindja, numri i një llogarie bankare, numri i identifikimit personal, numri i telefonit mobile etj.

Përfitimi ekonomik që mund të nxirret nga sigurimi i këtyre informacioneve mund të konsistojë në kryerjen e transaksioneve financiare njësoj si zotëruesi i ligjshëm i të dhënave, blerjen e sendeve apo shërbimeve, të cilat përballohen nga të ardhurat e personit, të cilit i është vjedhur informacioni identifikues, etj. Kjo formë e veprimtarisë së paligjshme, ndëshkohet sipas Kodit Penal shqiptar në bazë të nenit 143/b që trajton veprën penale të mashtrimit kompjuterik të cilën do ta analizojmë në kapitujt në vijim[92].

Për ndëshkimin e veprimeve të impersonifikimit online, nuk duhet të jetë e nevojshme që të vërtetohet se identieti i rremë i krijuar lidhet me profilin online apo me të dhënat identifikuese të një personi të vërtetë[93]. Kështu, është plotësisht e mundur që profili i rremë

[91]Reznik M. (2013), "*Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation",* Touro Law Review. Vol 29 (2), pp. 455-483.

[92]*Mashtrimi kompjuterik* -(neni 143/b).

[93]Për më shumë lidhur me këtë diskutim shiko: Bernal, P. (2014), "*Internet Privacy Rights: Rights to Protect Autonomy"*. New York: Cambridge University Press. pp. 255-256.

i krijuar të mos bazohet në të dhënat që karakterizojnë një përdorues të ligjshëm, e megjithatë, veprimi mbart ende rrezikshmëri shoqërore. Kjo mund të ndodhë kur krijuesi i profilit të rremë e përdor atë për arritjen e qëllimeve të paligjshme sikurse mund të jetë: shoqërizimi online me të mitur për t'i joshur ata drejt përfshirjes në veprime me natyrë seksuale, shpërndarja e materialeve me përmbajtje të paligjshme, dërgimi i mesazheve me përmbajtje kërcënuese ose ngacmuese ndaj përdoruesve të tjerë etj. Për këtë arsye, interesi që mbrohet në sajë të ndëshkimit të veprimeve të impersonifikimit online, nuk duhet të lidhet gjithmonë me faktin që këto veprime bazohen në kopjimin e identitetit të një personi real.Interesi i çdo personi për mbrojtjen e imazhit dhe reputacionit të tij është një nga interesat që preken shpesh nga praktikat e ndërtimit të profileve të rreme online, megjithatë, nuk është i vetmi interes që mund të cënohet nga këto praktika. Interesat e tjerë që mund të cënohen dhe që rrjedhimisht kërkojnë mbrojtje të veçantë, përfshijnë: mbrojtjen e të miturve nga praktikat e joshjes online prej personave të rritur që krijojnë profile të rreme, mbrojtjen e të drejtës të sigurisë personale ose të dinjitetit në rastet kur nëpërmjet profileve të rreme dërgohen respektivisht mesazhe me natyrë kërcënuese ose ofenduese. Si një nga rastet me pasoja tepër të rënda të krijimit të profileve të rreme në rrjetet sociale mund të përmendim rastin Shtetet e Bashkuara kundër Drew në Kaliforni[94].

Në rastin në fjalë, e pandehura Lori Drew së bashku me disa ndihmës të tjerë krijuan një profil të rremë në rrjetin social "My Space" në të cilin paraqitej një djalë me emrin Josh Evans. Më pas ata kontaktuan me Megan Meier një vajzë 14 vjeçare nëpërmjet rrjetit social, duke përdorur pseudonimin Josh Evans dhe filluan të shkëmbejnë mesazhe afeksioni me të për disa ditë me rradhë. Në një nga komunikimet e fundit që ata i dërguan vajzës nën emrin fiktiv virtual të "Josh" thuhej se: "*ai nuk e pëlqente më Meganin dhe se bota do të ishte një vend më i mirë nëse ajo nuk do të bënte pjesë në të".*Shumë pak kohë pas kësaj ngjarjeje Megan kreu vetëvrasje. Në Shtetet e Bashkuara të Amerikës vetëm një numër i vogël shtetesh kanë parashikuar në ligjet e tyre penale veprën penale të personifikimit fiktiv në internet. Këto shtete janë New Yorku, Texasi dhe Kalifornia[95].

[94]United States v. Drew, 259 F.R.D. 449, 458 (C.D. Cal. 2009).

[95]Reznik M. (2013), " *Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation. Touro Law Review"*. Vol 29 (2), pp. 455-483.

Në Kodin Penal të shtetit të NewYork-ut ka një dispozitë të veçantë që trajton rastin e prezantimit mashtrues të një personi. Në këtë dispozitë, krahas dënimit të rasteve kur përvetësimi i identitetit të një personi tjetër kryhet për qëllim përfitimi material apo për t'u shtirur si një person mbajtës i cilësive të caktuara ose nënpunës publik, dënohen edhe praktikat e prezantimit fiktiv me identitetin e një personi tjetër në internet. Konkretisht, thuhet se: *"një person është fajtor për kryerjen e veprës penale të prezantimit të rremë… kur ai… hiqet si një person tjetër real nëpërmjet komunikimeve në një faqe interneti ose me anë të mjeteve elektronike me qëllim realizimin e një përfitimi ose për të dëmtuar apo mashtruar personin tjetër, ose kur nëpërmjet komunikimeve të tilla prezantohet si një nënpunës publik në mënyrë që të bindë të tretët t'i nënshtrohen këtij autoriteti ose të veprojnë në përputhje me kerkesën e bërë prej tij"*[96].

Një tjetër shtet amerikan që e ka njohur praktikën e prezantimit mashtrues të një personi si një person tjetër në rrugë elektronike është edhe Kalifornia. Kështu, përveç ndëshkimit penal të rasteve kur prezantimi i rremë kryhet në botën fizike me qëllim mashtrimin apo dëmtimin e të tretëve, kjo sjellje dënohet edhe kur kryhet në mjedisin dixhital. Në nenin 528/5 të Kodit Penal të Kalifornisë thuhet se: *"çdo person, i cili me dijeni prezantohet në mënyrë mashtruese si një person tjetër real nëpërmjet një faqeje interneti ose mjeteve të tjera elektronike, pa pëlqimin e këtij të fundit, dhe me qëllim dëmtimin, frikësimin, kërcënimin, ose mashtrimin e personit tjetër është fajtor për kryerjen e një krimi".* Një pasqyrim më gjithëpërfshirës i kësaj praktike kriminale gjendet ne Kodin Penal të Teksasit. Kjo shpjegohet edhe me faktin se dispozita që parashikon veprën penale të përvetësimit të identitetit online është relativisht e re, pasi ajo është përfshirë në tekstin e Kodit Penal në vitin 2009. Në këtë mënyrë, hartuesit e saj kanë pasur mundësinë e studimit të zhvillimeve kriminale në këtë drejtim dhe t'i përgjigjen në mënyrë më të plotë dhe efikase të tilla praktikave. Në Seksionin 33. 07 të Kodit Penal të Teksasit jepet ky përkufizim i veprës penale të "përvetësimit të identitetit online" (*impersonifikimit online*):

a) Kryen vepër penale personi, i cili pa marrë miratimin e një personi tjetër dhe me qëllimin për të dëmtuar, mashtruar, frikësuar ose kërcënuar një person, përdor emrin ose personalitetin e një personi tjetër për të:

[96]Neni 190.25 (4) i Kodit Penal të shtetit të New York-ut.

(i) krijuar një faqe web-i në një rrjet social tregtar ose një faqe tjetër interneti;

(ii) për të postuar ose dërguar një ose më shumë mesazhe nëpërmjet një rrjeti social tregtar ose faqeje tjetër interneti, nëpërmjet një programi të postës elektronike apo të shkëmbimit të mesazheve në grup ose në mënyrë tjetër.

b) Kryen vepër penale personi, i cili dërgon mesazhe të postës elektronike, mesazhe të menjëhershme (instant message), mesazhe tekst ose një komunikim tjetër të ngjashëm që tregon emrin, adresën e domainit, numrin e telefonit, ose një të dhënë tjetër të informacionit indentifikues që i përket një personi tjetër: [97]

(i) pa pasur pëlqimin e personit tjetër;

(ii) me qëllimin për të dëmtuar ose mashtruar një person.

Në Kodin Penal shqiptar nuk ka ndonjë dispozitë të veçantë që të ndëshkojë rastet e krijimit të profileve të rreme në rrjete sociale apo përdorimit mashtrues të profilit të një personi tjetër, kur këto kryhen për një qëllim të caktuar të paligjshëm. Për sa i takon veprimeve të vjedhjes në mënyrë mashtruese të të dhënave të llogarisë së një personi në një rrjet social dhe përdorimit të tyre për të hyrë në këtë llogari, ato mund të dënohen në bazë të nenit 192/b, si hyrje e paautorizuar kompjuterike në një sistem kompjuterik apo në një pjesë të tij.

Megjithatë, edhe në këtë rast mbrojtja që mund të sigurohej kundrejt veprimeve në fjalë do të ishte e paplotë. Nëpërmjet kësaj dispozite, mund të dënohet thjesht hyrja e paautorizuar në llogarinë e profilit personal të përdoruesit në një rrjet social, por nuk dënohen aktivitete të mëtejshme të paligjshme që mund të kryhen nga autori pas përvetësimit të profilit të përdoruesit të ligjshëm, si psh. postimi i materialeve me natyrë ofenduese ose denigruese në drejtim të këtij të fundit. Në praktikën e deritanishme të organeve të ndjekjes penale, rastet e krijimit të profileve të rremë ose të vjedhjes se të dhënave të llogarisë në një rrjet social janë cilësuar si falsifikim kompjuterik.

[97] Me *informacion identifikues* do të kuptohet çdo informacion që në mënyrë të veçuar ose duke u bashkuar me informacione të tjera, e identifikon një person, ku përfshihen : a) emri dhe numri i sigurimeve shoqërore, datëlindja; b) të dhënat biometrike unike, si gjurmët e gishtërinjve, grafikët regjistrues të zërit, imazhe të retinës ose të irisit; c) numri unik i identifikimit elektronik, adresa etj; d) informacion identifikues i telekomunikimeve ose pajisjet e aksesit në to.

Falsifikimi kompjuterik, parashikohet si vepër penale në nenin 186/a të Kodit Penal. Në fakt, kjo dispozitë nuk mund adresojë plotësisht problemet e impersonifikimit online. Vepra penale e falsifikimit kompjuterik përfshihet në kreun III të Kodit Penal "Vepra kundër pasurisë dhe në sferën ekonomike", në seksionin VIII të tij të emërtuar "Falsifikimi i dokumenteve". Marëdhëniet juridike që merren në mbrojtje në mënyrë parësore nga kjo dispozitë janë marrëdhëniet e vendosura për mbajtjen dhe administrimin e rregullt të dokumenteve të administratës publike ose personave juridikë privatë, që ruhen në format elektronik, dixhital.

Ndërkohë, veprimet e paligjshme të impersonifikimit online prekin në radhë të parë interesa të mirëfillta private, që lidhen me mbrojtjen e të drejtës së imazhit dhe reputacionit të personit dhe mbrojtjen e privatësisë së tij nga çdo akses dhe përdorim i paautorizuar i të dhënave të tij personale.

Në këto kushte, mendojmë që zgjidhja më e mirë do të ishte përfshirja e një dispozite të re në Kodin Penal që të trajtojë çështjet e impersonifikimit online. Kjo dispozitë mund të vendosej në seksionin VIII "Vepra penale kundër moralit dhe dinjitetit", të Kreut II "Vepra penale kundër personit", dhe në mënyrë të veçantë krahas neneve 121-123 të Kodit Penal që mbrojnë të drejtën e individit për jetën private.

Si pikë referimi në këtë drejtim, mund të shërbente formulimi që ju bëhet këtyre veprimeve në Kodin Penal të Teksasit, i cili bën një mbulim të plotë të formave të ndryshme në të cilat mund të zhvillohet veprimtaria mashtruese e vjedhjes apo imitimit të identitetit virtual të një personi.

2.6. Ndërhyrjet që prekin integritetin e të dhënave dhe sistemeve kompjuterike

1. Phishing (Peshkimi)

Phishing është një formë kontakti virtual, në përpjekje për të marrë nëpërmjet mashtrimit informacion sensitive si fjalëkalime. Një lloj mashtrimi për tëvjedhur të dhëna të rëndësishme, si: numra të kartave të kreditit, fjalëkalime, të dhëna personale, skema mashtruese, me qëllim marrjen e të dhënave personale ose financiare.Nëpërmjet përdorimit të teknikave të phishing, përdoruesit e shërbimeve të postës elektronike apo frekuentuesit e rrjeteve sociale mund të orientohen në mënyrë mashtruese që të bëjnë identifikimin (log in) në një faqe web të caktuar, e cila është projektuar në mënyrë të tillë që të duket si faqja

origjinale e kompanisë ofruese të shërbimeve në fjalë. Kështu faqet mashtruese të identifikimit të përdoruesve ngjasojnë në masë të madhe me faqet origjinale identifikuese të kompanive të tilla si Yahoo, Gmail, Facebook etj.

Duke qenë se përdoruesi mendon se faqja web në të cilën ka hyrë është faqja origjinale, ai shënon aty të dhënat identifikuese që janë emri i përdoruesit dhe fjalëkalimi. Në momentin që ai përpiqet të identifikohet (të bëjë log in) në faqen mashtruese me këto të dhëna, ato i kalojnë automatikisht keqbërësit që ka ndërtuar skemën mashtruese[98].

2. *E-mail spoofing. Dërgimi i emaileve të kopjuara*

Kjo praktikë përdoret në ato raste kur një haker ka arritur të sigurojë akses në adresën e e-mailit të një personi apo organizate dhe më pas i dërgon mesazhe email gjithë personave të tjerë që gjenden në listën e kontakteve në adresën e e-mailit të imituar. Këto mesazhe mund të ngjallin besim tek marrësi apo të nxisin kureshtjen e tij pasi sipas rastit mund të përmbajnë:

a) Një lidhje (*link*), e cila supozohet se është dërguar nga një prej kontakteve të postës elektronike. Kështu mesazhi i dërguar, ndërtohet në mënyrë të tillë, sikur vetë personi adresa e e-mailit të të cilit është hakuar i sugjeron marrësit të e-mailit që të kontrollojë lidhjen e dërguar. Për shkak të besimit që ka përdoruesi në adresën nga e cila i ka ardhur mesazhi si dhe për shkak të kuriozitetit mbi përmbajtjen e lidhjes së treguar ai klikon mbi të. Në fakt, në sajë të klikimit që i bën linkut, përdoruesi i hap rrugë aktivizimit të një programi të dëmshëm në kompjuterin e tij dhe në sajë të tij keqbërësi mund të fitojë kontroll mbi kompjuterin dhe të mbledhë informacione të ndryshme konfidenciale përfshirë edhe kontaktet e postës elektronike. Në këtë mënyrë, ai mund të vazhdojë të përdorë më tej taktikën e dërgimit të e-maileve të dëmshme në drejtim të viktimave të rradhës.[99]

b) Një material që kërkohet të shkarkohet si psh. piktura, muzikë, filma, dokumentare etj, të cilët përmbajnë të fshehur një program të dëmshëm. Edhe në këtë rast duke menduar se e-maili është dërguar nga një mik, përdoruesi ka shumë gjasa që ta shkarkojë materialin dhe

[98]Shiko: *How to hack facebook password.* në http://www.rafayhackingarticles.net/; si dhe Newman, R. C. (2010). "*Computer Security: Protecting Digital Resources".*Ontario CA:Jones and Bartlett Publishers, pp. 33.

[99]Criddle, L. "*What is Social Engineering".* Available at: http://www.webroot. com.

bashkë me të edhe programin që i mundëson keqbërësit të marrë kontroll mbi kompjuterin e tij dhe të monitorojë çdo veprim që kryhet nëpërmjet tij.

3. Përhapja e viruseve

Nje virus kompjuteri është program kompjuterik që infekton programet e tjera të kompjuterit duke i modifikuar ato në një mënyrë të tillë që përfshin dhe kopjimin e vetë virusit.Nga pikëpamja teknike, infektimi i kompjuterit nga viruset mund të kryhet në një shumëllojshmëri mënyrash. Megjithatë, mënyrat kryesore që përdoren zakonisht për përhapjen e viruseve janë:

a) ***Pranimi i opsioneve të caktuara pa lexuar përmbajtjen e tyre***

Një nga mënyrat më të shpeshta të infektimit të kompjuterit lidhet me pranimin nga ana e përdoruesit të opsioneve të caktuara që shfaqen në ekran pa i lexuar me kujdes apo pa e kuptuar përmbajtjen e veprimit që kërkohet të autorizohet prej tyre. Kjo mund të ndodhë psh. kur gjatë kërkimit në internet shfaqet një njoftim apo dritare ku thuhet se kompjuteri është infektuar ose që kërkohet instalimi i një mekanizmi shtesë (plug-in), dhe përdoruesi pa e kuptuar natyrën e veprimit që kërkohet të autorizohet prej tij, e pranon atë. Gjithashtu, gjatë instalimit ose azhornimit të një programi, përdoruesi pyetet nëse dëshiron që të instalojë edhe programe të tjera shtesë, të cilat në fakt, mund të përmbajnë edhe kode të dëmshme (viruse) të projektuara për të monitoruar veprimtarinë e përdoruesit gjatë përdorimit të programit.

b) ***Hapja e materialeve bashkëngjitur e-mailit***

Këtë praktikë e kemi shpjeguar edhe më sipër dhe lidhet me faktin që në shumë raste, për shkak të imitimit të adresave të e-mailit të kontakteve të njohura për përdoruesin, ai nuk ka dyshime mbi natyrën e rrezikshme të materialeve që i dërgohen nga adresa e supozuar e një kolegu pune, miku apo familjari të tij.

Në raste të tjera, mund të ndodhë që e-mailet që përmbajnë materiale të bashkëngjitura të dërgohen nga adresa e-mail krejtësisht të panjohura për përdoruesindhe megjithatë, ai i nisur nga kureshtja mund të shkarkojë materialin për të marrë dijeni mbi përmbajtjen e tij. Një veprim i tillë i pakujdesshëm mund të bëhet shkak për infektimin e kompjuterit me një virus që gjendet në materialin e shkarkuar[100].

[100]Këto emaile njihen ndryshme me emërtimin ‘Spam’.

c) *Shkarkimi i materialeve në mënyrë pirate*

Rreziku i infektimit nga viruset është kurdoherë i pranishëm edhe në rastet kur vizitohen faqe interneti, të cilat, ofrojnë mundësinë e shkarkimit në mënyrë pirate (falas) të filmave, këngëve, programeve komjuterike, librave etj. Kjo pasi në një pjesë të mirë të rasteve, materialet e shkarkuara përmbajnë viruse të ndryshme.

d) *Shkarkimi i programeve nga burime jo të sigurta*

Në rastin kur synon të shkarkojë një program kompjuterik të caktuar, përdoruesi duhet të jetë i vëmendshëm që burimi ngai i cili po shkarkon programin i përket një subjekti të besueshëm dhe të autorizuar për shpërndarjen e programit në fjalë. Shkarkimi i të njëjtit program, jo nga burimi origjinal mund të shoqërohet me instalimin e viruseve që mund të gjënden në të[101].

e) *Hapja e faqeve jo të sigurta të internetit*

Infektimi i kompjuterit me viruse mund të ndodhë edhe thjeshtë nëpërmjet hapjes së faqeve të internetit, të cilat nuk paraqiten të besueshme nga pikëpamja e parametrave të sigurisë. Në momentin që vizitohen faqe të tilla, mundet që të nisë një shkarkim automatik i kodeve të dëmshme në kompjuter. Në këtë drejtim është shumë e rëndësishme që kompjuteri të jetë i pajisur me mekanizma të lartë sigurie, pasi në një rast të tillë çdo përpjekje për shkarkimin automatik të të dhënave të ndryshme në kompjuter do të bllokohej nga programi përkatës i sigurisë.

2.7. DDoS (Distributed Denial of Service) - Sulmet e shpërndara për refuzimin e ofrimit të shërbimit

Denial of servis (DoS) që do të thotë (mohimi i shërbimit), është sulmi ndaj një sistemi kompjuterik mëmë tepër kërkesa nga sa mund të përballojë ky sistem. Kështu sistemi përmbytet dhe si pasojë nuk mund tu përgjigjet kërkesave të përdoruesve të rregullt duke e bërë të pamundur ofrimin e këtij shërbimi[102].

---

[101] *How does a computer get infected with a virus or spyware?*, Avaliable at: http://www.computerhope.com/issues/ch001045. htm.

[102] Poonia, A.S., Bhardwaj, A. dhe Dangayach, G.S. (2011), "*Cyber Crime: Practices and Policies for its Prevention".* The First International Conference on Interdisciplinary Research and Development,Tajlandë.

Sulmet e shpërndara për refuzimin e shërbimeve të ofruara në sajë të një rrjeti elektronik publik njihen shkurtimisht me termin DDoS (Distributed Denial of Service).

Mënyra e organizimit të sulmit nga ana e hakerave paraqitet si më poshtë:

a) Hakeri identifikon një numër të madh sistemesh që paraqesin dobësi (vulnerabël) në internet.

b) Më pas ai instalon programin DDoS të kontrollit në distancë, duke krijuar kështu të ashtuquajturat sisteme '*të nënshtruara'*

c) Hackeri kontrollon programet e kontrollit në distancë nëpërmjet një pajisjeje 'udhëzuese' e cila drejton sistemet e nënshtuara që të sulmojnë sistemin objekt sulmi.

d) Gjatë sulmit, paketa të mëdha informacionesh, që kanë të bëjnë me kërkesën për të vendosur një lidhje me serverin e sistemit të sulmuar, dërgohen prej rrjetit të kompjuterave të kontrolluar nga hakeri. Për shkak të fluksit të madh të paketave me informacion të dërguara, sistemi në fjalë ndeshet me një vërshim komunikimesh dhe si rrjedhim ai fiket ose refuzohet aksesi në të i përdoruesve të ligjshëm[103].

Efekti i një sulmi DDoS është i ngjashëm me rastin kur një person do të përdorte një sistem automatik të formimit të numrave telefonikë (automated dialing system) për të realizuar thirrje të vazhdueshme telefonike në drejtim të numrit telefonik të vënë në dispozicion psh. nga një biznes që ofron shërbime kateringu. Thirrjet automatike të bëra në mënyrë të vazhdueshme ndaj numrit të biznesit në fjalë, do të bllokonin linjën e tij telefonike dhe si rrjedhim, klientët do e kishin të pamundur që të bënin porosi nëpërmjet telefonit. Ndërkohë, gjatë realizimit të një sulmi DDoS, keqbërësi përdor një rrjet kompjuterash të kompromentuar, të njohur ndryshe si 'kompjutera fantazmë' për të dërguar një fluks të madh të dhënash ndaj komjuterit/sistemit që synohet të sulmohet. Kompjuterat 'fantazëm' janë kompjutera që janë vënë nën kontroll nëpërmjet programeve të veçanta (bots)- programe që në mënyrë mashtruese dhe shpesh edhe të fshehtë depërtojnë në kompjuterat e përdoruesve të ligjshëm. Botnet është një rrjet kompjuterash të infektuar nga maleare/viruse. Kompjuteri infektuar merr emrin "bot" pasi kontrollohet në distancë duke e shëndërruar në robot, i cili sulmon sisteme të tjera kompjuterike.

[103]Tanase, M. (2002).*"Barbarians at the Gate: An Introduction to Distributed Denial of Service Attacks."* URL: http://www.securityfocus.com/infocus/1647.

Përdoruesit e këtyre kompjuterave nuk janë në dijeni dhe nuk kanë kontrollin e kompjuterave të tyre. Hacking gabimisht përdoret në praktikë për të përshkruar çdo veprimtari kriminale me kompjuterat[104].

Në vijim, programet *boot* shndërrojnë kompjuterat e përdorur nga individët, bizneset, agjencitë qeveritare, institucionet arsimore etj, në kompjutera fantazëm, të cilët kryejnë funksionet e komanduara nga sulmuesi në sajë të intruksioneve që ai bën në distancë. Kompjuterat fantazëm integrohen në një rrjet të quajtur 'botnet', ndërkohë që personi, i cili kontrollon dhe përdor rrjetin e kompjuterave të kompromentuar njihet si 'bot herder'. Rrjeti më pas mund të përdoret për qëllime fitimprurëse duke e vënë në shërbim të kriminelëve kompjuterikë, të cilët, e përdorin këtë 'ushtri fantazëm dixhitale' për të fituar para nga mbyllja e faqeve Web, apo për të zhvatur para nga zotëruesit e ligjshëm të tyre, për të dërguar mesazhe e-mail spam, për të tërhequr përdoruesit drejt skemave të mashtrimit online, apo për të instaluar programe *adware* në kompjuterat e përdoruesve. Këto të fundit, janë programe që mundësojnë shfaqjen në mënyrë automatike të njoftimeve me natyrë promocionale me anë të të cilave, synohet të realizohet një përfitim nga ana e subjektit kontrollues të programit adware[105].

Një kompjuter mund të bëhet pre e manipulimit nga një program 'bot', nëpërmjet mënyrave të ndryshme si: nëpërmjet e-maileve që përmbjanë bashkëngjitur materiale të rrezikshme, apo që udhëzojnë përdoruesin të vizitojë një faqe të caktuar në Web, e cila më pas shfrytëzon pikat e dobëta të motorit të kërkimit të përdoruesit për të përhapur programe të dëmshme në kompjuterin e tij apo nëpërmjet shkarkimit të drejtëpërdrejtë nga Interneti të materialeve që përmbajnë të fshehura viruse të ndryshme. Komandat që mund të dërgojë sulmuesi nëpërmjet rrjetit të kompjuterave të manipuluar mund të konsistojnë në dërgimin e mesazheve spam, përhapjen e wormeve ose viruseve, përhapjen e mëtejshme të programit 'bot', kërkimin e kompjuterave për gjetjen e të dhënave private si fjalëkalime apo informacione financiare.

---

[104] www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37.

[105] Brenner, S. (2010), *"Cybercrime : Criminal Threats from Cyberspace"*. Santa Barbara: ABC-CLIO, pp. 41-42.

Aktiviteti kriminal që gjeneron nga përdorimi i *botneteve*, në praktikë, mund të konsistojë në një ndarje të qartë rolesh midis individëve të ndryshëm që përmbushin detyra të caktuara, të veçanta. Në këtë aktivitet mund të identifikohen disa procese të realizuara nga persona të ndryshëm: (1) shkruajtja/krijimi i programeve që përdoren për manipulimin e sistemeve kompjuterike; (2) infektimi i Web serverave popullorë dhe përdorimi i tyre për përhapjen e programeve të dëmshme; (3) grumbullimi i të gjithë kompjuterave të vënë nën kontroll në një ose disa rrjete; (4) përdorimi i kompjuterave të vënë nën kontroll për dërgimin e mesazheve të padëshiruara promocionale, mbledhjen e të dhënave personale; (5) shitjen e informacioneve të mbledhura kur ato kanë natyrë financiare; (6) përdorimi i informacioneve me natyrë financiare për të ndërmarrë veprime të mashtrimit me kartat e kreditit apo për të krijuar karta ATM-je të klonuara[106].

Llojet më të ndeshura të sulmeve DDoS janë:

1. Mbingarkesa e zonës memorizuese të të dhënave që përpunohen *- (Buffer Overflow Attacks*).

Në këtë rast sulmuesi përfiton nga mangësitë në shkruajtjen e kodeve, si psh. një program që nuk kontrollon madhësinë e të dhënave të vendosura në buffer[107]. Kështu, sulmuesi shkakton tejmbushjen e buffer-it duke ndryshuar vlerën e variablës së një programi në një numër më të madh nga ai i parashikuar dhe duke zbatuar një kod arbitrar në bazë të një llogarie përdoruesi të privilegjuar (*privileged user account)*.

Një praktikë e tillë ndodh kur në një program apo gjatë zbatimit të një procesi të caktuar nga ana e kompjuterit bëhen përpjekje për të ruajtur më shumë të dhëna nga sa është kapaciteti që mban programi apo procesi në fjalë. Në një vërshim të tillë, të dhënat që tejkalojnë limitin maksimal të përpunimit mund të përmbajnë kode të dëmshme të projektuara sipas rastit për të iniciuar në mënyrë arbitrare operacione të caktuara në kompjuterin e sulmuar, për të dëmtuar dosje të dhënash, apo për të zbuluar informacione me natyrë konfidenciale.

---

[106] McQuade, S. (2008). *Encyclopedia of Cybercrime*. Westport: Greenwood Press. pp.13.

[107]Termi 'Buffer' përdoret për të treguar një pjesë në memorien e shkurtër të sistemit kompjuterik, në të cilën ruhen të dhënat, gjatë kohës së përpunimit ose transmetimit. Avaliable at: http://www.oxforddictionaries.com/definition/english/buffer.

Duke qenë se madhësia e të dhënave tejkalon limitin maksimal përpunues që mund të mbajë programi apo procesi përkatës që zbatohet në kompjuterin e sulmuar, ato *'vërshojnë'* në pjesë të tjera të memories së kompjuterit, çka bën të mundur hyrjen në mënyrë të paautorizuar të hackerit në sistemin e brendshëm të kompjuterit[108].

2. Sulmet nëpërmjet paketave shumë të vogla të informacionit *(Teardrop attacks).*

Në mënyrë që paketat e mëdha të informacionit të transmetohen nëpërmjet një rrjeti komunikimi, shpesh është e nevojshme që ato të ndahen në fragmente më të vogla duke marrë për bazë njësinë maksimale të transmetimit që përballon rrjeti.

Shumë pajisje të sistemit operativ (të njohura si *kernel*) të prodhuara më parë, kontrollonin dhe refuzonin fragmente informacioni që kishin përmasa shumë të mëdha por nuk kontrollonin fragmentet me përmasa shumë të vogla, nën vlerën e njësisë minimale të transmetimit. Infiltruesit e paligjshëm shfrytëzonin këtë mangësi dhe ndërtonin paketa më të vogla se ato të pranueshmet, duke shkaktuar ristartimin e sistemit ose ndalimin e tij.

3. Sulmet e copëzuara (Smurf Attacks)

Fillimisht, një kompjuteri apo serveri i dërgohet një protokoll ICMP (Internet Control Message Protocol), i cili përdoret për të treguar nëse kompjuteri/serveri i caktuar është i lidhur me Internetin. Në momentin që kompjuterit i dërgohet ky protokoll, ai i dërgon në përgjigje një paketë të dhënash[109] personit që ka dërguar protokollin verifikues ICMP.

Mesazhi që përmbahet në paketë konfirmon faktin që kompjuteri në fjalë, është i lidhur me internetin. Në një sulm të copëzuar, hakeri ndryshon adresën të cilës duhet t'i shkojnë paketat e përgjigjes në mënyrë të tillë që këto të dhëna të mos shkojnë në drejtim të kompjuterit që ka kërkuar informacionin verifikues, por në drejtim të sistemit objekt sulmi[110]. Në sajë të kësaj metode, hakeri vë nën kontroll rrjete të ndryshme të ligjshme në internet dhe më pas bën që nga adresat e këtyre rrjeteve të shkojnë kërkesa në drejtim të sistemit kompjuterik objekt sulmi.

---

[108]Poonia, A.S., Bhardwaj, A. dhe Dangayach, G.S. (2011), "*Cyber Crime: Practices and Policies for its Prevention".* The First International Conference on Interdisciplinary Research and Development,Tajlandë.

[109]Kjo paketë të dhënash në gjuhën informatike njihet me termin Enhanced Computer-to-Human Output (ECHO) dhe i referohet mesazhit final të dërguar nga kompjuteri në drejtim të përdoruesit të kompjuterit.

[110]Gralla, P. (1998), "*How the Internet Works",* Indianapolis: Que Corporation, pp. 273.

Nga mbingarkesa me kërkesa për dhënie informacioni, ky sistem bllokohet duke mos ju përgjigjur dot kërkesave të përdoruesve të ligjshëm.

4. Mesazhet e keqformuara

Një sulmues kompjuterik mund të krijojë e më pas dërgojë mesazhe të keqformuara në drejtim të kompjuterit server të synuar me qëllim ndërprerjen e shërbimit të tij. Mesazhet e keqformuara janë mesazhe protokoll me sintaksë të gabuar. Kur serveri merr mesazhe të tilla, ai mund të ç'orientohet dhe të reagojë në mënyra të ndryshme si:

a) krijimi i spiraleve të pafundme të analizës gramatikore dhe kuptimit të mesazhit;

b) ndërprerje e funksionimit të pajisjes;

c) pamundësi për të përpunuar mesazhe të tjera normale;

d) ekzekutim i kodeve arbitrare nga ana e sulmuesit etj.

5. Mesazhet e rreme (spoofed messages)

Një sulmues mund të vendosë mesazhe të rreme (fiktive) në një seksion të caktuar të komunikimit me qëllim që të ndërpresë shërbimin ose të vendosë nën kontroll (vjedhë) seksionin. Shembujt tipikë në këtë drejtim janë:

a) Rënia e thirrjes (call teardown); b) Mashtrimi me tarifat.

Rënia e thirrjes – në këtë rast sulmuesi monitoron një dialog SIP që po zhvillohet dhe siguron të dhëna në lidhje me seksionin përkatës të komunikimit[111].

Më pas, ai dërgon mesazhe për përfundimin e thirrjes (si psh. SIP Bye) në drejtim të paisjes komunikuese ndërkohë që përdoruesit e saj janë duke biseduar. Pas marrjes së mesazhit mbyllës, pajisja do të mbyllë menjëherë seksionin përkatës të komunikimit.

2.8. Sulmet kundër konfidencialitetit të të dhënave

1. Përgjimi

Aktivitetet e paligjshme të përgjimit të të dhënave që kalojnë në ndërfaqen e një rrjeti kompjuterik njihen ndryshe me termin *sniffing*[112], ndërsa pajisjet e përdorura për këtë qëllim emërtohen *'sniffer'*.

[111]Kërksat njihen me termin SIP Register.

[112]Ndërfaqja e një rrjeti kompjuterik përfaqëson pikën e ndërlidhjes midis një kompjuteri dhe një rrjeti publik ose privat. http://docs.oracle.com/javase/tutorial/networking/nifs/definition.html.

Pajisjet përgjuese (*sniffer*) përfaqësojnë mjetet dixhitale analoge të paisjeve përgjuese që përdoren në fushën e telekomunikimeve. Ndërsa paisjet përgjuese janë mjete fizike që regjistrojnë transmetimet analoge të komunikimeve të kryera nëpërmjet linjave telefonike, pajisjet sniffer janë programe që lejojnë përdoruesin e tyre të vëzhgojë dhe regjistrojë paketat e të dhënave që përmban komunikimi midis personave i kryer nëpërmjet kompjuterave.

Ashtu sikurse pajisjet përgjuese të bisedave telefonike duhet të vendosen në një nga linjat që synohen të monitorohen në mënyrë që të funksionojnë, përgjimi elektronik mund të kryhet vetëm në një segment të rrjetit me fushë veprimi lokale (Local Area NetWork). Kështu, nuk është e mundur që të përgjohet trafiku që kalon në një sërë pikash të rrjetit, që ndodhen larg rrjetit objekt përgjimi[113].

Hackerat shfrytëzojnë këtë teknikë për të siguruar të dhëna sensitive siç mund të jenë fjalëkalime, adresa emaili ose dosje të ndryshme. Praktika e *sniffing (përgjimit)* mund të ndeshet në formën pasive ose aktive[114].

Snifferat (përgjuesit) pasivë presin kalimin e të dhënave në rrjet në mënyrë që të dhënat të mblidhen përpara se të arrijnë në destinacion. Ndërkohë, praktikat aktive të sniffing bazohen në përdorimin e teknikave të caktuara mashtruese, të cilat shkaktojnë rrjedhjen e të dhënave në rrjet për të bërë të mundur mbledhjen e mëtejshme të tyre nga ana e sulmuesit[115].

Pasi ka realizuar me sukses hyrjen në një kompjuter, hackeri mund të përdorë programe të posaçme të njohura me emërtimin *'rootkits',* me qëllim që të fshehë praninë e *fileve* të vendosura në kompjuter pas ndërhyrjes së paligjshme. Fjala *root* në gjuhën e zakoshme të hakerave përdoret për të treguar veprimin e sigurimit të të drejtave të administrimit në një sistem kompjuterik. Ndërsa fjala *kit* i referohet programeve që instalohen në mënyrë të paligjshme në kompjuterin e përdoruesit.

---

[113]Dittrich D., dhe Himma K.E. (2006), "*Hackers, Crackers and Computer Criminals"* ; në Bidgoli, H. *Handbook of Information Security: Information Warfare; Social, Legal, And International Issues; And Security Foundations"*, Vol. 2. Bakersfield: John Wiley & Sons, Inc., pp.157.

[114] *Po aty*.

[115]Ealy K. (2003), "*A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention"*. SANS Institute. pp. 12.

Metodat më të zakoshme të përdorura nga hakerat për vënien në kontroll të komunikimeve në një rrjet komunikimi elektronik janë dy: njëra konsiston në përgjimin e paketave të komunikimit të transmetuara në të njëjtën bandë trasmetimi sikurse përdoruesi i synuar, ndërsa tjetra, konsiston në përdorimin një pajisjeje manipuluese dhe dublikimin e bisedës edhe në pajisjen e kontrolluar nga hakeri.

Sipas mënyrës së parë, pajisja përgjuese që përdor hakerindodhet në të njëjtën zonë transmetimi me telefonin e përdoruesit A dhe mund të përgjojë të gjitha sinjalet dhe komunikimet që kalojnë përmes një nyje lidhëse (*hub*) të të gjithë trafikut të komunikimeve të realizuara në zonën përkatëse të komunikimit.

Hakeri mundet gjithashtu të sigurojë akses në pajisjen që bën lidhjen e mjetit komunikues me internetin, të konfigurojë një portë monitoruese për të gjitha komunikimet me zë që kryhen nëpërmjet një rrjeti lokal virtual,dhe të dublikojë më pas komunikimin në pajisjen e tij përgjuese.

Sipas mënyrës së dytë të përgjimit, hakeri vendos nën kontroll rrugën e komunikimit të përdorur nga një përdorues A. Kështu, nëse ai ka akses fizik në sinjalin përkatës, më pas e dërgon këtë sinjal në dy drejtime.

3. Llojet e autorëve të veprave penale në fushën e kibernetikës

Sikurse çdo formë tjetër e kriminalitetit dhe krimet në fushën e kibernetikës po shkaktojnë pasoja të rënda për individët dhe institucionet shtetërore. Nga të dhënat e statistikave vërehet se në kryerjen e këtyre veprave të krimeve kibernetike, marrin pjesë persona me aftësi të lartë intelektuale dhe profesionale.

Autori i këtyre krimeve mund të karakterizohet kryesisht si një person i ri, inteligjent, shumë i motivuar, punëtor i besueshëm, si një njeri që ka logjikë të fortë, i cili njeh mirë sistemin kompjuterik, mundësitë dhe mënyrën e shfrytëzimit të tij. Nisur nga motivet të cilat i nxisin dhe qëllimet të cilat dëshirojne të arrijnë me veprimet e tyre, autorët e veprave penale në fushën. e krimeve kibernetike, ndahen në amatore dhe kriminelë profesionistë[116].

[116]GORDON/FORD. (2006)*, "On the Definition and Classification of Cybercrime",* Journal in Computer Virology, Vol. 2, No. 1, pp. 13-20.

Në grupin e parë hyjnë personat të cilët ushtrojnë aftësi profesionale të ndryshme si juristë, ekonomistë, punëtorë administrate etj, që për shkaqe të ndryshme hyjnë në veprimtari ilegale. Kriminelët profesionistë janë persona të cilët kanë përvojë dhe njohuri të shumta,të cilët paraqesin rrezikshmëri të lartë shoqërore. Karakteristika themelore e tyre është se adaptohen në situata të reja, si rezultat i zhvillimit të teknologjisë. Grupi i tretë janë ata persona të magjepsur me teknologjinë e re informatike deri në atë masë sa çdo aspekt i jetës së tyre është i lidhur me kompjuterat. Ata posedojnë njohuri teknike të tilla që i çojnë në veprime kriminale dhe zgjedhin të sulmojnë sisteme të caktuara[117].

4. Format e kryerjes së krimeve kibernetike

Krimet kibernetike janë zhvilluar që kur teknologjia informatike ka filluar të zhvillohet në përmasa të gjëra dhe shumë mënyra të kryerjes së veprave penale janë ndryshuar dhe po vazhdojnë të ndryshohen. Në funksionimin eçdo sistemi kompjuterik ekzistojnë pesë faza të cilat paraqesin pika kritike për mbrojtje nga kriminaliteti kompjuterik të cilat janë: a). Hyrja; b). Dalja; c). Programimi; d). Përdorimi; e). Bartja.

a). Hyrja,faza kur futen të dhënat në kompjuter është çasti i kryerjes ku kryhen më shumë krime me një manipulim të njohur me emrin "përzjerje e të dhënave". Këto manipulime mund të kryhen në shumë mënyra si:

1. Plotësimi i të dhënave;Ndryshimi i të dhënave; Ndërrimi i të dhënave ekzistuese;
2. Fshirja e të dhënave ekzistuese.

b). Faza tjetër e veprimit kriminal është dalja. Kjo fazë ka formën e vjedhjes të të dhënave. Teknika që përdoret më së shumti është kopjimi i të dhënave të softwerit ose programeve. Këto vjedhje kryhen nga punëtorët e pandershëm, në bashkëpunim me një apo më shumë persona nga jashtë[118].

c). Veprat e kriminalitetit kompjuterik në fazën e programimit kanë të bëjnë me njërën nga këto forma:

---

[117]M. CHAWKI. (2005), *A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy*, DROIT-TIC.

[118]Schjolberg S. (2004), *Computer Related Offences.* A presentation at the Octopus Interface, Strasbourg 2004, available at www.coe.int.

(1) Ndërrimi i programeve; (2) Fshirja e instruksioneve të rëndësishme;

(3) Modifikimi i programeve; (4) Sabotazhi i programeve.

Nëse do ta krahasonim këtë fazë me atë të manipulimeve në hyrje del qartë se nevojiten më tepër njohuri specifike dhe profesionalitet më i lartë në aftësitë informatike dhe teknikat e përdorura.

d). Përdorimi, ka të bëjë me një numër të vogël të qëndrave kompjuterike të cilat kanë marrë masa mbrojtëse, me qëllim të pengimit të shfrytëzimit të paautorizuar të sistemit komjuterik nga ana e punonjësve në mënyrë të paautorizuar.

e). Mbartja është një prej niveleve më të ndjeshme të sistemit informatik për shkak se është shumë e vështirë të sigurohet mbrojtja fizike e lidhjeve të komunikimit[119].

