UNIVERSITETI I EVROPËS JUGLINDORE
SOUTH EAST EUROPEAN UNIVERSITY
УНИВЕРЗИТЕТ НА ЈУГОИСТОЧНА ЕВРОПА

FAKULTETI I DREJTËSISË
FACULTY OF LAW
ПРАВЕН ФАКУЛТЕТ

TEZA:

“Krimi kibernetik në RMV – aspekte krahasimore me vendet e UE-së”

Kandidat:
Kaltrina Dardhishta

Mentor:
Doc. Dr. Vedije Ratkoceri

Tetovë, qershor 2020

DEKLARATA E AUTORËSISË

Nën përgjegjësinë time personale, deklaroj se përmbajtja e temës së magjistraturës së paraqitur është punë origjinale e shkruar prej meje, e cila nuk është prezantuar asnjëherë para ndonjë institucioni tjetër për vlerësim dhe nuk është botuar i tëri ose pjesë të veçanta të tij. Të gjitha referencat dhe citimet në tekst janë bërë në bazë të burimeve të paraqitura në fusnota.

Me respekt

_____

( )

PËRMBAJTJA

ABSTRAKT

Krimi kibernetik, si një nga format më të zhvilluara të kriminalitetit në përgjithësi, është shumë prezent në shoqëri dhe paraqet kërcënim serioz për të. Rritja e numrit të viktimave të krimit kibernetik, ka bërë që t'i kushtohet rëndësi kësaj çështje në nivel ndërkombëtar. Rrezikshmëria e krimit kibernetik qëndron në faktin se kryhet nga persona shumë inteligjent, gjë që e vështirëson zbulimin e tyre dhe kapjen e kryerësve. Llojet apo kategoritë e krimit janë nga më të ndryshmet. Kur janë në fjalë shtetet, agjensionet e ndryshme botërore, organizatat ndërkombëtare, bizneset e mëdha, në të shumtën e rasteve, krimet kibernetike kryhen me qëllim që kryerësit të realizojnë dobi të mëdha pasurore, duke shkaktuar dëm të madh material ndaj viktimave.

Në këtë hulumtim janë analizuar në mënyrë të veçantë legjislacioni i RMV-së dhe legjislacionet e disa vendeve të UE-së, duke shtjelluar se si është i rregulluar krimi kibernetik dhe çfarë masa janë ndërmarr në secilin prej shteteve. E gjithë kjo, me qëllim të vetëm, që nëpërmjet analizës komparative të arrihen rezultate se çka mungon te ne dhe si duhet të veprohet për luftimin e krimit kibernetik.

Në RMV, për dallim nga shtetet e UE-së, ka mungesë të madhe të ekspertëve që hulumtojnë krimin kibernetik e njëkohësisht edhe mungesë të funksionimit të institucioneve të posaçme për luftimin e tij. Nga kjo rezulton se krimit kibernetik nuk trajtohet në mënyrë të duhur tek ne, nga e cila pamundësohet zbulimi dhe mundësohet përhapja më e madhe e krimit në fjalë.

Fjalët kyçe: krimi kibernetik, kryerës, legjislacion, institucione, strategji

ABSTRACT

Cybercrime, as one of the most developed forms of crime in general, is very present in society and poses a serious threat to it. The increase in the number of victims of cybercrime has made it important to address this issue internationally. The danger of cybercrime lies in the fact that it is perpetrated by very intelligent people, which makes it difficult to detect them and catch the perpetrators. The types or categories of crime are very different. When it comes to states, various world agencies, international organizations, big businesses, in most cases, cybercrime is committed in order for the perpetrators to realize great material benefits, causing great material damage to the victims.

In this research, the legislation of the Republic of North Macedonia and the legislation of some EU countries have been analyzed in a special way, explaining how cybercrime is regulated and what measures have been taken in each of the states. All this, with the only purpose of achieving results through comparative analysis of what we lack and how to act to combat cybercrime.

In the Republic of North Macedonia, unlike the EU countries, there is a great lack of experts who investigate cybercrime and at the same time a lack of functioning of special institutions to fight it. It follows that cybercrime is not being treated properly in our country, which makes it impossible to detect them and allows the crime to spread more widely.

Keywords: cybercrime, perpetrators, legislation, institutions, strategies

HYRJE

Çdo ditë e më shumë teknologjia bashkëkohore po zhvillohet. Mjetet e ndryshme teknologjike po avansohen me një hov të madh. Në këtë mënyrë, në më pak se dy dekada, këto mjete u bënë pjesë e pandashme e përditshmërisë së jetës së njerëzve dhe rëndësia e tyre në kontinuitet rritet deri në masën që mund të thuhet se ato e kontrollojnë apo diktojnë jetën e njerëzve. Në mënyrë paralele me këto zhvillime, gjithashtu u paraqitën dhe u përhapën edhe forma të krimeve që nuk janë hasur më parë. Pikërisht lëndë hulumtimi në këtë punim është një nga format më të reja të kriminalitetit në ditët e sotme, përkatësisht krimi kibernetik.