5. Roli i faktorëve kriminogjen në krimet kibernetike dhe masat për parandalimin e tyre

5.1. Faktorët kriminogjen objektiv

Në kriminalitetin kompjuterik ashtu si në forma të tjera kriminalitetit, ndikojnë mjaft faktorë të caktuar kriminogjen objektiv. Faktorët objektiv së pari duhen kërkuar në specifikat e vetë teknologjisë informatike dhe shpejtësisë së zhvillimit të saj. Veçoritë që bëjnë dallimin midis kësaj forme të kriminalitetit dhe formave të tjera janë:

1. Krimet kibernetike , janë krime të një shoqërie të zhvilluar bashkëkohore që shkojnë paralel me shkallën e arritjes së zhvillimit ekonomik, sa më e lartë është shkalla e zhvillimit aq më të sofistikuara janë mënyrat e kryerjes.
2. Këto lloj krimesh ndeshen në mjediset urbane të cilat njëkohësisht janë të varura në jetën e përditshme nga përdorimi i teknologjisë informatike.
3. Krimet kibernetike janë globale si për nga përhapja ashtu edhe nga pasojat.
4. Duke qënë se nevojiten shkallë të mjaftueshme dijesh, që sa më e lartë të jetë ajo aq më e vështirë është të parandalohet autori i veprës, kuptojmë se ndeshet tek njerëzit e arsimuar.

[119]Gordon/Hosmer/Siedsma/Rebovich. (2003), "*Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime"*, available at*:* *www.ncjrs. gov/ pdffiles 1/nij /grants /198421 .pdf*. Regarding the number of the cases in early cybercrime investigations, see: Schjolberg. (1983), "*Computers and Penal Legislation, A study of the legal politics and a new technology",* pp 6, available at*:* www.cybercrimelaw.net /documents/ Strasbourg.pdf.

5. Krimet kibernetikejanë vështirë të luftohen dhe parandalohen, sepse edhe aplikimi i mjeteve me të sofistikuara,'nuk jep garanci për mbrojte të sigurtë.

5.2. Faktorët kriminogjen subjektiv

Përveç faktorëve kriminogjen objektiv, ekzistojnë dhe faktorët subjektiv të krimeve kibernetike të cilat janë:

1. Motivi për shkak të të cilit autori potencial i veprës penale do të ndërmarrë veprimin;
2. Gadishmëria e autorit të veprës që të pranoi rrezikun potencial;
3. Mundësia që veprimi kriminal të kryhet.

Për të saktësuar këto faktorë nevojitet një analizë e shkurtër e secilit, që do të trajtohet në vazhdim. Kur individët do të kryejnë një veprim kriminal është vërtetuar se rolin determinant në të e kanë motivet si faktorë psikologjik, të cilët nën ndikimin e rrethanave të jashtme apo të brendshme shtyjnë një person të caktuar të kryejë një vepër penale.

Motivet zakonisht janë nga më të ndryshmet, ku mund të përmendim: *motivet fmanciare, arsyet emocionale, konkurenca ekonomike, problemet mentale, motivet politike, qëndrimi personal, kodi etik, etj.*

Gadishmëria e individit që të futet në veprimtari kriminale është pasojë e pandershmërisë së tij. Kjo lidhet me karakterin e tij, që praktikisht është e pamundur të vërtetohet. Duke qënë se nuk ekziston ndonjë mbrojtje absolute e sistemit, mundësia e kryerjes së një krimi të tillë ekziston deri në një farë shkalle e cila ndryshon në varësi të ambjentit në të cilin shfrytëzohet teknologjia informatike[120].

[120]Armstrong Il. (2003), "*Real Risk or Shadow?The Threat of Cyberterrorism*". Articles and Features, available at: http://www.scmagazine.com.

KAPITULLI III: VËNDIMARRJA E BE NË LUFTËN KUNDËR KRIMIT KIBERNETIK NJË DEKADË E ZHVILLIMEVE LIGJORE EUROPIANE

1. Konventa e Budapestit "Mbi Krimet Kibernetike"

Për arsye të ndryshimeve të mëdha që lidhen me informatikën dhe shtrirjen botërore të këtyre rrjeteve dhe për arsye të shfaqjes së formave të reja të kriminalitetit (psh, në fushën e pedopornografisë), ka pasur një ndërgjegjësim ndërkombëtar me qëllim organizimin e luftës kundër këtyre formave të reja të kriminalitetit. Këshilli i Evropës ka miratuar disa rekomandime[121].

Duhet të përmendim gjithashtu edhe Rezolutën nr. 1 e miratuar nga Ministrat Evropianë të Drejtësisë gjatë konferencës së tyre të 21"™ në Pragë, në Qershor 1997, e cila i rekomandonte Komitetit të Ministrave të mbështeste aktivitetet nëlidhje me kiberkriminalitetin që organizohet nga Komiteti Evropian për problemet kriminale. Qëllimi është të përafrohen legjislacionet penale kombëtare dhe të bëhet i mundur përdorimi i mjeteve efikase të hetimit në fushën e veprave informatike. Së fundi, duhet të mbahet parasysh planveprimi i miratuar nga kryetarët e shteteve dhe të qeverive të Këshillit të Evropës me rastin e Samitit të tyre të dytë (Strasburg, tetot 1997), me qëllim që t'i jepeshin përgjigje të përbashkëta zhvillimit të teknologjive të reja të informacionit, bazuar në vlerat dhe normat e Këshillit të Evropës. Kështu, me 23 Nëntor 2001 në Budapest u nënshkrua "Konventa mbi Kiberkriminalitetin". Ky instrument është plotësuar nga një protokoll shtesë në lidhje me inkriminimin e akteve me natyrë raciste dhe ksenofobe duke përdorur sistemet informatike, i nënshkruar në Strasburg me 28 Janar 2003.

Me qëllim krijimin e një rregulloreje për parandalimin dhe luftimin e krimeve kibernetike, për respektimin e të drejtave të njeriut dhe mbrojtjen e të dhënave personale të tyre, shtetet anëtare të Këshillit të Evropës dhe shtetet e tjera nënshkruese duke konsideruar që qëllimi i

[121] *Rec.* nr. R (85) 10 mbizbatimin praktik te Konventes Evropiane te Ndihmes se Ndersjelle Gjyqesore ne lidhje me leterporosite me qellim mbikeqyq'en e telekomunikacionevc, nr. R (88) *2* per masar e luftes • kunder piraterise ne fushen e te drejtave te autorit, nr. R (87) 15 qe synon te rregulloje perdorimin e te dhe-nave me kar^krer personal ne sektorin e policise, *nr.* R (95) 4 mbi mbrojrjen e te dhenave me karakter per-sonal ne fushen e sherbimeve te telekomunikacionit, nr. 89) 9 mbi kriminalitetin ne lidhje me kompjuteret, nr. R (95) 13 ne lidhje me problemet e procedures penale qe lidhen me teknologjine e informaconit.

Këshillit të Evropës është që të arrihet një unitet sa më i madh ndërmjet anëtarëve të tij, duke njohur vlerën e nxitjes së bashkëpunimit me shtetet e tjera nëpërmjet nënshkrimit të Konventës së Budapestit (21 nentor 2001), bën të mundur ndjekjen në mënyrë prioritare të një politike të përbashkët penale që ka për qëllim mbrojtjen e shoqërisë nga krimi kibernetik,ndërmjet të tjerash adaptimin e një legjislacioni të përshtatshëm dhe nxitjen e një bashkëpunimi ndërkombëtar të ndërgjegjshëm për ndryshimet e thella të sjella nga dixhitalizimi, konvergjenca dhe globalizimi i vazhdueshëm i rrjeteve kompjuterike. Të shqetësuar nga rreziku që rrjetet kompjuterike dhe informacioni kompjuterik mund të përdoret gjithashtu për kryerjen e veprave penale dhe faktet e lidhura me këto vepra mund të memorizohen, të ruhen dhe të transferohen nëpërmjet këtyre mjeteve kërkojnë një bashkëpunim ndërkombëtar të gjerë, të shpejtë dhe efektiv në çështjet penale. Mirëpritja e zhvillimeve të fundit avancon më tej mirëkuptimin dhe bashkëpunimin ndërkombëtar në luftimin e krimit kibernetik, duke përfshirë veprimet e Kombeve të Bashkuara, të OECT-së, Bashkimit Europian dhe të G-8-ës.

Këto shtete, të bindura që konventa aktuale është e nevojshme për të frenuar veprimet e drejtuara kundër konfidencialitetit, integritetit dhe disponueshmërisë të sistemeve kompjuterike, rrjeteve dhe të dhënave kompjuterike, sikurse dhe keqpërdorimit të këtyre sistemeve, rrjeteve dhe të dhënave, nëpërmjet sigurimit që kjo veprimtari e tillë të kriminalizohet, sikurse përshkruhet në këtë konventë, dhe nëpërmjet krijimit të forcave të mjaftueshme për luftimin efektiv të këtyre veprave kriminale duke lehtësuar zbulimin, hetimin dhe ndjekjen penale të këtyre veprave penale në të dyja nivelet kombëtare dhe ndërkombëtare, dhe duke siguruar marrëveshjet për bashkëpunim ndërkombëtar të shpejtë dhe të besueshëm, kanë marrë në konsideratë:

1. Rekomandimin Nr. R (85) 10, që përmban aplikimin praktik të Konventës Evropiane mbi Asistencën e dyanshme në çështjet penale, në përputhje me letërporositë mbi interpretimin e telekomunikacioneve;
2. Rekomandimin Nr. R (88) 2 mbi piraterinë në aspektet e të drejtës së autorit dhe të drejtave të fqinjësisë;
3. Rekomandimin Nr. R (87) 15, që rregullon përdorimin e të dhënave personale në sektorin e policisë;

4. Rekomandimin Nr. R (95) 4 mbi mbrojtjen e të dhënave personale në fushën e shërbimeve të telekomunikacionit me referencë në shërbimet telefonike;
5. Rekomandimin Nr. R (89) 9 mbi krimet e lidhura me kompjuterat, duke dhënë udhëzimet për legjislaturat kombëtare, përsa i përket përcaktimit të krimeve kompjuterike të caktuara;
6. Rekomandimin Nr. R (95) 13, përsa i përket problemeve të ligjit të procedurës kriminale lidhur me teknologjinë informative.[122]

Konventa është e hapur për t'u nënshkruar nga shtetet anëtare të Këshillit të Evropës dhe nga shtete joanëtare që kanë marrë pjesë në hartimin e saj. Sipas konventës krimet kibernetike ndahen në:

1. ***Vepra penale kundër konfidencialitetit, integritetit dhe disponueshmërisë të të dhënave dhe sistemeve kompjuterike në të cilën bëjnë pjesë:*** Hyrjet e paligjshme, Interpretimi i paligjshëm, Interferenca e të dhënave, Interferenca e sistemeve, Keqpërdorimi i pajisjeve;

2. ***Krimet e lidhura me kompjutera, të cilat ndahen në:*** Falsifikimet e lidhura me kompjuterat, Mashtrimet e lidhura me kompjuterat, Veprat penale të lidhura me përmbajtjen ku bëjnë pjesë veprat penale të lidhura me pornografinë e fëmijëve;

3. ***Veprat penale të lidhura me dhunimin e të drejtës së autorit dhe të drejtave të tjera të lidhura me të***.

Çdo palë duhet të adaptojë legjislacion të tillë dhe masa të tjera që mund të jenë të nevojshme që të sigurohet që veprat penale, të përmëndura më lart, të parashikuara në konventë, të jenë të dënueshme me sanksione efektive proporcionale dhe frenuese, të cilat përfshijnë edhe heqjen e lirisë[123].

1.1. Përafrimi i rregullave për veprat kriminale kibernetike

Konventa e vitit 2001 përshkruan një numër të madh veprimesh, të cilat ligjvënësit kombëtarë janë të ftuar t'i inkriminojnë. Ajo i klasifikon këto veprime në katër kategori (nenet 2-10):

---

[122]Explanatory Report para 11.

[123]The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8 November 2002.

a) Vepra kundër konfidencialitetit, paprekshmërisë dhe disponibilitetit të të dhënave dhe të sistemeve informatike: (hyrja e paligjshme në një sistem informatik; përgjimi i të dhënave informatike; cënimi i paprekshmërisë së të dhënave informatike; cënimi i paprekshmërisë së sistemeve informatike; abuzimime aparaturat nëpërmjet prodhimit ose gjetjes së aparaturave të përgatitura ose të përshtatura për të kryer njërën nga veprat e mësipërme, ose nëpërmjet posedimit të një aparature të tillë për kryerjen e njërës nga veprat e treguara më lart)[124];
b) Vepra informatike: (falsifikim informatik; mashtrim informatik);
c) Vepra që kanë të bëjnë me përmbajtjen: (vepra të lidhura me pornografinë e tëmiturve);
d) Vepra që kanë të bëjnë me cënimin e pronësisë intelektuale dhe të drejtave të lidhura me të[125].

Palët duhet të inkriminojnë edhe tentativën dhe bashkëpunimin. Gjithashtu është parashikuar dhe përgjegjësia penale e personave juridikë. Sanksionet duhet të jenë efektive, proporcionale dhe riedukuese, pa përjashtuar ato me burgim.

1.2. Rregullat e Proçedurës Penale

Nga neni 14-22, konventa rendit nje seri dispozitash «që janë të nevojshme për të caktuar kompetencat dhe procedurat... me qëllim hetimi ose procedimin penal të veçantë (neni 14 § 1). Por rregullat e procedurës duhet të përputhen me normat kombëtare të mbrojtjes së të drejtave të njeriut dhe të lirive themelore të parashikuara nga KEDNJ e vitit 1950 (neni 15 § 1).

- *Cilat janë këto masa proceduriale?*

Së pari, janë masat konservative. Konventa parashikon se palët duhet të miratojnë dispozita që mundësojnë ruajtjen e shpejtë të të dhënave informatike të ruajtura (neni 16) si dhe ruajtjen dhe shpërndarjen e shpejtë të të dhënave që kanë të bëjnë me trafikun (neni 17).

---

[124]*Convention on Cybercrime (ETS no. 185), Explanatory Report*, p. 61, available at: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[125]Të gjitha këto vepra penale kryhen me dashje. Neni 3 i Protokollit te vitit 2003 shton edhe parashikimin e përgjegjësisë penale të shpërndarjes së materialeve raciste dhe ksenofobe me anë të sistemeve informatike, kërcënimet me nuanca raciste dhe ksenofobe, si dhe mohimin ose minimizimin e theksuar apo justifikimin e genocidit ose të krimeve kundër njerëzimit.

Parashikohen gjithashtu masa edhe me aktive të cilat i detyrojnë ligjvënësit të parashikojnë me ligj detyrimin për një person që të japë të dhënat që posedon (neni 18), kontrolli dhe sekuestrimi i të dhënave informatike të ruajtura (neni 19), mbledhja në kohë reale e të dhënave në lidhje me trafikun (neni 20)[126] dhe përgjimi i të dhënave në lidhje me përmbajtjen e komunikimeve të veçanta dhe të transmetuara me anë të sistemeve informatike (neni 21).

1.3. Bashkëpunimi ndërkombëtar për parandalimin dhe luftimin e kriminalitetit kompjuterik

Bashkëpunimi ndërkombëtar për parandalimin dhe luftimin e krimeve në fushën e kibernetikës lidhet me karakterin global të këtyre krimeve, që do të thotë koordinim i veprimeve nga të gjitha shtetet si dhe vendosje e standardeve ndërkombëtare në fushën e mbrojtjes së sistemeve kompjuterike. Një bashkëpunim efikas do të ndikonte në zbulimin dhe në parandalimin e veprave penale në fushën e kibernetikës[127].

Ajo që nuk duhet harruar në asnjë moment është se nuk ekziston mbrojtja absolute dhe çdo sistem informativështë i ekspozuar ndaj rreziqeve të vërteta, por duhet që madhësia e rrezikut ekzistues të kufizohet në kufijtë më të pranueshëm. Për të realizuar të gjithë këtë duhet patur gjithmonë parasysh strategjia gjithëpërfshirëse pa të cilën është e pamundur implementimi i zgjidhjeve efikase që mund të japin rezultat. Aplikimi në praktikë i masave të propozuara në këtë punim praktikisht do të shërbente si masë parandaluese dhe njëkohësisht do të ndihmonte në ndërgjegjësimin e personave të çdo moshe, në respektimin e të drejtës së shfrytëzimit të papenguar të sistemeve kompjuterike dhe të çdo të drejte tjetër lidhur me këto sisteme[128]. Duke pasur parasysh faktin se shoqëritë në gjithë botën mbështeten tek teknologjitë e informacionit dhe komunikimit, gjyqtarët dhe prokurorët e çdo shteti që ka ratifikuar Konventën e Budapestit duhet të jenë të përgatitur që të përballen me krimin kibernetik dhe provat elektronike.

---

[126] *Convention on Cybercrime (ETS no. 185), Explanatory Report*, pp. 200-202, available at: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[127] Gercke M. (2008), "*National, Regional and International Legal Approaches in the Fight Against Cybercrime*", in Journal ofInformation Law and Technology, Issue 1, pp. 7-14.

[128] C. Carr (Ed). (2000), "*The Book of War*". New York: Random House, pp.18-24.

Teksa në shumë vende organet e zbatimit të ligjit kanë arritur t'i fuqizojnë kapacitetet e tyre për hetimin e krimit kibernetik dhe t'i sigurojnë provat elektronike, duket se kjo nuk është arritur po në atë shkallë edhe nga gjyqtarët dhe prokurorët. Përvoja sugjeron se në pjesën më të madhe të rasteve, gjyqtarët dhe prokurorët hasin vështirësi kur përballen me realitetet e reja të botës kibernetike.

Kështu që nevojiten përpjekje të posaçme që gjyqtarët dhe prokurorët të përshtaten që ta ndjekin penalisht dhe ta gjykojnë krimin kibernetik dhe t'i përdorin provat elektronike nëpërmjet trajnimit, krijimit të rrjeteve dhe specializimeve dhe për këtë është e nevojshme një bashkëpunim mëi gjerë ndërkombëtar.

Ky koncept është krijuar që t'u vijë në ndihmë këtyre përpjekjeve. Ai është zhvilluar nga Projekti i Këshillit të Evropës për Krimin Kibernetik dhe nga Rrjeti i Lisbonës për institucionet e trajnimit të gjyqësorit në bashkëpunim me një grup pune të përbërë prej palëve të interesuara gjatë vitit 2009.

Qëllimi i këtij koncepti është t'u vijë në ndihmë institucioneve të trajnimit të gjyqësorit që të zhvillojnë programe trajnimi për krimin kibernetik dhe për provat elektronike për gjyqtarët dhe prokurorët dhe ta integrojë këtë trajnim në trajnimet e rregullta fillestare dhe ato të vazhduara(domethënë që ai të institucionalizohet). Përveç kësaj, ky koncept do të mbështesë krijimin e rrjeteve të gjyqtarëve dhe prokurorëve në mënyrë që njohuritë e tyre të përmirësohen dhe që të ketë një mbështetje të vazhdueshme – dhe jo vetëm ad hok – për iniciativat për trajnime nga partnerët e interesuar.

2. Teoritë e Juridiksionit

Jo më pak se pesë teori të ndryshme mbi juridiksionin janë aplikuar së bashku nga gjykata dhe qeveritë, me qëllim dhënien e juridiksionit një gjykate të caktuar duke ndikuar negativisht në juridiksionin e gjykatave të tjera.

2.1. Teoria e Territorialitetit

Teoria sipas të cilës juridiksioni përcaktohet mbi bazën e vendit ku është kryer vepra tërësisht ose pjesërisht, buron nga i ashtuquajturi modeli Uestfalian (Westphalian) i sovranitetit, i cili përfshin dhe i referohet tri parimeve themelore:

1. Parimi i kontrollit ekskluziv mbi territorin e vendit;

2. Parimi i mosndërhyrjes dhe mosndikimit[129];
3. Parimi i barazisë midis shteteve[130].

Edhe pse shumë i diskutuar dhei kundërshtuar, modeli duket se ka të paktën një pranim të përgjithshëm në lidhje me përmbajtjen e këtyre parimeve, edhe pse duhet thënë se barazia midis shteteve në shumicën e rasteve është vetëm formale[131].

Duke pasur parasysh se shteti ka sovranitet mbi territorin, ai padyshim do të ketë juridiksion mbi çdo sjellje të paligjshme që ndodh në atë territor, pavarësisht faktit nëse është kryer ose jo nga një prej shetasve të tij[132].

Një rast kompleks i aplikimit të teorisë së territorialitetit është rasti *Bavaria v. Somm*, evidentuar në Amtsgericht të Mynihut, Gjermani, në vitin 1999.

Felix Bruno Somm, një qytetar nga Zvicra, drejtor menaxhues i një kompanie të shërbimeve informatike, u akuzua nga Gjermania si përgjegjës për aksesin në materiale pornografike të fëmijëve dhe kafshëve me karakter të dhunshëm të ruajtura në serverin e kompanisë e vendosur në SHBA.

Gjykata Gjermane konsideroi se kishte juridiksion mbi Z.Somm sepse edhe pse ishte zvicerian, ai jetonte në Gjermani, duke iu referuar kështu teorise territoriale të juridiksionit.

---

[129]HardingCH e Lim C. L. (1999), "The Significance of Westphalia: An Archaeology of the International Legal Order", *in* Christopher Harding and C. L. Lim (eds), *Renegotiating Westphalia: Essays and Commentary on the European and Conceptual Foundations of ModernInternational Law*, The Hague / Boston / London, Martinus Nijhoff Publishers, pp. 1-23., seealso Krasner D.S. (1999), *Sovereignty: OrganizedHypocrisy*, New Jersey, Princeton University Press, pp. 44-46.

[130]Fitz PatrickJ. (2002), "Sovereignty, Territoriality, and the Rule of Law", *Hastings International and Comparative Law Review*, vol. 25, pp. 304,310. Brown S, *International Relations in a Changing Global System: Toward a Theory of the World Polity*, Boulder, Colorado, Westview Press, 1992, p. 74.

[131]BeaulacS, *The Power ofLanguage in the Making of International Law: The Word Sovereignty in Bodin and Vattel and the Myth ofWestphalia*, Leiden / Boston, Martinus Nijhoff Publishers, 2004, pp. 71.

[132]AntoliseiF. (2000), *Manuale di Diritto Penale. Parte Generale*, 15ª ed., Milano, Dott. A. Giuffrè Editore, p. 118.

2.2. Teoria e kombësisë

"Teoria e kombësisë" është quajtur edhe "teoria e personalitetit aktiv", sepse merret kryesisht me kombësinë e personit që ka kryer sulmin[133].

Duke qenë gjerësisht i njohur fakti sipas të cilit një vend ka kontroll pothuajse të pakufizuar mbi shtetasit e tij, sipas kësaj teorie vendi mendohet të ketë të drejtë që të ushtrojë juridiksionin e tij mbi këta individë, pavarësisht se ku ndodhen dhe pavarësisht se çfarë bëjnë[134].

Kudo që të jetë kryer vepra, brenda ose jashtë vendit, duhet mbajtur parasysh se shkelësi ndoshta ka njohuri më të mira të ligjeve të shtetit të tij sesa të ligjeve të shtetit tjetër. Gjithashtu, një veprim mund të konsiderohet i ligjshëm në territorin ku është kryer, ndërsa mund të konsiderohet i paligjshëm (krim) në territorin e vendit nga ku vjen personi.

Çështja, Shtetet e Bashkuara v. Galaxy Sport është një shembull i mirë i aplikimit të kësaj teorie. Kompania shënjestronte konsumatorët në Shtetet e Bashkuara, duke reklamuar biznesin e saj në të gjithë Amerikën nëpërmjet radios, gazetës dhe televizorit.

Reklamat e saj ftonin klientët të vinin baste me kompaninë nëpërmjet telefonatave të gjata, falas, ose nëpërmjet internetit[135].

Për shak se kompania ishte e vendosur në Antigua, gjykata në lidhje me apelimin e kësaj çështje nuk ishte në gjëndje të ushtronte juridiksion e saj.

Megjithatë presidenti i kompanisë ishte një qytetar i SHBA-së, dhe si i tillë mund të çohej në gjykatë. Zoti Jay Cohen, më 10 Gusht të vitit 2000, pas një gjyqi kryesuar nga gjykatësi Thomas P.Griesa u dënua me njëzet e një muaj burg.

---

[133]Christopher L. Blakesley. (1988) "*Jurisdictional Issues and Conflicts of Jurisdiction*", *in* M. Cherif Bassiouni (ed.), "*Legal Responses to International Terrorism. U.S. Procedural Aspects"*, Dordrecht, Martinus Nijhoff Publishers, pp. 139.

[134]Ray A, (2002), "*International Cyber-Jurisdiction: A Comparative Analysis*", American Business Law Journal, vol. 39 , pp. 539.

[135]UNITED STATES ATTORNEY'S OFFICE, NORTHERN DISTRICT OF FLORIDA, "*International Computer 'Hacker' Sentenced to More Than Three Years in Federal Prison*", online athttp://www.usdoj.gov/criminal /cybercrime / bentleySent.pdf,last visited September 2,2008.

Në shyrtimin e apelimit të këtij vendimi për dënimin e dhënë, Gjykata e Apelit la në fuqi vendimin e Gjykatës së Rrethit pa e vënë në dyshim dhe pa e diskutuar çështjen e juridiksionit.

2.3. Teoria e personalitetit pasiv

Ndërsa "teoria e kombësisë" merret me kombësinë e autorit të veprës, duke i dhënë juridiksion gjykatave kombëtare, e kundërta e saj, "teoriae personalitetit pasiv" ka të bëjë me kombësinë e viktimës[136].

Arsyet për dhënien e juridiksionit mbi një vepër penale janë të ngjashme për të dyja teoritë. Kështu, kur i referohemi kësaj teorie, janë gjykatat e shtetit të cilit i përket viktima, që marrin juridiksionin[137].

Në fushën e kiber kriminologjisë, një shembull i ushtrimit të juridiksionit sipas teorisë së personalitetit pasiv është dënimi më 25 Korrik të vitit 2003, nga gjykatat federale në Hartford, Connecticut, SHBA, nga Gjyqtari Alvin W.Thompson, i qytetarit rus Alexey Ivanov, i cili kishte jetuar në Chelyabinsk, Rusi, për pirateri komjuterike në SHBA[138].

2.4. Teoria e Mbrojtjes

"Teoria e mbrojtjes" e quajtur edhe ("parimi i sigurisë") është ndoshta më pak e përdorur, nëse është përdorur ndonjëherë, midis teorive që sanksionojnë juridiksionin. Kjo teori ka të bëjë me interesin kombëtar ose ndërkombëtar të rrezikuar.

Teoria lejon caktimin e juridiksionit për shtetin, qoftë kombëtar apo ndërkombëtar, që shikon interesin e tij në rrezik për shkak të një sulmi kibernetik[139].

---

[136] Christopher L. Blakesley. (1988), "*Jurisdictional Issues and Conflicts of Jurisdiction*", pp. 139.

[137]Fitzpatrick J. (2002), "*Sovereignty, Territoriality, and the Rule of Law*", Hastings International and Comparative Law Review, vol. 25, pp. 313, note 37.

[138]*U.S.A. v. Ivanov* (2003), 172 C.C.C. (3d) 551 (Nfld.C.A.). See also U.S. DEPARTMENT OF JUSTICE. UNITED STATES ATTORNEY, "*Russian Man Sentenced for Hacking into Computers in the United States*", onlineat http://www.usdoj.gov/criminal/cybercrime/ivanovSent.htm , last visited September 2, 2008.

[139]Christopher L. Blakesley. (1988) "*Jurisdictional Issues and Conflicts of Jurisdiction*", pp. 139.

2.5. Teoria e Universalitetit

"Teoria e universalitetit" është e bazuar në karakterin ndërkombëtar të veprës dhe ndryshe nga teoritë e tjera lejon çdo shtet që të kërkojë ushtrimin e juridiksionit mbi veprat, edhe nëse këto vepra nuk kanë efekt të drejtpërdrejtë në shtetin që ushton juridiksionin[140].

Dy kërkesa janë të nevojshme për marrjen dhe ushtrimin e juridiksionit: (1) shteti i cili merr juridiksionin duhet të ketë të pandehurit në paraburgim;[141](2) krimi duhet të jetë veçanërisht i rëndë dhe fyes për komunitetin ndërkombëtar [142].

Kështu, krimi i parë për t'u konsideruar në kuadrin e juridiksionit universal është pirateria, e ndjekur nga trafikimi i të dhënave. Pas Luftës së Dytë Botërore, krimet e luftës, krimet kundër njerëzimit, aktet terroriste, rrëmbimi dhe sabotimi i aeroplanëve, aparteidi, tortura dhe shkelje të tjera të të drejtave të njeriut progresivisht u bënë subjekt i jurisdiksionit universal[143].

2.6. Juridiksioni sipas konventës

Natyra dhe shtrirja globale e kriminalitetit kompjuterik ka sfiduar pikëpamjet tradicionale mbi veprimin e kufizuar territorial të së drejtës penale. Duke qenë se në ditët e sotme, njerëzit mund të komunikojnë përtej detit dhe përtej kufinjve, ka bërë që keqbërësit të jenë prezent dhe të shkaktojnë dëme kudo ku ka një lidhje interneti.

Edhe kur shkelësi dhe personi i dëmtuar ndodhen nën juridiksionin e të njëjtit shtet, për shkak të natyrës që ka komunikimi në rrugë elektronike, të dhënat që paraqesin rëndësi për hetimin dhe gjykimin e veprës tejçohen dhe ruhen nëpërmjet pajisjeve që ndodhen në disa juridiksione të tjera.

---

[140]Christopher L. Blakesley. (1988) "*Jurisdictional Issues and Conflicts of Jurisdiction*", pp. 141.

[141]Bassiouni M. Cherif. (1992), "*Policy Considerations on Inter-State Cooperation inCriminal Matters*", Pace Yearbook of International Law, vol. 4, pp. 126-128.

[142]Kenneth C. Randall. (1988), "*Universal Jurisdiction under International Law*", *Texas Law Review*, vol. 66, pp. 788.

[143]Bassiouni M. Cherif. (1992),"*Crimes against Humanity in International Criminal Law"*, Dordrecht, Martinus Nijhoff Publishers, pp. 511-513. Shiko Bassiouni M. Cherif, "*Crimes against Humanity in International Criminal Law"*, pp. 513.

Një situatë e tillë, jo vetëm që paraqet një pafundësi mundësish për keqbërësit por edhe një sfidë të madhe për agjensitë ligj zbatuese[144].

Duke marrë parasysh gjeografinë e veçantë fizike dhe virtuale të veprave penale që kryhen në hapësirën kibernetike, në Konventën e Këshillit të Evropës "Për Krimin në fushën e Kibernetikës" janë vendosur disa rregulla të rëndësishme për të përcaktuar juridiksionin në ndjekjen e veprave në rastet kur në një mënyrë apo në një tjetër, fakti i paligjshëm ka prekur interesat e disa shteteve njëkohësisht, thënë ndryshe konventa rregullon çështjet e juridiksionit duke gërshetuar teorinë e territorialitetit me atë të kombësisë. Më konkretisht në përputhje me parashikimet e Konventës:

1. Secila palë merr masa legjislative ose masa të tjera që janë të nevojshme për të caktuar juridiksionin për çdo vepër penale të kryer në pajtim me përcaktimet e konventës, kur një vepër e tillë kryhet[145]:

a. *në territorin e tij;*
b. *në bordin e një anijeje që mban flamurin e atij shteti;*
c. *në bordin e një avioni të regjistruar sipas ligjit të atij shteti;*
d. *nga njeri prej shtetasve të saj, nëse vepra penale është e dënueshme sipas ligjit penal ku ajo është kryer ose nëse vepra është kryer jashtë juridiksionit territorial të çdo shteti.*

2. Secili shtet mund të rezervojë të drejtën për të mos zbatuar ose për të zbatuar vetëm në raste të caktuara, ose kushte të caktuara rregullat juridiksionalë të parashikuara në paragrafët (1) b – (1) d të nenit 22 të Konventës ose të ndonjë pjese të tyre.

3. Secila palë merr masa të tilla që janë të nevojshme për të caktuar juridiksionin mbi të gjitha veprat penale të përmendura në nenin 24, paragrafi (1) i kësaj konvente, në rastet kur kryerësi i prezumuar i veprës penale është prezent në territorin e saj dhe ajo nuk e ekstradon atë tek një palë tjetër, kryesisht mbi bazën e shtetësisë së tij/saj pas kërkesës së bërë për ekstradim.

4. Konventa nuk përjashton asnjë juridiksion penal të ushtruar në pajtim me ligjin vendas.

---

[144]Clough, J. (2012). "*The Council of Europe Convention on Cybercrime: Defining 'Crime' in a Digital World".* Criminal Law Forum, Vol 23(4). Heidelberg: Springer, pp. 36.

[145] Neni 22 i Konventës.

5. Nëse më shumë se një palë pretendon juridiksionin mbi një vepër që prezumohet e kryer në pajtim me konventën, palët e interesuara, kur është e përshtatshme, bëjnë një konsultë për të përcaktuar juridiksionin më të përshtatshëm për të bërë ndjekjen penale.

Në pikën 1/a gjen shprehje parimi i territorialitetit. Në bazë të këtij parimi një shtet mund të kërkojë juridiksionin e tij, psh. kur personi i cili ka kryer një sulm ndaj një sistemi kompjuterik dhe sistemi i cënuar gjëndet brenda territorit të të njëjtit shtet, ose kur të paktën sistemi ndaj të cilit është kryer sulmi ndodhet në territorin e tij[146].

Po ashtu në pikat b) dhe c) i jepet zbatim parimit të territorialitetit bazur në faktin se në legjislacionet e brendshme të shumë shteteve anijet dhe avionët që kanë statusin e përmendur në dispozitë janë konsideruar vazhdimisht si një vazhdim i terrirorit të shtetit. Pika d) i përmbahet parimit të shtetësisë në themel të të cilit qëndron ideja se shtetasit e një shteti të caktuar duhet t'i përmbahen ligjeve të atij shteti edhe kur ata ndodhen jashtë territorit të tij. Në mënyrë që një shtet të mund të ushtrojë juridiksionin e tij për një krim kompjuterik të kryer nga një shtetas i tij jashtë territorit të atij shteti duhet që vepra të jetë njëkohësisht e dënueshme edhe në territorin e shtetit tjetër ku është kryer vepra. Kushti i dënimit të dyfishtë të sjelljes së paligjshme kërkohet për sa kohë që vepra penale është kryer në territorin e një shteti të caktuar. Nëse vepra është kryer në një hapësirë ku nuk shtrihet juridiksioni territorial i asnjë shteti (si psh. në ujrat ndërkombëtare ose hapësirat ajrore ndërkombëtare), atëherë mjafton që vepra penale të jetë e ndëshkueshme sipas ligjit të shtetit, shtetësinë e të cilit mban autori i saj, për t'u ushtruar juridiksioni i këtij shteti.

3. Direktiva 95/46 - KE "Për Mbrojtjen e të Dhënave Personale"

Direktiva 95/46/EC është teksti kryesor i referimit në nivelin Evropian për sa i përket çështjes së mbrojtjes së të dhënave personale. Direktiva 95/46/EC mbulon çfarëdo forme të përpunimit të të dhënave personale pa marrë parasysh teknologjinë e përdorur. Qëllimi kryesor i Direktivës 95/46 është të mbrojë të drejtat dhe liritë themelore të personit dhe në mënyrë të veçantë të drejtën për jetë private lidhur me proceset përpunuese të të dhënave personale duke parashtruar standartet bazë që duhet të respektohen nga ana e subjekteve përpunuese.

[146]Amelie M. Weber. (2003), "*The Council of Europe's Convention on Cybercrime"*, 18 Berkeley Tech. L.J. pp. 425- 435.

Në këtë drejtim, rregullat kryesore janë ato që kanë të bëjnë me cilësinë e të dhënave, ligjshmërinë e përpunimit të tyre dhe kufizimet e mundshme që mund të zbatohen ndaj përpunuesve të të dhënave. Në përcaktimin që bën direktiva '*e dhënë personale*' është çdo informacion i lidhur me një person fizik të identifikuar ose të identifikueshëm, ndërsa me 'përpunim të të dhënave' do të kuptohet çdo proces i kryer mbi të dhënat personale si grumbullimi, regjistrimi, ruajtja, konsultimi, përdorimi, zbulimi nëpërmjet transmetimit, shpërndarjes, ose vënia në dispozicion në çdo mënyrë tjetër. Në aspektin teknik ofrimi i shërbimeve të komunikimeve elektronike publike, shoqërohet nga kryerja e proceseve të tilla si grumbullimi, regjistrimi, ruajtja apo shpërndarja e të dhënave. Si rrjedhim, aktiviteti i ushtruar prej tyre, do të bjerë në hapësirën e rregullimit të direktivës, për sa kohë që gjatë proceseve të ofrimit të shërbimit përkatës të komunikimit publik aksesohen ose trajtohen të dhëna me natyrë personale.

Parashikimet mbi cilësinë e të dhënave kanë të bëjnë me detyrimin për një përpunim të ndershëm dhe të ligjshëm të të dhënave personale, dhe mbledhjen e tyre për qëllime legjitime të përcaktuara dhe të shprehura qartë. Këto të dhëna duhet gjithashtu të jenë të mjaftueshme, të kenë lidhje me procesin që synohet të realizohet dhe të mos tejkalojnë qëllimet për të cilat ato grumbullohen dhe/ose përpunohen[147].

Ndërsa ligjshmëria e përpunimit analizohet duke marrë në konsideratë dy çështje kryesore: Së pari, nëse personi, të dhënat e të cilit do të përhapen ka dhënë pëlqimin e tij të lirë dhe të qartë; Së dyti, nëse përpunimi është i nevojshëm për realizimin e interesave të ligjshme të kontrolluesit[148].

Vlen të theksohet se e drejta e kontrolluesit për të pasur akses në të dhënat personale dhe për t'i përpunuar ato është një zgjidhje që duhet të konsiderohet si mjeti i fundit dhe që për më tepër i nënshtrohet disa kufizimeve.

[147]Shiko nenin 6 të Direktivës 95/46/EC.

[148]Në nenin 7 të Direktivës thuhet se shtetet anëtare duhet të sigurojnë që përpunimi i të dhënave personaletë kryhet vetëm: (a) nëse subjekti i të dhënave personale ka dhënë pëlqimin,nepermjet përmbushjes se një kontrate, për të cilën subjekti i të dhënave është palë kontraktuese, me qellimmbrojtjen e interesavejetikë të subjektit të të dhënave qoft kjo për përmbushjen e një detyrimi ligjor të kontrolluesit apopër kryerjen e një detyre ligjore me interes publik ose ushtrimin e një kompetence të kontrolluesit ose të një pale të tretë, së cilës i janë përhapur të dhënat.

Së pari, zbulimi i të dhënave personale për realizimin e një interesi legjitim të kontrolluesit, nuk mund të kryhet nëse një interes i tillë bie në kundërshtim me interesat për respektimin e të drejtave dhe lirive themelore të subjektit të të dhënave. Së dyti, në çdo rast të ndërmarrjes së një praktike të ligjshme kontrolluese, kontrolluesi ka detyrimin që t'i sigurojë subjektit të të dhënave informacion mbi përpunimin e të dhënave të tij personale, si dhe të paktën informacion mbi qëllimet e përpunimit, kategoritë e të dhënave të përpunuara dhe për marrësit e kategoritë e marrësve, të cilëve u përhapen të dhënat personale.

4. Direktiva 2002/58 – KE për "e-Privatësinë"

Direktiva 2002/58[149] sqaron më tej dhe plotëson Direktivën 95/46 në lidhje më përpunimin e të dhënave personale në sektorin e komunikimeve elektronike dhe njihet gjerësisht si Direktiva e Privatësisë. Kjo Direktivë synon në mënyrë të veçantë të sigurojë respektimin e plotë të të drejtës për jetë private dhe të drejtës për mbrojtjen e të dhënave personale të parashikuar në nenet 7 dhe 8 të Kartës së të Drejtave Themelore të BE-së.

Direktiva vë theksin në parimin e afirmuar tashmë brenda Bashkimit Evropian se të gjitha shtetet anëtare duhet të sigurojnë mbrojtjen e fshehtësisë së komunikimeve të realizuara nëpërmjet rrjeteve të komunikimeve publike dhe të të dhënave personale e private që përmbahen në këto komunikime. Rregullimet e saj gjejnë zbatim ndaj komunikimeve të bëra nëpërmjet rrjeteve të komunikimeve elektronike publike duke përfshirë ndër të tjera komunikimet me email, fax, sms si dhe forma të tjera të komunikimit në internet. Për më tëper, direktiva përmban rregulla të veçanta mbi përpunimin e të dhënave personale, mbrojtjen e privatësisë në fushën e komunikimeve elektronike si dhe rregulla mbi komunikimet tregtare të padëshiruara (spam) etj.

Në tekstin e direktivës afirmohet edhe njëherë se të dhënat që kanë të bëjnë me pajtimtarët, të përpunuara brenda rrjetit të komunikimeve elektronike për të krijuar lidhje dhe për të transmetuar informata përmbajnë informata mbi jetën private të personave fizikë dhe kanë lidhje me të drejtën për respektimin e korrespondencës së tyre.

[149]Kjo Direktivë ka zëvendësuar Direktivën 97/66 të Paralamentit Evropian dhe Këshillit të 15 dhjetorit 1997 "Mbi përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në fushën e telekomunikimeve" duke përshtatur parashikimet e saj ndaj zhvillimeve të reja teknologjike në fushën e komunikimeve elektronike.

Në lidhje me fshehtësinë e komunikimeve, kërkohet që pjesëmarrësit në një komunikimi të informohen paraprakisht rreth një aktiviteti regjistrues të zbatuar nga ana e ofruesit të shërbimit si dhe për qëllimin dhe kohëzgjatjen e ruajtjes së të dhënave të komunikimit.

Për sa i përket përdorimit të programeve përgjuese, të pajisjeve të fshehta për marrjen e të dhënave, ose pajisjeve të tjera të ngjashme të cilat janë të afta të depërtojnë në kompjuterin e përdoruesit pa dijeninë e tij në mënyrë që të sigurojnë akses në informacionin e ruajtur aty, ose të përgjojnë aktivitetet e kryera nga përdoruesi, theksohet se këto praktika mund të dhunojnë rëndë jetën private të përdoruesve.

Përdorimi i pajisjeve të tilla, duhet lejuar vetëm për shkaqe të ligjshme, dhe me dijeninë e përdoruesve të prekur nga veprimet në fjalë[150].

Vëmëndje e veçantë i kushtohet gjithashtu marrjes së masave të përshtatshme teknike dhe organizative nga ana e ofruesve të shërbimeve të komunikimeve elektronike publike për të garantuar sigurinë e shërbimeve të tyre[151].

Masat e marra prej ofruesve të shërbimeve të komunikimeve elektronike publike duhet të paktën: të sigurojnë që të dhënat personale të jenë të aksesueshme vetëm nga personeli i autorizuar dhe vetëm për qëllime të ligjshme; të mbrojnë të dhënat personale të ruajtura/transmetuara nga çdo shkatërrim aksidental ose i paligjshëm si dhe nga ruajtja, përpunimi aksesi ose përhapja e paligjshme ose e paautorizuar; dhe të sigurojnë zbatimin e një politike sigurie në lidhje me përpunimin e të dhënave personale.

Parimet e vendosura në Direktivën 95/46, gjejnë shprehje në rregulla specifike në Direktivën 2002/58, të cilat zbatohen në fushën e shërbimeve të komunikimeve elektronike publike.

[150]Shiko Direktivën 2002/58 të Paralamentit Evropian dhe Këshillit të 12 qershorit 2002 mbi përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në fushën e komunikimeve elektronike, pika 24. E vlefshme në: http://eur-lex.europa.eu.

[151]Shiko nenin 4 të Direktivës 2002/58.

5. Direktiva 2006/24 - KE "Mbi Ruajtjen e të Dhënave"

Direktiva 2006/24[152] synon të harmonizojë kuadrin ligjor të shteteve anëtare të BE-së për sa i takon detyrimeve të sipërmarrësve të rrjeteve dhe të shërbimeve të komunikimeve elektronike publike për ruajtjen e të dhënave të caktuara që administrohen dhe përpunohen prej tyre, në mënyrë që këto të dhëna të vihen në dispozicion të autoriteteve të ndjekjes penale me qëllim zbulimin, hetimin dhe ndjekjen e veprave penale, sikurse përcaktohet në ligjin e brendshëm të secilit shtet.

Sipas përcaktimeve të direktivës, sipërmarrësit e rrjeteve dhe shërbimeve në fjalë detyrohen të ruajnë dhe të administrojnë, për një periudhë nga 6 muaj deri në 2 vjet, kategori të caktuara të dhënash për pajtimtarët ose përdoruesit e tyre.

Informacionet që kërkohet të ruhen lidhen kryesisht me të dhëna që janë të nevojshme për:

- Përcaktimin e vendndodhjes dhe identifikimin e origjinës së komunikimit;
- Identifikimin e pajisjes fundore të përdorur gjatë komunikimeve;
- Përcaktimin e vendndodhjes dhe identifikimin e destinacionit të komunikimeve;
- Identifikimin e datës, kohës dhe kohëzgjatjes së komunikimit;
- Identifikimin e llojit të komunikimit.

Në sajë të ruajtjes së këtyre të dhënave mund të merret informacion i plotë mbi komunikimet zanore dhe me SMS/MMS të një përdoruesi, mbi emailet e shkëmbyera apo mbi faqet e vizituara prej tij në internet.

Në tekstin e direktivës theksohet gjithashtu se sipërmarrësit e rrjeteve ose shërbimeve të komunikimeve elektronike në dispozicion të publikut, duhet të respektojnë disa parime minimale të sigurisë në lidhje me të dhënat e ruajtura për këto qëllime. Kështu, të dhënat e ruajtura duhet të vazhdojnë të gëzojnë të njëjtën cilësi dhe t'i nënshtrohen të njëjtit nivel mbrojtjeje sikurse të dhënat që qarkullojnë në rrjet. Kërkohet gjithashtu të merren masat e duhura teknike dhe organizative për mbrojtjen e të dhënave nga shkatërrimet/humbjet aksidentale ose të kundraligjshme, apo përpunimi, aksesi, zbulimi i paautorizuar i tyre, si dhe për të siguruar aksesin në të dhëna vetëm të personelit të autorizuar.

[152]Direktiva 2006/24 KE *'Mbi ruajtjen e të dhënave të krijuara ose të përpunuara lidhur me ofrimin e shërbimeve të komunikimeve elektronike të disponueshme për publikun ose të rrjeteve të komunikimit publik'* që amendon Direktivën 2002/58.

Miratimi i direktivës pasoi ngjarjet e sulmeve terroriste në Madrid në vitin 2004 dhe në Londër në vitin 2005 dhe ishte shprehje e nevojës së ngutshme të shteteve anëtare të BE-së për harmonizimin e përpjekjeve për hetimin dhe ndjekjen e krimeve me rrezikshmëri të lartë shoqërore. Pavarësisht faktit se rrethanat specifike në të cilat, të dhënat e ruajtura do të vihen në dispozicion të autoriteteve të ndjekjes penale, përcaktohen në ligjin e brendshëm, theksohet se kushtet që duhen përmbushur dhe procedurat e ndjekura prej tyre duhet të respektojnë kërkesat mbi domosdoshmërinë dhe proporcionalitetin e ndërhyrjes.

Rendi juridik i vendosur nëpërmjet Direktivës 2006/24 është vlerësuar prej disa shteteve anëtare si kontradiktor me të drejtën për respektimin e jetës private dhe është pezulluar apo kundërshtuar veprimi i ligjeve të brëndshme që synojnë të bëjnë të zbatueshme direktivën në të drejtën e brendshme[153].

Së fundmi, pajtueshmëria e saj me parimet e respektimit të të drejtave dhe lirive themelore të njeriut është marrë në shqyrtim edhe nga Gjykata Evropiane e Drejtësisë.
Në Dhjetor 2013, Gjykata Kushtetuese e Austrisë dhe Gjykata e Lartë e Irlandës iu drejtuan Gjykatës Evropiane të Drejtësisë për të marrë mendimin e saj mbi pajtueshmërinë e Direktivës *'Mbiruajtjen e të dhënave'* me Kartën e të Drejtave Themelore të BE-së dhe veçanërisht me nenin 7 të saj, që njeh të drejtën e çdo personi për respektimin e jetës së tij private dhe familjare si dhe me nenin 8, ku njihet e drejta për mbrojtjen e të dhënave personale.

Më 8 Prill 2014 gjykata nxori një vendim, me anë të të cilit ka deklaruar pavlefshmërinë e parashikimeve të direktivës. Sipas këtij vendimi, direktiva është e papajtueshme me nenet 7 (e drejta për respektimin e jetës private dhe familjare), dhe 8 (e drejta për mbrojtjen e të dhënave personale) të Kartës. Në vendim thuhet se: *Direktiva 2006/24 nuk parashtron rregulla të qarta dhe preçize për përcaktimin e shkallës së ndërhyrjes së autoriteteve shtetërore në ushtrimin e të drejtave themelore të parashikuara në nenet 7 dhe 8 të Konventës.*

---

[153]Në Austri, Suedi, Gjermani, Irlandë, Rumani dhe Bullgari, gjykatat e brendshme janë shprehur për papajtushmërinë ligjeve të brendshme që synojnë të bëjnë të zbatueshme Direktivën 2006/24 me të drejtën e individit për jetë private. Shiko: *Data Retention Directive* në https://wiki.openrightsgroup.org .

Si rrjedhim, Direktiva krijon hapësirë për një ndërhyrje të gjerë dhe serioze në këto të drejta themelore brenda rendit juridik të Bashkimit Evropian duke mos e kufizuar ndërhyrjen nëpërmjet parashikimeve të qarta që sigurojnë ushtrimin e saj vetëm në ato raste kur paraqitet tejet e nevojshme[154].

Duke vendosur detyrimin për ruajtjen e të dhënave të caktuara të jashtme të komunikimit, dhe duke lejuar autoritetet kompetente kombëtare që të marrin dijeni mbi këto të dhëna, Direktiva 2006/24 devjion nga sistemi i mbrojtjes së privatësisë i vendosur nga Direktivat 95/46 dhe 2002/58 në lidhje me përpunimin e të dhënave personale në sektorin e komunikimeve elektronike, të cilat parashikojnë mbrojtjen e fshehtësisë së komunikimeve dhe të të dhënave të trafikut si dhe detyrimin për t'i fshirë ose bërë të paidentifikueshme këto të dhëna, kur ato nuk janë më të nevojshme për qëllime të transmetimit të komunikmit apo të faturimit[155].

Më tej Gjykata vazhdon arsyetimin e saj: *Direktiva synon të kontribuojë në luftën kundër krimit të organizuar, por nuk vendos kërkesën për ekzistencën e një lidhjeje midis të dhënave, për të cilat kërkohet ruajtja dhe rrezikut që kërcënon sigurinë publike, dhe në mënyrë të veçantë nuk e ka kufizuar detyrimin e ruajtjes së të dhënave në lidhje me (i) të dhëna që i përkasin një periudhe të caktuar kohore dhe/ose një zone të caktuar gjeografike, apo ndaj një rrethi të caktuar personash që janë të predispozuar për t'u përfshirë në një mënyrë ose në një tjetër, në një krim të rëndë, ose (ii) në lidhje me persona, ruajtja e të dhënave të të cilëve, për arsye të tjera, mund të kontribuojë në parandalimin, zbulimin ose hetimin e veprave penale të rënda*[156].

Për më tepër, Direktiva nuk vendos kushte substanciale dhe proceduriale lidhur me aksesin në të dhëna të autoriteteve kompetente kombëtare dhe përpunimin e mëtejshëm të tyre… nuk përcaktohet shprehimisht që përdorimi i mëtejshëm i të dhënave në fjalë, duhet të kufizohet rreptësisht me qëllimin e parandalimit dhe zbulimit të veprave penale të rënda

[154]Paragrafi 65 i Vendimit.

[155]Paragraf 32 i Vendimit.

[156]Paragraf i 59 i Vendimit.

të mirë përcaktuara; në të parashikohet vetëm se çdo shtet anëtar duhet të përcaktojë procedurat që duhet të ndiqen dhe kushtet që duhet të plotësohen në mënyrë që të sigurohet aksesi në të dhënat e ruajtura në përputhje me kërkesat e domosdoshmërisë dhe proporcionalitetit.

Nëpërmjet miratimit të Direktivës 2006/24, legjislatura e BE-së ka tejkaluar kufizimet që vendosen në përputhje me parimin e proporcionalitetit në kuadër të neneve 7, 8 dhe 52(1)[157] *të Kartës së të Drejtave Themelore*[158].

Me deklarimin e pavlefshmërisë së parashikimeve të Direktivës "Mbi ruajtjen e të dhënave" statusi aktual i saj mbetet i paqartë. Në një memorandum të Komisionit Evropian thuhet se '*edhe në kushtet e pavlefshmërisë së Direktivës, ruajtja e të dhënave do të vazhdojë të lejohet në përputhje me Direktivën 2002/58 'Mbi përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike'.* Ky qëndrim lë të kuptohet se, autoritetet vendase mund të vazhdojnë të kërkojnë ruajtjen e të dhënave për qëllime të ndjekjes penale, por në ushtrimin e kompetencave të tyre, ato duhet të kujdesen që ruajtja dhe përpunimi i mëtejshëm i të dhënave të respektojë kërkesat për ruajtjen e privatësisë sipas Direktivës 2002/58.

6. Vendimi-kuadër i 24 Shkurtit 2005 në lidhje me sulmet kundër sistemeve të informimit

Të gjitha shtetet anëtare e kanë ratifikuar Konventën e Këshillit të Evropës të 28 Janarit 1981 për mbrojtjen e personave në lidhje me trajtimin e automatizuar të të dhënave me karakter personal. Ekzistojnë shumë pak statistika të besueshme mbi shtrirjen e vërtetë të fenomenit të kriminalitetit informatik, por është parë se sistemet e informimit që mbajnë këto lloj të dhënash janë objekt i sulmeve edhe nga ana e organizatave kriminale, dhe se gjendja po bëhet gjithnjë e më shqetësuese sidomos përballë rrezikut të sulmeve terroriste

[157]Në nenin 52(1) të Kartës thuhet se 'Çdo kufizim në ushtrimin e të drejtave dhe lirive të njohura nga Konventa duhet të parashikohet në ligj dhe të respektojë thelbin e këtyre të drejtave dhe lirive. Ato mund t'i nënshtrohen kufizimeve të parimit të proporcionalitetit, vetëm nëse këto janë të nevojshme dhe plotësojnë realisht synimet e interesave të përgjithshme të njohura nga Bashkimi Evropian ose i përgjigjen nevojës për mbrojtjen e të drejtave dhe lirive të të tjerëve'.

[158] Paragrafi 69 i Vendimit.

kundër sistemeve të informimit që janë pjesë e infrastrukturave kritike të shteteve anëtare[159].

Gjatë mbledhjes së Këshillit Evropian në Lisbonë në Mars të vitit 2000, Këshilli nënvizoi rëndësinë që merr tranzicioni drejt një ekonomie konkurruese, dinamike dhe të bazuar tek njohja. Ai ftoi Këshillin dhe Komisionin të hartonin një plan global veprimi për të shfrytëzuar të gjitha mundësitë. Ky plan veprimi, i hartuar nga Këshilli dhe Komisioni dhe i miratuar nga Këshilli Evropian i Feiras në Qershor 2000, përmban veprime që synojnë forcimin e sigurisë të mjeteve dhe parashikon zhvillimin e një qëndrimi të bashkërënduar dhe koherent përballë kriminalitetit informatik, parashikuar për në fund të vitit 2002. Vendimi-kuadër në lidhje me urdhrin evropian të ndalimit, aneksi i Konventës Europol dhe vendimi i Këshillit për krijimin e Eurojust-it përmbajnë referencat për kriminalitetin informatik, i cili duhet përkufizuar në një mënyrë akoma më të saktë. Në kontekstin e këtyre instrumenteve, kriminaliteti informatik përbëhet nga sulmet kundër sistemeve të informacionit ashtu siç përkufizohen nga ky vendim- kuadër, i cili do të bëjë të mundur të arrihet një nivel shumë më i lartë përafrimi të elementëve përbërës të këtyre shkeljeve.

Në komunikatën e tij COM (2007)[160], komisioni sqaron se për të përballuar me sukses sfidën e sigurisë, me të cilën ndeshet shoqëria e informatikës, Komuniteti Evropian ka përgatitur një qëndrim të trefishtë në lidhje me sigurinë e rrjeteve dhe të informacionit: masa të posaçme në lidhje me sigurinë e mjeteve dhe informacionit, një kuadër rregullues për komunikacionet elektronike dhe luftën kundër kiberkriminalitetit, por duhet gjithashtu të parashikohet sa më shpejt miratimi i instrumenteve legjislative specifike për luftën kundër kiberkriminalitetit. Një problem i veçantë, i cili e bën të nevojshme miratimin e një rregulloreje është ai që ka të bëjë me krimet informatike të kryera në kuadrin e përvetësimit të paligjshëm të identitetit.

[159]Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (based on proposal COM(2010) 517 final of 30/09/2010 - accompanying impact assessment and its summary).

[160]Commission Communication to the European Parliament and the Council, of 11 September 2007, on Public-Private Dialogue in Security Research and Innovation.

Me fjalën "përvetësim të identitetit" kuptohet në përgjithësi përdorimi i të dhënave të identitetit personal, psh, numri i një karte krediti, për kryerjen e veprave të tjera penale. Në shumicën e shteteve anëtare është mjaft e vështirë që autori i veprës të procedohet për mashtrim ose për një vepër tjetër penale, dhe mjaft rrallë që ai të procedohet për përvetësim të identitetit dhe kjo sepse mashtrimi konsiderohet si një vepër më e rëndë. Megjithatë përvetësimi i identitetit nuk përbën akoma një figurë krimi në të gjitha shtetet. Në praktikë do të ishte më e lehtë të provohej ky krim se sa ai i mashtrimit nëse përvetësimi i identitetit do të konsiderohej si vepër penale nga të gjitha shtetet.

Ky vendim-kuadër në lidhje me sulmet kundër sistemeve të informimit plotëson gjithashtu vendimin-kuadër për luftën kundër terrorizmit, i cili mbulon aktet terroriste që i shkaktojnë dëme të rënda një infrastrukture të caktuar, përfshirë edhe një sistem informatik, dhe që vë në rrezik jetën njerëzore ose sjell humbje të rënda ekonomike. Këto instrumente, të perdorura së bashku, do të garantojnë që shtetet anëtare të Bashkimit Evropian të kenë një legjislacion penal efikas në luftën kundër kiber kriminalitetit dhe të përforcojnë bashkëpunimin ndërkombëtar kundër terrorizmit.

Objektivat e këtij vendimi-kuadër janë: i) të garantojë që sulmet kundër sistemeve informatike të marrin dënime efektive, proporcionale dhe riedukuese me anë të përafrimit të rregullave të së drejtes penale, ii) të përmirësojë dhe të nxisë bashkëpunimin gjyqësor duke shmangur vështirësitë e mundshme.

Në nenin e tij të parë vendimi-kuadër përkufizon sistemin informatik si «çdo pajisje e izoluar ose çdo grup pajisjesh të lidhura ose në lidhje me njëra-tjetrën që bëjnë të mundur, në sajë të një programi, trajtimin e automatizuar të të dhënave informatike, të ruajtura, të punuara, të marra ose të transmetuara nga këto pajisje me qëllim funksionimin, përdorimin, mbrojtjen dhe mirëmbajtjen e tyre».

Të dhënat informatike përkufizohen në nenin l b, si «çdo paraqitje informacioni ose nocionesh në një formë të tillë që të mund të trajtohen nga një sistem informatik, përfshirë këtu edhe një program që i mundëson këtij të fundit të kryejë një funksion të caktuar»[161].

[161]Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (based on proposal COM(2010) 517 final of 30/09/2010 - accompanying impact assessment and its summary).

Veprat penale të dënueshme sipas neneve 2 dhe 3 të këtij vendimi-kuadër janë: i) hyrja e paligjshme në sistemet informatike, të paktën për ato raste kur veprimi nuk është pa pasoja, ii) cënimi i paprekshmërisë së një sistemi duke futur, transmetuar, dëmtuar, fshirë, ndryshuar, hequr ose bërë të papërdorshme të dhëna të ndryshme informatike, iii) cënimi i paprekshmërisë të të dhënave me anë të fshirjes, dëmtimit, ndryshimit, ose heqjes nga sistemi. Neni 4 parashikon se veprimet duhettë jenë bërë me dashje. Në përgjithësi, dënimet duhet të jenë efektive, proporcionale dhe riedukuese.

7. Roli i aktorëve kryesorë europianë në luftën kundër krimit kibernetik

7.1. Europol - Zyra e Policisë Evropiane

Bashkëpunimi ndërkombëtar policor në fushën penale është një nga mënyrat me efiçente për parandalimin dhe goditjen me efikasitet të krimit të organizuar dhe krimit kibernetik. Shtetet e ndryshme të botës kanë kohë që janë ndërgjegjësuar me faktin se krimi i organizuar dhe krimi kibernetik nuk mund të luftohet dhe aq më pak të mposhtet, duke luftuar vetëm. Pikërisht ky ndërgjegjësim i hapi rrugë në vitet '60, bashkëpunimit të policive mes gjashtë shteteve anëtare të BE-së, i quajtur TREVI, i cili me hyrjen në fuqi të Traktatit të Bashkimit Europian dhe shtimit të mëtejshëm të shteteve anëtare të Bashkimit, si dhe me shfaqjen e nevojës për në bashkëpunim më të përforcuar në kuadrin e hapjes së kufinjve me anë të marrëveshjes së Shengenit, u shndërrua në EUROPOL, pra në Policinë e Bashkimit Europian. EUROPOL, është një strukturë e krijuar në bazë të një konvente, bazuar në nenin3 të Traktatit të Bashkimit Europian, hartuar në 18 Korrik 1995[162]. Struktura e EUROPOL-it dhe konventa e nxjerrë për ta formalizuar atë, u krijuan duke patur parasysh problemet imediate që paraqiste terrorizmi, dhe krimi i organizuar.

Duke qënë se kriminaliteti është një aktivitet dinamik, format më të cilat ai paraqitet janë gjithmonë në ndryshim, dhe pikërisht për këtë shkak Konventa ka lënë një hapësirë për format që nuk janë përfshirë në të, të cilat Europoli mund ti ndjekë me miratim nga Këshilli i Europës, sipas procedurës së caktuar. Në këtë aspekt edhe lufta kundër krimit kibernetik është një fushë prioritare për Europolin.

[162]Vullenti për të krijuar Europolin, ka qenë i pranishëm ne Europë që prej vitit 1991, kur Kancelari Gjerman, Helmut Josef Michael Kohl, parashtroi nevojën për të krijuar një organ të tillë.

Për të lehtësuar punën e Europol-it, të gjitha vendet anëtare, madje edhe disa shtete të treta, kanë ngritur stukturat e tyre dhe kanë vënë në dispozicion personel që të punojë me Europolin. Numri i personelit të gatshëm ndryshon sipas vendit, dhe shkon nga njësi më të mëdha në një numër të kufizuar individësh specifike. Por ky rrjet është zhvilluar me kalimin e kohës. Një qendër operative është ngritur pranë Drejtorive të Europolit, e cila koordinon të gjithë informacionin që kalon nga i ashtuquajturi sistemi i informacionit të sigurtë në shkëmbimin e aplikimeve informatike. Aktiviteteti i Europol-it në luftën kundër krimeve kibernetike bazohet nëdisa objektiva kryesore, si më poshtë:

a) Të lehtësojë shkëmbimin e informacionit midis shteteve anëtare;
b) Të përfitojë, ndërlidhë dha analizojë informacionin;
c) Të njoftojë autoritetet kompetente pa vonesë, për informacione që kanë lidhje me to dhe të bëjë indentifikimin e lidhjeve mes tyre;
d) Të ndihmojë hetimet në shtete anëtare, duke siguruar të gjithë informacionin e nevojshëm;
e) Të mbajë një sistem të kompjuterizuar për të grumbulluar të dhëna;
f) Të zhvillojë njohuritë e ekspertëve në lidhje me procedurat hetimore të autoriteteve kompetente të shteteve anëtare, si dhe të sigurojë konsulencë mbi hetimet;
g) Të përgatisë raporte të përgjithshme për situatën konkrete;
h) Të trajnojë anëtarë të autoriteteve kombëtare;
i) Të organizojë dhe hartojë metoda teknike parandalimi dhe procedura investigative në fushën e krimeve kibernetike[163].

Si pengesë për bashkëpunimin më efikas të Europolit me policitë e shteteve përkatëse aktualisht paraqiten dallimet në kodet penale dhe ne kodet e procedurës penale, siç janë autorizimet e ndryshme të seksioneve të policive dhe shërbimeve informative. Këto pengesa veçanërisht janë të pranishme lidhur me çështjen se deri në çfarë kufiri aktiviteti joformal i policisë konsiderohet si fazë paraprake - operative, dhe kur fiton karakter të dhunës, siç është p.sh. përdorimi i mjeteve teknike me të cilat ndërhyhet në jetën private të njeriut. Këto pengesa e vështirësojnë zbulimin dhe ndëshkimin e autorëve të veprave

[163] https://www.europol.europa.eu/content/page/about-europol -17.

penale, prandaj këto pengesa duhet të evitohen sa me parë, ngaqë kriminaliteti nuk i njeh kufinjtë e shteteve[164].

7.2. ENISA- Agjencia e Bashkimit Evropian për Sigurinë e Rrjeteve dhe të Informacionit

Kjo agjenci është krijuar me qëllimin e forcimit të kapaciteteve të BE-së, të shteteve anëtare të saj, dhe të komunitetit të biznesit në parandalimin, trajtimin dhe qëndrimin ndaj problemeve të sigurisë së rrjeteve dhe të informacionit. Për arritjen e këtij objektivi, ENISA është projektuar si një qendër e ekpertizës në fushën e sigurisë së rrjeteve dhe informacioneve dhe fokusohet në nxitjen e bashkëpunimit midis sektorit publik dhe atij privat[165]. Detyrat kryesore të agjencisë janë:

a) këshillimi dhe asistimi i Komisionit Evropian dhe shteteve anëtare mbi çështje të sigurisë së informacionit dhe dialogu me përfaqësues të industrisë për trajtimin e problemeve të lidhura me sigurinë e produkteve hardware dhe software;
b) mbledhja dhe studimi i të dhënave mbi incidente të ndryshme të sigurisë që kanë prekur vendet evropiane dhe mbi rreziqet e reja që janë shfaqur;
c) promovimi i metodave të vlerësimit dhe menaxhimit të rrezikut me qëllim rritjen e kapaciteteve për t'u përballur me kërcënimet ndaj sigurisë së informacionit;
d) rritja e ndërgjegjësimit dhe e bashkëpunimit midis aktorëve të ndryshëm veprues në fushën e sigurisë së informacionit, duke zhvilluar dukshëm partneritetin sektor publik/privat me industrinë në këtë fushë.

7.3. Eurojust- Njësia Gjyqësore e Bashkëpunimit Evropian

Eurojust-i u krijua me një vendim të Këshillit Europian, i miratuar në vitin 2002. Eurojust është institucioni të cilit i është besuar forcimi i luftës kundër krimeve të rënda përmes bashkëpunimit më të ngushtë brenda Bashkimit Europian në fushën e zbatimit të ligjit. Eurojust-i është një institucion që bashkërendon aktivitetin e prokurorive kombëtare të shteteve anëtare dhe përbëhet nga 27 përfaqësues kombëtarë: gjyqtarë, prokurorë, dhe oficerë policie, të dërguar nga shtetet anëtare.

---

[164] Feasibility Study for a European Cybercrime Centre, pagg. 85-89, available at: RAND Europe URL: http://www.rand.org/randeurope.

[165] *Po Aty*, pagg. 93, available at: RAND Europe URL: http://www.rand.org/randeurope.

Ky institucion i përmbush detyrat e tij me ndihmën e një ose disa prej anëtarëve kombëtarë, ose duke vepruar në mënyrë kolegjiale. Për më tepër, çdo shtet anëtar mund të emërojë një ose më shumë korrespondentë kombëtarë, të cilët po ashtu, mund të shërbejnë si pika kontakti për rrjetin europian gjyqësor. Eurojust-i ka kompetencë që të hetojë dhe të procedojë në krimet e rënda, veçanërisht krimin e organizuar ose krimin ndërkufitar. Qëllimi i Eurojust-it është që të nxisë bashkëpunimin mes autoriteteve kompetente në shtetet anëtare, por edhe të lehtësojë ndihmën ligjore të ndërsjellë ndërkombëtare, si dhe t'u përgjigjet kërkesave për ekstradim ose urdhrave europianë të arrestit[166].

Eurojust-i kontribuon po ashtu, në hetimin e veprave penale edhe nëpërmjet analizave të kryera nga Europoli. Ka një mbivendosje në kompetencat e këtyre dy institucioneve në lidhje me hetimin e krimeve kompjuterike, mashtrimin dhe korrupsionin, pastrimin e produkteve të krimit, krimin ndaj mjedisit, si dhe pjesëmarrjen në një organizatë kriminale. Neni 85 TFBE (ish neni 31 TBE)[167] parashikon se misioni i EUROJUST është që të mbështesë dhe të forcojë koordinimin dhe bashkëpunimin midis strukturave kombëtare, pjesë të hetimit dhe proçedimit penal në lidhje me krimet e rënda që prekin dy ose më shumë shtete anëtare ose që kërkojnë proçedimin e përbashkët në bazë të operacioneve të përbashkëta dhe informacioneve që japin strukturat e shteteve dhe Europolit. Parlamenti Europian dhe Këshilli kanë të drejtë të miratojnë rregullore dhe të përcaktojnë strukturën e Eurojust-it si dhe fushën e veprimit dhe detyrat. Detyrat mund të përfshijnë:

a) nisjen e një hetimi penal si edhe propozimin për fillimin e proçedimit penal;
b) koordinimin e hetimeve dhe proçedimeve;
c) forcimin e bashkëpunimit gjyqësor, duke përfshirë zgjidhjen e konflikteve juridiksionale.

Kufizimet e kompetencave të Eurojust-it janë përfshirë në nenin 85(2) TBE[168], sipas të cilit aktet formale të bashkëpunimit gjyqësor do të realizohen nga autoritetet kombëtare kompetente.

[166] Feasibility Study for a European Cybercrime Centre, pagg. 90-93, available at: RAND Europe URL: http://www.rand.org/randeurope.

[167] Neni 85 TFBE (ish neni 31 TBE).

[168] Neni 85(2) TBE.

KAPITULLI IV: RREGULLIMI I KRIMIT KIBERNETIK NË SHQIPËRI NË KUADËR TË HARMONIZIMIT TË LEGJISLACIONIT TË BRENDSHËM ME ATË EUROPIAN

1. Legjislacioni shqiptar mbi krimet kibernetike, Ratifikimi i Konventës së Budapestit

Vitet e fundit Shqipëria ka punuar për vendosjen dhe implementimin e standardeve ndërkombëtare për luftën ndaj krimit të organizuar, pastrimit të parave dhe korrupsionit.

Në legjislacionin kombëtar funksionojnë mjaft ligje si: ligji për nënshkrimin elektronik, informacionin e klasifikuar shtetëror, mbrojtjen e të dhënave personale, komunikimin elektronik, përgjimin e telekomunikimeve, për librin, për shërbimin postar, etj.

Gjithashtu janë ndërrmarrë politika dhe janë miratuar dokumente dhe strategji që ndihmojnë në luftën kundër krimeve kompjuterike,ndër të cilat mund të përmendim: (1) Strategjinë Ndërsektoriale të Shoqërisë së Informacionit; (2) Dokumentin e politikave për komunikimet elektronike në RSH; (3) Dokumentin e politikave të zhvillimit të telekomunikacioneve në RSH; (4) Vendimet e Këshillit të Ministrave për miratimin e dokumenteve të politikave dhe strategjive, etj.

Disa prej ligjeve që ndihmojnë në sigurimin e sistemeve të shoqërisë së informacionit, janë paraqitur si më poshtë:

- Ligji Nr. 9880, datë.25.2.2008 "*Për nënshkrimin elektronik*";
- Ligji Nr. 9887, datë. 10.3.2008, "*Për mbrojtjen e të dhënave personale*";
- Ligji Nr. 9643, datë. 20.11.2006, i ndryshuar,"*Për prokurimet publike*", që realizon mundësinë e prokurimit elektronik;
- Ligji Nr. 9723, datë. 3.5. 2007, "*Për Qendrën Kombëtare të Regjistrimit*";
- Ligji Nr. 9918, datë. 19.5.2008, "*Për komunikimet elektronike në Republikën e Shqipërisë*";

Deri në ndryshimet e vitit 2008, nuk kanë qenë parashikuar vepra penale në fushën kompjuterike, edhe pse sistemet kompjuterike ishin bërë pjesë e shoqërisë shqiptare. Këtu përfshihet harmonizimi i legjislacionit kombëtar me atë ndërkombëtar për luftën kundër krimeve kibernetike[169].

[169]Denisa. A. (2010), "*Mbi disa ceshtje te se drejtes penale dhe procedural penale"*, Tirane, fq. .48.

Problematika që shtrohej në lidhje me ndëshkimin ndaj krimeve të kryera në hapësirën kibernetike nuk bazohej tek pasojat e natyrës fizike që mund të shkaktoheshin ndaj një sistemi kompjuterik, por bazohej në praktikat e paligjshme që mund të kryheshin kundër sistemeve kompjuterike ose nëpërmjet tyre.

Risitë që paraqiste fusha përkatëse dhe karakteristikat e veçanta të saj shtonin nevojën e padiskutueshme për një ndërhyrje normative e cila shtrinte fushën e zbatimit të ligjit penal edhe ndaj sjelljeve kriminale të ndodhura në hapësirën kibernetike.

Mënyra e konsumimit të këtyre veprave penale (modus operandi) ndryshonte në mënyrë thelbësore nga format tradicionale të krimit dhe si rrjedhojë, aplikimi i normave ekzistuese penale ndaj sjelljeve të paligjshme të realizuara nëpërmjet sistemeve kompjuterike rrezikonte ndjeshëm të cënonte parimin e taksivitetit.

Një arsye tjetër që shoqëroi përfshirjen e normave të reja juridiko-penale, lidhej me vullnetin e ligjvënësit për të përafruar legjislacionin shqiptar me legjislacionin e Bashkimit Evropian.

Lidhur me këtë, Republika e Shqipërisë me Ligjin Nr. 8888, datë 25.4.2002 (botuar në fletoren zyrtare nr. 18 faqe 18) ka ratifikuar "Konventën për Krimin Kibernetik", ndërsa në vitin 2004 është ratifikuar edhe protokolli shtesë i kësaj konvente. Konventa për Krimin Kibernetik është miratuar nga Komiteti i Ministrave të Këshillit të Evropës në Sesionin e 109 (më 8 Nëntor 2001) dhe u hap për nënshkrim në Budapest, më 23 Nëntor 2001, në Konferencën Ndërkombëtare për Krimin Kibernetik.

Në këtë drejtim mund të themi se dispozitat e përfshira rishtazi në Kodin Penal shqiptar në luftën kundër krimit kompjuterik janë në koherencë të plotë me Konventën e Këshillit të Evropës "*Mbi krimin kibernetik*".

Për më tepër, një qëndrim i tillë, nuk duhet interpretuar vetëm në funksion të synimit të përgjithshëm për përmbushjen e detyrimeve që lidhen me integrimin e Shqipërisë në familjen e madhe europiane, por edhe në funksion të një synimi praktik që lidhet me nevojën për krijimin e koncepteve uniforme dhe vendosjen e standardeve të përbashkëta të bashkëpumimit për të luftuar luftuar një fenomen me natyrë ndërkombëtare.

2. Krimi kibernetik si një vepër penale në legjislacionin e brendshëm

Për të reflektuar angazhimet e Shqipërisë në kuadër të Konventës së Krimit Kibernetik, Ministria e Drejtësisë ndërmori nismën për parashikimin e shtesave në Kodin Penal të Republikës së Shqipërisë dhe në Kodin e Procedurës Penale.

Këto nisma u finalizuan respektivisht me miratimin e ligjit nr. 10023, datë 27.11.2008[170] dhe nr. 10054, datë 29.12.2008[171]. Draftimi i këtyre ligjeve u bazua në një studim të gjerë krahasues të instrumenteve ndërkombëtare (Konventës dhe Protokollit), rekomandimeve të organizmave ndërkombëtarë dhe Agjencisë Kombëtare të Shoqërisë së Informacionit, si dhe të legjislacioneve penale të disa shteteve evropiane për këtë fushë.

Gjatë procesit të hartimit të këtij projektligji, i cili është mbështetur në përvojat legjislative dhe në përmbajtjen e konventës, nisur dhe nga terminologjia specifike që mbart kjo fushë, është mbajtur parasysh që formulimi i dispozitave të jetë sa më i thjeshtë dhe i kuptueshëm për operatorët e së drejtës dhe qytetarët, duke qenë në koherencë me terminologjinë e përdorur në konventë, si dhe me mënyrën e ndërtimit dhe strukturimit të dispozitave në Kodin Penal.

Nisur nga specifika e veçantë teknike që ka fusha e teknologjisë së informacionit, kur nga operatorët e drejtësisë rezulton se kuptimi i një koncepti teknik është i paqartë në dispozitë, sugjerohet që të bëhet referimi tek përkufizimet ose dispozita e tjera të konventës, e cila është pjesë e sistemit të brendshëm juridik në përputhje me nenin 122 të Kushtetutës.

Në fakt, Kodi Penal, përpara shtesave të prezantuara me ligjin nr. 10023/2008, parashikonte në nenin 192/b1 të tij si vepër penale ndërhyrjen në transmetimet kompjuterike. Në vlerësimin e ekspertëve shqiptarë dhe të huaj, qoftë me eksperiencë juridike apo tekniko-informatike, kjo dispozitë ishte e karakterit të përgjithshëm dhe sintetik.

---

[170]Ligjit nr. 10023, datë 27.11.2008 për disa shtesa në ligjin nr. 7895 date 27.01.1995 "Kodi Penal i Republikës së Shqipërisë", (botuar në fletoren zyrtare nr. 2 faqe 2, të vitit 1995).

[171]Ligjit nr. 10023 datë 27.11.2008 (botuar në fletoren zyrtare nr.190 faqe nr. 9395, të vitit 2008). Në këtë ligj janë parashikuar dispozita që parashikojnë sanksione për veprime të kundraligjshme të kryera nëpërmjet kompjuterave, pajisjeve elektronike, rrjeteve elektronike etj, ku veçanërisht më të përhapurat do ti ilustojmë edhe me shembuj nga praktika gjyqësore.

Rrjedhimisht, përmbajtja e saj nuk i përgjigjej dhe nuk mbulonte në mënyrë të mjaftueshme sferën e atyre veprimeve, të cilat për nga natyra e tyre përmbajnë tipare dhe karakteristika objektive të dallueshme nga njëra-tjetra.

Për këtë arsye, si dhe nisur nga fakti se Konventa Evropiane parashikon për shtetet palë një sërë dispozitash penale lidhur me krimin kibernetik për t'u transpozuar në legjislacionin e brendshëm, doli e nevojshme parashikimi i dispozitave të reja, qoftë të karakterit material, qoftë të karakterit procedurial.

Duke i konsideruar veprat penale në fushën e kibernetikës të karakterit të veçantë në drejtim të vendit të kryerjes së veprës penale dhe të mundësisë së ardhjes së pasojës në vende relativisht distante nga kryerja e veprimeve, është shtuar një pikë e veçantë në normën penale që rregullon zbatimin e ligjit penal shqiptar për veprat penale të kryera nga shtetasit e huaj.

Në nenin 7 është shtuar gërma "j", në të cilën përcaktohet se "***shtetasit e huaj mbajnë përgjegjësi sipas ligjit penal shqiptar për kryerjen jashtë territorit shqiptar e veprave penale në fushën e teknologjisë së informacionit"*** në një prej dy rasteve alternative:

1. kur i janë shkaktuar dëm interesave të shtetit shqiptar; ose
2. kur i janë shkaktuar dëm interesave të shtetasve shqiptarë.

Neni 7 përbën një normë të vendosur në Pjesën e Përgjithshme të Kodit Penal, rrjedhimisht ai mund të gjejë zbatim për të gjitha veprat penale në fushën e teknologjisë së informacionit të përcaktuara në Pjesën e Posaçme të Kodit Penal ose në ligje të veçanta që parashikojnë vepra penale.

Për ligjet e veçanta duhet vënë në dukje përmbajtja e paragrafit të dytë të nenit 1/a të Kodit Penal "legjislacioni penal përbëhet nga ky kod dhe ligje të tjera që parashikojnë vepra penale".

Veprat penale kibernetike përfshijnë veprat penale që kryhen kundër ose nëpërmjet sistemeve dhe programeve kompjuterike që përmbajnë të dhëna kompjuterike. Ligji Nr. 10023/2008 shton në vijim si vepra penale ato sjellje, (të përcaktuara si të tilla nga Protokolli i Konventës për Krimin Kibernetik) që i referohen shpërndarjes kompjuterike të materialeve që kanë të bëjnë me genocidin, krimeve kundër njerëzimit, racizmin dhe ksenofobinë.

Nisur nga specifika e veçantë teknike që ka fusha krimeve kibernetike, kur nga operatorët e drejtësisë rezulton se kuptimi i një koncepti teknik është i paqartë në dispozitë, sugjerohet që të bëhet referimi tek përkufizimet ose dispozita e tjera të konventës, e cila është pjesë e sistemit të brendshëm juridik në përputhje me nenin 122 të Kushtetutës. Vlen të theksohet këtu se legjislatori nga njëra anë, ka synuar të disiplinojë materien përkatëse në sajë të përfshirjes së normave të reja penale, dhe nga ana tjetër, nuk ka bërë një shpjegim të koncepteve me natyrë teknike, duke e lënë kështu në dorë të doktrinës dhe praktikës gjyqësore detyrën e përcaktimit të termave në fjalë, si psh. sistem kompjuterik, të dhëna komjuterike, program komjuterik, etj.

Zgjidhja normative që ka dhënë ligjvënësi shqiptar në këtë drejtim ka qenë ajo përfshirjes së dispozitave të reja në tekstin e Kodit Penal në lidhje me veprat penale në fushën kompjuterike. Theksojmë gjithashtu se dispozitat që trajtojnë këto vepra penale nuk janë përfshirë në një titull të veçantë të kodit penal, por i janë bashkangjitur dispozitave të veprave të tjera ekzistuese me të cilat paraqesin më shumë ngjashmëri.

Me sa duket, ligjvënësi ka vlerësuar se veçantia që paraqet fusha përkatëse nuk përbën arsye të mjaftueshme për t'i ndarë veprat penale kompjuterike në një titull të veçantë. Për më tepër, kriteri i përdorur përgjithësisht nga ana e ligjvënësit për klasifikimin e veprave penale në krerë dhe seksione të veçanta brenda Kodit Penal bazohet në objektin juridik të cënuar, ndërkohë që format e reja të krimit kibernetik paraqisnin risi përsa i përket mënyrës apo mjetit të përdorur për kryerjen e tyre si dhe objektit material të cënuar, por objekti juridik i tyre mbetej sërisht po i njëjti.

Në pjesën në vijim të punimit paraqitet një analizë e mirëfilltë juridiko-penale e rrethanave të zbatimit të përgjegjësisë penale sipas dispozitave në fjalë. Ky shpjegim synon të nxjerrë në pah rreziqet që çdo idivid, biznes privat apo agjenci qeveritare duhet të marrë parasysh nga momenti që vendos të përdorë shërbimet e një rrjeti kompjuterik të ndërlidhur e në vazhdim.

Në fushën e krimeve kibernetike vlen të theksohet se vjedhjet nëpërmjet internetit janë mjaft të përhapura në Republikën e Shqipërisë. Në vendin tonë së fundmi po krijohet edhe praktika gjyqësore lidhur me interpretimin e mashtrimit kompjuterik[172].

[172]Zhilla.F- Canaj.E, Revista Polis, "*Pirateria ne internet rrezik edhe per shoqerine Shqiptare*", fq.43.

2.1. Shpërndarja kompjuterike e materialeve pro genocidit ose krimeve kundër njerëzimit

Ligji Nr. 10023/2008 shton në vijim si vepra penale ato sjellje, (të përcaktuara si të tilla nga Protokolli i Konventës për Krimin Kibernetik) që i referohen shpërndarjes kompjuterike të materialeve që kanë të bëjnë me genocidin, krimeve kundër njerëzimit, racizmin dhe ksenofobinë.

Konkretisht, është shtuar në Pjesën e Posaçme të Kodit Penal neni 74/a[173] "***shpërndarja kompjuterike e materialeve pro genocidit ose krimeve kundër njerëzimit***".

Me anë të kësaj vepre synohet që të ndëshkohen mbrojtësit e personave dhe ngjarjeve historike që kanë të bëjnë me krime kundër njerëzimit, duke injoruar sakrificën, vuajtjen dhe kujtimin e njerëzve qe ishin objekt i krimeve ndërkombëtare.

Objekt i krimit janë marrëdhëniet juridike te vendosura me ligj në Republikën e Shqipërisë që kanë të bëjnë me mbrojtjen e jetës, shëndetit dhe të drejtave e lirive të publikut të mbrojtura posaçërisht me legjislacionin penal kundër veprimeve kriminale.
Për shkak të objektit që merr në mbrojtje parashikimi i kësaj vepre penale, ajo është pozicionuar në Kreun I "*Krime kundër njerëzimit*". Nisur nga rrezikshmëria e kësaj vepre ajo është parashikuar si krim dhe për këtë fakt sanksioni penal është parashikuar të jetë tre gjer në gjashtë vjet.

Nga ana objektive, krimi kryhet në këto forma dhe mënyra të specifikuara në nenin 74/a:

a. Ofrimi në publik ose shpëndarja publikut e materialeve që përbëjnë genocid ose krime kundër njerëzimit, pra ka karakter masiv;
b. Ofrimi ose shpërndarja e materialeve realizohet me mënyra dhe mjete të posaçme, d.m.th. nëpërmjet sistemeve kompjuterike;
c. Këto materiale mohojnë, minimizojnë, miratojnë ose justifikojnë akte, që përbëjnë genocid ose krim kundër njerëzimit.

---

[173] 74/a "***shpërndarja kompjuterike e materialeve pro genocidit ose krimeve kundër njerëzimit***"
"*Ofrimi në publik ose shpërndarja e qëllimshme publikut, nëpërmjet sistemeve kompjuterike, e materialeve, që mohojnë, minimizojnë, në mënyrë të ndjeshme, miratojnë ose justifikojnë akte, që përbëjnë genocid ose krim kundër njerëzimit, dënohet me burgim tre deri në gjashtë vjet.*"

Për ta konstatuar krimin e kryer nuk kërkohet ardhja e domosdoshme e pasojave, këtu është fjala për pasoja morale, psikologjike dhe jomateriale.

Subjekt i krimit mund të jetë çdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm, i cili ofron ose i shpërndan materiale publikut, që përbëjnë genocid ose krim kundër njerëzimit, nëpërmjet sistemeve kompjuterike.

Konceptet e përdorura në këtë normë dhe me interes për zbatimin në praktikë janë:

1. Ofrimi ose shpërndarja e materialeve në publik. Ky formulim nënkupton që shpërndarësi i materialit mund të jetë burimi fillestar ose transmetues i dytë i materialeve. Nga ana tjetër, kërkohet që ky veprim t'i adresohet një numri personash që konsiderohet 'publik'. Jurisprudenca gjyqësore shqiptare ka pranuar se 'publik' përfshin një grup personash mbi shtatë persona, megjithatë ky koncept mbetet i hapur për t'u elaboruar;
2. Ofrimi ose shpërndarja e qëllimshme e materialeve. Në këtë pjesë konstatohet që kjo vepër penale kërkon nga ana subjektive ekzistencën e fajit në formën e dashjes në kryerjen e veprimit të ofrimit apo të shpërndarjes së materialeve, pra nga ana subjektive, krimi kryhet me dashje direkte dhe me qëllim te caktuar. Motivet nuk kanë rëndësi për cilësimin e krimit[174].
3. Mjeti i ofrimit ose i shpërndarjes së materialeve të jetë sistem kompjuterik. Përkufizimi i sistemit kompjuterik është dhënë në Konventën për Krimin Kibernetik, sipas të cilës "sistem kompjuterik" do të thotë çdo lloj pajisje apo grup i ndërlidhur ose pajisje të lidhura, një ose më shumë prej të cilave, vazhduese të një programi kryejnë proçesime automatike të të dhënave. Përbën sistem komjuterik aparatura që përbëhet nga një hardware dhe një software, i zhvilluar për proçesimin automatik të të dhënave dixhitale. Sistemi kompjuterik mund të përfshijë pajisjet për inputin, outputin dhe magazinimin. Sistemi mund të jetë i pavarur, por ai mund të jetë i lidhur në një rrjet me aparatura të ngjashme. Proçesimi automatik i të dhënave nënkupton se të dhënat në sistemin kompjuterik operohen nga një program kopmpjuterik pa ndërhyrjen e drejtpërdrejtë të njeriut.

[174]Neni 74/a të Kodit Penal.

Në ndryshim nga sistemi kompjuterik, program kompjuterik është një set udhëzimesh/ instruksionesh që mund të ekzekutohen nga kompjuteri për të arritur një qëllim të dëshiruar. Një kompjuter mund të performojë disa programe kompjuterike. Ndërsa rrjeti është një ndërlidhje midis dy ose më shumë kompjuterash. Lidhja mund të jetë tokësore (me tel ose kabëll) ose Wireless (radio, infra të kuqe ose satelit). Por lidhja mund të jetë edhe në të dyja mënyrat. Mbulimi i rrjetit mund të jetë gjeografikisht i vogël ose i madh, por vetë rrjetet mund të jenë të ndërlidhura me njëra-tjetrën. Për ilustrim, interneti është një rrjet global që përbëhet nga shumë rrjete të ndërlidhura, që përdorin të njëjtat protokolle. Sistemet kompjuterike mund të jenë të lidhura në rrjet si pika fundore ose si mjete për të ndihmuar komunikimin në rrjet. Ajo që është thelbësore është shkëmbimi i të dhënave në rrjet.

4. Përmbajtja e materialeve të tregojë qëndrimin pro të autorit të veprës penale ndaj genocidit ose krimeve kundër njerëzimit. Përkufizimet e genocidit dhe të krimeve kundër njerëzimit jepen në nenet 73 e 74 të Kodit Penal[175], ndaj shtjellimi i tyre do të ishte i tepërt. Qëndrimi pro genocidit apo krimeve kundër njerëzimit, si element i anës subjektive, nxirret duke ndërlidhur veprimin e kryer me dashje me përmbajtjen e materialeve që mohojnë, minimizojnë në mënyrë të ndjeshme, miratojnë ose justifikojnë genocidin apo krimet kundër njerëzimit. Nëse mohimi, miratimi apo justifikimi i akteve të genocidit ose krimeve kundër njerëzimit është lehtësisht i kuptueshëm, tek 'minimizimi' ka një lloj vlerësimi subjektiv të vështirë për t'u matur. Për këtë shkak, ligjvënësi ka parashikuar që minimizimi duhet të jetë në mënyrë të ndjeshme, pra i dukshëm.

2.2. Kanosja me motive racizmi dhe ksenofobie nëpërmjet sistemit kompjuterik

Një vepër tjetër penale është ajo e shtuar në nenin 84/a[176] "***kanosja me motive racizmi dhe ksenofobie nëpërmjet sistemit komputerik***". Me anë të kësaj dispozite synohen që të mbrohet jeta dhe shëndeti i personave të cilët i përkasin një etnie, kombësie, race apo feje të caktuar, në përputhje kjo me dispozitat kushtetuese, si dhe me instrumentet ndërkombëtare të të drejtave të lirive themelore të njeriut.

[175]Nenet 73-74 te Kodit Penal

[176]Neni 84/a të Kodit Penal**- Kanosja me motive racizimi dhe ksenofobie nëpërmjet sistemit kompjuterik**
"*Kanosja serioze pë vrasje ose plagosje të rëndë, që i bëhet një personi, nëpërmjet sistemeve kompjuterike, për shkak përkatësie etnike, kombësie, race apo feje, dënohet me gjobë ose me burgim deri në tre vjet*.

Për shkak të objektit që merr në mbrojtje, kjo dispozitë është pozicionuar në Kreun II të Pjesës së Posaçme të Kodit Penal "Vepra penale kundër jetës". Krime kundër jetës", në Seksionin I "Krime kundër jetës të kryera me dashje" dhe me konkretisht objekt i krimit janë marrëdhënie juridike të vendosura për të mbrojtur jetën dhe shëndetin e personit që i përket një etnie, kombësie, race, apo feje të caktuar. Në kuptimin e ngushtë, "racizmi" ndryshon nga "ksenofobia". Racizmi bazohet në dallimin racor, ndërsa ksenofobia bazohet në dallimin për shkak të qënies i huaj. Veç motivit, figura e kanosjes cilësohet në këtë dispozitë edhe për shkak të mjetit të kryerjes së veprës penale nëpërmjet sistemit komjuterik, për të cilin vlejnë shpjegimet e dhëna mbi nenin 74/a[177].

Nisur nga paraqitja e cilësuar me dy rrethana të kanosjes, të cilat janë tregues të një rrezikshmërie më të lartë se sa kanosja në formën e thjeshtë, ajo është parashikuar si krim dhe për këtë fakt sanksioni penal është parashikuar të jetë me gjobë ose me burgim gjer në tre vjet.

Nga ana objektive, krimi kryhet me veprime aktive kanosje serioze nëpërmjet sistemeve kompjuterike, kanosja është serioze për vrasje ose plagosje të rëndë.

Subjekt i krimit mund të jetë çdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm. **Nga ana subjektive**, krimi kryhet me dashje direkte dhe per motive racizmi ose ksenofobie.

2.3.Shpërndarja e materialeve raciste ose ksenofobike nëpërmjet sistemit kompjuterik dhe fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik

Në vijim, ligji nr. 10023/2008 përcakton si vepra penale "***shpërndarja e materialeve raciste ose ksenofobike nëpërmjet sistemit kompjuterik***" (neni 119/a[178]) dhe "***fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik***"(neni 119/b[179]).

[177]Neni74/a i K. Penal.

[178]Neni 119/a, **Shpërndarja e materialeve raciste ose ksenofobike nëpërmjet sistemit kompjuterik**
Ofrimi në publik ose shpërndarja e qëllimshme publikut, nëpërmjet sistemeve kompjuterike, e materialeve me përmbajtje raciste ose ksenofobike përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim deri në dy vjet.

[179]Neni 119/b, **Fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik**
Fyerja e qëllimshme publike, nëpërmjet sistemit kompjuterik, që i bëhet një personi, për shkak të përkatësisë etnike, kombësisë, racës apo fesë, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim deri në dy vjet.

Qëllimi i këtyre dispozitave është mbrojtja e dinjitetit dhe personalitetit të personave të cilët i përkasin një etnie, kombësie, race apo feje të caktuar. Për këtë shkak ato janë pozicionuar në Kreun II të Pjesës së Posaçme të Kodit Penal "Vepra penale kundër jetës. Krime kundër jetës", në Seksionin VIII"Vepra penale kundër moralit dhe dinjitetit".

Në të dyja këto vepra penale gjenden konceptet "sistem kompjuterik" dhe "motive raciste ose ksenofobie", të cilat janë rrethana që i cilësojnë këto dy vepra penale në dy drejtime:

1. Në drejtim të mjetit me të cilin kryhet vepra penale 'sistem kompjuterik', si pjesë e anës objektive të figurës së veprës penale; dhe
2. Në drejtim të motivit 'racor ose ksenofobik', si pjesë e anës subjektive.

Të dyja veprat për nga rrezikshmëria e ulët që paraqesin janë konsideruar si kundërvajtje penale duke parashikuar për të dyja si sanksion një masë dënimi më gjobë ose me burgim gjer në dy vjet.

Objekti i figurës së vepres penale "***shpërndarja e materialeve raciste ose ksenofobike nëpërmjet sistemit kompjuterik***" është objekt i posaçëm, pra janë marrëdhëniet juridike të vendosura për të siguruar ndjenjën e dinjitetit personal të personave që u përkasin racave të tjera.

Nga ana objektive, figura e veprës penale kryhet me anë të ofrimit ose të shpërndarjes publikut me anë të sistemeve kompjuterike të materialeve me përmbajtje raciste ose ksenofobike. Kjo formë ka karakter masiv dhe përmbajtja e këtyre materialeve ka karakter fyes, poshtërues, ksenofobike, përçmuese, frikësuese për personat e racave të tjera.

Subjekt i figurës së veprës penale mund të jetë çdo person që ka mbushur moshën dhe është i përgjegjshëm, i cili ofron ose shpërndan materiale me përmbajtje raciale ose ksenofobike, publikut. **Nga ana subjektive** kjo vepër kryhet me dashje direkte dhe me qëllim i cili është i posaçëm, racist ose ksenofobik.

Ndërsa **objekti** i veprës penale "***Fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik",*** është gjithashtu objekt i posaçëm, sepse ka të bëjë me nderin e dinjitetin e personave të veçantë që u përkasin një race, kombësie, etnie apo feje të caktuar.

Nga ana objektive vepra penale kryhet me anë të sistemit kompjuterik, fyerjes publikisht, pra ka karakter masiv. **Subjekt** i veprës penale të fyerjes mund të jetë çdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm.

Nga ana subjektive kjo vepër kryhet me dashje direkte ndaj një personi për motive racizmi ose ksenofobie.

Përsa i takon ***fyerjes me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik***, duhet vënë në dukje që me ligjin nr. 10054, datë 29.12.2008 "Për disa shtesa dhe ndryshime në Kodin e Proçedurës Penale", është parashikuar që në nenin 59 të Kodit të Proçedurës Penale ndër veprat penale që ndiqen me ankim të të dëmtuarit akuzues të jetë edhe fyerja me motive racizmi e ksenofobie (neni 119/b). Kjo shtesë ka patur si qëllim për të harmonizuar shtesat në Kodin Penal dhe për të ndjekur sistemin e Kodit Penal, i cili veprat penale mbi fyerjen ndaj një personi konkret i përfshin në rrethin e çështjeve që ndiqen vetëm me ankimin e të dëmtuarit akuzues, i cili edhe mund ta tërheqë atë gjatë proçedimit (sipas parashikimeve të nenit 284 të K.Pr.Penale)[180].

2.4. Mashtrimi kompjuterik

Një vepër tjetër penale është ajo e nenit 143/b[181] të Kodit Penal "***mashtrimi kompjuterik***". Me anë të kësaj dispozite synohet që të mbrohet pasuria e personave nga ndërhyrjet kompjuterike që u bëhet sistemeve të tyre. Me revolucionin teknologjik, mundësitë për kryerjen e një krimi të tillë, që përfshin edhe mashtrimin në kartat e kreditit, janë shumëfishuar. Pasuritë që administrohen në sistemet kompjuterike (fonde elektronike apo para të depozituara) janë bërë shenjestër e manipulimeve. Këto krime mund të kryhen nëpërmjet manipulimeve të hedhjes së të dhënave, ku hidhen të dhëna të pasakta ose nëpërmjet manipulimit të programeve dhe interferencave të tjera. Qëllimi i këtij parashikimi është kriminalizimi i çdo manipulimi në rrjedhën e proçesimit të të dhënave me synimin për të përfituar një transferim të paligjshëm të pasurisë dhe duke shkaktuar një pakësim të pasurisë së tjetrit.

---

[180]Neni 284 të K.Pr.Penale.

[181] Neni 143/b- **Mashtrimi kompjuterik**

Futja, ndryshimi, fshirja ose heqja e të dhënave kompjuterike apo ndërhyrja në funksionimin e një sistemi kompjuterik, me qëllim për t'i siguruar vetes apo të tretëve, me mashtrim, një përfitim ekonomik të padrejtë apo për t'i shkaktuar një të treti pakësimin e pasurisë, dënohen me burgim nga gjashtë muaj deri në gjashtë vjet dhe me gjobë nga 60 000 (gjashtëdhjetë mijë) lekë deri në 600 000 (gjashtëqind mijë) lekë.

Po kjo vepër, kur kryhet në bashkëpunim, në dëm të disa personave, më shumë se një herë ose kur ka sjellë pasoja të rënda materiale, dënohet me burgim nga pesë deri në pesëmbëdhjetë vjet dhe me gjobë nga 500 000 (pesëqind mijë) lekë deri në 5 000 000 (pesë milionë) lekë.

Meqë objekti kryesor i marrë në mbrojtje nga kjo dispozitë janë marrëdhëniet juridike të vendosura në sferën e sigurisë së të drejtës së pronësisë private ose publike të shtetit të mbrojtura nga legjislacioni penal nga veprimet ose mosveprimet kriminale, kjo dispozitë është pozicionuar në Kreun III të Pjesës së Posaçme "Vepra penale kundër pasurisë dhe në sferën ekonomike", në vjedhjet e cilësuara. "Ndryshim" i të dhënave nënkupton modifikimin e të dhënave ekzistuese, "fshirje" nënkupton shkatërrimin e të dhënës, duke e bërë atë të panjohur, "heqje" nënkupton çdo veprim që parandalon ose përfundon disponueshmërinë e të dhënës personit që ka akses. Për të siguruar që të mbuloheshin të gjitha manipulimet e mundshme, krahas elementëve: 'futja', 'ndryshimi', 'fshirja' ose 'heqja', teksti i kësaj norme përmban edhe fjalët 'ndërhyrja në funksionimin e një sistemi komjuterik' që tregon një veprim të përgjithshëm.

Manipulimet kompjuterike përbëjnë vepër penale nëse si rezultat i tyre zotëruesi i një pasurie pëson një pakësim të pasurisë së tij dhe nëse autori i veprës penale e kryen veprimin me dashje. Termat 'përfitim ekonomik' dhe 'pakësim i pasurisë' përfshijnë që nga paratë deri tek të drejtat e kredive, letrave me vlerë. Sigurisht, që për konceptin e ngushtë të 'mashtrimit', vlen edhe neni 143[182] i Kodit Penal, sipas të cilit mashtrimi përbën vjedhje të pasurisë në dy forma:

1. Nëpërmjet gënjeshtrës; ose
2. Nëpërmjet shpërdorimit të besimit.

Nga ana objektive krimi kryhet në forma dhe mënyra të ndryshme:

a. Me anë të futjes, ndryshimit, fshirjes ose heqjes së të dhënave kompjuterike;
b. Me anë të ndërhyrjes në funksionimin e një sistemi kompjuterik.

Në të gjitha rastet kërkohet ardhja e pasojave kriminale, dëmi material i shkaktohet një personi ose më shumë personave.

Subjekti i krimit mund të jetë çdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm.

Nga ana subjektive krimi kryhet me dashje te drejtëpërdrejtë për të marrë pasurinë e personit fizik, personit juridik apo shtetëror me qëllim për të nxjerrë përfitime materiale për vete ose për persona të tjerë.

[182] Neni 143/b i Kodit Penal.

Dashja dhe qëllimi në mashtrim lindin më përpara se të merret pasuria ose të drejtat e pasurisë. Gjithashtu parashikohen si rrethana të mëtejshme cilësuese në paragrafin e dytë bashkëpunimi, pasojat e rënda si dhe kryerja e kësaj vepre penale më shumë se një herë, të cilat shoqërohen me një rritje të marzheve të dënimit dhe konkretisht bëhen me burgim nga pesë gjer në pesëmbëdhjetë vjet dhe me gjobë nga pesëqindmijë gjer në pesë milionë lekë. Rrethanat cilësuese janë:

a) Me mashtrim të kryer në bashkëpunim kuptohet krimi kryer nga dy ose më tepër persona në marrëveshje midis tyre;
b) Me mashtrim te kryer në dëm të disa personave, kuptohet kur janë mashtruar dy, tre ose më tepër persona në kohë të ndryshme;
c) Me mashtrim të kryer më shumë se një herë, kuptohet veprimi i kryer për disa kohë kur personi ka mashtruar disa herë persona të ndryshëm, ose edhe të njëjtin person në interval kohor të shkurtër por nuk është dënuar për krimin e parë dhe vendimi nuk ka marrë formën e prerë;
d) Me mashtrim kur ka sjellë pasoja të rënda, kuptohet mashtrimi në përmasa të mëdha. Vlerësimi i pasojave të rënda bëhet në çdo rast konkret, sipas kritereve të pranuara nga Gjykata e Lartë.

Një koncept tjetër i ri që përdoret në këtë dispozitë (si edhe në disa vepra të tjera kompjuterike) është ai i të dhënave kompjuterike, të cilat duhet të jenë të përshtatshme për t'u procesuar.

Kjo do të thotë që e dhëna duhet vendosur në një formë të tillë që të mund të procedohet drejtpërdrejt nga sistemi kompjuterik, ajo mund të jetë në formë elektronike ose në formë tjetër direkt të procesueshme.

Mashtrimi kompjuterik përbën një vepër penale e cila paraqet një rrezikshmëri të lartë shoqërore dhe sjell përfitime të padrejta ekonomike për autorin e veprës penale si dhe dëme pasurore, që i shkaktohen personave të tjerë.

Për këtë arsye kjo vepër penale është konsideruar si krim dhe për këtë fakt sanksioni është parashikuar të jetë me burgim nga gjashtë muaj gjer në gjashtë vjet dhe me gjobë nga gjashtë dhjetë mijë gjer në gjashtë qind mijë lekë. Më konkretisht lidhur me fgurën e veprës penale të parashikuar nga neni 143/b/1 të K.Penal është shprehur edhe Gjykata e

Lartë në çështjen me palë: Prokuroria e rrethit Gjyqësor Tiranë kundër shtetasve me iniciale XH.G, M.P, A.K, E. SH, S.SH, S.K[183].

Për vlerësimin e përgjegjësisë penale të të gjykuarve gjykata ka analizuar në mënyrë të veçantë elementin e figurës te veprës penale në referim të nenit 143/b/1 të K.Penal, dhe konkretisht anën objektive dhe subjektive, si më poshtë:

Nga pikëpamja e anës objektive sipas gjykatës provohet që të gjykuarit, me veprimet e tyre kanë konsumuar një figurë vepre penale, konkretisht atë të *"Mashtrimit kompjuterik"* të parashikuar nga neni 143/b/1 i K.Penal. Vepra penale e *"Mashtrimit kompjuterik"* konsumohet në formën e veprimeve aktive kriminale siç janë futja, ndryshimi, fshirja ose heqja e të dhënave kompjuterike apo ndërhyrja në funksionimin e një sistemi kompjuterik. Nga të gjitha provat, rezulton se të gjykuarit, kanë realizuar shitje të aparateve "dreambox" në dyqanet e tyre me të cilat ofrohej ndjekja e disa programeve, ekskluzivitetin e të cilave e kishte vetëm kompania "Digitalb" në paketat e saj. Kjo vepër, nga ana objektive, është kryer në formën e ndryshimit të të dhënave kompjuterike, pasi aparati "Dreambox" që ata kanë shitur, funksionon duke përdorur një kartë Smart të abonuar, e cila është në gjendje të dekriptojë "çelësin" dhe më tej lidhet me internetin, duke bërë të mundur ndarjen e "çelësit/kodeve" në të gjitha aparatet e tjerë, të cilët nuk përdorin kartën Smart. Në momentin që klienti merr aparatin "Dreambox", pasi lidhet me sinjalin e internetit, merr çdo të dhënë kodesh nga "Dreambox" serveri dhe kështu përftohet pamja vizive. Karta Smart rezulton se është pjesë përbërëse e sistemit kompjuterik.

Në lidhje me anën subjektive, gjykata argumenton se të gjykuarit e kanë kryer veprën penale me dashje, pasi e kanë parashikuar pasojën kriminale dhe me ndërgjegje e kanë lejuar. Gjithashtu sipas gjykatës në lidhje me veprën penale të "Mashtrimit kompjuterik" një element i rëndësishëm është edhe qëllimi, që në rastin konkret ekziston, pasi qëllimi i të gjykuarve ka qenë për t'i siguruar vetes një përfitim ekonomik të padrejtë, konkretisht shumën për çdo pajisje "Dreambox" të shitur. Nga sa më sipër Gjykata e Lartë ka çmuar të lërë në fuqi Vendimin e Gjykatës së Apelit Tiranë që ka deklaruar fajtorë personat e sipërcituar për veprën penale të mashtrimit Kompjuterik të parashikuar nga 143/b/1 i K.Penal.

[183] Vendim i Gjykatës së lartë Nr.00-2013-1587 (261), datë 02.10.2013.

2.5. Falsifikimi kompjuterik

Një vepër penale kompjuterike e shtuar me ligjin nr. 10023/2008 është edhe "***falsifikimi kompjuterik***" (neni 186/a[184]). Me anë të kësaj dispozite synohet të mbrohet autenticiteti i të dhënave kompjuterike nga futja, ndryshimi, fshirja apo heqja e të dhënave kompjuterike në mënyrë të padrejtë, për t'i paraqitur e përdorur ato si autentike. Ky lloj falsifikimi është i cilësuar nga ana objektive për shkak të mënyrës së veçantë të kryerjes së tij.

Specifike për këtë vepër penale është që veprimet e futjes, ndryshimit, heqjes apo fshirjes së të dhënave kompjuterike të jenë kryer pa të drejtë. Kjo reflekton idenë që një sjellje e tillë nuk është gjithnjë e dënueshme, por mund të jetë e ligjshme ose e justifikuar si rast i ushtrimit të një të drejte.

Kjo vepër për shkak të rrezikshmërisë shoqërore të lartë është konsideruar si krim duke parashikuar një dënim me burgim nga gjashtë muaj gjer në gjashtë vjet. Gjithashtu parashikohen si rrethana të mëtejshme cilësuese në paragrafin e dytë kryerja e veprës nga personi që ka për detyrë ruajtjen dhe administrimin e të dhënave kompjuterike (e cilësuar në subjektin aktiv të veprës penale), në bashkëpunim (e cilësuar nga ana subjektive dhe objektive), më shumë se një herë (e cilësuar në të gjithë unitetin e veprës penale) ose ka sjellë pasoja të rënda për interesin publik (e cilësuar në anën objektive) të cilat shoqërohen me një rritje të marzheve të dënimit me tre gjer në dhjetë vjet.

Objekt i krimit janë marrëdhëniet juridike të vendosura për të siguruar interesat publik, të mbrojtura nga legjislacioni penal. Në këtë figurë falsifikimi kryhet në kompjuter, kundër interesit publik.

Nga ana objektive, krimi kryhet me forma e mënyra të ndryshme:

a) Futja, ndryshimi, fshirja ose heqja e të dhënave kompjuterike;

---

[184]Neni 186/a, **Falsifikimi kompjuterik**

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

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

b) Këto veprime kryhen pa të drejtë në mënyrë të paligjshme për krijimin e të dhënave të rreme në mënyre që t'i përdorin si autentike;
c) Për figurën e krimit nuk është me rëndësi nëse të dhënat e rreme janë drejtëpërdrejtë të lexueshme apo të kuptueshme. Në çdo rast pasojat e krimit janë të dukshme. Lidhja shkakësore është e drejtëpërdrejtë.

Subjekt i krimit është i përgjithshëm por edhe i posaçëm. Në paragrafin e parë subjekti i krimit mund të jetë çdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm dhe që kryen krimin e falsifikimit kompjuterik. Në paragrafin e dytë ku parashikohen rrethanat e cilësuara, subjekti është i posaçëm, janë personat që kanë për detyrë ruajtjen ose administrimin e të dhënave kompjuterike.

Nga ana subjektive krimi kryhet me dashje të drejtëpërdrejtë dhe me qëllim paraqitje ose përdorimin e të dhënave si autentike.

2.6. Hyrja e paautorizuar kompjuterike

Vepra penale "***Hyrja e paautorizuar kompjuterike***" parashikohet nga neni 192/b[185] e Kodit Penal, e cila është krim për shkak të marrëdhënieve që cënon, formave që realizohet dhe pasojat që shkakton. Me anë të kësaj dispozite synohet të mbrohet përmbajta e të dhënave kompjuterike nga aksesi i paautorizuar. Hyrja e paautorizuar, që mund të shfaqet edhe në formën e tejkalimit të kompetencës për të hyrë në një sistem kompjuterik, është një vepër penale e cila konsumohet vetëm me kryerjen e veprimit të hyrjes në sistem dhe njohjes me të dhëna që përmban sistemi, duke mos përjashtuar mundësinë që autori i veprës të përgjigjet për veprat e tjera sipas parashikimeve të neneve pasues. "Hyrja e paautorizuar kompjuterike" mbulon shkeljen bazë të kërcënimeve kundër sigurisë (konfidencialitetit, integritetit dhe disponueshmërisë) së sistemit kompjuterik dhe të të dhënave. Nevoja për mbrojtjen e tyre reflekton interesat e individëve dhe të organizatave për të administruar, operuar dhe kontrolluar sistemet e tyre në mënyrë të pashqetësuar.

[185]Neni 192/b- **Hyrja e paautorizuar kompjuterike**

Hyrja e paautorizuar apo në tejkalim të autorizimit për të hyrë në një sistem kompjuterik a në një pjesë të tij, nëpërmjet cenimit të masave të sigurimit, dënohet me gjobë ose me burgim deri në tre vjet. Kur kjo vepër kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile,

të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga tre deri në dhjetë vjet.

Ndërhyrja e thjeshtë e paautorizuar si ‘piratimi’ është e paligjshme, sepse mund t’i shkaktojë pengesa të ndryshme përdoruesve legjitimë të sistemeve dhe të të dhënave, si dhe mund të shkaktojë ndryshimin ose shkatërrimin e tyre me kosto të larta për rikonstruksionin e tyre. Ndërhyrje të tilla mund të japin akses tek të dhënat konfidenciale (duke përfshirë fjalëkalimet) pa pagesë, madje duke i inkurajuar piratët kompjuterikë për të kryer vepra penale kompjuterike më të rënda, si mund të jetë mashtrimi kompjuterik.

Objekt i krimit janë marrëdhëniet juridike të vendosura për të siguruar rregullsinë dhe saktësinë e programeve kompjuterike në dëm të interesave të personave ose ato publike ushtarake, sigurisë civile, të rendit publik, etj.

Nga ana objektive krimi kryhet në forma dhe mënyra të ndryshme, me hyrje të paautorizuar apo me tejkalim të kompetencave për të hyrë në një sistem kompjuterik ose në një pjesë të tij, nëpërmjet cënimit të masave të sigurimit.Në këtë figurë, të rëndësishme janë pasoja qe sjell vepra dhe element i domosdoshëm është cënimi i masave të sigurimit.

Subjekt i krimit është i përgjithshëm ose i posaçëm, pra mund të jetë çdo person që hyn në mënyrë të paautorizuar apo në tejkalim të autorizimit për të hyrë në një sistem kompjuterik apo në një pjesë të tij.

Nga ana subjektive krimi kryhet me dashje të drejtpërdrejtë. Rrethanat cilësuese të krimit janë kur ai kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetsisë apo në çdo sistem tjetër kompjuterik me rëndësi publike.Këto rrethana janë të cilësuara për shkak të rrezikshmërisë shoqërore të lartë të cilat vlerësohen në çdo rast konkret nga gjykata.

Mjeti më efektiv i parandalimit të hyrjes së paautorizuar, sigurisht që është vendosja dhe zhvillimi i masave efektive të sigurisë. Megjithatë, një mjet efektiv përbën edhe kriminalizimi i saj. Kriminalizimi i këtij veprimi i jep një mbrojtje shtesë sistemit dhe të dhënave kompjuterike.

“Hyrja” përfshin aksesin në një pjesë ose në të gjithë sistemin kopmpjuterik (hardware, komponentë të tjerë përbërës, të dhëna të depozituar, direktoritë etj). Megjithatë, ajo nuk përfshin dërgimin e thjeshtë të një emaili ose të një fashikulli (file) tek ai sistem. “Hyrja” apo aksesi përfshin edhe veprimin nga një kompjuter tjetër, i lidhur në rrjet telekomunikimi publik ose tek një sistem kompjuterik i të njëjtit rrjet, si psh një LAN (rrjet lokal) ose

intraneti brenda një organizate. Mënyra e komunikimit (në distancë, wireless apo në afërsi) nuk ka rëndësi për veprën penale.

Gjithashtu në paragrafin e dytë të nenit 192/b të Kodit Penal parashikohen si rrethana cilësuese hyrja e paautorizuar në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik me rëndësi publike. Kryerja e kësaj vepre në rrethanë të cilësuar është përcaktuar si krim, për shkak të rrezikshmërisë shumë të lartë shoqërore që mbart kjo vepër, duke aplikuar për këtë qëllim një marzh dënimi më të lartë se paragrafi i parë dhe konkretisht dënimin me burgim nga tre gjer në dhjetë vjet. Në cilësimin e kësaj vepre penale është mbajtur në konsideratë interesi publik (duke listuar për nga rëndësia fushën ushtarake, sigurinë kombëtare, rendin publik e me radhë). Këto rrethana përfundojnë me hipotezën "çdo sistem tjetër kompjuterik me rëndësi publike" duke lënë të hapur në çmim të pushtetit gjyqësor elaborimin e këtij koncepti për zgjidhjen e mundshme të rasteve që mund të ndeshen në praktikë.

2.7. Përgjimi i paligjshëm i të dhënave kompjuterike

Në Kodin Penal është shtuar neni 293/a[186], i cili parashikon si vepër penale ***"përgjimin e paligjshëm"***, me të cilin synohet mbrojtje e të dhënave kompjuterike nga ose brenda një sistemi kompjuterik nga përgjimet e paligjshme. Kjo vepër për shkak të rrezikshmërisë shoqërore të lartë është konsideruar si krim, duke parashikuar një dënim nga tre gjer në shtatë vjet burgim.

Kjo normë penale merr në mbrojtje të drejtën e privatësisë në transmetimin/ komunikimin e të dhënave. Kjo vepër penale dhunon privatësinë e komunikimit në të njëjtën mënyrë si përgjimi tradicional dhe regjistrimi i bisedave telefonike midis personave. E drejta e privatësisë përbën të drejtë themelore të sanksionuar nga Kushtetuta jonë, si dhe nga neni 8 i Konventës Evropiane të të Drejtave të Njeriut. Kriminalizimi i përgjimit të paligjshëm të të dhënave kompjuterike në nenin 293/a të Kodit Penal e mbron këtë të drejtë në të gjitha format e transferimit elektronik të të dhënave, qofshin me telefon, fax, email.

---

[186] Neni 293/a- **Përgjimi i paligjshëm i të dhënave kompjuterike**

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

Për këtë shkak krahas transmetimit të të dhënave kompjuterike janë parashikuar edhe emetimet elektromagnetike. Përgjimi me mjete teknike ka lidhje me dëgjimin, monitorimin dhe mbikqyrjen e përmbajtjes së komunikimeve, deri tek përftimi i përmbajtjes së të dhënave qoftë në mënyrë të drejtpërdrejtë nëpërmjet aksesit dhe përdorimit të sistemit kompjuterik, ose në mënyrë të tërthortë, nëpërmjet përdorimit të pajisjeve përgjuese. Përgjimi mund të përfshijë edhe regjistrimin e të dhënave. Mjetet teknike përfshijnë pajisje teknike të fiksuara në linjat e transmetimit, si edhe pajisjet për të mbledhur dhe regjistruar komunikimet wireless. Ato mund të përfshijnë përdorimin e software, fjalëkalimeve dhe kodeve.

Neni 293/a merr në mbrojtje transmetimin jo publik të të dhënave kompjuterike dhe ky term cilëson natyrën e proçesit të transmetimit (komunikimit) dhe jo natyrën e të dhënave të transmetuara. Të dhënat e komunikuara mund të jenë informacion në dispozicion të publikut, por palët dëshirojnë të komunikojnë në mënyrë konfidenciale. Një rast tjetër mund të jetë që të dhënat mund të mbahen sekret për qëllime tregtie derisa shërbimi të paguhet (si në rastin e Pay-TV).

Komunikimi në formën e transmetimit të të dhënave kompjuterike mund të ndodhë: brenda një sistemi kompjuterik (duke shkuar nga CPU tek ekrani ose printeri); ndërmjet dy sistemeve kompjuterike që i përkasin të njëjtit person; dy kompjuterave që komunikojnë me njëri-tjetrin; ose një kompjuteri dhe një personi (p.sh nëpërmjet tastierës).

Në paragrafin e dytë të nenit 293/a të Kodit Penal parashikohen si rrethana cilësuese, kryerja e kësaj vepre nga/ose brenda sistemeve kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile apo në çdo sistem tjetër kompjuterik me rëndësi publike, dënohet me burgim nga shtatë deri në pesëmbëdhjetë vjet.

Objekti i krimit është i përgjithshëm dhe i posaçëm. Objekti i përgjithshëm i krimit janë marrëdhëniet juridike të vendosura për të siguruar paprekshmërine e të dhënave kompjuterike nga çdo mjet apo mënyrë. Objekti i posaçëm janë marrëdhëniet juridike për të siguruar paprekshmërinë e të dhënave kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile.

Nga ana objektive krimi kryhet me anë të përgjimit të paligjshëm, me mjete teknike të transmetimeve jopublike të të dhënave kompjuterike, përfshirë emetimet elektromagnetike

ose nga një sistem kompjuterik që mban të dhëna kompjuterike. Që vepra të konsiderohet e konsumuar mjafton përgjimi i paligjshëm, pasoja nuk është element i domosdoshëm.

Subjekt i krimit mund të jetë çdo person që kryen përgjim të paligjshëm të të dhënave kompjuterike.

Nga ana subjektive krimi kryhet me dashje. Rrethanat e cilësuara janë kur krimi kryhet brenda sistemeve kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile apo në çdo sistem tjetër kompjuterik, me rëndesi publike. Këto rrethana vlerësohen në çdo rast konkret nga gjykata.

2.8. Ndërhyrja në të dhënat kompjuterike, ndërhyrja në sistemet kompjuterike, keqpërdorimi i paisjeve

Mbas nenit 293/a është shtuar neni 293/b[187] i cili parashikon si vepër penale ndërhyrjet e paautorizuara në të dhënat kompjuterike. Interesi ligjor i marrë në mbrojtje me anë të kësaj norme është integriteti dhe funksionimi siç duhet, apo përdorimi i të dhënave kompjuterike të ruajtura apo të programeve kompjuterike. "Dëmtimi" dhe "shtrembërimi" janë veprime që shkaktojnë një ndryshim negativë të integritetit ose të informacionit të të dhënave apo programeve. "Fshirja" e të dhënave i shkatërron ato dhe i bën të panjohura. Ndërsa "suprimimi" nënkupton çdo veprim që parandalon ose përfundon disponibilitetin e të dhënave të personit, i cili ka akses në kompjuter.

Këto akte janë të dënueshme penalisht nëse kryhen në mënyrë të paautorizuar, pra personi që i ka kryer nuk e ka të drejtën për një veprim të tillë. Kjo do të thotë që testimi ose mbrojtja e një sistemi kompjuterik i autorizuar nga pronari apo përdoruesi i tij janë në ushtrim të një të drejte, dhe nuk përbën vepër penale. Gjithashtu enkriptimi nuk përbën vepër penale. Kjo vepër për shkak të rrezikshmërisë shoqërore të lartë është konsideruar si krim, duke parashikuar një dënim nga gjashtë muaj deri në tre vjet.

---

[187] Neni 293/b, **Ndërhyrja në të dhënat kompjuterike**

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

Në vijim, parashikohen si rrethana cilësuese kryerja e kësaj vepre nga ose brenda sistemeve kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile apo në çdo sistem tjetër kompjuterik me rëndësi publike dënohet me burgim nga shtatë gjer në pesëmbëdhjetë vjet.

Objekti i krimit është i përgjithshëm dhe i posaçëm; *Objekti i përgjithshëm* i krimit janë marrëdhëniet juridike të vendosura për të siguruar paprekshmërine e të dhënave kompjuterike nga çdo mjet apo mënyrë; *Objekti i posaçëm* janë marrëdhëniet juridike për të siguruar paprekshmërinë e të dhënave kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile.

Nga ana objektive krimi kryhet nëpërmjet dëmtimit, shtrembërimit, ndryshimit, fshirjes apo suprimimit të paautorizuar të të dhënave kompjuterike.

Subjekt i krimit mund të jetë çdo person që kryen përgjim të paligjshëm të të dhënave kompjuterike. **Nga ana subjektive** krimi kryhet me dashje.

Pas nenit 293/b është shtuar nenin 293/c[188] i cili parashikon si **vepër penale ndërhyrjen në sistemet kompjuterike**, nëpërmjet krijimit të pengesave serioze dhe të paautorizuara që cënojnë funksionimin normal të sistemit kompjuterik. Termi 'pengesë' i referohet veprimeve që ndikojnë në funksionimin normal të sistemit kompjuterik. Këto pengesa krijohen nëpërmjet futjes, dëmtimit, shtrembërimit, ndryshimit, fshirjes apo suprimimit të të dhënave kompjuterike.

Dy janë kushtet që duhet të plotësojë veprimi pengues:

(1) Të jetë i një karakteri serioz, duke mos përcaktuar vlerë ekonomike të pasojës apo ndonjë kriter tjetër objektiv matës, shkalla e seriozitetit do të çmohet rast pas rasti në gjykatë. Në këtë pikë, duhen konsideruar formën, masën, apo frekuencën të të dhënave që kanë sjellë një efekt shtrembërues domethënës në mundësinë e pronarit apo përdoruesit për të përdorur sistemin komjuterik.

[188]Neni 293/c, **Ndërhyrja në sistemet kompjuterike**

Krijimi i pengesave serioze dhe të paautorizuara për të cenuar funksionimin e një sistemi kompjuterik, nëpërmjet futjes, dëmtimit, shtrembërimit, ndryshimit, fshirjes apo suprimimit të të dhënave, dënohet me burgim nga tre deri në shtatë vjet. Kur kjo vepër kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga pesë deri në pesëmbëdhjetë vjet.

Një rast i tillë mund të jetë nëpërmjet programeve që gjenerojnë refuzimin e shërbimit, kodet e këqija apo viruset që ngadalësojnë veprimtarinë e sistemit kompjuterik;
(2) Të jetë i paautorizuar, pa leje apo jashtë detyrave funksionale të personit që vepron. Me anë të këtij parashikimi penal është marrë në mbrojtje interesi i operatorëve dhe i përdoruesve të sistemeve komjuterike për t'i mundësuar atyre një funksionim normal.

Objekti i përgjithshëm i krimit janë marrëdhëniet juridike të vendosura për të siguruar funksionimin e sistemit kompjuterik nga ndërhyrje të mbrojtura nga legjislacioni penal.

Objekti i posaçëm i krimit është i parashikuar në paragrafin e dytë ku janë të parashikuara rrethanat e cilësuara.

Nga ana objektive krimi kryhet me ndërhyrje në sistemin kompjuterik nëpërmjet krijimit të pengesave serioze, futjes, dëmtimit, shtrembërimit, ndryshimit, fshirjes apo suprimimit të të dhënave.

Subjekt i krimit mund të jetë çdo person që krijon pengesa serioze dhe cënon funksionimin e një sistemi kompjuterik.

Nga ana subjektive krimi kryhet me dashje. Rrethanat cilësuese janë kur krimi kryhet brenda sistemeve kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetsisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike. Këto rrethana vlerësohen në çdo rast konkret nga gjykata.

Pas nenit 293/c është shtuar neni 293/ç i cili parashikon si **vepër penale keqpërdorimin e pajisjeve** sipas të cilit prodhimi, mbajtja, shitja, dhënia në përdorim, shpërndarja apo çdo veprim tjetër për vënien në dispozicion të një pajisjeje, ku përfshihen edhe një program kompjuterik, një fjalëkalim kompjuterik, një kod hyrjeje apo një e dhënë e tillë e ngjashme, të cilat janë krijuar ose përshtatur për hyrjen në një sistem kompjuterik ose në një pjesë të tij me qëllim kryerjen e veprave penale të parashikuara në nenet 192/b, 293/a, 293/b, 293/c.

Kjo vepër për shkak të rrezikshmërisë shoqërore të lartë është konsideruar si krim, duke parashikuar një dënim me burgim nga gjashtë muaj gjer në pesë vjet. Duke qenë se fusha e kibernetikës (e teknologjisë informatike) është në zhvillim dinamik shumë të shpejtë, përgjithësisht në të gjitha këto dispozita është lënë një koncept i bardhë i tipit "çdo sistem

tjetër i ngjashëm" apo "një e dhënë e tillë e ngjashme" për t'iu përgjigjur zhvillimit të ardhshëm të teknologjisë.

Objekt i krimit është funksionimi normal i sistemit kompjuterik, sigurimi i të dhënave kompjuterike, të mbrojtura posaçërisht nga legjislacioni penal[189].

Nga ana objektive krimi kryhet në forma dhe mënyra të ndryshme:

a) Me anë të prodhimit të një pajisje ku përfshihet edhe një program kompjuterik, fjalëkalim kompjuterik, kod hyrje, etj;

b) Me anë të mbajtjes, shitjes apo dhënies në përdorim të pajisjes;

c) Me anë të shpërndarjes ose çdo veprim tjetër të një pajisje ku përfshihet edhe një program kompjuterik;

d) Me një kod hyrje apo një e dhënë e tillë e ngjashme për të hyrë në sistemin kompjuterik. Pasojë e veprës është mosfunksionimi normal i sistemit kompjuterik.

Subjekt i krimit mund të jetë çdo person që ka mbushur moshën dhe është i përgjegjshëm, i cili kryen një nga veprimet e mësipërme.

Nga ana subjektive krimi kryhet me dashje të drejtëpërdrejtë, për të kryer një nga veprat penale të parashikuara nga nenet 192/b, 293/a, 293/b dhe 293/c.

Miratimi i ligjit nr. 10023/2008 përbën një zhvillim cilësor të legjislacionit penal shqiptar dhe një hap të rëndësishëm në drejtim të përafrimit të legjislacionit të brendshëm me atë ndërkombëtar.

3. Statistikat e krimeve kibernetike në Shqipëri

- Statistikat e veprave penale kibernetike për periudhën Janar-Dhjetor 2010

Gjatë periudhës Janar-Dhjetor 2010 janë evidentuar **65** raste, me 60 autorë, nga të cilët ndaluar e arrestuar **10** persona, në gjendje të lirë 50 persona.

---

[189] Neni 293/ç

Keqpërdorimi i pajisjeve

Prodhimi, mbajtja, shitja, dhënia në përdorim, shpërndarja apo çdo veprim tjetër, për vënien në dispozicion të një pajisjeje, ku përfshihen edhe një program kompjuterik, një fjalëkalim kompjuterik, një kod hyrjeje apo një e dhënë e tillë e ngjashme, të cilat janë krijuar ose përshtatur për hyrjen në një sistem kompjuterik ose në një pjesë të tij, me qëllim kryerjen e veprave penale, të parashikuara në nenet 192/b, 293/a, 293/b e 293/c të këtij Kodi, dënohen me burgim nga gjashtë muaj deri në pesë vjet."

- **Të ndara sipas qarqeve, veprat penale janë:**

Tabela nr.1[190]

Nr	Drejtoria Policisë Qarkut	VP të evidentuara	VP të Zbuluara	Autorë gjithsej	Arrest dhe Ndal	Ne gj. të lirë	Larguar nga vendi
1	Durrës	-	-	-	-	-	-
2	Elbasan	1	-	-	-	-	-
3	Fier	2	-	-	-	-	-
4	Gjirokastër	1	1	1	-	1	-
5	Korçë	2	-	-	-	-	-
6	Lezhë	-	-	-	-	-	-
7	Shkodër	1	1	1	-	1	-
8	Tiranë	35	27	39	8	31	-
9	Vlorë	1	1	1	-	1	-
10	Qendra	22	12	18	2	16	-
	Shuma e krimeve kompjuterike	65	42	60	10	50	-

- **Të ndara sipas veprave penale, janë si më poshtë:**

i. **1** rast për veprën penale "Kanosja me motive racizmi dhe ksenofobie nëpërmjet sistemit kompjuterik", neni 84/a i Kodit Penal, me **1** autor, në gjendje të lirë.

ii. **1** rast për veprën penale "Fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik", neni 119/b, autor **1** , në gjendje të lirë.

iii. **31** raste për veprën penale "Mashtrimi kompjuterik", neni 143/b i Kodit Penal, me **30** autorë, nga të cilat **10** arrestuar, në gjendje të lirë **20**.

iv. **16** raste për veprën penale "Falsifikimi kompjuterik", neni 186/a i Kodit Penal, me **15** autorë, në gjendje të lirë **15**.

6 raste për veprën penale "Hyrje e paautorizuar kompjuterike", neni 192/b, me **6** autorë, në gjendje të lirë **6**.

[190] http://www.pp.gov.al/web/Statistika_19_1. php.

v. **1** rast për veprën penale "Përgjim i paligjshëm i të dhënave kompjuterike", neni 293/a i Kodit Penal, me **1** autor, në gjendje të lirë **1**.

vi. **5** raste për veprën penale "Ndërhyrje në të dhënat kompjuterike", neni 293/b i Kodit Penal, me **4** autorë, në gjendje të lirë **4**.

vii. **4** raste për veprën penale "Ndërhyrje në sistemet kompjuterike", neni 293/c i Kodit Penal, me **2** autorë, në gjendje të lirë **2.**

- **Statistikat e veprave penale kibernetike për periudhën Janar-Nëntor 2011**

  Gjatë periudhës Janar-Nëntor 2011 janë evidentuar **82** vepra penale, ku janë implikuar **111** autorë, nga të cilët **26** të arrestuar dhe ndaluar dhe **85** të ndjekur në gjendje të lirë.

  Krahasuar me të njëjtën periudhë të një viti më parë, janë evidentuar **17** vepra penale më shumë, me **51** autorë më shumë, me **16** autorë të arrestuar më shumë, dhe **35** autorë në gjëndje të lire më shumë.

- **Sipas qarqeve veprat penale të evidentuara ndahen si më poshtë :**

Tabela nr.2[191]

Nr	Drejtoria Policisë Qarkut	VP të evidentuara	VP të zbuluara	Autorë gjithsej	Arrest dhe Ndal	Ne gj. të lirë	Larguar nga vendi
1	Durrës	-	-	-	-	-	-
2	Elbasan	4	2	2	-	2	-
3	Dibër	1	-	-	-	-	-
4	Fier	2	1	1	-	1	-
5	Gjirokastër	-	-	-	-	--	-
6	Korçë	-	-	-	-	-	-
7	Lezhë	-	-	-	-	-	-
8	Shkodër	-	-	-	-	-	-
9	Tiranë	49	45	76	13	63	-
10	Vlorë	2	1	1	-	1	-
11	Qendra	24	22	31	13	18	-
	Shuma krime kompjuterike	**82**	**71**	**111**	**26**	**85**	-

[191] http://www.pp.gov.al/web/Statistika_19_1.php.

- **Të ndara sipas drejtimeve veprat penale janë:**

Tabela nr.3[192]

1	Krime të IT	61	52	94	26	68	-
2	Krime të Sist. Komp.	21	19	17		17	-
IV	**Shuma**	**82**	**71**	**111**	**26**	**85**	**-**

- **Statistikat e veprave penale kibernetike për periudhën Janar-Dhjetor 2012**

Gjatë periudhës Janar-Dhjetor 2012 nga strukturat e hetimit të krimeve kompjuterike janë evidentuar **83** vepra penale, nga të cilat janë zbuluar **54** prej tyre, me **71** autorë, **5** të arrestuar në flagrancë dhe **66** në gjëndje të lirë. Krahasuar me të njëjtën periudhë të një viti më parë, janë evidentuar **1** vepër penale më shumë, me **40** autorë më pak, me **21** autorë të arrestuar dhe **19** autorë në gjendje të lirë më pak.

- **Sipas qarqeve veprat penale të evidentuara ndahen si më poshtë:**

Tabela nr.4[193]

Nr	Drejtoria Policisë Qarkut	VP të evidentuara	VP të zbuluara	Autorë gjithsej	Arrest dhe Ndal	Ne gj. të lirë	Larguar nga vendi
1	Durrës	4	3	5	-	5	-
2	Dibër	-	-	-	-	-	-
3	Elbasan	2	2	2	-	2	-
4	Fier	2	-	-	-	-	-
5	Gjirokastër	1	1	1	-	1	-
6	Korçë	1	1	1	-	1	-
7	Lezhë	1	1	1	-	1	-
8	Shkodër	3	1	1	-	1	-
9	Tiranë	36	27	36	3	33	-
10	Vlorë	3	-	-	-	-	-
11	Kukës	-	-	-	-	-	-
12	Qendra	30	19	24	2	22	-
	Shuma krime kompjuterike	**83**	**55**	**71**	**5**	**66**	-

[192] http://www.pp.gov.al/web/Statistika_19_1. php.

[193] Po Aty.

- **Të ndara sipas drejtimeve, veprat penale janë:**

Tabela nr.5[194]

Nr	**Krime Kompjuterike**	Evidentuar	Zbuluar	Autorë gjithsej	Arrest dhe Ndal	Në gj. të lirë	Larguar
1	**Në fushën e teknologjisë dhe informacionit**	34	23	28	-	28	-
2	**Nëpërmjet sistemit kompjuterik**	49	32	43	5	38	-
3	**Shuma total**	**83**	**55**	**71**	**5**	**66**	-

- **Të ndara sipas veprave penale, janë si më poshtë:**

i. Mashtrimi kompjuterik neni 143/b janë evidentuar **35** raste me **35,** nga të cilët **5** të arrestuar dhe **30** autor në gjëndje të lirë.

ii. Falsifikimi kompjuterik neni 186/a është evidentuar vetëm **11** raste, me **6** autor.

iii. Ndërhyrje në të dhënat kompjuterike, neni 293/b, është evidentuar **14** raste, me **11** autor. Ndërhyrje në sistemin kompjuterik, neni 293/c, është evidentuar **8** raste, me **8** autor.

iv. Hyrje e paautorizuar kompjuterike, neni 192/b, është evidentuar **12** raste, me **8**autor.

v. Kanosja me motive racizmi dhe ksenofobike, neni 84/a, **1** rast me **1** autor në gjendje të lirë.

vi. Shpërndarje e materialeve raciste ose ksenofobike neni 119/a, 1 rast pa autor.

vii. Pornografia me të mitur 117/2, 1 rast pa autor.

- **Statistikat e veprave penale kibernetike, për periudhën Janar-Dhjetor 2013**

Gjatë periudhës Janar-Dhjetor 2013 nga strukturat e hetimit të krimeve kompjuterike janë evidentuar **108** vepra penale nga të cilat janë zbuluar **63** prej tyre, me **69** autorë, nga të cilët **58** në gjëndje të lire **9** arrestuar dhe **2** në kërkim.

Krahasuar me vitin 2012 janë evidentuar **25** vepra penale më shumë, me **2** autorë më pak, **4** të arrestuar në flagrancë më shumë, **8** autorë në gjendje të lirë më pak dhe **2** persona në kërkim më shumë.

[194] http://www.pp.gov.al/web/Statistika_19_1. php.

- **Sipas qarqeve, veprat penale të evidentuara ndahen si më poshtë:**

Tabela nr.6[195]

Nr	Drejtoria Policisë Qarkut	VP të evidentuara	VP të zbuluara	Autorë gjithsej	Arrest dhe Ndal	Ne gj. të lirë	Larguar nga vendi
1	Durrës	6	2	2	-	2	-
2	Dibër	-	-	-	-	-	-
3	Elbasan	7	3	3	-	3	-
4	Fier	3	3	3	-	3	-
5	Gjirokastër	2	2	2	-	2	-
6	Korçë	1	-	-	-	-	-
7	Lezhë	4	1	1	-	1	-
8	Shkodër	4	-	-	-	-	-
9	Tiranë	54	32	33	5	28	-
10	Vlorë	2	1	2	-	2	-
11	Kukës	-	-	-	-	-	-
12	Berat	4	2	2	-	2	-
13	Qendra	21	17	21	4	15	2
	Shuma krime kompjuterike	**108**	**63**	**69**	**9**	**58**	**2**

- **Të ndara sipas drejtimeve:**

Tabela nr.7[196]

Nr	**Krime Kompjuterike**	Evidentuar	Zbuluar	Autorë gjithsej	Arrest dhe Ndal	Në gj. Të lirë	Larguar
1	**Në fushën e teknologjisë dhe informacionit**	34	21	28	7	19	2
2	**Nëpërmjet sistemit kompjuterik**	74	42	41	2	39	-
3	**Gjithsej**	**108**	**63**	**69**	**9**	**58**	**2**

[195] http://www.pp.gov.al/web/Statistika_19_1. php.

[196] Po Aty.

- **Të ndara sipas veprave penale, janë si më poshtë:**
  - **i.** Hyrja e pautorizuar kompjuterike, neni 192/b, evidentuar **11** raste me **7** autor në gjendje të lirë.
  - **ii.** Ndërhyrje në të dhënat kompjuterike neni 293/b, është evidentuar **22** raste me **13** autor, nga të cilët **3** arrestuar dhe **10** në gjendje të lirë.
  - **iii.** Ndërhyja në sistemet kompjuterike neni 293/c, evidentuar **4** raste me **6** autor nga të cilët **4** të arrestuar dhe **2** në kërkim.
  - **iv.** Nëpërmjet sistemit kompjuterik.
  - **v.** Mashtrimi kompjuterik neni 143/b janë evidentuar **42** raste, me **26** autorë nga të cilët **2 t**ëarrestuar.
  - **vi.** Falsifikimi kompjuterik, neni 186/a, është evidentuar **19** raste me **10** autorë, në gjendje të lirë.
  - **vii.** Shpërndarja e materialeve raciste ose ksenofobike nëpërmjet sistemit kompjuterik, neni 119/a, evidentuar **1** rast me **1** autor.
  - **viii.** Fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik, neni 119/b i Kodit Penal, **1** rast, me **1** autor.
  - **ix.** Pornografia, neni 117/2, evidentuar **1** rast me **2** autorë në gjendje të lirë.
  - **x.** Shpifja (nëpërmjet internetit), neni 120, evidentuar **1** rast me **1** autor.
  - **xi.** Kanosja për shkak të detyrës nëpërmjet sistemit kompjuterik, neni 238 i Kodit Penal, **2** raste me **2** autorë në gjendje të lirë.
  - **xii.** Neni 84/a,"Kanosja nëpërmjet sistemit kompjuterik", **1** rast pa autorë.
  - **xiii.** Neni 119 e 121, ''Fyerja'' dhe ''Ndërhyrja pa të drejtë në jetën private'', **3** raste pa autorë.

- **Statistikat e veprave penale kibernetike për periudhën Janar-Dhjetor 2014**

  Gjatë periudhës Janar-Dhjetor 2014 nga strukturat e hetimit të krimeve kompjuterike janë evidentuar **180** vepra penale, zbuluar **76**, me **86** autorë, nga të cilët **74** në gjendje të lirë **10** të arrestuar dhe **2** në kërkim.

  Krahasuar me të njëjtën periudhë të vitit të kaluar, janë evidentuar **72** vepra penale më shumë, me **17** autorë më shumë, **1** autor të arrestuar më shumë.

- **Sipas qarqeve veprat penale të evidentuara ndahen si më poshtë :**

Tabela nr.8[197]

Nr	Drejtoria Policisë Qarkut	VP të evidentuara	VP të zbuluara	Autorë gjithsej	Arrest dhe Ndal	Në gj. të lirë	Larguar nga vendi
	Durrës	7	1	1		1	
	Korçë	4	2	2		2	
	Dibër	1	-	-	-	-	
	Berat	1	-	-	-	-	
	Fieri	5	4	4	-	4	
	Elbasan	5	4	4		4	
	Shkodër	9	3	3	-	3	
	Kukës	2	2	3	3	-	
	Lezhë	3	3	3	-	3	
	Tiranë	61	27	31	6	25	
	Vlorë	6	4	5	-	5	
	Qendra	77	27	30	1	29	
	Shuma krime kompjuterike	**180**	**76**	**86**	**10**	**76**	

- **Të ndara sipas drejtimeve:**

Tabela nr.9[198]

Nr	KRIME KOMPJUTERIKE	Evidentuar	Zbuluar	Autorë gjithsej	Arrestuar	Gjendje të lirë	Larguar
1	**Në fushën e teknologjisë dhe informacionit**	53	29	30	2	28	-
2	**Nëpërmjet sistemit kompjuterik**	127	47	56	8	50	-
3	**Gjithsej**	**172**	**76**	**86**	**10**	**78**	

[197] http://www.pp.gov.al/web/Statistika_19_1. php.

[198] Po Aty.

- **Të ndara sipas veprave penale ato paraqiten si më poshtë:**

i. Neni 119/a, "Shpërndarja e materialeve raciste ose ksenofobike nëpërmjet sistemit kompjuterik", evidentuar **1** rast, pa autor.

ii. Neni 143/b, "Mashtrimi Kompjuterik", evidentuar **49** raste, me **14** autorë në gjendje të lirë, **1** arrestuar.

iii. Neni 186/a, "Falsifikim Kompjuterik'', evidentuar **28** raste, me **20** autor, nga të cilët **4** arrestuar dhe **16** në gjendje të lirë.

iv. Neni 192/b, "Hyrja e paautorizuar kompjuterike", evidentuar **14** raste, me **7** autor në gjendje të lirë.

v. Neni 293/a, "Përgjimi i paligjshëm i të dhënave kompjuterike", evidentuar **1** rast me **2** autorë në gjendje të lirë.

vi. Neni 293/b, "Ndërhyrja në të dhënat kompjuterike", evidentuar **33** raste me **16** autorë, nga të cilët **2** të arrestuar dhe **14** në gjendje të lirë.

vii. Neni 293/c, "Ndërhyrja në sistemet kompjuterike", evidentuar **4** raste, me **3** autorë në gjendje të lirë.

viii. Neni 121 "Ndërhyrje të padrejta në jetën private", **4** raste pa autor.

ix. Neni 117, paragrafi i tretë, "Pornografia", evidentuar **38** raste me **14** autorë në gjendje të lirë.

x. Neni 121/a "Përndjekja", evidentuar **4** vepër penale, zbuluar **3**, me **2** autor të proceduar në gjendje të lirë, **1** arrestuar.

xi. Neni 137/a "Vjedhja e rrjetit të komunikimeve elektronike", evidentuar **1** vepër penale, zbuluar **1**, me **1** autor në gjendje të lirë.

xii. Neni 149/a "Shkelja e të drejtave të pronësisë industriale", evidentuar **1** vepër penale, zbuluar **1**, me **1** autor i cili është proceduar në gjendje të lirë.

xiii. Shpifja parashikuar nga neni 120 i Kodit Penal, evidentuar **1** rast me **1** autor në gjendje të lirë.

4. Kuadri i strukturave institucionale që merren me sigurinë dhe krimin kibernetik në Shqipëri

Institucionet shtetërore, kanë strukturat dhe grupet e tyre të punës që merren me fushën e teknologjisë së komunikimit dhe të informacionit, dhe kanë përgjegjësi që lidhen me sigurinë institucioneve të tyre, por dhe me sigurinë në kiberhapsirë. Kjo tregon se vetë zbatimi i politikave përqendrohet brenda këtyre institucioneve. Si rezultat për luftimin e krimit kibernetik lind nevoja e bashkëpunimit ndërmjet strukturave të ndryshme publike dhe private dhe krijimi i një autoriteti kombëtar kryesor që do punojë dhe do ketë përgjegjësi për mbrojtjen kibernetike.

Ky autoritet mund të realizojë detyra të tilla si: shkëmbimi i informacionit dhe publikimi i informacioneve për incidentet, koordinimi me përdoruesit e sistemeve për mbrojtjen kibernetike, trajnime në fushën e mbrojtjes kibernetike, përgatitja e detyrave për garantimin e sigurisë kibernetike, marrja e masave parandaluese dhe menaxhimi i kërcënimeve në nivel kombëtar, hartimi dhe zbatimi i një strategjie kombëtare të mbrojtjes kibernetike, përcaktimi i rregullave për sigurinë e informacionit në sistemet shtetërore, përmirësimi i metodave të vlerësimit të rrezikut dhe analiza e riskut, përcaktimi i mangësive të sigurisë së informacionit, propozimi i paketave ligjore për sigurinë, etj. Në këtë agjenci apo strukturë duhet të punojnë specialistë dhe ekspertë në fushat e sistemeve të komunikimit dhe të informacionit, të mbrojtjes dhe sigurisë fizike, sigurisë së informacionit, të administrimit të të dhënave kompjuterike, ekspertë teknikë për pajisjet filtruese, të faqeve të internetit, ekspertë të auditit, ekspertë të ligjeve, etj.

Programet e monitorimit dhe mbikëqyrjes së incidenteve në rrjetet e informacionit dhe komunikimit janë të shumëllojshme dhe ndryshojnë nga një institucion publik në një kompani private përfshirë këtu edhe sistemin bankar. Shkëmbimi i informacionit midis institucioneve publike, lidhur me rastet konkrete për incidentet e sigurisë së informacionit, janë të papublikuara dhe mbahen të fshehura brenda institucioneve, pa kërkuar mendimin dhe ekspertizën e specialistëve të fushës përkatëse.

Strukturat dhe organet e ndryshme të qeverisë, në zbatim të legjislacionit në fuqi për mbrojtjen kibernetike, duhet të përcaktojnë rregullat dhe përgjegjësitë mbi masat e sigurisë së informacionit dhe të stimulojnë nëpërmjet testimeve të ndryshme aftësitë dhe kapacietet

e strukturave në përballimin ose jo të këtyre sulmeve. Shpërndarja në sasi e mjeteve të komunikimit, mbi të gjitha në epokën e zhvillimit të teknologjisë së informacionit, krijon një situatë të komplikuar, me përfshirjen e aktorëve të ndryshëm në një mjedis publik, të cilët operojnë në administrimin publik të institucioneve.

Nga ana tjetër procesi i modernizimit të administratës publike, jo vetëm nga ana praktike, por edhe nga ndryshimet e politikave, tregon rritjen e tendencave të risive teknologjike të administrimit të të dhënave dhe informacionit. Në këtë rast del hapur risku i përdorimit nga individë të ndryshëm të hapësirës kibernetike të një shteti tjetër. Institucionet ligjore kombëtare të vendit të angazhuara aktualisht në fushën e informacionit dhe kibernetikës janë në progres të vazhdueshëm në konsolidimin sipas standarteve europiane. Ekzistojnë aktualisht disa struktura institucionale të cilat merren me zbatimin e strategjisë së dokumenteve të politikave, vendimeve dhe ligjeve në fuqi dhe që lidhen direkt me mbrojtjen e teknologjisë së komunikimit dhe të informacionit. Këto struktura janë:

- **Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT),** është autoriteti qëndror për identifikimin, parashikimin dhe marrjen e masave për mbrojtjen ndaj kërcënimeve/sulmeve kompjuterike, në përputhje me legjislacionin në fuqi[199].
- **Drejtoria e Sigurimit të Informacionit të Klasifikuar (DSIK)**[200], është autoriteti që kontrollon dhe garanton sigurinë e sistemeve të klasifikuara të komunikimit dhe informacionit dhe bën akreditimin e tyre nëpërmjet lëshimit të Certifikatës së Sigurisë për këto të fundit.
- **Autoriteti Kombëtar për Certifikimin Elektronik (AKCE)**[201]**,** është autoriteti që ka përgjegjësinë e mbikëqyrjes së zbatimit të Ligjit "Për Nënshkrimin Elektronik" dhe të akteve nënligjore të nxjerra në zbatim të tij. AKCE bën akreditimin e ofruesve të shërbimit të certifikimit elektronik.
- **Autoriteti i Komunikimeve Elektronike dhe Postare (AKEP),** kontrollon zbatimin e masave të nevojshme mbrojtëse teknologjike për mbrojtjen e të dhënave personale të

[199]Per me shume: VKM Nr.766, datë 14.9.2011 "Për krijimin e Agjencisë Kombëtare për Sigurinë Kompjuterike (ALCIRT)", e ndryshuar.

[200]DSIK, http://www.nsaalbania.gov.al .

[201]AKCE, www.**akce**.gov.al/ .

pajtimtarëve dhe siguron integritetin dhe sigurinë e rrjeteve të komunikimeve elektronike publike. AKEP, në ushtrimine veprimtarisë së saj ka për qëllim informimin e publikut, palëve të interesuara dhe të sipërmarrësve të tregut të komunikimeve elektronike me treguesit kryesore të këtij tregu, nëpërmjet raporteve periodike të publikuar në faqen e Internetit të AKEP (www.akep.al)[202].

- **Komisioneri për Mbrojtjen e të Dhënave Personale,** është autoriteti përgjegjës i pavarur, që mbikëqyr dhe monitoron, në përputhje me ligjin, mbrojtjen e të dhënave personale elektronike gjatë ruajtes, përpunimit dhe transmetimit të tyre, duke respektuar e garantuar të drejtat dhe liritë themelore të njeriut.
- **Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI)**[203]**,** është përgjegjëse për administrimin e infrastrukturës qeveritare të Çelësit Publik (PKI) dhe siguron pajtueshmërinë me nenin 19 të ligjit nr.9880, datë 25.2.2008 "Për nënshkrimin elektronik". Në shërbimet që ofron nëpërmjet Qendrës së të Dhënave Qeveritare (Datacenter Qeveritar), për administratën publike, garanton autentifikim dhe identifikim të sigurtë, internet të sigurtë dhe DNS të sigurtë.
- **Policia e Shtetit,** është organi përgjegjës për parandalimin, zbulimin dhe hetimin e veprave penale, ndër të cilat përfshihen dhe veprat penale në fushën e TI, që ndiqen nga Sektori i Krimit Kompjuterik.
- **Prokuroria e Përgjithshme,** përmes sektorit të krimeve kibernetike ushtron ndjekjen penale për vepra penale në fushën e kibernetikës. Kjo strukturë kontrollon aktivitetin e njësive të posaçme për ndjekjen e krimeve kibernetike, që janë ngritur në prokuroritë e rretheve gjyqësore. Hetimi i veprave penale kibernetike do të jetë objektivi kryesor i këtij sektori dhe i njësive të posaçme që janë ngritur nëpër rrethe. Kjo është një nismë e rëndësishme që ka për qëllim parandalimin dhe luftimin e krimit kibernetik dhe rritjen e bashkëpunimit midis organeve gjyqësore dhe prokurorisë, pasi në nivel operativ mungon ende një bashkëpunim i frytshëm midis organeve ligj zbatuese.

---

[202]Lidhur me rolin e AKEP në sigurinë e rrjeteve dhe/ose shërbimeve të ofruara nga sipërmarrësit e rrjeteve dhe të shërbimeve të komunikimeve publike shih, LIGJ Nr. 9918, datë 19.5.2008 "Per Komunikimet Elektronike dhe Postare në Republikën e Shqipërisë", neni 122.AKEP, http://www.akep.al.

[203]AKSHI, http://www.akshi.gov.al.

- **Shërbimi Informativ i Shtetit (SHISH),** përmes seksionit të krimit kibernetik, ka për detyrë kërkimin, zbulimin dhe analizimin e krimeve kibernetike që cënojnë sigurinë kombëtare[204].
- **Ministria e Mbrojtjes,** luan një rol të rëndësishëm në ruajtjen e sigurisë kibernetike përmes Drejtorisë së Automatizimit dhe Inovacionit, si dhe përmes institucioneve të përmendura më poshtë që janë në varësi të Ministrit të Mbrojtjes (DSH dhe AISM).
- **Shtabi i Përgjithshëm i Forcave të Armatosura të Republikës së Shqipërisë, nëpërmjet** Drejtorisë së Ndërlidhjes, përgjigjet për zhvillimin e Sistemeve të ndërlidhjes dhe të Informacionit (SNI) në Forcat e Armatosura të Republikës së Shqipërisë duke u mbështetur në standardet kombëtare, të NATO-s dhe ato ndërkombëtare.
- **Drejtoria e Shifrës (DSH),** është Autoriteti Kombëtar për Sigurimin e Komunikimeve dhe Autoriteti Kombëtar i Shpërndarjes.
- **Agjencia e Inteligjencës së Mbrojtjes dhe Sigurisë (AISM),** përmes sektorit të Mbrojtjes Kibernetike dhe Infosec ka si detyrë parashikimin, identifikimin dhe analizimin e kërcënimeve kibernetike që cënojnë sistemet TIK të FASH.
- **Banka e Shqipërisë,** ka autoritetin e organit që ka të drejtën ekskluzive të japë miratimin për fillimin e aktivitetit bankar nëpërmjet dhënies së liçencës, si dhe të mbikëqyrë aktivitetin e çdo subjekti, i cili ka marrë liçencë për ushtrimin e veprimtarisë bankare në Republikën e Shqipërisë. Në fushën e sigurisë së sistemeve të TIK, subjekti përcakton objektiva, strategji dhe kërkesa të sigurisë si dhe miraton procedura për administrimin, për operimin, për ruajtjen e sistemeve, për mbrojtjen e të dhënave si edhe për nxjerrjen jashtë përdorimit te tyre.

Me gjithë implementimin aktual të legjislacionit që rregullon fushën e mbrojtjes së informacionit dhe luftën kundër krimeve kibernetike, ka rrugë të gjatë për të ecur drejt ndryshimeve. Janë disa hapa të cilat duhet të qartësohen dhe zhvillohen më tej si:

a. Përcaktimi i standardeve të përbashkëta duke u bazuar në standardet ndërkombëtare dhe që lidhen me sigurimin e mbrojtjes së informacionit, standarde që duhet të zbatohen nga të gjithë ofruesit dhe përdoruesit e rrjeteve të komunikimit;

[204]SHISH, http://www.shish.gov.al.

b. Krijimi i një strukture kyçe në nivel kombëtar, e cila do të merret me monitorimin, reagimin ndaj incidenteve, përgatitjen e masave për parandalimin e këtyre incidenteve, detyra të cilat mund të kryhen nga CERTs[205].

Sipas Konventës mbi Krimet Kibernetike të Këshillit të Europës, është e domosdoshme krijimi i grupeve të reagimit ndaj incidenteve dhe emergjencave kompjuterike dhe përfshirja e këtyre grupeve në një strukturë të vetme. Kjo strukturë duhet të jetë në gatishmëri që në çdo ditë të javës të sigurojë masa emergjente në lidhje me sulmet kriminale në rrjetet kompjuterike dhe detajet në lidhje me këto kërcënime.

Hartimi i një strategjie kombëtare mbi mbrojtjen e informacionit duhet ndërtuar duke marrë si model vendet perëndimore dhe SHBA. Kjo strategji do të përcaktonte detyrimet dhe përgjegjësitë e çdo institucioni publik apo privat, duke ndihmuar në krijimin e një infrastrukture kritike kombëtare të teknologjisë së komunikimit dhe të informacionit në vendin tonë.

Me anë të këtij dokumenti politikash dhe direktivash do të përcaktoheshin të gjitha standartet e BE-së dhe të NATO-s kundër krimit kompjuterik, duke vendosur balanca ndërmjet detyrimeve e përcaktimeve ndërkombëtare, përgjegjësive kombëtare, dimensionit trans-nacional të hapësirës së informacionit, të drejtave të individit dhe sigurisë së qytetarëve.

Legjislacioni ndërkombëtar ka një dimension të gjerë dhe përfshin çështje të ndryshme që kanë lidhje me informacionin dhe komunikimin. Çështje të tilla si: lufta kundër terrorizmit dhe krimit të organizuar, pastrimit të parave, mashtrimit kompjuterik etj. Dimensioni global i rrjeteve të komunikimit ku hyn dhe interneti, ligjet dhe rregullat brenda vendit nuk mund të ulin rrezikshmërinë e kërcënimeve kompjuterike.

Zbatimi i një marrëveshje ligjore ndërmjet dy ose më shumë palëve, do ndihmonte në bashkëpunimin ndërmjet vendeve dhe përcaktimeve ligjore të secilit vend, si rezultat në mbrojtjen dhe sigurinë e hapsirës kibernetike.

Paketa e parë ligjore europiane që shfaq ligjet mbi krimet kompjuterike është Konventa e Këshillit të Europës mbi Krimet kibernetike e vitit 2001, ndërsa paketa e dytë ligjore e BE-së ka funksion rregullator lidhur me krimet kompjuterike.

[205]http://www.enisa.europa.eu/act/cert.

Kjo paketë përfshin një sërë direktivash si dhe vendimin e Këshillit të Europës të vitit 2005, mbi sulmet kundër sistemeve të informacionit[206] dhe direktivat e BE-së të tilla si: çështje që mbulojnë fushat ligjore për mbrojtjen e të dhënave personale (95/46/EC, 2002/58/EC[207]); për shërbimet e shoqërisë së informacionit (2000/31/EC)[208]; për komunikimet elektronike (2002/58/EC)[209]; për ripërdorimin e informacioneve në sektorin shtetëror (2003/98/EC); për ruajtjen e të dhënave personale (2006/24/EC) etj. Legjislacioni i BE-së përcakton me anë të këtyre direktivave zbatimin nga shtetet anëtare dhe përshtatjen me ligjet kombëtare lokale, duke shtuar sanksione kundër sulmeve dhe kërcënimeve kompjuterike.

Është i rëndësishëm koordinimi mes institucioneve dhe agjencive të përmendura më sipër duke përdorur rregullat dhe bazën ligjore për përqendrimin e politikave në lehtësimin e procedurave për mbrojtjen kundër krimeve kibernetike.

Strukturat dhe institucionet e ndryshme në vendit tonë, që operojnë në fushën e teknologjisë së informacionit dhe komunikimit, duhet të angazhohen dhe përfshihen në aktivitete, konferenca dhe veprimtari të ndryshme, të cilat organizohen nga organizatat ndërkombëtare, në mënyrë që niveli i njohurive dhe informacionit, rekomandimet dhe standardet e duhura që kanë këto organizata, të mund të implementohen edhe në vendin tonë.

Siguria e informacionit lidhet gjithashtu me mbështetjen politike vendimarrëse dhe ligjore, jo vetëm teknike. Ndërhyrja në nivel politik do të ndihmojë në harmonizimin e legjislacionit në këtë fushë dhe do të lehtësojë marrëdhëniet për sigurinë kibernetike me vendet e tjera. Rritja e numrit të krimeve në faqet e internetit, ka ndikuar në zhvillimin e teknologjisë së informacionit. Ky zhvillim ka sjellë si rezultat shtrirjen e mbrojtjes kibernetike në nivel ndërkombëtar. Meqenëse mungojnë pengesat konkrete në hapësirën virtuale dhe sulmet kibernetike ndodhin sa më shpesh, kontrolli dhe koordinimi ndërmjet autoriteteve të ligjit është thelbësor.

[206]http://ec.europa.eu/justice/doc_centre/privacy/law/index_en.htm.

[207]http://ec.europa.eu/internal_market/e-commerce/index_en.htm.

[208]http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.

[209]http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0098:EN:HTML.

Strukturat e zbatimit të ligjit brenda vendit tonë duhet të përfshihen në bashkëpunime të ndërsjellta me Interpolin, Europolin dhe agjenci të tjera ndërshtetërore, të cilat operojnë në luftën kundër krimit kibernetik.

Meqënëse hapësira e informacionit ka dimension global, kërcënimi dhe sulmet mund të ndodhin nga brenda dhe jashtë kufijve të shtetit, pra është i nevojshëm bashkëpunimi i fortë me shtetet, organizatat ndërkombëtare, kompanitë private, agjencitë e rrjeteve kompjuterike, ekspertët ligjorë, institutet akademike, etj. Qeveria duhet të jetë motorri që duhet të vë në lëvizje hallkat e strukturave në varësi të saj dhe të nxisë bashkëpunimin ndërmjet strukturave të mbrojtjes së informacionit brenda dhe jashtë territorit të vendit.

Për të arritur zhvillime të reja në bashkëpunimin ndërkombëtar duhen shfrytëzuar edhe pjesëmarrjet e vendit tonë në organizatat ndërkombëtare dhe komitetet, konferencat ku diskutohet mbi zhvillimin e mbrojtjes së informacionit. Janë disa organizata ndërkombëtare të rëndësishme si Kombet e Bashkuara (OKB), ku në mbledhjet mbi çështjet e sigurisë së informacionit drejtohen nga një grup i nivelit të lartë ekspertësh të Forumit të Qeverisjes së Internetit (IGF), si dhe Bashkimi Ndërkombëtar i Telekomunikacionit (ITU). Organizatë tjetër ndërkombëtare që merret me kërkime në fushën e sigurisë së informacionit është Instituti i Kombeve të Bashkuara për trajnime dhe kërkime, me zyrën qëndrore në Gjenevë.

Shteti shqiptar duhet të krijojë ura bashkëpunimi me këto organizata dhe sidomos me agjencitë evropiane, jo vetëm në shkëmbimin e eksperiencave, por dhe në trajnimin e specialistëve shqiptar në këto struktura.

5. Përdorimi i internetit në Shqipëri. Të dhënat Statistikore të AKEP-it

Përdorimi i Teknologjisë së Informacionit është rritur ndjeshëm në vitet e fundit. Sipas të dhënave të publikuara nga AKEP, aksesi broadband internet ka pasur rritje të ndjeshme si për lidhjet broadband fiks me 14% gjatë vitit 2013, ashtu dhe në mobile broadband, respektivisht për lidhjet me kartë modem dhe USB me 88 - 101% gjatë vitit 2013, dhe me një rritje të aksesit nëpërmjet cards/modems/keys u rrit me rreth 22% në krahasim me fundvitin 2013.

Gjatë gjashtë mujorit të pare të 2014 numri i pajtimtarëve me akses broadband nga rrjetet fikse pati një rritje prej 3.3% kundrejt vitit 2013, dhe shumica e operatorëve kanë

pasur rritje të numrit të pajtimtarëve. Numri total i lidhjeve broadband fiks në fund të vitit 2013 arriti në 182.556, ndërsa gjatë gjashtëmujorit të parë të 2014 numri i pajtimtarëve me akses broadband nga rrjetet fikse pati një rritje prej 3.3% kundrejt vitit 2013 duke arritur kështu ne 188,668, dhe shumica e operatorëve kanë pasur rritje të numrit të pajtimtarëve.

Përdoruesit e internetit në Shqipëri janë rritur me disa herë në vitet e fundit. Sipas të dhënave të publikuara nga Bashkimi Ndërkombëtar i Telekomunikacionit, penetrimi i internetit në Shqipëri në dhjetë vitet e fundit është rritur nga 0.97% në vitin 2003 në mbi 63.3 % në vitin 2014 (shiko fig.1).

Figura-1. Numri i pajtimtarëve me akses Broadband nga rrjete Fikse 2003-2014[210]

Viti	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**
Shqipëria	**0.97**	**2.42**	**6.04**	**9.61**	**15.04**	**23.86**	**41.20**	**45.00**	**49.00**	**54.66**	**60.10**	**63.30**

Ajo që evidentohet është fakti se numri i shkeljeve të sigurisë së rrjeteve dhe sigurisë së informacionit është duke u rritur me shpejtësi duke shkaktuar humbje financiare dhe duke krijuar rreziqe dhe kërcënime të reja për zhvillimin e Shoqërisë së Informacionit. Në këtë kuadër rëndësi të veçantë ka bërja e ndryshimeve ligjore për t'iu përshtatur marrëdhënieve ekzistuese mes publikut dhe institucioneve shtetërore në mënyrë që të ofrohet mbrojtje të përshtatshme për përdoruesit, për të rritur besimin e tyre në teknologjitë e informacionit dhe për të inkurajuar përdorimin e avancuar dhe të sigurt të këtyre teknologjive.

Vlerësohet si tejet e nevojshme marrja e veprimeve dhe masave specifike për të ndërgjegjësuar shoqërinë lidhur me rreziqet potenciale në fushën e sigurisë së rrjeteve dhe sistemeve për eliminimin e këtyre rreziqeve, përfshirë mbrojtjen e fëmijëve nga përmbajtjet e paligjshme në hapësirën kibernetike. Incidentet e sigurisë që ndikojnë në funksionimin e duhur të rrjeteve, sistemeve dhe shërbimeve që ndërhyjnë në privatësinë e komunikimit është e nevojshme të menaxhohen duke u mbështetur në praktikat më të mira botërore për menaxhimin e incidenteve të tilla, nëpërmjet Ekipeve për Reagim ndaj Emergjencave Kompjuterike (ang. Computer Emergency Response Team (CERT).

[210] AKEP, http://www.akep.al .

6. Trajnimet mbi krimin kibernetik në Shqipëri

Duke pasur parasysh zhvillimin e krimeve kibernetike dhe pasojat që ato kanë në një shoqëri të prirur drejt teknologjisë, gjyqtarët dhe prokurorët duhet të jenë të përgatitur që të përballen me krimin kibernetik dhe provat elektronike. Edhe pse shumë vende të zhvilluara kanë ngritur organet dhe strukturat e posaçme për të parandaluar dhe luftuar fenomenin e krimit kibernetik, duke fuqizuar kapacitetet e tyre për hetimin e krimit kibernetik dhe për sigurimin e provave elektronike, duket se kjo nuk është arritur po në atë shkallë edhe nga gjyqtarët dhe prokurorët në Shqipëri.

Në pjesën më të madhe të rasteve në Shqipëri, gjyqtarët dhe prokurorët hasin vështirësi kur përballen me realitetet e reja të botës kibernetike. Kështu që nevojiten përpjekje të posaçme që gjyqtarët dhe prokurorët të përshtaten dhe aftësohen lidhur krimin kibernetik nëpërmjet trajnimit, krijimit të rrjeteve dhe specializimeve. Një nismë për të arritur këtë qëllim është zhvilluar nga Projekti i Këshillit të Evropës për Krimin Kibernetik dhe nga Rrjeti i Lisbonës për institucionet e trajnimit të gjyqësorit në bashkëpunim me një grup pune të përbërë prej palëve të interesuara gjatë vitit, ku theksohet se trajnimi i gjyqtarëve dhe prokurorëve në lidhje me veçoritë që paraqesin krimet kibernetike është mjaft i rëndësishëm për të kuptuar dhe vlerësuar drejt nëse në rastet e paraqitura për gjykim plotësohen elementët e nevojshëm për ekzistencën e veprës penale[211].

Kështu, njohja e teknikave të përdorura nga keqbërësit për realizimin e veprave penale kibernetike është e nevojshme për të përcaktuar nëse shkelja e kryer ka plotësuar elementin material (objektiv) si element i domosdoshëm për të vërtetuar kryerjen e veprës penale dhe zbatimin si rrjedhim të përgjegjësisë penale.

Trajnimi i gjyqtarëve dhe prokurorëve mbi këto çështje përfshin trajnimin fillestar dhe vazhdues nëpërmjet përgatitjes së materialeve përkatëse trajnuese, ashtu sikurse përfshirjen e moduleve trajnuese mbi temat në fjalë, në kurrikulat e institucioneve që realizojnë edukimin e gjyqtarëve dhe prokurorëve të ardhshëm.

---

[211] *Trajnim për krimin kibernetik për gjyqtarë dhe prokurorë: një koncept*, Departamenti iShoqërisë së Informacionit dhe Aksionit kundër Krimit Drejtoria e Përgjithshme e të Drejtave të Njeriut dhe Çështjeve Ligjore Strasburg, Francë 8 Tetor 2009, www.coe.int/cybercrime.

Për tu përmendur në këtë kontekst është trajnimi i mbajtur për zbatimin e legjislacionit mbi krimin kibernetik në Shqipëri me 16-17 Prill 2009, organizuar nga Prokuroria e Përgjithshme me bashkëpunimin e Këshillit të Europës me objektiv kryesor nxitjen e zbatimit të legjislacionit shqiptar në hetimin, ndjekjen, gjykimin dhe bashkëpunimin ndërkombëtar kundër krimit kibernetik si dhe trajnimi i organizuar në kuadër të krijimit të strukturave të specializuara, nga Prokuroria e Përgjithshme në bashkëpunim me Misionin PAMECA më datë 10.06.2014, për të diskutuar mbi fenomenin e krimit kibernetik dhe tendencat e tij[212].

[212]Prokuroria e Përgjithshme. http://www.pp.gov.al/.

KAPITULLI V: HETIMI I KRIMIT KIBERNETIK DHE PROVAT KOMPJUTERIKE

1. Karakteristikat e provave kompjuterike dhe parimet e trajtimit të tyre

Provat kompjuterike karakterizohen nga disa cilësi që veshtirësojnë trajtimin e tyre dhe që kërkojnë aftësi të mira profesionale dhe kualifikimin e duhur për tu marrë me evidentimin dhe ruajtjen e tyre.

Më konkretisht prova kompjuterike rezulton të jetë e pashfaqur, njësoj si gjurmët e gishtave apo ADN-ja, ajo i kapërcen kufinjtë juridikë shpejt dhe mund të ndryshohet, dëmtohet apo prishet me lehtësi dhe mbi të gjitha është e ndjeshme ndaj faktorit kohë[213].

Kur kemi të bëjmë me prova komjuterike, pikërisht për shkak të karakteristikave dhe natyrës së veçantë që paraqesin, duhen zbatuar me rigorozitet parimet e mëposhtme:

- *Procesi i mbledhjes, sigurimit dhe transportimit të provave kompjuterike nuk duhet ta ndryshojë provën.*
- *Prova kompjuterike mund të ekzaminohet vetëm nga persona të kualifikuar posaçërisht për këtë gjë.*
- *Çdo veprim i kryer gjatë bllokimit, transportimit apo ruajtjes së provës kompjuterike, duhet të dokumentohet.*
- *Personeli policor duhet të bëjë kujdes kur bllokon pajisje kompjuterike me cilësinë e provës. Hyrja jo e duhur tek të dhënat e ruajtura në pajisjen kompjuterike mund të dhunojë ligjet, për këtë arsye, atyre mund t'ju duhet të sigurojnë autoritet ligjor përpara se të veprojnë më tej. Ata duhet menjëherë të kontaktojnë prokurorinë për tu konsultuar nëse kanë juridiksionin e duhur.*

Përveç problemeve ligjore në rastin e ndërhyrjes tek të dhënat e ruajtura në kompjuter, personeli policor duhet gjithashtu të kuptojë që të dhënat në kompjuter apo provat komjuterike në përgjithësi janë shumë delikate. Vetëm personeli posaçërisht i kualifikuar duhet të ekzaminojë dhe analizojë provat kompjuterike[214].

---

[213]Chamelin, & L. Territo (Eds), (2003). "*Criminal Investigation".* (8th ed). New York: McGraw- Hill Companies, Inc, pp. 6-22.

[214]Kovacich, G. L. & Boni, W. C. (2000). H*igh-technology crime investigator'shandbook:Working in the global information environment*. Woburn, MA: Butterworth- Heinemann. pp. 13-22.

2. Prova kompjuterike dhe legjislacioni procedurial penal shqiptar

Me ligjin nr.10054 date 29.12.2008 "*Për disa shtesa dhe ndryshime në kodin e procedures penale*" në nenin 191 të kodit të procedurës penale u shtua neni 191/a me këtë përmbajtje: *"Neni 191/a* : *Detyrimi për paraqitjen e të dhënave kompjuterike.*

1.Gjykata, në rastin e procedimeve për vepra penale në fushën e teknologjisë së informacionit, me kërkesë të prokurorit ose të të dëmtuarit akuzues, urdhëror, mbajtësin ose kontrolluesin të dorëzojnë të dhënat kompjuterike të memorizuara në një sistem kompjuterik apo në një mjet tjetër memorizimi.

2. Gjykata, në këto procedime, urdhëron edhe dhënësin e shërbimit, për dorëzimin e çdo informacioni për abonentët e pajtuar, për shërbimet e ofruara nga dhënësi[215].

3. Kur ka arsye për të menduar se nga vonesa mund t'u vijë një dëm i rëndë hetimeve, prokurori vendos, me akt të motivuar, detyrimin për paraqitjen e të dhënave kompjuterike, të përcaktuara në pikat 1 dhe 2 të ketij neni dhe njofton menjëherë gjykatën. Gjykata vlerëson vendimin e prokurorit brenda 48 orëve nga njoftimi.

Përkufizimi i të dhënave kompjuterike dhe sistemeve kompjuterike është dhënë në Konventën "Për krimin në fushën kibernetikës" ratifikuar nga Parlamenti Shqiptar me ligjin 8888 datë 25.04.2002 Për ratifikimin e "Konventës për Krimin në Fushën e Kibernetikës"[216].

Neni 1 i Koventës[217] sanksionon se:

"Sistem kompjuterik" do të thotë çdo lloj pajisje apo grup i ndërlidhur, a) ose pajisje të lidhura, një ose më shumë prej të cilave, vazhduese të një programi kryejnë procesime automatike të të dhënave.

"Të dhëna komjuterike" do të thotë çfarëdolloj përfaqësimi i fakteve, b) informacioni apo konceptesh në një formë të përshtatshme për procesim në një sistem kompjuterik, që përfshijnë një program të përshtatshëm për punën e një sistemi komjuterik për të kryer një funksion.

---

[215] *Neni 191/a Kodi i pr.Penale* : *Detyrimi për paraqitjen e të dhënave kompjuterike.*

[216] Shiko, ligjin nr.10054 date 29.12.2008 "*Për disa shtesa dhe ndryshime në Kodin e Procedures Penale*".

[217] Shiko, ligjin 8888 datë 25.04.2002 *Për ratifikimin e "Konventës për krimin në fushën e kibernetikës*".

"Dhënës shërbimesh" do të thotë:

(i) çfarëdo enti publik apo privat, që i siguron shërbimin e tij përdoruesve, me mundësinë për të komunikuar nëpërmjet një sistemi kompjuterik; dhe

(ii) çfarëdo entiteti tjetër, që proceson apo memorizon të dhëna kompjuterike në të mirë të një shërbimi të ketillë komunikimi apo të përdoruesve për këtëshërbim.

Neni 18 pika 3 i Koventës jep përkufizimin e informacionit të abonentit sipas të cilit:

"Informacion abonenti" do të thotë çfarëdo informacion i futur në formën e të dhënave kompjuterike apo çfarëdo forme tjetër, që mbahen nga dhënësi i shërbimit, që kanë të bëjnë me abonuesit e shërbimeve të tij, të ndryshme nga të dhënat e trafikut ose të përmbajtjes, nëpërmjet të cilave ai mund të tregojë:

(i) tipin e shërbimit të komunikimit të përdorur, kushtet teknike dhe përiudhën e shërbimit;

(ii) identitetin e abonentit/ave, adresën gjeografike apo postare, numrin e telefonit apo numrat e tjerë hyrës, informacion mbi faturat dhe pagesën, të siguruara në bazë të marrëveshjes apo të marrëveshjeve të shërbimit;

(iii) çdo informacion tjetër në ambientin e instalimit të pajisjeve të komunikimit, të disponueshme në bazën e marrëveshjes apo të marrëveshjeve të shërbimit.

Ndërsa referuar legjislacionit të brendshëm procedural në nenin 208/a të Kodit të Procedures Penale është rregulluar, ***Sekuestrimi i të dhënave kompjuterike sipas të cilit:***

1. Në rastin e procedimeve për vepra penale në fushën e teknologjisë së informacionit, gjykata, me kërkesë të prokurorit, vendos sekuestrimin e të dhënave dhe sistemeve kompjuterike. Në këtë vendim, gjykata përcakton të drejtën për të hyrë, kërkuar dhe marrë të dhënat kompjuterike në sistemin kompjuterik, si dhe ndalimin për kryerjen e veprimeve të mëtejshme apo sigurimin e të dhënave ose të sistemit kompjuterik.
2. Kur ekzistojnë shkaqe të arsyeshme për të menduar se të dhënat e kërkuara kompjuterike janë memorizuar në një sistem kompjuterik, apo në një pjesë të tij, dhe këto të dhëna janë në mënyrë të ligjshme të kapshme prej/ose janë të disponueshme nga sistemi kompjuterik fillestar që kontrollohet, gjykata, me kërkesë të prokurorit, urdhëron menjëher kërkimin ose hyrjen edhe në këtë sistem kompjuterik.
3. Në zbatim të vendimit të gjykatës, prokurori ose oficeri i policisë gjyqësore, i deleguar nga prokurori, merr masa:

(i) për të ndaluar kryerjen e veprimeve të mëtejshme ose për të siguruar sistemin kompjuterik, vetëm të një pjese të tij ose të një mjeti tjetër memorizimi të dhënash;

(ii) për të nxjerrë dhe marrë kopje të të dhënave kompjuterike;

(iii) për të penguar hyrjen në të dhënat kompjuterike ose për t'i hequr këto të dhëna nga sistemet kompjuterike me të drejtë hyrje;

(iv) për të siguruar paprekshmërinë e të dhënave përkatëse të memorizuara.

4. Për zbatimin e këtyre veprimeve, prokurori mund të urdhërojë thirrjen e një eksperti, i cili ka njohuri rreth funksionimit të sistemeve kompjuterike apo masave të zbatuara për mbrojtjen e të dhënave kompjuterike në të. Eksperti i thirrur nuk mund të refuzojë detyrën pa shkaqe të arsyeshme.

Në nenin 299/a të Kodit të Procedurës Penale është rregulluar, ***Ruajtja e përshpejtuar dhe mirëmbajtja e të dhënave kompjuterike, sipas të cilit:***

1. Prokurori mund të urdhërojë ruajtjen e përshpejtuar e të dhënave kompjuterike të caktuara, duke përfshirë të dhënat e trafikut, kur ka shkaqe të mjaftueshme për të besuar se të dhënat mund të humbasin, dëmtohen ose ndryshohen.
2. Në rastin kur të dhënat kompjuterike janë në zotërim ose në kontroll të një personi, prokurori mund të urdhërojë këtë person t'i ruajë dhe t'i mirëmbajë keto të dhëna kompjuterike për një përiudhë deri në 90 ditë, me qëllim zbulimin dhe nxjerrjen e tyre.
3. Personi i ngarkuar për ruajtjen dhe mirëmbajtjen e të dhënave kompjuterike detyrohet të mbajë sekret procedurat dhe veprimet e kryera sipas pikës 2 të ketij neni, deri në përfundim të hetimeve.

Në nenin 299/b të Kodit të Procedurës Penale është rregulluar, ***Ruajtja e përshpejtuar dhe zbulimi i pjesshëm i të dhënave kompjuterike, sipas të cilit:***

1. Personi i ngarkuar me ruajtjen e përshpejtuar të të dhënave të trafikut, detyrohet të marrë të gjitha masat e nevojshme, për të garantuar se të dhënat e ruajtura janë të vlefshme, pavarësisht nëse një apo më shumë dhënës shërbimesh kanë qenë të përfshirë në transmetimin e komunikimit, si dhe t'i sigurojë prokurorisë ose oficerit të policisë gjyqësore, të autorizuar, zbulimin e një sasie të mjaftueshme të të dhënave të trafikut, në mënyrë që të mundësohet identifikimi i dhënësit të shërbimit dhe shtegu, nepërmjet të cilit komunikimi është transmetuar.

Përkufizimi '*të dhëna trafiku'* është dhënë në Konventën për krimin në fushën kibernetikës ratifikuar nga Parlamenti Shqiptar me ligjin 8888 date 25.04.2002 Për ratifikimin e "Konventës për Krimin në Fushën e Kibernetikës": Sipas nenit 1 të Koventës, "*Të dhëna trafiku*" do të thotë çdo lloj të dhënash kompjuterike, të lidhura me komunikimin nëpërmjet një sistemi kompjuterik të prodhuara nga një sistem kompjuterik që përfaqëson një pjesë në zinxhirin e komunikimit, duke treguar origjinën e komunikimit(eve) destinacionin, rrugën, kohën, datën, përmasat, kohëzgjatjen apo tipin e shërbimit të poshtëshënuar.

3. Pajisjet elektronike, tipet, përshkrimi dhe provat e mundshme

Një hard disk i brendshëm kompjuteri apo një hard disk i jashtëm dhe çdo pajisje tjetër elektronike, të gjetura në vendin e ngjarjes mund të përmbajnë informacion të vlefshëm si provë gjatë një hetimi apo procedimi penal. Vete pajisja me informacionin e depozituar që mund të përmbajë në vetvete, mund të shërbëjë si provë kompjuterike[218].

3.1. Sistemet kompjuterike

Nje sistem kompjuterik përbëhet nga hardware dhe software që përpunon të dhënat dhe përfshin:

- Një motherboard që përmban hard disk, mikroprocesorë dhe lidhje interface.
- Një ekran ose një pajisje për transmetim video.
- Një tastierë.
- Një mi (maus).
- Drivera dhe komponentë periferike apo të brendshëm.

Një sistem kompjuterik dhe komponentët e tij mund të përbëjnë prova të rëndësishme gjatë hetimit. Një hardware, një software, dokumentet, email-i dhe dosjet bashkëngjitur, historiku i navigimit në internet, diskutimet në dhomat e chat-it, fotografitë, database-t, rekordet financiare etj, mund të përbëjnë dhe të përmbajnë prova të mundshme dhe të vlefshme për hetimin[219].

---

[218]Chamelin, & L. Territo (Eds), (2003). "*Criminal Investigation".* (8th ed). New York: McGraw- Hill Companies, Inc, pp. 18-29.

[219]Stephenson, P. (2000*). "Investigating computer-related crimes".* New York: CRC Press LLC, pp. 22-27.

Sistemet kompjuterike dhe pajisjet e lidhura me to mund të përbëjnë provë të vlefshme për një hetim apo procedim. Gjithashtu edhe informacioni që përmbajnë mund të vlejë si provë e mundshme, mund të përmendim këtu softin, dokumente, foto, informacion financiar, mesazhe e mail, histori të eksplorimit në internet, listë kontaktesh dhe çdo të dhënë tjetër të ruajtur në kompjuter. Janë gjithashtu të rëndësishme, funksionet, kapacitetet, si dhe çdo informacion tjetër identifikues që lidhet me sistemin kompjuterik, komponentet dhe lidhjet, përfshirë protokollin e internetit (IP), adresat e rrjetit lokal (LAN), MAC adresat, adresat e work interface card (NIC), etj[220].

3.2. Pajisjet për ruajtjen e informacionit

Pajisjet e ruajtjes së informacionit mund të variojnë në madhësi dhe në mënyrën si ato ruajnë të dhënat. Personeli policor në vendngjarje, duhet të kuptojë se pavarësisht madhësisë apo tipit**,** këto pajisje mund të përmbajnë informacion të vlefshëm për hetimin ose procedimin.

Si provë kompjuterike e vlefshme mund të shërbejnë pajisjet e mëposhtme:

- **Hard disqet.** Hard disqet, (hard drivers) janë pajisje të ruajtjes së informacionit që konsistojnë në një '*circuit board*' të jashtëm të lidhur me kabllo dhe me pllaka xhami, qeramike, apo metali të magnetizuara, në pjesën e brendshme, për të ruajtur të dhëna. Personeli në vendngjarje mund të gjejë hard disqe që nuk janë të instaluar apo të lidhur me një kompjuter. Këto mund të përmbajnë prova materiale të rëndësishme[221].
- **Hard disqet e jashtëm**. Këto pajisje rrisin aftësitë e ruajtjes së të dhënave të kompjuterit dhe shërbejnë si mbajtëse lëvizëse të dhënash. Zakonisht një hard disk i jashtëm kërkon ushqyes rryme dhe një portë USB, FireWire, Ethernet, ose lidhje wireless me sistemin kompjuterik.
- **Mediat e lëvizshme.** (Removable media), janë gjithashtu pajisje që shërbejnë për depozitimin dhe transferimin e të dhënave digitale. Ndryshe këto i quajmë: Disketa, CD (Compact Disk), Zip Disketa etj.

[220]Kovacich, G. L. & Boni, W. C. (2000). "*High-technology crime investigator's handbook:Wworking in the global information environment"*. Woburn, MA:Butterworth- Heinemann, pp.12-53.

[221]Clifford (Ed). *Cybercrime: The investigation, prosecution, and defense of a computer-related crime* (pp. 11-68). Durham, NC: Carolina Academic Press.

- **Thumb drive.** Janë pajisje të lehta që lidhën me portë USB, njihen dhe me emrin Flashdrive, Pendisk ose ndonjëherë thjesht USB. Janë të lehtë për tu fshehur dhe transformuar. Mund të gjenden edhe si pjesë ose të maskuara si orë dore, vegël xhepi shumëpërdorimshe, si mbajtëse çelësash, stilolaps etj.
- **Kartat e Memories.** Kartat e memories janë pajisje të vogla për mbajtjen e të dhënave të cilat zakonisht përdoren me aparatet fotografike, video kompjuterike, celularë, luajtës muzike MP3 etj.

3.3. Pajisjet e dorës

Pajisje të dorës janë pajisje të lëvizshme të ruajtjes së të dhënave që sigurojnë komunikim, fotografim, video regjistrim, navigim, zbavitje dhe manaxhim të informacionit personal. Paisjet e dorës të tilla si telefonët celularë, smartphone, PDA-të, pajisjet kompjuterike multimediale, pagers, GPS-ët , mund të përmbajnë softe aplikative, të dhëna apo informacione të tilla si SMS-të, mesazhe e-mail, historik të eksplorimit në internet, lista kontaktesh foto, rekorde financiare. Të gjitha keto mund të përbëjnë elementë të rëndësishëm prove për hetimin apo procedimin[222].

Është e rëndësishme që të kemi parasysh se:

- E dhëna ose prova kompjuterike mund të humbasë nëse ndërpritet rryma elektrike që e ushqen;
- E dhëna ose prova kompjuterike në disa pajisje të tilla si telefonat smart apo mobil mund të mbishkruhet ose të prishet nëse pajisja mbetet e aktivizuar;
- Softi që është i vlefshëm për telefona smart ose mobil mund të aktivizohet në distancë duke e bërë telefonin të papërdorshëm dhe t'i bëjë të dhënat që ndodhen në të të pa-aksesueshme, nëse telefoni humbet apo vidhet. Ky soft mund të prodhojë rezultate të njëjta nëse aktivizohet në një pajisje të bllokuar nga agjencitë e zbatimit të ligjit. Personeli që shkon i pari në vendgjarje duhet të bëjë kujdes që të mos humbasin të dhënat e ruajtura në pajisjen e bllokuar që shërben si provë materiale[223].

[222]Clifford, R.D. (2001). "*Cybercrime, the investigation, prosecution and defense of a Computerrelated crime"*, Carolina Academic Press, United States, pp.169.

[223]Model Code of Cybercrime Investigative Procedure, Article VII, at: http://www.cybercrimes.net/MCCIP/art7.htm.

3.4. Pajisjet periferike

Pajisje periferike janë ato pajisje, të cilat lidhen me një kompjuter ose sistem kompjuterik për të rritur kapacitetin aksesues të përdoruesit dhe funksionet e kompjuterit.

Vetë pajisjet si dhe funksionet që ato kryejnë apo lehtësojnë janë të gjitha prova të mundshme. Informacioni që ruhet në pajisje mund të përbëjë provë gjithashtu, të tilla si numrat e faksit apo thirrjet hyrëse dhe dalëse, dokumentet e fundit të skanuar, fotokopjuar apo printuar, si dhe informacioni për arsyet e përdorimit të pajisjes. Këto pajisje mund të jenë dhe burim provash të tjera të tilla si gjurmët e gishtave, ADN, etj.

Personeli që mbërrin i pari në vendngjarje duhet të ketë dijeni dhe të marrë në konsideratë si prova të mundshme edhe elementë të tjerë të vendngjarjes që lidhen me informacionin dixhital të tilla si, pajisjet elektronike, ose teknologji të tjera që funksionojnë në mënyrë të pavarur, të lidhura ose bashkangjitur një sistemi.

*3.5. Aparate të tjera elektronike dhe periferike që vlejnë si prov***a**

Aparaturat elektronike si ato të renditura më poshtë, mund të përmbajnë informacion me vlerë për një hetim. Përveç rasteve të emergjencës, aparatura të tilla nuk duhet të përdoren dhe informacioni që mund të përmbajnë nuk duhet të preket direkt. Nëse situata kërkon që këto aparatura të kontrollohen menjëherë, të gjitha veprimet që do të ndërmerren duhet të dokumentohen me hollësi. Të dhënat mund të humbasin nëse aparatura nuk operohet me saktësi ose nëse të dhënat nuk kontrollohen sipas procedurës së kërkuar.

Më poshtë do të paraqiten shembuj të aparaturave elektronike, komponenteve dhe pajisjeve të tjera të cilat personi i parë në vendngjarje duhet të mbledhë si provë kompjuterike:

- Regjistrues audio.
- Aksesorë të GPS.
- Sekretari telefonike.
- Cip kompjuteri.
- Peixher.
- Telefonë pa kordon.
- Fotokopje.
- Celularë.
- Duplikues për hard-drive.

- Pajisje faksi.
- Printera.
- Pajisje shumëfunksionale (printer, skaner, fotokopje, dhe faks).
- Pika aksesi pa tela "wireless".
- Aksesorë dhe bateri për laptop.
- Karta smart.
- Video-regjistrator (VCR).
- Skaner.
- Pajisje për identifikimin e telefonuesit.
- Karta e memorjes së kompjuterit (PCMCIA).
- PDA.

Trajtim i veçantë mund të kërkohet për të ruajtur integritetin dhe vlerën faktuese të këtyre pajisjeve elektronike. Personi i parë në vendngjarje duhet të sigurojë pajisjet dhe të kërkojë asistencë nga një person i trajnuar në mbledhjen e provës kompjuterike. Kur mblidhen pajisjet elektronike, komponentët, dhe pjesë të tjera si ato të renditura më lart, duhet pasur parasysh që të mblidhni kabllot dhe adaptoret përkatës të këtyre pajisjeve[224].

4. Pajisjet dhe mjetet investigative

Në shumicën e rasteve, objektet apo pajisjet që përmbajnë prova kompjuterike, mund të trajtohen duke përdorur pajisje standarde. Personeli në vendgjarje duhet të bëjë kujdes me mbledhjen dhe paketimin e provave, për të evituar, transformimin, dëmtimin apo shkatërrrimin e tyre. Duhet evituar përdorimi i pajisjeve që emetojnë ose prodhojnë elektricitet statik ose fushë magnetike.

Nëse vendgjarja ku do të fiksohen prova dixihitale është komplekse, duhet kërkuar asistencë e specializuar nga punonjës që janë posaçërisht të trajnuar në këtë profil[225].

---

[224]Parker, D. B. (1999). *Sharing infrastructures: Cybercrime intelligence*. Paper presented at a conference on cybercrime and terrorism, Stanford, CA.

[225]Chamelin, & L. Territo (Eds), *Criminal Investigation* (8th ed). New York: McGraw- Hill Companies, Inc. f. 33-54.

Personeli në vendgjarje përveç mjeteve me cilësi që përmendëm më sipër duhet të jetë i pajisur edhe me çanta që shërbejnë për vendosjen e provave, të cilat duhet të jenë të pajisura me material izolues alumini për të paketuar pajisjet e ndryshme elektronike, siç janë telefonët smart apo celular, për të evituar pikërisht frekuencat e radios, apo për të mos lejuar një thirrje hyrëse apo SMS në pajisjen në fjalë, që mund të transformojë provën materiale.

5. Sigurimi dhe vlerësimi i vendit të ngjarjes ku është konsumuar një vepër penale kibernetike

Pasi të ketë arritur sigurinë në vendin e ngjarjes, personeli duhet të identifikojë vizualisht për tu siguruar nëse është ruajtur integriteti i provave të mundshme kompjuterike dhe atyre tradicionale. Menjëherë çdo gjë duhet të fotografohet.

- ***Hapat që rekomandohet të ndërmerren janë:***

1. Ndjekja e politikave të departamentit për sigurimin e vendit të ngjarjes.
2. Sigurimi i menjëhershëm i të gjitha pajisjeve elektronike, përshirë dhe pajisjet personale apo portable (të lëvizshme).
3. Duhet të sigurohet që asnjë person i pa-autorizuar të mos prekë pajisjet kompjuterike në vendin e ngjarjes.
4. Duhet të refuzohet i çdo oferte për ndihmë apo asistencë teknike nga persona të pa-autorizuar.
5. Duhet të largohen të gjithë personat nga vendgjarja apo perimetri i afërt i vendit ku është bërë bllokimi i provës.
6. Sigurimi që kushtet e pajisjet elektronike nuk janë transformuar.
7. Nëse kompjuteri apo pajisja elektronike është e fikur, nuk duhet tentuar për ta vënë në punë.
8. Komponentë të tjerë, si tastiera, mausi, pajisje portable të ruajtjes së informacionit apo objekte të tjera mund të përmbajnë gjurmë gishtash, ADN, etj. Personeli i parë në vendngjarje duhet të marrë të gjitha masat për tu siguruar që prova të mos kompromentohet (prishet) gjatë dokumentimit[226].

[226]Model Code of Cybercrime Investigative Procedure, Article VII, at: http://www.cybercrimes.net/MCCIP/art7.htm.

- ***Nëse një kompjuter është i ndezur ose kur nuk duket qartë nëse është i ndezur apo jo, personeli i parë në vendin e ngjarjes duhet të:***
    1. Shikojë apo dëgjojë për indikacione apo tregues, që kompjuteri është i ndezur. Vini veshin dhe dëgjoni për zhurmën e ventilatorit në motherboard, zhurmën e rrotullimit të hard-diskut, si dhe shikoni nëse diodat e emetimit të dritës janë të ndezura (LEDs).
    2. Kontrollojë me sy ekranin për të parë mos ka ndonjë sinjal që tregon se prova kompjuterike mund të jetë shkatërruar. Shikoni për fjalë të tilla si **delete** (prish), **format** (formato), **remove** (hiq), **copy** (kopjo), **move** (lëviz), **cut** (pres), **wipe** (fshij).
    3. Shikojë nëse ka indikacione që kompjuteri mund të jetë aksesuar nga një kompjuter apo apo pajisje në distancë.
    4. Shikojë për shenja të ndonjë komunikimi aktiv apo në vazhdimësi me kompjutera të tjerë ose përdorues të tjerë si mesazhet në windows apo dhomat e chat-it në internet.
    5. Marrë shënim të gjitha kamerat ose kamerat WEB dhetëpërcaktojë nëse janë aktive në atë moment.
    6. Zhvillimet në teknologji dhe lidhjet në komunikim kanë bërë të mundur që edhe pajisjet me të zakonshme dhe konvencionale të lidhen me njëra-tjetrën, me kompjuterat dhe me internetin. Ky mjedis në zhvillim kaq të shpejtë shtron si detyrë esenciale për punonjësit e zbatimit të ligjit të kenë njohuri për provat kompjuterike në telefona, video-kamera apo pajisje të tjera shtëpiake.

6. Dokumentimi i vendit të ngjarjes

Dokumentimi i vendit të ngjarjes krijon një rekord për hetimin. Është e rëndësishme të regjistrohet në mënyrë të saktë vendndodhja, përshkrimi i përgjithshëm, gjendja e rrymës elektrike dhe ushqimit të pajisjeve, rrjeti i internetit kabllor ose wireless, telefonat celularë, PDA-të, apo pajisjet të tjera të ruajtjes së informacionit dixhital. Personeli në vendngjarje duhet të ketë dijeni për faktin që jo çdo provë kompjuterike mund të gjendet afër kompjuterit apo pajisjeve të tjera.

Personelit mund ti duhet të lëvizë kompjuterin apo pajisjet e tjera për të parë numrin serial ose elementë të tjerë identifikimi. Nëse lëvizja bëhet kur pajisja është e ndezur mund të dëmtohet prova kompjuterike që ajo përmban. Prandaj kompjuterat dhe pajisjet e tjera asnjëherë nuk duhen lëvizur pa i fikur përpara.

Dokumentimi i vendit të ngjarjes duhet të përfshijë një xhirim të detajuar me video, fotografim, skica dhe vizatime me qëllim që të gjitha detajët të kujtohen me lehtësi me vonë. Pjesë e dokumentimit duhet të jenë edhe informacione të tilla si vendndodhja e kompjuterave në zyrë, e pajisjeve periferike etj[227].

Vendngjarja mund të zgjerohet në shumë vende, personat që shkojnë të parët në vendngjarje duhet të dokumentojnë të gjitha lidhjet fizike në hyrje dhe dalje të kompjuterave ose aparaturave të tjera.

Çdo lidhje kompjuterike e pranishme që lidh kompjuterat dhe aparatura të tjera me njëra-tjetrën dhe internetin duhet regjistruar. Prania e lidhjeve kompjuterike mund të tregojë që prova të tjera mund të ekzistojnë përveç atyre të mbledhura në vendngjarjen kryesore. Disa rrethana mund të mos lejojnë personat që shkojnë të parët në vendngjarje të mbledhin të gjitha aparaturat elektronike ose pjesë të tyre në një vendngjarje ose vend tjetër. Ligjet në fuqi, politikat e agjencisë, ose faktorë të tjerë mund të ndalojnë mbledhjen e disa sistemeve kompjuterike dhe aparaturave të tjera elektronike si dhe informacionin që mbartin, megjithatë, këto aparatura duhet të përfshihen në dokumentimin e vendngjarjes[228].

7. Mbledhja e provave

Personi që shkon i pari në vendngjarje duhet të ketë autoritetin e duhur, si p.sh. vëzhgimi i vendngjarjes, aprovim, ose urdhër gjykate, për të kontrolluar dhe mbledhur fakte në një vendngjarje krimi kibernetik.

Personi i parë në vendngjarje duhet të jetë i aftë të prezantojë autoritetin me të cilin ai/ajo mund të marrë provën dhe duhet të ndjekë udhëzimet e agjencisë, të konsultohet me një drejtues, ose të kontaktojë një prokuror nëse ngrihet pyetja e autoritetit[229].

---

[227]Po aty

[228]Stephenson P. (2000*). Investigating computer-related crimes*. New York: CRC Press LLC, pp. 14-32.

[229]Kovacich, G. L. & Boni, W. C. (2000). H*igh-technology crime investigator's handbook:Working in the global information environment*. Woburn, MA:Butterworth- Heinemann., pp.22-44.

Provat elektronike duhet të merren me kujdes për të ruajtur integritetin e aparaturës elektronike si dhe të të dhënave që përmban. Disa prova elektronike kërkojnë teknika mbledhjeje, paketimi dhe transportimi të veçanta. Të dhënat mund të dëmtohen ose tjetërsohen nga fushat elektromangetike si ato të prodhuara nga elektriciteti statik, magnetet, transmetuesit me radio, dhe aparatura të tjera. Aparaturat e komunikimit si për shembull celularët, celularët me internet, PDA-të dhe pexherat duhet të sigurohen dhe parandalohen nga marrja ose transmetimi i të dhënave pasi të identifikohen dhe të mblidhen si prova materiale. Për të parandaluar ndryshimin e provës elektronike gjatë mbledhjes, personi i parë në vendin e ngjarjes duhet që në fillim:

(i) Të dokumentojë aktivitetin në kompjuter, pjesë të tij, ose aparatura;

(ii) Të konfirmojë statusin e kompjuterit, të kontrollojë për drita që ndriçojnë, ventilatorë që lëvizin, dhe tinguj të tjerë që tregojnë që kompjuteri ose aparatura elektronike është e ndezur. Nëse statusi i kompjuterit nuk mund të përcaktohet nga këta tregues, vëzhgoni monitorin për të përcaktuar nese është i ndezur, i fikur, ose në gjendje "gjumi".

- ***Pas identifikimit të statusit të kompjuterit, duhen ndjekur disa hapa në varësi të situatës si më poshtë:***

Situata 1: Monitori është ndezur. Shfaq një program, aplikim, produkt pune, foto, email, ose faqe interneti në ekran.

(i) Fotografoni ekranin dhe regjistroni informacionin që shfaqet aty;

(ii) Kaloni tek "Nëse kompjuteri është i ndezur (ON)"(shiko situatën 7).

Situata 2: Monitori është i ndezur dhe duket screensaver ose një foto.

(i) Lëvizni pak mausin pa shtypur asnjë buton dhe pa lëvizur mekanizmin rrotullues mbi të. Vëreni vetëm aktivitetin në ekran që shkakton pamjen të ndryshojë në faqe për të hyrë, produkt pune, pse shfaqjen të tjera të dukshme;

(ii) Fotografoni ekranin dhe regjistroni informacionin që shfaqet aty;

(iii) Kaloni tek "Nëse kompjuteri është i ndezur (ON)"(shiko situatën 7).

Situata 3:Monitori është ndezur, megjithatë ekrani është bosh sikur monitori të ishte i fikur.

(i) Lëvizni pak mausin pa shtypur asnjë buton dhe pa lëvizur mekanizmin rrotullues mbi të. Ekrani do ndryshojë nga ekran bosh në ekran për të hyrë, produkt pune, ose shfaqje tjetër. Vëreni ndryshimin në shfaqjene ekranit;

(ii) Fotografoni ekranin dhe regjistroni informacionin që shfaqet aty;

(iii) Kaloni tek "Nëse kompjuteri është i ndezur (ON)".

Situata 4a: Monitori është fikur. Ekrani është bosh (me ngjyrë të zezë).

(i) Nëse monitori është i fikur, atëherë ndizeni. Ekrani ndryshon nga bosh në faqe për të hyrë në kompjuter, produkt pune, ose shfaqje të tjera të dukshme. Vëreni ndryshimin në ekran;

(ii) Fotografoni ekranin dhe regjistroni informacionin që shfaqet aty;

(iii) Kaloni tek "Nëse kompjuteri është i ndezur (ON)"(shiko situatën 7).

Situata 4b:Monitori është fikur.Ekrani është bosh (me ngjyrë të zezë).

(i) Nese monitori është i fikur, atëherë ndizeni. Ekrani nuk ndryshon, ngelet bosh. Vëreni ndryshimin në ekran;

(ii) Fotografoni ekranin bosh;

(iii) Kaloni tek "Nëse kompjuteri është i ndezur (OFF)".

Situata 5: Monitori është i ndezur. Ekrani është bosh.

(i) Lëvizni pak mausin pa shtypur asnjë buton dhe pa lëvizur mekanizmin rrotullues mbi të, prisni për përgjigje;

(ii) Nëse ekrani nuk ndryshon dhe mbetet bosh, sigurohuni që monitori është i lidhur me linjën elektrike. Nëse ekrani mbetet bosh, kontrolloni kompjuterin për drita të ndezura, degjoni ventilatorin ose tregues të tjerë për të parë që kompjuteri është i ndezur;

(iii) Nëse ekrani mbetet bosh dhe kompjuteri nuk jep asnjë shenjë të jetë i ndezur, kaloni tek **"**Nëse kompjuteri është i ndezur (OFF)"(shiko situatën 6).

Situata 6: Për kompjuterat e tavolinës (Desktop), dhe minikompjuterat duhen ndjekur këto hapa:

1. Dokumento, fotografo, dhe skico të gjithë telat, kabllot, dhe aparaturat e tjera të lidhura me kompjuterin;

2. Etiketo kabllin kryesor dhe të gjithë kabllot, telat ose USB të lidhura me kompjuterin si dhe lidhjet korresponduese me çdo kabllo, tel, USB në kompjuter;
3. Fotografo kabllot e etiketura, telat dhe USB si dhe lidhjet korresponduese të etiketuara;
4. Hiq dhe siguro kabllin elektrik nga mbrapa kompjuterit dhe priza në mur, zgjatuesi, ose bateria;
5. Stakoni dhe siguroni të gjithë kabllot, telat dhe USB nga kompjuteri dhe dokumento aparaturën ose pajisjen e lidhur në anën tjetër;
6. Vendosni ngjitëse mbi vendin e disketës, nëse ka;
7. Sigurohuni që vendet për CD ose DVD janë në vendet e tyre, vëreni nëse këto vende janë bosh, kanë CD brenda ose nuk janë kontrolluar, me pas mbylleni vendin e CD me ngjitëse që të mos hapet më;
8. Vendosni ngjitëse tek butoni i ndezjes;
9. Regjistroni markën, modelin, numrin serial, dhe çdo shenjë tjetër të vendosur nga përdoruesi;
10. Regjistroni kompjuterin dhe të gjithë kabllot, telat, aparaturat dhe pjesët e tjera sipas procedurave të agjencisë;
11. Paketoni provat e mbledhura sipas procedurave të agjencisë për të parandaluar dëmtime ose tjetërsime gjatë transportit dhe magazinimit;

- Për kumpjuterat laptop, duhet të ndiqen këto hapa:

1. Dokumento, fotografo, dhe skico të gjithë telat, kabllot, dhe aparaturat e tjera të lidhura me laptopin.
2. Etiketo të gjithë telat, kabllot dhe aparaturat të lidhura me laptopin si dhe lidhjet që përfaqësojnë.
3. Fotografo dhe etiketo kabllot, telat, dhe aparaturat e lidhura me laptopin dhe lidhjet e tyre korresponduese të etiketuara.
4. Hiq dhe siguro kabllin elektrik dhe të gjitha bateritë nga laptopi.
5. Stako dhe siguro të gjithë kabllot, telat dhe USB nga kompjuteri dhe dokumento pajisjen ose aparaturën e lidhur në anën tjetër.
6. Vendos ngjitëse mbi vendin e disketës, nëse ka.

7. Sigurohuni që vendet për CD ose DVD janë në vendet e tyre, vëreni nëse këto vende janë bosh, kanë CD brenda ose nuk janë kontrolluar, më pas mbylleni vendin e CD me ngjitëse që të mos hapet më.
8. Vendosni ngjitëse tek butoni i ndezjes.
9. Regjistroni markën, modelin, numrin serial, dhe çdo shenjë tjetër të vendosur nga përdoruesi.
10. Regjistroni kompjuterin dhe të gjithë kabllot, telat, aparaturat dhe pjesët e tjera sipas procedurave të agjencisë.
11. Paketoni provat e mbledhura sipas procedurave të agjencisë për të parandaluar dëmtime ose tjetërsime gjatë transportit dhe magazinimit.

Situata 7: Nëse kompjuteri është i ndezur "ON".

Për qëllime praktike, të heqësh kompjuterin nga priza kur e sekuestron atë është mundësia më e sigurtë. (Mos përdorni komandën Start Shut down) Nëse provat e një krimi janë të dukshme në ekran do ju duhet kërkuar asistencë nga personeli i specializuar për kapjen dhe ruajtjen e të dhënave të paqëndrueshme.

- ***Në rastet e mëposhtme, rekomandohet stakimi i menjëhershëm nga priza*:**

(i) Informacioni ose aktiviteti në ekran tregon se të dhënat po fshihen ose mbishkruhen.

(ii) Ka të dhëna që një proces shkatërrues po kryhet në aparaturën për ruatjen e të dhënave në kompjuter.

(iii) Sistemi ndizet në një mënyrë tipike të Microsoft® Windows®. Po të hiqet priza nga mbrapa kompjuterit, informacioni do të ruhet mbi përdoruesin e fundit dhe kohën kur është futur në kompjuter, dokumentet e përdorur së fundmi, komandat e dhëna së fundmi, si dhe informacion tjetër i vlefshëm.

- **Në situatat e mëposhtme, stakimi i menjëhershëm nuk rekomandohet:**

Të dhënat e dukshme janë në ekran të thjeshtë. Personi i parë në vendngjarje duhet të kërkojë ndihmën e një personi të specializuar, i cili ka eksperiencë dhe është i trajnuar në kapjen dhe ruajtjen e të dhënave të paqëndrueshme para se të vazhdojë.

Treguesit e mëposhtëm tregojnë nëse pikat e mëposhtme janë aktive ose në përdorim:

- Dritare dialogu;
- Dokument i hapur;

- Të dhëna të ruajtura;
- Dritare të mesazheve në çast;
- Pornografi fëmijësh;
- Kontrabandë;
- Dokumenta financiare;
- Të dhëna;
- Aktivitet i paligjshëm i dukshëm.

Për kompjutera, servera, ose një grup kompjuterash të lidhur me njëri-tjetrin, personi i parë në vendngjarje duhet të sigurojë vendngjarjen dhe të kërkojë asistencë nga personeli i trajnuar në mbledhjen e provës elektronike nga një sistem i ndërlikuar kompjuterik.

8. Paketimi, transportimi dhe magazinimi i provës kompjuterike

Prova kompjuterike, (kompjuterat dhe pajisjet elektronike ku ajo ruhet), është e brishtë dhe e ndjeshme ndaj temperaturave ekstreme, lagështirës, tronditjes, elektricitetit statik dhe fushave magnetike.

Personi i parë në vendngjarje duhet të marrë masa kur dokumenton, fotografon, paketon, transporton, dhe magazinon provën elektronike për të evituar tjetërsimin, dëmtimin dhe shkatërrimin e provës.

Të gjitha veprimet në lidhje me identifikimin, mbledhjen, paketimin, transportimin, dhe magazinimin e provës elektronike duhet të dokumentohen me hollësi.

Kur paketohet prova elektronike për transportim, personi i parë në vendngjarje duhet:

- Të sigurojë që të gjitha provat elektronike të mbledhura janë dokumentuar, etiketuar, shënuar, fotografuar, regjistruar me video ose skicuar, dhe inventarizuar para paketimit. Të gjitha lidhjet dhe pajisjet e lidhura duhet të etiketohen për rikonfigurim të thjeshtë të sistemit më vonë.
- Të ketë parasysh që prova elektronike mund të përmbajë fshehje, gjurme ose provë biologjike dhe të marrë masat e duhura për ta ruajtur atë. Regjistrimi i provës elektronike duhet të bëhet para kryerjes së proceseve të provës se fshehur, gjurmës ose asaj biologjike.
- Të paketojë të gjitha provat elektronike në paketim antistatik. Vetëm çantat e letrës dhe zarfet, kutitë e kartonit, dhe kontenierët antistatikë duhet të përdoren për paketimin e

provës elektronike. Materialet plastike nuk duhet të përdoren kur mblidhen provat elektronike sepse lënda plastike mund të prodhojë ose përçojë elektricitet statik dhe të lejojë lagështirën dhe kondensimin që të zhvillohet, i cili mund të dëmtojë ose shkatërrojë provën.

- Të sigurojë që të gjitha provat elektronike të paketohen në mënyrë të tillë që të parandalohet përkulja, gërvishtja ose deformime të tjera.
- Të etiketojë në mënyrë të qartë dhe të rregullt të gjithë kontenierët e përdorur për paketimin dhe ruajtjen e provës elektronike.
- Të lërë celularët, ose telefonat smart në gjendjen e gjetur (të fikur ose të ndezur).
- Të paketojë celularët ose telefonat smart në materiale që nuk përçojnë sinjalin si për shembull; çanta izolimi, materiale për mbrojtje nga frekuencat e radios, ose letër alumini për të ndaluar marrjen/dërgimin e të dhënave nga aparati. (Personi i parë në vendngjarje duhet të ketë kujdes nga paketimi jo i rregullt, ose heqja nga paketimi i sigurtë, sepse aparati mund të jetë në gjendje pastaj të dërgojë/marrë të dhëna nëse ka sinjal të lirë komunikimi).
- Të mbledhë të gjithë telat dhe adaptoret për të gjitha pajisjet elektronike të sekuestruara.

Kur transportohen provat kompjuterike, personi i parë në vendngjarje duhet:

- Të ruajë provën elektronike larg fushave magnetike si ato të prodhuara nga transmetuesit e radios, magnetet e altoparlantit, dhe magnetet e dritave të emergjencës. Rreziqe të tjera të mundshme përfshijnë ngrohëset, pajisjet si dhe materialet që mund të prodhojnë elektricitet statik.
- Të shmangë mbajtjen e provës elektronike në makinë për një kohë të gjatë. Ngrohtësia, i ftohti dhe lagështira mund ta shkatërrojnë provën kompjuterike.
- Të sigurohet që kompjuterat dhe pajisjet elektronike janë të paketuara dhe të ruajtura gjatë transportit për të parandaluar dëmtime nga goditjet dhe vibrimi.
- Të dokumentojë transportin e provës elektronike dhe të mbajë zinxhirin e ruajtjes mbi provën e transportuar.

Kur ruhen provat kompjuterike, personi i parë në vendngjarje duhet të:

- Të sigurojë që prova elektronike është inventarizuar në përputhje me politikat e agjencisë.

- Të sigurojë që prova elektronike të ruhet në një vend të sigurtë, mjedis të kontrolluar nga ana klimaterike ose një vend që nuk ka temperatura të larta ose lagështirë.
- Të sigurojë që prova elektronike nuk është ekspozuar ndaj fushave magnetike, lagështirës, pluhurit, vibrimit, ose elemente të tjerë që mund ta shkatërrojnë.

Një prove elektronike e mundshme dhe e vlefshme që përfshin data, orë, dhe konfigurime të sistemit, mund të humbasë për shkak të magazinimit të tejzgjatur nëse bateria ose burimi i energjisë që ruan këtë informacion është prishur. Aty ku është e aplikueshme, duhet informuar ruajtësi i provës dhe eksperti kriminalistik që pajisjet elektronike funksionojnë me bateri dhe duhet kushtuar vëmendje për të ruajtur të dhënat.

Nëse sekuestrohet më shumë se një kompjuter si provë, të gjithë kompjuterat, kabllot, dhe aparaturat e lidhura me to duhet të etikohen në mënyrë të saktë për të lehtësuar montimin nëse është e nevojshme. Kompjuterat e sekuestruar më pas mund të etiketohen në rend alfabetik. Lidhjet dhe kabllot korrespondues mund të etiketohen me shkronjën e caktuar për kompjuterin dhe një numër unik për të siguruar montimin e saktë.

9. **Termat që përdoren më shpesh në fushën e krimit kibernetik, që mund të shërbejnë edhe si prova të vlefshme kompjuterike**

- **Analog:** Mund të shkruhet edhe *analogue*. Një pajisje ose sistem që paraqet vlera të ndryshueshme si sasi fizike që ndryshojnë vazhdimisht. Një pajisje tipike analoge është një orë në të cilën akrepat lëvizin vazhdimisht rreth numrave. Në orë e tillë mund të tregojë çdo kohë gjatë gjithë ditës. Një orë kompjuterike në të kundërt mund të paraqesë vetëm një numër të kufizuar kohe (p.sh. në çdo të dhjetën e sekondës).
- **Bandwidth (Gjerësia e brezit):** Sasia e informacionit ose të dhënave që mund të dërgohen në një lidhje rrjeti gjatë një përiudhë të caktuar kohe. Bandwidth-i zakonisht jepet në *bits për sekondë* (bps), *kilobits për sekondë* (kbps), ose *megabits për sekondë* (mps).
- **Bit-by-bit duplicate copy (Kopja dublikatë bit-by-bit:** Procesi i kopjimi të të dhënave të ruajtura në një media kompjuterike në mënyrë që të replikojë të dhëna në nivelin më të ulët. Termi "*bit copy*" i referohet duplikimit të zerove dhe njëshave (bits) që janë forma binare e të dhënave kompjuterike.

- **BIOS:** Basic Input Output System (Sistemi Bazë i Inputit dhe Outputit). Tërësia e rutinave të ruajtura në një memorie që vetëm mund të lexohet, në një fushë qarku të sistemit që ndez një kompjuter, dhe më pas e transferon kontrollin në sistemin veprues. BIOS hap kanale komunikimi me komponetët e kompjuterit si .p.sh. driver-at e hard diskut, tastierën, monitorët, printerat, dhe portat e komunikimit. Një nga ndryshimet më të shpeshta që i bëhen BIOS-it është kur ndryshohet renditja sipas së cilës kompjuteri i kërkon njësitë në të cilat mund të jetë i vendosur sistemi operativ (për shembull: një kompjuter mund të ndizet nëpërmjet pajisjes USB, CDROM-it ose hard-diskut dhe renditja se me cilën prej tyre do të bëhet ndezja mund të ndryshojë).
- **Blackberry:** Një pajisje dore që funksionon si telefon celular, organizues personal, kërkues (browser) interneti jokabllor, altoporlant, walkie-talkie për distancë të gjatë, dhe mini-laptop. Mund të përdoret për të dërguar dhe marrë mesazhe email-esh dhe tekste.
- **Blog:** Vjen nga Weblog. Një sërë xhornalesh (journals) të postuara në një faqe Web-i të vetme në rend kronologjik duke filluar nga i fundit. Blog-et në përgjithësi përfaqësojnë personalitetin e autorit ose reflektojnë qëllimin e faqes së Web-it ku është blog-u.
- **BMP:** Emri i gjatë i Bitmap, një format skedari imazhi që përdoret zakonisht për të ruajtur imazhe ose fotografi kompjuterike.
- **Buffer:** Një lloj memorie që i mban të dhënat përkohësisht dhe lejon që të dhënat të lexohen ose shkruhen në sasi më të mëdha për të përmirësuar përformancën e kompjuterit. Buffer – i përdoret për të ruajtur përkohësisht të dhëna që lexohen ose presin që të dërgohen në një pajisje si hard disku, CD-ROM, printeri, ose tape drive-ri (pajisje për ruajtjen e të dhënave).
- **Kabllo:** Një sërë kabllosh dhe fibrash optike të mbledhura së bashku, që përdoren si komponentë dhe pajisje për të komunikuar ose transferuar të dhëna.
- **CAT-5/Kategoria-5:** Një kabël që mund të transmetojë të dhëna më shpejtësi të madhe (100 megabits për sekondë edhe me shpejt). Kabllot CAT-5 përdoren gjerësisht për aplikime zëri dhe të dhënash në shtëpi.
- **CAT-5e:** CAT-5 me cilësi më të lartë. I njëjtë me kabllon CAT-5, por me specifikime të një cilësie më të lartë.

- **CAT-6/Kategoria-6 (ANSI/TIA/EIA-568-B.2-1):** Një standard kablloje për 'Gigabit Ethernet' dhe ndërlidhje të tjera që janë të përshtatshme me standarte të vjetra me kabllo CAT-5, CAT-5e dhe Cat-3. Një kabllo Cat-6 ka specifikime më pak fleksibël për interferencën në kanale dhe zhurmën në sistem. Kablloja standarde është e përshtatshme për lidhjet 10BASE–T, 100BASE–TX, dhe 1000BASE–T (Gigabit Ethernet).
- **CD/CD-ROM:** Compact Disc (Kompakt Disk)—Memorie që vetëm mund të lexohet). Një kompakt disk që përmban të dhëna që mund të aksesohen nga një kompjuter.
- **CD-R:** Compact Disc (Kompakt Disk)—I regjistrueshëm. Një disk në të cilin të dhënat mund të shkruhen, por që nuk mund të ndryshohen.
- **CD-RW:** Compact Disc (Kompakt Disk) —I Rishkrueshëm. Një disk në të cilin në dhënat mund të shkruhen, rishkruhen, ndryshohen ose fshihen.
- **Chat Room (Sallë Bisedimi):** Një *internet klient* që iu lejon përdoruesve që të komunikojnë në kohë reale duke përdorur tekste të shtypura në tastierë, simbole ose audio.
- **Compact Flash Card:** Një pajisje e vogël, e heqshme për ruajtje në masë, që bazohet në tekonlogjinë e memories *flash* – një teknologji ruajtjeje që nuk ka nevojë për bateri për mbajtur të dhënat pafundësisht. Ekzistojnë dy llojë kartash *compact flash cards*: Lloji i parë i kartave është 3.3mm i trashë; dhe kartat e llojit të dytë janë 5.5mm.
- **Compressed File (Skedar i kompresuar):** Një skedar, madhësia të cilit është zvogëluar duke përdorur një algoritëm që heq ose kombinon të dhënat e tepërta për të lehtësuar transferimin. Një skedar i kompresuar zakonisht nuk mund të lexohet nga pjesa me madhe e programeve pa u ç'kompresuar më parë.
- **Cookies:** Skedarë të vegjël tekstesh në një kompjuter që ruajnë informacion për informacionin që ka aksesuar një përdorues ndërsa ka bërë kërkime në internet.
- **CPU:** Central Processing Unit (Njësia Qendrore e Përpunimit). Një chip mikropërpunues që përmban disa mijë deri në disa milionë tranzitorë që kryejnë funksione të ndryshme në të njëjtën kohë. Njerëzit shpeshherë e ngatërrojnë me shtëpizën ose shasinë e kompjuterit. Mirëpo, procesori paraqet komponentë të brendshëm dhe nuk mund të shihet jashtë sistemit. Pa marrë parasysh se për çfarë lloj

kompjuteri bëhet fjalë, procesori punon në ekzekutimin e një sërë instruksionesh të memorizuara, që janë të njohura si program.

- **Skedarë të fshirë:** Skedarë që nuk kanë më lidhje me një tabelë për shpërndarjen e skedarëve ose një tabelë master (kryesore) skedarësh. Skedarët e fshirë janë akoma resident në media, por nuk mund të aksesohen nga sistemi operues.
- **DHCP:** Dynamic Host Configuration Protocol (Protokolli Dinamik i Konfigurimit të Hostit). Një sërë regullash që përdoren nga pajisjet e komunikimit, si kompjuterat, routerat, ose adoptorët e rrjetit për të lejuar pajisjet që të kërkojnë dhe të marrin një adresë IP nga serveri që ka një listë adresash gati për t'u vendosur.
- **Dixhital (fotografi, video, audio):** Një sistem dixhital që përdor vlera të veçanta dhe jo spektriumin e vazhdueshëm të vlerave të analogut. Fjala "dixhital" mund t'i referohet llojit të ruajtjes dhe transferimit të të dhënave, funksionimit të brendshëm të një pajisjeje ose llojin e pamjes video.
- **Kamera Kompjuterike:** Një kamer e palëvizshme që regjistron imazhe në një format dixhital. Ndryshe nga kamerat tradicionale analoge që regjistrojnë intensitete pafundësisht të ndryshme të dritës, kamerat kompjuterike regjistrojnë numra të ndryshëm për ruajtje në një flash memory card ose disk optik.
- **Provat Kompjuterike:** Informacioni i ruajtur ose i transmetuar në formë binari që mund të prezantohet dhe të jetë i besueshëm për gjykatën.
- **DivX:** Një emër marke produktesh të krijuara nga DivX, Inc., përfshirë edhe DivX Codec, që është bërë e famshme për shkak aftësisë për të kompresuar segmente të gjatë videosh në madhësi të vogla, ndërsa ruajnë një cilësi relativisht të lartë vizuale. Është një nga kodet, ose programet për kodimin dhe ç'kodimin e të dhënave kompjuterike, që shpeshherë kanë të bëjnë me ripping (kopjimi i përmbajtjeve video dhe audio), ku multi media audio dhe video transferohen në hard disk dhe transkodohen. Si rezultat, DivX është diskutuar shpesh për shkak të përdorimit të saj në replikimin dhe shpërndarjen e DVD-ve që gëzojnë të drejtën e autorit.
- **Docking Station:** Një pajisje që bën të mundur që kompjuterat laptop dhe notebook të përdorin pajisje periferike dhe komponentë që zakonisht janë të lidhura me kompjuterat, si p.sh. skanera, tastiera, monitorë dhe printera.

- **Dongle:** Një kopje e pajisjes së mbrojtjes dhe sigurisë që jepet së bashku me software-in. ‘Dongle’ pengon përdorimin dhe duplikimin e paautorizuar të software-it sepse çdo kopje e programit kërkon funksionimin e një ‘dongle’.
- **DSL:** *Digital Subscriber Line*. Një teknologji moderne kompjuterike me shpejtësi të lartë që lejon komunikim të dhënash me shpejtësi të lartë nëpërmjet linjave telefonike midis përdoruesve të fundit dhe kompanive telefonike.
- ***DVD:*** *Digital Versatile Disk.* Një kompakt disk me kapacitet të lartë që mund të ruajë një sasi të dhënash deri në 28 përqind më të lartë se sa një CD-ROM standart. DVDs gjendent në formate DVD-R, DVD-RË, DVD+R, DVD+RË, dhe BlueRa.
- **Fusha Elektromagnetike:** Fusha e forcës e lidhur me ngarkesën elektrike në lëvizje që ka komponentë elektrik edhe magnetik dhe që përmban një sasi të caktuar energjie elektromagnetike. Altoparlantet e transmitorët e radiove që zakonisht gjenden në bagazhin e makinave të patrullimit, janë shembuj të pajisjeve që prodhojnë fusha elektromagnetike.
- **Pajisje elektronike:** Një pajisje që operon në bazë të parimeve të drejtimit të lëvizjes së elektroneve. Shembuj të pajisjeve elektronike janë sistemet kompjuterike, skanerat dhe printerat.
- **Evidenca elektronike:** Informacion ose të dhëna me vlerë hetuese që ruhen ose transmetohen nga një pajisje elektronike.
- **Pajisje për ruajtjen elekronike:** Çdo mjet që mund të përdoret për të regjistruar informacion në mënyrë elektronike. Shembuj të tillë janë hard disqet, kasetat magnetike, kompakt disqet, kasetat video dhe audio. Shembuj të pajisjeve për ruajtje elektronike që mund të hiqen janë thumb drive-rat, smart media, flash cards, floppy disks, dhe Zip® disks.
- **Kodimi (Shifrimi):** Çdo procedurë e përdorur në kriptografi për të konvertuar tekstin e thjeshtë në tekst të shifruar për të parandaluar çdokënd, përveç personit me çelësin korrespondues, të cilit i është dërguar, që të lexojë të dhënat.
- **EPROM:** Erasable programmable read-only memory (Memorie që mund të fshihet, e programueshme dhe që vetëm mund të lexohet). Një lloj chip-i, memorje kompjuteri që

i ruan të dhënat kur ka ndërprerje të energjisë elektrike. Sapo programohet, një EPROM mund të fshihet vetëm duke e ekspozuar atë në dritë të fortë ultraviolet.

- **Ethernet:** Metoda standarte e aksesit LAN (rrjeti i zonës lokale) që lidh pajisjet elektronike me rrjetin, modemin e kabllos, ose modemin DSL për akses në internet.
- **Evidencë shfajësuese:** Evidencë që tregon që një akuzë nuk mbështet me evidencë.
- **Faraday (Faradej):** Një njësi e pamatshme ngarkese elektrike e barabartë me afërsisht 6.02 x 1023 mbartës ngarkese elektrike. Kjo është e barabartë me një mol, që gjithashtu njihet si kostantja e Avogadros. Çantat e izolimit Faraday përdoren për parandaluar që telefonat celularë dhe pajisjet të lidhen me sinjalet e komunikimit.
- **Formati i Skedarit:** I referohet llojit të kasetës bazuar në strukturën e skedarit, organizimin e tij ose si një skedar i veçantë e trajton informacionin (tingujt, fjalët, imazhet) që ajo përmban. Një format skedari zakonisht tregohet nga tre ose katër shkronjat në fund të emrit të skedarit MS-DOS, p.sh., .doc ose .jpg.
- **Firewall (Muri i Zjarrit):** Një mur zjarri lejon ose bllokon trafikun brenda dhe jashtë një rrjeti privat ose kompjuterit të përdoruesit, dhe është metoda kryesore për ta ruajtur një kompjuter nga ndërhyrësit. Ai përdoret gjithashtu për të ndarë një server Web-i publik të kompanisë nga rrjetet e saj të brendshme dhe për të ruajtur sigurinë e segmenteve të rrjeteve të brendshme.
- **FireWire:** Një autobus serial (kanal komunikimi) më shpejtësi të lartë, që lejon lidhjen e deri në 63 pajisjeve. Përdoret gjerësisht për të shkarkuar video nga camcordera dixhital në kompjuter.
- **Reaguesi i parë:** Officeri i parë i zbatimit të ligjit ose ndonjë zyrtar tjetër i sigurisë për publikun që arrin në një vendngjarje krimi.
- **GPS:** Global Positioning System (Sistemi i Pozicionimit Global). Një sistem satelitësh dhe pajisjesh marrëse që përdoren për të gjetur vendndodhjen e pozicioneve në Tokë. GPS përdoret në vlerësimin e pasurive të patundshme.
- **GIF:** Graphics Interchange Format (Formati i Ndërkëmbimit të Grafiqeve). Një nga formatet më të zakonshme të skedarëve për imazhet grafikeështë jpg. Përdoret gjërësisht në internet për shkak të kompresionit të lartë, dhe si rrjedhojë e madhësisë së

vogël të skedareve. Skedarët GIF kanë .gif në fund të emrit të skedarit dhe mund të krijohen ose editohen në pjesën më të madhe të aplikimeve grafike më të zakonshme.

- **Hard Copy:** Një riprodhim i përhershëm të dhënash të çdo lloj medie që është e përshtatshme për përdorim të drejpërdrejt nga një person, p.sh., faqet e printuara ose të dërguara me faksimile.
- **Hard Drive:** Një pajisje për ruajtjen e të dhënave që përbëhet nga një fushë qarku e jashtme, të dhëna të jashtme lidhje me energjinë elektrike, një xham i brendshëm, ose një pllakë qeramike ose metali e ngarkuar magnetikisht që ruan të dhëna. Llojet më të zakonshme të hard drive-rave janë IDE dhe SCSI.
- **Hardware:** Komponentët fizikë që përbëjnë një sistem kompjuterik si p.sh. tastiera, monitori dhe miu.
- **Header:** Në shumë disiplina të shkencave kompjuterike, një 'header' është një njësi informacioni që i paraprin një objekti të dhënash. Në një transmision rrjeti, header-i është një pjesë e paketës së të dhënave dhe përmban informacion transparent rreth skedarit ose transmisionit. Për sa i përket menaxhimit të skedarëve, një 'header' është pjesa në fillim të çdo skedari ku ruhet infomacioni për arsye arkivimi. 'Header-i' i një skedari mund të përmbajë datën në të cilën skedari është krijuar, datën në të cilën është azhornuar dhe madhësinë e skedarit. 'Header-i' mund të aksesohet vetëm nga sistemi operues ose nga programe të specializuara.
- **Të dhënat e fshehura:** Shumë sisteme kompjuteri kanë një opsion për të mbrojtur informacionin nga përdoruesit e rastësishëm duke e fshehur atë. Një ekzaminim i shpejtë i sistemit mund të mos i shfaqë skedarët, direktoritë ose ndarjet e fshehura një personi të patrajnuar. Një ekzaminim më shkencor do të dokumentojë prezencën e këtij lloji informacioni.
- **Host:** Një kompjuter në rrjet që i ofron burime ose shërbime kompjuterave të tjerë në të njëjtin rrjet. Një pajisje host mund të ofrojë një sërë shërbimesh, si p.sh. SMTP (e-mail) dhe HTTP (Web).
- **IM:** Instant Messenger (Komunikim në kohë reale). Një lloj shërbimi komunikimi të bën të mundur që përdoruesit të komunikojnë në kohë reale me anë të internetit. Është analoge me bashkëbisedimin telefonik, por komunikimi bëhet me anë të tekstit.

- **Internet Protocol (IP) Address (Adresa e Protokollit të Internetit:** Një numër binar 32-bit, që në mënyrë unike identifikon një host të lidhur me internetin ose hoste të tjera interneti, për të komunikuar me anë të transferimit të paketave të të dhënave. Një adresë IP jepet në format prej katër bashkësish numrash të ndarë me pika, që përbëhet nga vlera decimale për të katërta bitet, të ndara me pika, p.sh. 127.0.0.1.
- **IRC:** Internet Relay Chat (Bashkëbisedim më anë të Komunikimit në Internet). Një klient bashkëbisedimi në internet që lejon shumë përdorues në të njëjtën kohë, me anë të të cilit përdoruesit komunikojnë në kanale që referohen si dhoma bashkëbisedimi.
- **ISDN:** Integrated Services Digital Network (Rrjet Dixhital i Shërbimeve të Integruara). Një lidhje interneti me linjë telefoni kompjuterike me shpejtësi të lartë.
- **ISP:** Internet Service Provider (Ofruesi i Shërbimit të Internetit). Një biznesmen që ofron akses në internet. Ofruesit e shërbimeve të vogla të internetit ofrojnë shërbim më anë të modemit dhe ISDN-së, ndërsa ata që ofrojnë shërbime të madhësive më të mëdha ofrojnë lidhje me linja private.
- **JPG:** Joint Photographic Experts Group (Grupi i përbashkët i ekspertëve fotografik). Gjithashtu edhe JPEG. Një teknikë kompresimi (ngjeshjeje) që përdoret për të ruajtur imazhe dhe fotografi. Zvogëlon madhësinë e imazheve pa ulur cilësinë e tyre, përdoret gjerësisht në webin mbarëbotëror.
- **Latent (e pashfaqur):** Ekzistuese, megjithëse jo të dukshme, por që mund të bëhen të dukshme.
- **Adresa MAC:** Gjithashtu njihet edhe si adresa e hardware-it ose adresa e ethernetit. Një identifikues unik specific për kartën e rrjetit brenda kompjuterit. Lejon që serveri DHCP të komunikojë që kompjuteri lejohet që të aksesohet në rrjet. Adresat MAC shkruhen si XX–XX–XX–XX–XX–XX, ku X-të përfaqësojnë numrat ose shkronjat nga A në F.
- **Media magnetike:** Përfshin drive-rat e hard disqeve, kasetat, bobinat, disketat, ose kasetat që përdoren për të ruajtur të dhëna në mënyrë magnetike.
- **Pajisje për ruajtjen e medias:** Shembuj të tillë janë drive-rat e disqeve, kasetave, Zip®, thumb-et , floppy disqet, CD-të, dhe DVD-të. Ndryshe nga memoria kryesore, pajisjet e ruajtjes së medias, i ruajnë të dhënat edhe kur kompjuteri është i fikur.

- **Karta e memories:** Një pajisje për ruajtjen e memories që mund të hiqet, që zakonisht përdoret për të ruajtur imazhe në kamera kompjuterike, por që mund të përdoret edhe për të ruajtur çdo lloj të dhënash.
- **MiniDV:** Një vidio kasetë e dizenjuar për përdorim në camcorders dixhital MiniDV. Kasetat MiniDV mund të kenë deri në 530 rrjesha rezolucion videoje.
- **MP3:** Është një akronim për MPEG-1 ose MPEG-2 audio layer 3. MP3 është pjesa e fundit e skedarit për MPEG audio layer 3. Layer 3 është një nga tre skemat koduese për kompresimin e sinjaleve audio. Layer 3 përdor kodimin e audio të mbështetura në përceptim dhe kompresim psikoakustik për të hequr pjesët e tepërta dhe të panevojshme në një sinjal akustik.
- **MPEG:** Moving Picture Experts Group (Grupi i Ekspertëve të Filmit). Një standard për të kompresuar regjistrim video. Skedarët MPEG shpesh kanë mpg në fund të emrit të skedarit.
- **Multimedia Player:** Një hard disk ose pajisje elekronike e bazuar në flash memory, si p.sh një MP3 player, që mund të ruajë dhë të luajë skedarë në një ose më shumë skedarë të medias që përfshijnë: MPEG, DivX, dhe Xvid, audio, MP3, WAV, Ogg Vorbis, BMP JPEG, GIF, imazhe, dhe Adobe Flash Interaktiv media dhe Flash LITE.
- **Rrjet:** Një konfigurim kompjuterash dhe pajisjesh të pavarura, të lidhura më anë të kabllove komunikuese ose teknologjive jokabllore që mund të ndajnë informacionin dhe burimet.
- **Lidhjet e rrjetit:** Një lidhje komunikimi kabllore ose jokabllore midis një grupi kompjuterash ose pajisjesh me qëllim ndarjen e informacionit dhe burimeve.
- **Sistemi Operues:** Një program kompjuterik që kontrollon komponentët e një sistemi kompjuterik dhe lehtëson operimin e aplikimeve. Microsoft® Windows®, Microsoft® Windows® XP, Vista®, Linux, Apple® dhe MacOS janë sisteme operimi të zakonshme.
- **Evidencë Elektronike Origjinale:** Pajisjet fizike dhe të dhënat që përmbahen nga këta artikuj në momentin e konfiskimit.
- **Palm:** Një nga modelet e ndryshme të asistentëve personal dixhital të tregtuara nga Palm, Inc.

- **Skedar i mbrojtur me fjalëkalim:** Një skedar i konfiguruar që tu mohojë akses përdoruesve që nuk vendosin fjalëkalimin e saktë (një karakter specifik ose një kombinim karakteresh). Siguria duke kundërshtuar aksesin, nuk modifikon përmbajtjen e skedarit, ajo thjesht pengon aksesin e personave që nuk kanë fjalëkalim.
- **PCMCIA:** Personal Computer Memory Card International Association (Shoqata Ndërkombëtare për Kartën e Memories së Komjuterit Personal). Një shoqatë përgjegjëse për të shpallur standardet për kartat e integruara të qarqeve, ku përfshihen edhe kartat e PC-ve dhe Kartat Ekspres.
- **PCMIA:** Personal Computer Manufacturer Interface Adaptor (Adaptor i Prodhuesit për Ndërfaqen e Kompjuterit Personal). Përdoret për të zgjeruar funksionin e kompjuterave personal.
- **PDA:** Personal Digital Assistant (Asistent Dixhital Personal). Një pajisje dore që mund të funksionojë si telefon celular, dërgues faksi dhe organizues personal. Shumë PDA inkorporojnë aftësi për të njohur shkrimin e dorës dhe zërin. Gjithashtu njihet edhe si palmtop, kompjuter dore ose kompjuter xhepi.
- **Periferal:** Çdo pajisje e përdorur në një sistem kompjuterik që nuk është pjesë e kompjuterit kryesor, dmth e memories dhe mikroprocesorit. Pajisjet periferike mund të jenë të jashtme, si për shembull mausi, tastiera, printeri, monitori, Zip® drive-ri i jashtëm ose skaneri, ose i brendshëm si drive-ri CD-ROM, CD-R drive, ose modem i brendshëm.
- **Kompjuter Personal (PC):** Një kompjuter, çmimi, madhësia dhe vetitë e të cilit e bëjnë të përdorshëm për individët.
- **Kabllo Printeri:** Një kabllo që lidh një printer me një kompjuter.
- **Portë:** Një ndërfaqe me anë të së cilës një kompjuter komunikon me një pajisje ose sistem tjetër. Kompjuterat personal kanë lloje të ndryshme portash. Në brendësi, ekzistojnë porta të ndryshme për lidhur ‘disk drives’, ‘display screens’, dhe ‘keyboards’. Në pjesën e jashtme, kompjuterat personal kanë porta për të lidhur modemat, printerat, mausët dhe pajisjet e tjera periferike.
- **Replikatori i Portës:** Një pajisje që përmban porta kompjuteri të zakonshme (p.sh., seriale, paralele, dhe porta rrjeti) që futen në një kompjuter notebook. Një replikator

porte është i ngjashëm me një ‘docking station’, por një ‘docking station’ zakonisht ofron mundësi për një tjetër fushë zgjeruese.

- **Printer Spool File:** Një skedar i përkohshëm që krijohet kur ekzekutohet një komandë printimi.
- **Procesor:** Skema logjike që iu përgjigjet dhe përpunon udhëzimet bazë që drejtojnë një kompjuter. Termi procesor zakonisht ka zëvendësuar termin njësia qendrore përpunuese (CPU). Procesori i një kompjuteri personal dhe ai i inkorporuar në pajisje të vogla, shpeshherë quhet mikroprocesor.
- **PS2:** PlayStation 2. Një video game shumë e përdorshme.
- **PSP:** PlayStation i transportueshëm. Një video game dore që është hedhur në treg në 2005 nga Sony. Përdor një Disk Universal Media dhe një kartë memorie Stick PRO Duo për ruajtje informacioni. PSP-ja gjithashtu luan muzikë dhe shfaq fotografi.
- **Karantinë:** Statusi i çdo pajisjeje ose materiali që është izoluar, në pritje të një vendimi për përdorimin e tij.
- **RAM:** Random Access Memory (Kujtesë e gjallë). Memorie kompjuteri që ruan të dhëna.
- **Remote (Në distancë):** Skedarë, pajisje, dhe burime të tjera që nuk janë të lidhura direkt në një kompjuter.
- **Media që mund të hiqet:** Pajisje që ruajnë të dhëna dhe që mund të hiqen me lehtësi nga sistemi kompjuterik, ose pajisje si p.sh. floppy disks, CD, DVD, bobina, dhe kaseta rezervë e të dhënave.
- **Emri i ekranit:** Emri që një përdorues zgjedh të përdor kur komunikon me të tjerët online. Emri i ekranit mund jetë emri i vetë personit, variacione të ndryshme të emrit të personit, ose një pseudonim. Emrat e ekranit nevojiten për aplikimet e mesazheve të menjëhershme (IMP).
- **Screen Saver:** Është një program i domosdoshëm që parandalon që një monitor të dëmtohet nga një imazh i pandryshueshëm. Ai gjithashtu mund të ofrojë kontroll aksesi.
- **Seizure Disk:** Një floppy disk i përgatitur në atë mënyrë që të ndez një sistem kompjuteri dhe ta mbrojë atë nga tjetërsimi aksidental ose i paqëllimshëm i të dhënave.

- **Kabllo Seriale:** E pajisur me një kamera kompjuterike. Përdoret për të lidhur kamera kompjuterike në një kopjuter personal në mënyrë që imazhet të mund të shkarkohen në hard diskun e kompjuterit.
- **Server:** Një kompjuter që iu ofron disa shërbime kompjuterave të tjerë që janë lidhur më të më anë të rrjetit.
- **SIM:** Subscriber Identity Module (Moduli i Identitetit të Abonentit). Karta SIM është karta smart e vendosur në telefonat celularë GSM. SIM identifikon llogarinë e përdoruesit në rrjet, realizon autentifikimin dhe ofron hapësirë për ruajtjen e të dhënave për të dhëna të një përdoruesi bazë dhë informacion mbi rrjetin. Ajo gjithashtu mund të kombinojë disa aplikime që operojnë një telefon që është i përputhshëm.
- **Sleep Mode (Gjendje gjumi):** Gjithashtu Suspend Mode (Gjendje pezull). Një gjendje për ruajtjen e energjisë që pezullon energjinë elektrike në hard drive dhe monitor, rezulton në ekran të fikur.
- **Karta Smart:** Ndryshe edhe kartë chip, ose kartë e qarkut të integruar. Një kartë në madhësinë e një xhepi me qarqe të integruara që mund të përpunojnë informacion. Ka dy kategori kryesore të kartave smart. Kartat e memories përmbajnë vetëm komponentë memorie nonvolatile (të qendrueshëm)dhe ndoshta një sasi logjike specifike sigurie. Kartat e mikroprocesorit përmbajnë komponentë memorie volatile (të paqëndrueshëm) dhe mikroprocesor.
- **Software:** Programe kompjuterike të dizenjuara për të kryer funksione specifike, si p.sh. *word processing*, llogaritje, menaxhim rrjeti, zhvillim faqeje Web-i, menaxhim skedari ose menaxhim inventari.
- **Solid-state drive (SSD)** – paraqet pajisje për ruajtjen e të dhënave që shfrytëzojnë memorie gjysmëpërçuese, mikroçipe që përmbajnë pjesë mobile. Kjo pajisje i ruan të dhënat e përhershme me qëllim që të sigurohet qasje në to në të njëjtën mënyrë sikurse dhe në rastin e hard-diskut tradicional. Ndonjëherë quhet edhe "solid-state disk" ose disk elektronik. Në krahasim me disqet elektromekanike, SSD-të janë më pak të ndjeshme ndaj goditjeve fizike, nuk bëjnë zhurmë, kanë kohë më të shkurtë të qasjes te të dhënat dhe fshehtësi më të madhe, por kanë çmim më të lartë. SSD-të shfrytëzojnë pajisje të njëjta për t'u lidhur sikurse edhe hard-disqet, prandaj lehtë zëvendësohen në

shumicën e aplikacioneve. Për shkak se tek pajisjet SSD të dhënat ruhen në mënyrë krejtësisht tjetër, ato bartin më vete edhe sfida të reja për ekspertizat dixhitale.

- **Stand-Alone Computer (Kompjuter më vete):** Një kompjuter që nuk është i lidhur me një rrjet ose kompjuter tjetër.
- **Steganografi:** Procesi i fshehjes së skedarëve brenda skedarëve të tjerë.
- **Administrator sistemi:** Një përdorues që ka privelegjet më të mëdha për tu aksesuar në një sistem kompjuterik.
- **Temporary and Swap Files (Skedarët e Përkohshëm dhe Swap):** Për të përmirësuar përformancën e një kompjuteri, shumë aplikime dhe sisteme operimi kompjuterike ruajnë përkohësisht të dhëna nga memoria e sistemit ose RAM-i në skedarë në hard drive. Këto skedarë, që janë zakonisht të fshehura dhe të paaksesueshme, mund të përmbajnë informacion të dobishëm për hetuesin.
- **Thumbnail:** Një prezantim në miniaturë e një faqeje ose një imazhi që përdoret për të identifikuar një skedar me anë të përmbajtjes. Skedari hapet duke klikuar në *thumbnail*. Thumbnail-et janë një opsion për menaxhimin e skedarëve, si Windows Explorer, dhe ata gjenden në programet grafike dhe për editimin e fotove për të kërkuar imazhe të ndryshme në një skedar.
- **Touch Screen:** Një ekran që shfaq video që ka një panel transparent që është i ndjeshëm ndaj prekjes dhe mbulon ekranin. Një përdorues mund të prekë ekranin për të aktivizuar funksionet e kompjuterit në vend që të përdorë një pajisje treguese si p.sh, një maus ose një stilolaps të lehtë.
- **USB:** Universal Serial Bus. Një lidhje ndërfaqjeje hardware-i kompjuteri që lehtëson përdorimin e shumë pajisjeve periferale ku përfshihen tastierat, mausët, joystics, skanerat, printerat, pajisjet për ruajtje të jashtme, telefonat celurarë, telefonat smart, PDA-të, dhe dongle-at e software-it.
- **Virus:** Një program software që mund të përhapet dhe riprodhohet në kompjuterat e lidhur dhe dëmton dhe korrupton skedarët ose aplikimet e ligjshme në kompjuter.
- **VoIP:** Voice over Internet Protocol (Protokolli i zërit më anë të Internetit). Teknologjia e përdorur për të transmetuar bashkëbisedime zanore në një rrjet të dhënash duke përdorur protokollin e internetit. Rrjeti i të dhënave mund të jetë Internet ose Intranet i

inkoporuar. **Volatile Memory (Memorie e Paqëndrueshme):** Memorie që humbet përmbajtjen kur ikën ose kur nuk ka energji.

- **WAV:** Shkurtim për WAVeform. Një lloj skedari audio. Zakonisht ka 'WAV'në fund të emrit të skedarit.
- **Jokabllor:** Çdo lloj pajisje kompjuterike që mund të aksesojë një rrjet pa lidhje kabllore.
- **Router Jokabllor:** Një pajisje rrjet që përbëhet nga pika aksesi jo kabllore (stacione bazë), një switch LAN kabllor dhe një router për të lidhur kompjuterat dhe pajisjet periferale në një shërbim interneti. Routerat jokabllor janë një mënyrë e përshtatshme për të lidhur një numër të vogël kompjuterash të lidhur më kabllo dhe çdo lloj numri kompjuterash të lidhur pa kabllo me internetin.
- **Write Protection (Mbrojtja ndaj të shkruajturit):** Software ose hardware që parandalon që të dhënat të shkruhen në një pajisje për ruajtje të dhënash. 'Write protection' siguron që prova kompjuterike nuk modifikohet pasi është marrë.
- **Xvid:** Një library vidio kodek me burime të hapura (software për kompresim videoje) që respekton standartin MPEG-4.
- **Zip®:** Disk drive për ruajten e të dhënave, i lëvizshëm.
- **Skedar Zip®:** Një skedar që është zvogëluar në madhësi për të lejuar transferim më të shpejtë midis kompjuterave, ose për të kursyer hapësirën e ruajtjes. Disa skedarë të kompresuar, kanë **exe** në fund të emrit të skedarit, që tregon që dosja mund të hapet vetë, pa ndihmën e ndonjë software (programi).

KAPITULLI VI: KONKLUZIONE DHE REKOMANDIME

1. Hartimi dhe zbatimi i një strategjie të mbrojtjes së hapësirës kibernetike

Shoqëritë në mbarë botën janë të tërhequra ndaj përfitimeve të mëdha që sjell teknologjia e informacionit dhe komunikimit dhe qeveritë në vendet e zhvilluara po investojnë në këtë fushë. Këto përfitime që i kalojnë shtetit dhe qytetarëve të tij kanë nevojë të mbrohen nga sulmet kibernetike, sepse kanë rëndësi për sigurinë e vendit.

Hapësira kibernetike si një hapësirë pa kufinj kërkon një bashkëpunim dhe koordinim ndërkombëtar për të garantuar sigurinë kibernetike. Gjithashtu me anëtarësimin në NATO dhe progresin e bërë drejt anëtarësimit në BE, Shqipëria gjithnjë e më shumë është pjesë aktive e iniciativave dhe programeve të sigurisë kibernetike dhe duhet të përmbushë angazhimet e saj ndaj vendeve aleate.

Rritja e përdorimit të internetit dhe tendenca për një botë gjithnjë e më të ndërlidhur rrit dhe rreziqet me të cilat përballemi. Shqipëria duhet të marrë të gjitha masat për hartimin e politikave, standardeve, udhëzimeve dhe procedurave bazuar në standardet dhe praktikat më të mira për të garantuar sigurinë kibernetike, për të siguruar një mbrojtje ndaj rreziqeve kibernetike duke respektuar në çdo moment parimet e të drejtave dhe lirive themelore si dhe parime të tjera demokratike.

Siguria kibernetike nuk mund të konsiderohet si një problem, i cili prek apo i takon një institucioni, institucioneve shtetërore, sektorit privat ose qytetarëve. Ajo është problem i cili prek gjithë fushat e jetës dhe shoqërisë. Si i tillë kërkon marrjen e masave të nevojshme të sigurisë nga të gjithë përdoruesit e teknologjisë së informacionit dhe hapësirës kibernetike.

Shteti shqiptar ka investuar në infrastrukturën e teknologjisë, por ka mungesa përsa i përket hartimit dhe zbatimit të një strategjie të mbrojtjes së hapësirës kibernetike. Në disa prej çështjeve të trajtuara në këtë studim, i vihet theksi rëndësisë së krijimit të strategjisë kombëtare për sigurinë kibernetike.

Ky studim mbështet përafrimin e përbashkët në strukturat e propozuara në vendet e zhvilluara dhe informon se si vendet e zhvilluara, mund të arrijnë rezultate konkrete ndaj problemeve të sigurisë kibernetike. Strategjia kombëtare e mbrojtjes kibernetike në vendit tonë duhet të përmbajë përafrimet dhe modelet më të suksesshme, një pjesë prej të cilave janë zbatuar në vendet e zhvilluara.

Strategjitë dhe programet duhet t'i përshtaten nevojave dhe gatishmërisë së vendit për t'i zbatuar ato, pa shmangur pasqyrimin e nevojave të ardhshme të vendit. Strategjia më e mirë për vendin tonë do të ishte ndërtimi i kapaciteteve të sigurisë kibernetike në periudhën kur kërkohet dhe është më e nevojshme.

- ***Objektivat strategjike që duhet të ndiqen për përmbushjen e këtij vizioni janë:***

1. Plotësimi i kuadrit ligjor në fushën e sigurisë kibernetike;
2. Rritja e ndërgjegjësimit për sigurinë kibernetike;
3. Rritja e nivelit të njohurive, aftësive dhe kapaciteteve për ekspertizë në fushën e sigurisë kibernetike;
4. Ngritja e njësive të specializuara;
5. Identifikimi dhe mbrojtja e Infrastrukturave Kritike të Informacionit (CIIP);
6. Krijimi dhe implementimi i kërkesave bazë të sigurisë kibernetike;
7. Shtimi i investimeve për rritjen e sigurisë në rrjetet/sistemet shtetërore.

1.1. Plotësimi i kuadrit ligjor në fushën e sigurisë kibernetike

Në përputhje me zhvillimet dhe iniciativat do të ndërmerren hapat e nevojshëm për të analizuar, përshtatur dhe plotësuar legjislacionin në fushën kibernetike. Në mënyrë të vazhdueshme duhet të bëhet vlerësimi i praktikave më të mira botërore, rekomandimeve dhe iniciativave ndërkombëtare të fushës, në mënyrë të veçantë ato të BE-së, duke përshtatur masat në fushën e krimeve kibernetike në përputhje me angazhimet e marra ndaj partnerëve ndërkombëtarë, nëpërmjet përshtatjes dhe miratimit të tyre duke garantuar kështu forcimin e sigurisë kibernetike dhe luftën kundër krimit kibernetik. Në analizën e kryer në këtë studim rezulton se kuadri ekzistues ligjor dhe institucional ka disa paqartësi, të cilat duhen adresuar gjatë plotësimit të legjislacionit, si më poshtë:

a) Modernizimin e legjislacionit në fuqi dhe rishikimin periodik të tij për të adresuar sigurinë kibernetike të lidhur me zhvillimet e hapësirës kibernetike në Shqipëri dhe harmonizimin me legjislacionin ndërkombëtar, me qëllim që ai të ngelet i përshtatshëm dhe efektiv.
b) Dhe më konkretisht duhet të ndërmerren nisma ligjore, për të nxitur: përdorimin e nënshkrimeve elektronike të kualifikuara në transaksionet elektronike; përdorimin e identifikimit elektronik të sigurtë në shërbimet e qeverisjes elektronike, me qëllim

garantimin e identitetit në botën virtuale, qoftë ky për personat fizikë dhe ata juridikë; përdorimin sa më të gjerë të certifikatave për faqe interneti dhe web servera për të garantuar identitetin e sigurt të faqeve të institucioneve publike dhe kompanive të tjera private të cilat ofrojnë shërbime elektronike në bashkëveprim të institucioneve publike ndaj qytetarëve, apo ndaj biznesit.

c) Gjithashtu duhet të ndërmerren nisma legjislative që në kodin tonë penal të përfshihet një dispozitë e veçantë për përcaktimin e përgjegjësisë penale ndaj operatorëve të rrjeteve të komunikimeve, në rastin kur evidentohet shkelja e detyrimeve të tyre për mbrojtjen e sigurisë dhe fshehtësisë së komunikimeve që ata transmetojnë, pasi natyra e veprimtarisë që kryejnë, operatorët e rrjeteve të komunikimeve si dhe ofruesit e këtyre shërbimeve, u krijon atyre mundësi të mëdha praktike për të qenë në kontakt me mesazhet ose bisedat e transmetuara nëpërmjet një rrjeti të tillë, duke pasur kështu mundësi që të ndikojë në destinacionin dhe integritetin e tyre. Kjo do të thotë që edhe mundësitë për të cënuar paprekshmërinë dhe fshehtësinë e korrespondencës nga ana e këtyre subjekteve janë shumë më të mëdha.

d) Nga ana tjetër, edhe pse ligjvënësi shqiptar ka bërë përpjekje të shumta për t'iu përgjigjur krimit kibernetik duke përfshirë në Kodin Penal dispozita të veçanta për forma të veçanta të këtij lloj kriminaliteti, konstatohet se dispozitat aktuale janë të shpërndara në mënyrë jo sistematike në krerë e seksione të ndryshme të Kodit Penal. Kjo për shkak të kriterit kryesor të ndjekur për strukturimin e dispozitave në kodin tonë penal, që është objekti juridik i prekur nga vepra penale dhe për faktin se në Kodin Penal, për shkak të natyrës së tij, nuk mund të përfshihen përkufizime të zgjeruara apo shpjegime termash, të cilat janë të nevojshme për të kuptuar realisht veçoritë e kriminalitetit kompjuterik e për të lehtësuar identifikimin dhe hetimin e formave të tij nga ana e organeve ligjzbatuese. Në këtë kuadër për lehtësimin e zbatimit praktik dhe rrijen e efektivitetit të tyre do të ishte mirë që të tilla vepra penale të përfshiheshin në një ligj të veçantë. Referuar Ligjit nr. 10023, të vitit 2008, me anë të të cilit në kodin tonë penal u përfshinë dispozita të reja mbi krimin kibernetik duhet të ndërmerren nisma të tilla me qëllim që t'i kushtohet rëndësi shpjegimit teorik të rrethanave të zbatimit të dispozitave përkatëse, si dhe ilustrimit praktik të formave në të cilat mund të

kryhen shkeljet me qëllim për të shmangur çdo paqartësi në kuptimin dhe zbatimin e drejtë të këtyre dispozitave.

e) Gjithashtu duhet të ndërmerren nisma legjislative për të rregulluar format e reja të krimeve kibernetikike, pasi në kodin penal shqiptar nuk ka ndonjë dispozitë të veçantë që të ndëshkojë p.sh rastet e krijimit të profileve të rreme në rrjete sociale apo përdorimit mashtrues të profilit të një personi tjetër, i njohur ndryshe si impersonifikimi online (*online impersonation)*, kur këto kryhen për një qëllim të caktuar të paligjshëm. Duhet theksuar se duke qenë se krimet kibernetike përfaqësojnë veprime të kryera në hapësirën virtuale, brenda komunitetit përkatës virtual, i cili konsiston në një miksim të identiteteve reale dhe atyre virtuale, joekzistente në botën materiale, ai paraqet ndryshime thelbësore nga krimi tradicional. Në këtë këndvështim është e nevojshme të krijohet një përqasje e re në caktimin e përgjegjësisë penale në veçanti, si dhe në administrimin e drejtësisë penale në përgjithësi, pasi standardet aktuale të zbatimit të ligjit penal ndaj formave tradicionale të krimit nuk mund t'i përshtaten plotësisht veçorive specifike që paraqet kriminaliteti kibernetik. Një zgjidhje e mundshme për këtë do të ishte gjykimi i këtyre krimeve nga seksione të veçanta brenda gjykatave të përbëra nga gjyqtarë me njohuri të specializuara në fushën përkatëse.

f) Urdhërimi/detyrimi i kryerjes së auditimit periodik dhe vlerësimit të përshtatshmërisë dhe efektivitetit të sigurisë së sistemeve të informacionit në përputhje me bazën ligjore dhe rregullatore në fuqi. Kjo, për të plotësuar legjislacionin aktual në fuqi që parashikon auditimin e database-ve shtetërore duke lënë jashtë spektrit të veprimit sistemet në tërësi[230].

g) Krijimi i një sistemi raportues të unifikuar për individët dhe bizneset mbi raportimin e krimit kibernetik në mënyrë që të merren masat e nevojshme, si dhe institucionet e forcimit të ligjit të mund të përcaktojnë shkallën sesa krimi kibernetik në Shqipëri ndikon tek individët dhe në ekonomi.

[230]Ligji Nr. 10325, datë 23.9.2010 "*Për Bazat e të Dhënave Shtetërore*" dhe VKM nr. 945, datë 2.11.2012 për miratimin e rregullores "*Administrimi i Sistemit të Bazave të të Dhënave Shtetërore*"

1.2. Rritja e ndërgjegjësimit për sigurinë kibernetike

Botërisht vlerësohet se shumica e sulmeve kibernetike kanë sukses si pasojë e keqkonfigurimit apo moszbatimit të masave minimale të mbrojtjes nga përdoruesit e teknologjisësë informacionit.

a) Një pjesë e madhe e përdoruesve të Internet-it, janë të predispozuar për t'u bërë viktimë e krimit kompjuterik për shkak të mungesës së njohurive përkatëse. Në implementimin e modeleve të sigurisë, si në nivel përdoruesish personal, ashtu edhe në nivel ndërmarrjeje duhet marrë parasysh ndikimi i faktorit njerëzor. Për këtë arsye është shumë e rëndësishme që në hartimin e strategjive për mbrojtjen nga krimi kibernetik t'i kushtohet vëmendja e duhur edhe marrjes së masave për edukimin e përdoruesve mbi rreziqet që vijnë nga përdorimi i internetit dhe mbi mënyrat se si mund të mbrohen prej tyre. Është e rëndësishme që ata të kuptojnë qartë se cilat janë rolet dhe përgjegjësitë e tyre brenda sistemit[231].

b) Theksojmë gjithashtu se vetëm ndërmarrja e fushatave informuese nuk do të ishte e mjaftueshme për të arritur objektivat e synuara parandaluese. Studime të ndryshme kanë treguar se ndërmarrja e masave edukuese nuk është efektive nëse përdoruesit nuk janë të ndërgjegjshëm për faktin që janë në rrezik. Shteti duhet të ndërmarrë iniciativa dhe të hartojë programe për edukimin dhe ndërgjegjësimin e përdoruesve të internetit. Këto programe do të përfshijnë të gjitha nivelet e administratës publike si: specialistët IT, administratorët e sistemeve dhe TIK, etj. Shpërndarja dhe publikimi i informacionit mbi rreziqet e hapësirës kibernetike, nxjerrja e udhëzimeve dhe këshillave për një siguri minimale duhet të jetë një proces i vazhdueshëm nëpërmjet të cilit do të synohet të rritet ndërgjegjësimi dhe siguria e përdoruesve të thjeshtë. Përveç publikimit të tyre në faqet zyrtare të internetit të institucioneve të specializuara duhet të bashkëpunohet në mënyrë të ngushtë me median për të siguruar një informim sa më të gjerë dhe të shpejtë të publikut.

[231]DeWitt A. (2007). *Usability issues with security of electronic mail.* Tezë Doktorale. Universiteti i Bruneit, Fakulteti i Sistemeve të Informacionit dhe Informatikës. fq, 20.

c. Për të rritur dhe zhvilluar kulturën për rreziqet që vijnë nga përdorimi i pakujdesshëm i internetit, për një përdorim të sigurtë të hapësirës kibernetike, duhet të vlerësohet futja e programeve edukative në sistemin arsimor në lëndë të veçanta të sistemit shkollor parauniversitar dhe atij universitar nëpërmjet mbështetjes së studimeve shkencore në fushën e veprave penale që cënojnë sigurinë e rrjeteve të komunikimeve elektronike publike dhe të përdoruesve të tyre[232].

d. Gjithashtu nisma të rëndësishme për të luftuar dhe parandaluar krimin kibernetik do të ishin: krijimi i webfaqeve publike që përmbajnë informacion mbi mënyrat e parandalimit të krimit kompjuterik; përgatitja e materialeve dhe zhvillimi i kurseve me natyrë edukuese; përpunimi i rekomandimeve për punonjësit e ndërmarrjeve publike apo private; mbështetja me kapacitetet e duhura teknike për të parandaluar rreziqet në një sektor apo ent specifik; si dhe ndihma ndaj personave të dëmtuar nga krimi kompjuterik.

e. Një faktor tjetër që do të ndikonte në parandalimin dhe luftimin e krimit kibernetik do të ishte edhe bashkëpunimi midis aktorëve publikë dhe privatë si një nga sektorët më të prekshëm nga sulmet kibernetike. Rritja e ndërgjegjësimit dhe zbatimi i standardeve të sigurisë nga ky sektor duhet të ngrihet dhe të funksionojë efektivisht një model i vazhdueshëm bashkëpunimi ndërmjet organeve të zbatimit të ligjit dhe ofruesve të shërbimit të internetit nëpërmjet promovimit të shkëmbimit dhe ndarjes të kulturave dhe praktikave më të mira në këtë fushë. Kjo do të përfshinte kryerjen e seminareve të rregullta teknike dhe ligjore, si dhe dhënien e rezultateve të nxjerra nga hetimet e kryera në bazë të ankesave të ardhura nga ofruesit e shërbimit ose nga informacione, të cilat mblidhen duke u bazuar në aktivitetin kriminal që njihet dhe raportohet nga ofruesit e shërbimit[233].

---

[231]Weirich, D. dhe Sasse, M. A. (2001). *"Pretty Good Persuasion: A first step towards effective password security for the Real World"*, punim i paraqitur në: New Security Paradigms Workshop, Cloudcroft, New Mexico, USA, 2001, pp. 137-143.

[233]Këto propozime bazohen në punimin *"Udhëzime për bashkëpunimin ndërmjet organeve të zbatimit të ligjit dhe ofruesve të shërbimit të Internetit kundër krimit kibernetik"*, hartuar nga Divizioni i Krimit Ekonomik në Drejtorinë e Përgjithshme të të Drejtave të Njeriut dhe Çështjeve Ligjore të Këshillit të Evropës. Botimet e Këshillit të Evropës. Strasburg: 2008, fq. 3- 4.

Partneriteti publik-privat është shumë i rëndësishëm në vendet e zhvilluara dhe ndikon në funksionimin e sigurisë kibernetike, pasi sektori privat ka kapacitete teknike për të siguruar pajisje dhe mjete, trajnime me ekspertë të cilët mbështeten në strategji, ndërsa roli i qeverisë është më shpesh si koordinator ose si shpërndarës i informacionit duke influencuar në strategjinë kombëtare të sigurisë kibernetike. Mungesa e një bashkëpunimi gjithpërfshirës në këtë sektor, do të sillte si rezultat një reagim të papërshtatshëm ndaj rreziqeve kibernetike.

1.3. Rritja e nivelit të njohurive, aftësive dhe kapaciteteve për ekspertizë në fushën e sigurisë kibernetike

Për të parandaluar dhe luftuar fenomenin është e nevojshme realizimi i aktiviteteve, me qëllim ngritjen e kapaciteteve të burimeve njerëzore të nevojshme në fushën e sigurisë kibernetike duke krijuar p.sh. rregullore, për të përfshirë konceptin e sigurisë kibernetike në programet e shkollave fillore, shkollave të mesme, dhe të institucioneve të arsimit të lartë, si dhe duke krijuar mundësi për pjesëmarrje më të gjerë në konferenca ndërkombëtare, takime, seminare dhe ushtrime që kanë të bëjnë me sigurinë kibernetike, apo nëpërmjet organizimit të konferencave që do të diskutojnë edhe aspektet ekonomike, sociale dhe ligjore të sigurisë kibernetike. Rëndësi të veçantë në këtë aspekt ka edhe zhvillimi i kapaciteteve profesionale në strukturat e drejtësisë penale të përfshira në hetimin dhe luftën kundër krimit kibernetik i nevojshëm për të rritur nivelin e zbatimit të ligjit dhe përfshirjen në bashkëpunimin ndërkombëtar mbi këto probleme. Kjo nënkupton forcimin e kapaciteteve profesionale në luftën kundër krimit kibernetik nëpërmjet: rritjes së aftësive të punonjësve të agjencive ligjzbatuese, prokurorëve dhe gjyqtarëve; përmirësimit e ndërveprimit midis subjekteve private dhe publike duke përfshirë këtu ndërmarrjet private, shoqërinë civile ose institucionet akademike; ndërveprimit dhe ndërtimit të lidhjeve midis strategjive mbi krimin kompjuterik dhe strategjive të sigurisë kompjuterike, pasi këto dy strategji janë të ndërvarura dhe përforcuese të njëra-tjetrës; dhe menaxhimit të strategjive mbi krimin kompjuterik në mënyrë të tillë që ato të bëhen funksionale[234].

[234] *"Capacity building on cybercrime"* (Discussion Paper), Data Protection and Cybercrime Division, Council of Europe, Strasburg: 2013, pp. 5.

1.4. Ngritja e njësive të specializuara

Hetimi dhe ndjekja e veprave penale që prekin rrjetet dhe shërbimet e komunikimeve elektronike, si dhe analiza forense e provave elektronike kërkojnë posedimin e njohurive të veçanta. Në këtë kuptim, autoritetet e drejtësisë penale duhet të mbështeten në krijimin dhe forcimin e elementëve të mëposhtëm:

a) Ngritja e njësive të posaçme të krimit kompjuterik brenda strukturës së forcave policore ose njësive të larta teknike me përgjegjësi strategjike dhe operacionale;
b) Rritja e nivelit të njohurive të specializuara brenda sistemit gjyqësor;
c) Bashkëpunimi midis agjencive. Është shumë e rëndësishme që njësitë e krimit kompjuterik të bashkëpunojnë me shërbime të tjera të policisë (si psh. njësitë e krimit ekonomik, të mbrojtjes së fëmijëve) dhe institucione të tjera (si psh. njësitë e inteligjencës financiare, grupet e emergjencës kundër krimit kompjuterik etj);
d) Për të luftuar fenomenin e krimit kibernetik është i nevojshëm krijimi i një autoriteti kombëtar kryesor që të punojë dhe të ketë përgjegjësi për mbrojtjen kibernetike, i përbërë nga specialistë dhe ekspertë në fushat e sistemeve të komunikimit dhe të informacionit, të mbrojtjes dhe sigurisë fizike, sigurisë së informacionit, të administrimit të të dhënave kompjuterike, ekspertë teknikë për pajisjet filtruese të faqeve të internetit, ekspertë të auditit, ekspertë të ligjeve etj. Ky autoritet mund të realizojë detyra të tilla si: shkëmbimi i informacionit dhe publikimi i informacioneve për incidentet; koordinimi me përdoruesit e sistemeve për mbrojtjen kibernetike; trajnime në fushën e mbrojtjes kibernetike; përgatitja e detyrave për garantimin e sigurisë kibernetike; marrja e masave parandaluese dhe menaxhimi i kërcënimeve në nivel kombëtar; hartimi dhe zbatimi i një strategjie kombëtare të mbrojtjes kibernetike; përcaktimi i rregullave për sigurinë e informacionit në sistemet shtetërore; përmirësimi i metodave të vlerësimit të rrezikut dhe analiza e riskut; përcaktimi i mangësive të sigurisë së informacionit; propozimi i paketave ligjore për sigurinë; etj.

1.5. Identifikimi dhe mbrojtja e Infrastrukturave Kritike të Informacionit (CIIP) në Shqipëri

Sipas Konventës mbi Krimet Kibernetike të Këshillit të Europës është e domosdoshme krijimi i grupeve të reagimit ndaj incidenteve dhe emergjencave kompjuterike dhe përfshirja e këtyre grupeve në një strukturë të vetme. Kjo strukturë duhet të jetë në

gatishmëri që në çdo ditë të javës të sigurojë masa emergjente në lidhje me sulmet kriminale në rrjetet kompjuterike dhe detajet në lidhje me këto kërcënime.

Në këtë aspekt vendi ynë duhet të krijojë grupet e reagimit ndaj emergjencave kompjuterike kombëtare (CERTs), të ngjashme me struktura të tilla kombëtare si në vendet e zhvilluara. Një grup i tillë ka si mision mbrojtjen e teknologjisë së informacionit dhe komunikimit në hapësirën kibernetike, veçanërisht teknologjinë e qeverisë dhe infrastukturën kritike vartëse të internetit në vend. Vendet e BE-së po njohin vlerën dhe rëndësinë e grupeve të reagimit ndaj emergjencave komjuterike kombëtare, si një strukturë që i përgjigjet në mënyrën e duhur çdo lloj kërcënimi kibernetik.

Në rastin e vendit tonë mungon varësia nga mbrojtja e infrastrukturës kritike të informacionit (CIIP) dhe kjo tregon se mungon një motivim i fortë për investime në një shkallë të gjërë të burimeve që ka ky vend. Në këtë kontekst ngritja e nje grupi të reagimit ndaj emergjencave komjuterike kombëtare (CERTs) në Shqipëri është e domosdoshme, pasi shkëmbimet e informacionit midis institucioneve publike lidhur me rastet konkrete për incidentet e sigurisë së informacionit janë të papublikuara dhe mbahen të fshehura brenda institucioneve pa kërkuar mendimin dhe ekspertizën e specialistëve të fushës përkatëse.

Strukturat dhe organet e ndryshme të qeverisë në zbatim të legjislacionit në fuqi për mbrojtjen kibernetike duhet të përcaktojnë rregullat dhe përgjegjësitë mbi masat e sigurisë së informacionit dhe të stimulojnë nëpërmjet testimeve të ndryshme aftësitë dhe kapacitetet e strukturave në përballimin, ose jo, të këtyre sulmeve.

Motivimi për mbrojtjen dhe sigurinë e hapësirës kibernetike është një fushë në të cilën mirëkuptimi i vendit është i rëndësishëm, për këtë arsye përcaktimi i bazës ligjore/rregullative mbi të cilën operatorët e infrastrukturave kritike do të duhet të raportojnë mbi incidentet e rënda kibernetike është esenciale.

1.6. Krijimi dhe implementimi i kërkesave bazë të sigurisë kibernetike

Rritja e sigurisë në administratën shtetërore, rritja e përdorimit të sistemeve kompjuterike në administratën shtetërore, por dhe garantimi i sigurisë të tyre duhet të jetë një prioritetet i shtetit shqiptar.

a) Standarde, udhëzime dhe procedura të bazuara në praktikat më të mira ndërkombëtare duhet të përshtaten dhe miratohen për t'u zbatuar në administratën shtetërore.

b) Krijimi dhe miratimi i procedurave të analizës të rrezikut të sigurisë si një proces i vazhdueshëm dhe periodik për sistemet e përdorura dhe shërbimet elektronike të ofruara nga institucionet duhet të jetë prioritet, pasi zbatimi i tyre është një nga elementët kyç për rritjen e nivelit të sigurisë kibernetike.
c) Krijimi i programeve trajnuese dhe ndërgjegjësuese në fushën e sigurisë kibernetike për të gjithë nivelet e administratës konsiderohet si një proces, i cili garanton përdorimin, ngritjen dhe ofrimin e shërbimeve dixhitale të administratës në mënyrë të sigurt dhe të besueshme.

1.7. Shtimi i investimeve për rritjen e sigurisë në rrjetet/sistemet shtetërore

Prioritet duhet që t'i jepet shtimit të investimeve në hardware dhe software të automatizuara si masa proaktive dhe reaktive për të siguruar rritjen e sigurisë në rrjetet/sistemet shtetërore, kjo për të minimizuar kompromentimin e tyre si dhe për të rritur qëndrueshmërinë.

Gjithashtu duhet të inkurajohet ngritja e BCC-ve (Business Continuity Center) dhe DRC-ve (Disaster Recovery Center) për rrjetet/sistemet shtetërore si dhe ngritja e një sistemi monitorimi, i cili do t'i njoftonte në kohë institucionet, për rreziqet kibernetike që u kanosen duke monitoruar nyjet më të rëndësishme, trafikun dhe eventet që ndodhin në sistem për të mundësuar edhe nxjerrjen e konkluzioneve nga logimet që ruhen, pa ndërhyrë apo monitoruar përmbajtjen[235].

[235]Dokumenti i Politikave për Sigurinë Kibernetike, Republika e Shqipërisë, Tiranë, 2014.

LISTA E REFERENCAVE/BIBLIOGRAFIA

A. Literaturë

- Amelie, M. Weber. (2003), "*The Council of Europe's Convention on Cybercrime"*, 18 Berkeley Tech. L.J.
- Anrig, B., Benoist, E., etj. (2006). *Virtual Persons Applied to Authorization, Individual Authentication and Identification*. Në Identity in a Networked Society. FIDIS consortium.
- Antolise, F. (2000), *Manuale di Diritto Penale. Parte Generale*, 15ª ed., Milano, Dott. A. Giuffrè Editore.
- Antolisei, F. (2008). *Manuale di diritto penale: Parte speciale*, Vol.1. Milano: Giuffre.
- Arthur, J. Carter, IV & Perry A. (2004), *Computer Crimes*, 41 AM. CRIM. L. REV. Washington D.C.: The CSIS Press.
- Bakewell, E. J., Koldaro, M., & Tija, J. M. (2001). *Computer crime*. The American\ Criminal Law Review, 38, (3).
- Barkley, J. (1994). *Security in open systems*. NIST Special Publication 2007.
- Bassiouni, M. Cherif. (1992), "*Policy Considerations on Inter-State Cooperation in Criminal Matters*", Pace Yearbook of International Law, vol. 4.
- Beaulac, S. (2004). *The Power ofLanguage in the Making of International Law: The Word Sovereignty in Bodin and Vattel and the Myth ofWestphalia*, Leiden / Boston, Martinus Nijhoff Publishers.
- Bequai, A. (1978), *Computer Crime*, Lexington Books, Canada and United States.
- Bernal, P. (2014). *Internet Privacy Rights: Rights to Protect Autonomy*. New York: Cambridge University Press.
- Boshkoviq, M. (2000). *Kriminalisticka Metodika II*, Beograd.
- Brenner, S. (2001). *Defining cybercrime: A review of State and federal law*. In R. D.
- Brenner, S. (2010). *Cybercrime: Criminal Threats from Cyberspace.* Santa Barbara: ABC-CLIO.
- Brian, C. Lewis. (2004). *Prevention of Computer Crime Amidst International Anarchy*, 41 AM. CRIM. L. REV. 1353, 1359.
- Büllesbach, A. (2010). *Concise European IT Law*. Kluwer Law International.

- Calice, A. *I computer crimes nell'ordinamento giuridico italiano: inquadramento sistematico ed efficacia della risposta sanzionatoria'*, kursi 'Criminalità informatica e protocolli investigativi, Romë, janar 2006, f.24, sikurse është cituar nga Scognamilio, P. (2008), *Criminalita informatica: Commento organico alla legge 18 marzo 2008, n.48.* Napoli: Botimet Simone.
- Carlesi, Carlo. (2003). *Sicurezza informatica and 'computer crime*", Report, Istituto di Scienza e Tecnologie dell'Informazione "Alessandro Faedo, Pisa.
- Carter, D. (1995). *Computer crime categories*. FBI Law Enforcement Bulletin, 64, (7).
- Carter, D., & Bannister, A. J. (2000). *Computer crime*: *A forecast of emerging trends*. Paper presented at the Academy of Criminal Justice Sciences Annual Meeting, New Louisiana.
- Chamelin, & L. Territo (Eds). (2003). *Criminal Investigation* (8th ed). New York: McGraw- Hill Companies, Inc.
- CHAWKI, M. (2005). *A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy*, DROIT-TIC.
- Christopher, L. Blakesley. (1988) "*Jurisdictional Issues and Conflicts of Jurisdiction*", *in* M. Cherif Bassiouni (ed.), "*Legal Responses to International Terrorism. U.S. Procedural Aspects"*, Dordrecht, Martinus Nijhoff Publishers.
- Christopher, L. Blakesley. (1988). *Jurisdictional Issues and Conflicts of Jurisdiction, in* LEGAL RESPONSES TO INTERNATIONAL TERRORISM: U.S. PROCEDURAL ASPECTS (M.C. Bassiouni ed., Martinus Nijhoff Publishers).
- Clifford, R.D. (2001), *Cybercrime, the investigation, prosecution and defense of a Computer related crime*, Carolina Academic Press, United States.
- De Witt, A. (2007). *Usability issues with security of electronic mail.* Tezë Doktorale. Universiteti i Bruneit, Fakulteti i Sistemeve të Informacionit dhe Informatikës. f
- Denisa, A. (2010). "*Mbi disa ceshtje te se drejtes penale dhe procedural penale"*, Tirane,
- Devost, M. G. (1995). *National security in the information age*. Master thesis. University of Vermont.
- Dittrich, D., dhe Himma, K.E. (2006). *Hackers, Crackers and Computer Criminals* ; në Bidgoli, H. *Handbook of Information Security: Information Warfare; Social, Legal, And*

International Issues; And Security Foundations, Vol. 2. Bakersfield: John Wiley & Sons, Inc.

- Domenico, V. (2007). "*La nuova criminalita informatica. Evoluzione del fenomeno e strategie di contrasto*" Rivista di Criminologia, Vittimologia e Sicurezza.
- Ealy, K. (2003). *A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention.* SANS Institute.
- Fitz Patrick, J. (2002), "*Sovereignty, Territoriality, and the Rule of Law*", Hastings International and Comparative Law Review, vol. 25.
- Fitz Patrick,J. (2002). "*Sovereignty, Territoriality, and the Rule of Law*", Hastings International and Comparative Law Review, vol. 25, pp. 304,310. Brown S, *International Relations in a Changing Global System: Toward a Theory of the World Polity*, Boulder, Colorado, Westview Press, 1992.
- Ford, G (2006), *On the Definition and Classification of Cybercrime*, Journal in Computer Virology, Vol. 2, No. 1.
- Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. Great Britain: Pearson Education Limited.
- Gercke, M. (2008). "*National, Regional and International Legal Approaches in the Fight Against Cybercrime*", in Journal ofInformation Law and Technology, Issue 1.
- Grabosky P, N. (2001). *Virtual Criminality. Old Wine in New Bottle* ?, in Legal Studies, vol. 10, n. 2.
- Grabosky, P. (2006). "*Editor's Introduction*", in Crime Law and Social Change, vol. 46.
- Gralla, P. (1998). *How the Internet Works.* Indianapolis: Que Corporation.
- Harding, CH e Lim, C. L. (1999), "The Significance of Westphalia: An Archaeology of the International Legal Order", *in* Christopher Harding and C. L. Lim (eds), *Renegotiating Westphalia: Essays and Commentary on the European and Conceptual Foundations of ModernInternational Law*, The Hague / Boston / London, Martinus Nijhoff Publishers, pp. 1-23, see also Krasner D.S**.** (1999), *Sovereignty: OrganizedHypocrisy*, New Jersey, Princeton University Press.
- Hayden, E. (2006). *Cybercrime's impact on Information security, Cybercrime and Security*, IA-3.

- Icove, D. & Seger, K. (1995). *Computer crime: A crime fighters handbook*. Sebastopol, CA: O'Reilly & Associates, Inc.
- Katherine, M. Grzybowski. (2012). *An Examination of Cybercrime and Cybercrime Research*: *Self-control and Routine Activity Theory,* Arizona State University.
- Kenneth C, Randall. (1988), "*Universal Jurisdiction under International Law*", *Texas Law Review*, vol. 66.
- Kovacich, G.L. & Boni, W.C. (2000). *High-technology crime investigator's handbook: Wworking in the global information environment*. Woburn, MA:Butterworth- Heinemann.
- Latifi, V. (2004). *Kriminalistika*, Prishtinë.
- MASUDA. (1980). *The Information Society as Post-Industrial Society.*New Delhi: Vikas.
- McQuade, S. (2008). *Encyclopedia of Cybercrime*. Westport: Greenwood Press.
- Nabeth, T. *Identity of Identity*. Në Rannenberg, K., Royer, D., & Deuker, A. (2009). *The Future of Identity in the Information Society. Challenges and Opportunities.* Berlin, Springer.
- Nabeth, T. Identity of Identity. Në Rannenberg, K., Royer, D., & Deuker, A. (2009).*The Future of Identity in the Information Society. Challenges and Opportunities.* Berlin: Springer.
- O'Brien, James. (1999), *Management Information Systems* (4th). New York: Irwin/McGraw-Hill.
- Parker, D. B. (1999). *Sharing infrastructures: Cybercrime intelli*gence. Paper presented at a conference on cybercrime and terrorism, Stanford, CA.
- Pica, G. (1999). *Diritto penale delle tecnologie informatiche*, Torino: UTET.
- Picotti, L. (1996). *Commento all'art. 5 della legge n. 547 del 1993,* në *Legislazione penale.*
- Poonia, A.S., Bhardwaj, A. dhe Dangayach, G.S, (2011). *Cyber Crime: Practices and Policies for its Prevention.* The First International Conference on Interdisciplinary Research and Development, Tajlandë, 31 maj-1 qershor.
- R.Halili. (2008), *Kriminologjia*, Prishtine.
- Ray, A. (2002). *International Cyber-Jurisdiction: A Comparative Analysis*, American Business Law Journal, vol. 39.

- Reznik, M. (2013). *Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation.* Touro Law Review. Vol 29 (2).
- Rodota, S. (2003). *Europe and cyber security*. In James A. Lewis (Eds), *Security: Turning national solutions into international cooperation* (pp. 79-89). WashingtonD.C.: The CSIS Press.
- Sette, R. (2013). *Criminalità informatica. Analisi del fenomeno tra teoria, percezione e comunicazione sociale*, Clueb, Bologna.
- Sharma, V. (2011). *Information Technology Law - Law and Practice* (botimi i 3-të), New Delhi: Universal Law Publishing.
- Shipley, Greg. (2000). *How Secure Is Your Network*? *Network Computing*, 11.
- Smith, R.G., Grabosky, P & Urbas, G. (2004), *Cyber Criminals on Trial*, Cambridge University Press, Australia.
- Stephenson, P. (2000*). Investigating computer-related crimes*. New York: CRC Press LLC.
- Susan W, Brenner. (2004). *Toward a Criminal Law for Cyberspace: Distributed Security*, 10 B.U. J. SCI. & TECH. L.
- Taylor, R. W., & Loper, D. K. (2003). Computer crime. In C. R. Swanson, N. C.
- Vatis, M. (2003). International cyber-security cooperation: Informal bilateral models. In James A. Lewis (Eds), Security: *Turning national solutions into internationalcooperation.*
- Walden, I. (2007).*Computer Crimes and Digital Investigations*, Oxford University Press, 2007) *International & Comparative Law Quarterly*, Volume 57, Part 4.
- Wall, D. (2007). *Understanding Crime in the Information Age*, Polity Press, Routledge, London-New York.
- Wall, D. (Edited by). (2001). *Crime and the Internet*, Routledge, London-New York.
- Weirich, D. dhe Sasse, M. A. (2001). *"Pretty Good Persuasion: A first step towards effective password security for the Real World"*, punim i paraqitur në: New Security Paradigms Workshop, Cloudcroft, New Mexico, USA.
- Yar,M. (2006), *Cybercrime and Society*, London. Sage Publications.
- Zhilla, F & Canaj, E.2014). *Pirateria ne internet rrezik edhe per shoqerine Shqiptare*, Tirane: Revista Polis.

- Burime Parësore

A. Akte Normative

- Kodi Penal i Austrisë.
- Kodi Penal i Francës.
- Kodi Penal i Gjermanisë.
- Kodi Penal i Polonisë.
- Kodi i Procedurës Penale i Republikës së Shqipërisë.
- Ligji nr. 10023, dt. 27.11.2008 "*Për disa shtesa dhe ndryshime në Kodin Penal të R.SH*".
- Ligji Nr. 10325, datë 23.9.2010 "*Për Bazat e të Dhënave Shtetërore*" dhe VKM nr. 945, datë 2.11.2012 për miratimin e rregullores "*Administrimi i Sistemit të Bazave të të Dhënave Shtetërore*"
- Ligji nr. 8888, dt. 25.04.2002 '*Për Ratifikimn e Konventës për Krimin në fushën e Kibernetikës*'.
- Ligji nr. 9887, datë 10.03.2008, ndryshuar me ligjin nr. 48/2012 "*Për mbrojtjen e të dhënave personale*".
- Ligji nr.7895, dt. 27.1.1995 "*Kodi Penal i Republikës së Shqipërisë*", i ndryshuar.
- Ligji nr.8737, dt. 12.2.2001, '*Për Organizimin dhe Funksionimin e Prokurorisë në Republikën e Shqiëprisë*'.
- ***B. Akte tipike të BE***
- Direktiva 2002/58 "*Mbi përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike*".
- Direktiva 2006/24 KE "*Mbi ruajtjen e të dhënave të krijuara ose të përpunuara lidhur me ofrimin e shërbimeve të komunikimeve elektronike të disponueshme për publikun ose të rrjeteve të komunikimit publik*".
- Direktiva 95/46/EC "*Për mbrotjen e individëve në lidhje me përpunimin e të dhënave personale dhe qarkullimin e lirë të të dhënave të tilla*".
- Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (based

on proposal COM(2010) 517 final of 30/09/2010 - accompanying impact assessment and its summary).

- **Burime Dytësore**

A. Praktikë Gjyqësore

- CompuServe Germany case (Felix Somm decision)- Local Court [Amtsgericht] Munich File No.: 8340 Ds 465 Js 173158/95, available at:Cyber-Rights & Cyber-Liberties (UK).
- Court of Justice of the European Union, Press Release No 54/14, Luxembourg, 8 April 2014, Judgment in Joined Cases, C-293/12 and C- 594/12, Digital Rights Ireland and Seitlinger and Others. The full text of the judgment is published on the CURIA website on the day of delivery.
- *U.S.A. v. Ivanov* (2003), 172 C.C.C. (3d) 551 (Nfld.C.A.). See also U.S. Department of Justice. United States Attorney, "*Russian Man Sentenced for Hacking into Computers in the United States*", onlineat:
- http://www.usdoj.gov/criminal/cybercrime/ivanovSent.htm, last visited September 2, 2008.
- United States Attorney's office, Northern District of Florida, "*International Computer 'Hacker' Sentenced to More Than Three Years in Federal Prison*", online at:**http://www.usdoj.gov/criminal /cybercrime / bentleySent.pdf,last visited September 2, 2008.**
- United States v. Drew, 259 F.R.D. 449, 458 (C.D. Cal. 2009).
- Vendim i Gjykatës së lartë Nr.00-2013-1587 (261), datë 02.10.2013.

B. Burime dytësore nga website zyrtare

- Antonio, A. (2007), *Dal computer crime al computer-related crime*. Rivista di Criminolgia, Vittimologia e Sicurezza:
- Brown I. Eduards L. and Marsden C.,I*nformation Security and Cybercrime*, available at:http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1427776

- Communication from the Commission to the European Parliament, the Council and the Committee of the Regions, *Towards a general policy on the fight against cybercrime*, COM (2007) 267 final, Brussels, 22.5.2007, available at:www.europa.eu.
- *Convention on Cybercrime (ETS no. 185), Explanatory Report*, p. 61, available at:
- Dokumenti i Politikave për Sigurinë Kibernetike Republika e Shqipërisë, Tiranë, 2014.
- Feasibility Study for a European Cybercrime Centre, available at: RAND Europe URL: http://www.rand.org/randeurope.
- Gercke, M. *Understanding Cybercrime. A Guide for Developing Countries*, Draft April2009, available at www.itu.int.
- Gordon/Hosmer/Siedsma/Rebovich. (2003). *Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime*, available at:
- Hale. (2002), *Cybercrime: Facts & Figures Concerning this Global Dilemma*, CJI,Vol. 18, available at: http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37.
- http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.
- http://ec.europa.eu/internal_market/e-commerce/index_en.htm.
- http://ec.europa.eu/justice/doc_centre/privacy/law/index_en.htm.
- http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML
- http://www.cybercrimes.net/MCCIP/art7.htm.
- http://www.enisa.europa.eu/act/cert.
- http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf.
- http://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf.
- http://www.vittimologia.it/rivista/apruzzese%202007-01-01.pdf.
- Model Code of Cybercrime Investigative Procedure, Article VII, at:
- OECD. (2002). *Guidelines for the Security of Information Systems and networks: Towards a culture of security*. Retrieved March 13, 2004 from:
- OECD/IFP Project on "*Future Global Shocks"-"Reducing Systemic Cybersecurity Risk*", www.oecd.org/dataoecd/3/42/46894657. pdf.

- Parodi, C. (1998). *La tutela penale dei sistemi informatici e telematici: le fattispecie penali*, në Relazione presentata al Convegno Nazionale su "Informatica e riservatezza" del CNUCE, Pisa. I aksesueshëm në:www.privacy.it/cpisaparod.html.
- Raport shpjegues i Konventës së Këshillit të Evropës "*Mbi Krimin Kompjuterik*", http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.
- Rogers M. (1999). *Organized Computer Crime and More Sophisticated Security Controls*: *Which Came First the Chicken or the Egg*", in Telematic Journal of Clinical Criminology, available at www.criminologia.org.
- Rosini, Luciano. (2007). *Il computer crime e le strategie di constrasto*.Revista di Criminolgia, Vittimologia e Sicurezza: http://www.vittimologia.it/rivista/rosini%202007-01-01.pdf.
- Schjolberg S. (2004), *Computer Related Offences.* A presentation at the Octopus Interface 2004, Strasbourg, available at www.coe.int.
- Tanase, M. (2002). *Barbarians at the Gate: An Introduction to Distributed Denial of Service Attacks.* URL: http://www.securityfocus.com/infocus/1647.
- *Trajnim për krimin kibernetik për gjyqtarë dhe prokurorë: një koncept*, Departamenti i Shoqërisë së Informacionit dhe Aksionit kundër Krimit Drejtoria e Përgjithshme e të Drejtave të Njeriut dhe Çështjeve Ligjore Strasburg, Francë 8 Tetor 2009, www.coe.int/cybercrime.
- Vulpiani, Domenico.(2007). *La nuova criminalita informatica. Evoluzione del fenomeno e strategie di contrasto*" Rivista di Criminologia, Vittimologia e Sicurezza.: http://www. vittimologia.it/rivista/vulpiani%202007-01-01.pdf.
- Wendy McAuliffe. (2001), *Council of Europe Approves Cybercrime Treaty*, ZDNET UK NEWS, at http://newszdnet.co.uk/story/0t269-s209579600.html.