Kjo temë do të trajtohet në përgjithësi duke përfshirë edhe përhapjen dhe rregullimin legjislativ të tij në RMV. Njëkohësisht do të hulumtohen format e ndryshme të krimit kibernetik, ndikimi i tyre në jetën e përditshme, cënimi i të drejtave të njeriut të garantuara me Kushtetutë, fenomene këto për të cilat nevojitet një njohje paraprake më e thellë nëse dëshirohet që të parandalohen.

Gjithashtu do të analizohet se si mungesa e legjislacionit ndikon në rritjen apo mos sanksionimin e kriminalitetit duke pasur parasysh se në Republikën e Maqedonisë së Veriut nuk ekziston një ligj i posaçëm për krimin kibernetik por janë vetëm disa inkriminime në Kodin Penal.

Duke pasur parasysh se ky krim ka arritur të përhapet në masë të gjërë, përmes një analize komparative, në mënyrë të veçantë do të analizohet krimi kibernetik dhe lufta kundër tij në disa vende më të zhvilluara të Unionit Evropian, me qëllim që të arrijmë në përfundim se ku kemi ngecur ne si shtet dhe cilat hapa duhet t'i ndërmarrim drejtë luftimit të këtij fenomeni.

Metodologjia e hulumtimit

Për të trajtuar këtë temë, përkatësisht për ta hulumtuar krimin kibernetik në RMV dhe në disa vende të UE-së, do të përdoren metoda të ndryshme hulumtuese ose shkencore. Këto metoda janë:

- Metoda historike do të përdoret për të arritur deri te të dhënat apo njohuritë se kur ka filluar të paraqitet ky krim, sa ka qenë i zhvilluar dhe i rregulluar ligjërisht në të kaluarën;
- Metoda komparative do të përdoret për të krahasuar shtrirjen e krimit kibernetik duke përcaktuar ngjashmëritë dhe dallimet që ka ky fenomen në vendet e ndryshme të UE-së;
- Metoda normative do të përdoret për të shqyrtuar legjislacionin tonë dhe legjislacionet e shteteve që do të hulumtohen;
- Metoda statistikore do të shfrytëzohet për të paraqitur numrin e rasteve të zbuluara dhe sanksionuara tek ne, për të paraqitur të dhëna se si qëndron përhapja e këtij krimi në vendet e ndryshme të Evropës;
- Metoda e anketës nëpërmjet të cilës do anketoj një numër të caktuar personash për të ardhur deri në konkluza të ndryshme;

Gjithashtu do të shfrytëzohet literaturë adekuate duke përfshirë libra, punime shkencore, revista shkencore, burime të ndryshme nga interneti,shënimet zyrtare nga evidencat e institucioneve, etj.

KAPITULLI I PARË

Njohuri të përgjithshme mbi krimin kibernetik

1.1 Kuptimi i krimit kibernetik

Zhvillimet teknologjike, kompjuterët personal, telefonat e "mençur", interneti, sot luajnë një rol të madh në jetën e njerëzve. Ato kanë mundësuar lehtësim të dukshëm në shumë aspekte të ndryshme të përditshmërisë së çdo njeriu. Ardhja deri tek informacionet e sakta në mënyrën sa më të shpejtë të mundshme duke përfshirë këtu informacionet për situatat e ndryshme shoqërore, ekonomike, politike të të gjithë vendeve të botës, komunikimi i drejtpërdrejtë me persona të tjerë pa marrë parasysh vendndodhjen e tyre, kryerja e blerjeve të ndryshme nga web-faqet online, realizimi i pagesave të detyrueshme brenda sekondave dhe shumë dobi të tjera nga zhvillimet teknologjike, kanë ndikuar pozitivisht në masë të madhe tek ne. Në këtë mënyrë është krijuar edhe varshmëria nga këto mjete.

Por nga ana tjetër, përveç të mirave të shumta, me këto zhvillime janë avancuar edhe mënyrat për kryerjen e veprave penale apo krimeve të ndryshme, duke shkuar kështu në një nivel tjetër të kriminalitetit i cili as që ishte menduar më parë. Formë të këtij kriminaliteti paraqet krimi kibernetik i cili është bërë preokupim global, për shkak se paraqet shkallë të lartë të rrezikshmërisë shoqërore sepse vazhdimisht po përsoset e në të njëjtën kohë po bëhet shumë i vështirë që të kapet.

Për krimin kibernetik ekzistojnë përkufizime nga autorë dhe organizata të ndryshme që merren me studimin dhe luftimin e tij.

Konventa e Budapestit mbi Krimin Kibernetik, e miratuar nga Këshilli Evropian në vitin 2001, jep sqarime lidhur me disa terme. Kështu sipas kësaj Konvente:

"sistem kompjuterik" do të thotë çdo pajisje ose një grup i pajisjeve të ndërlidhura,ku në bazë të një programi, kryhet përpunimi automatik i të dhënave;

"të dhëna kompjuterike" do të thotë çdo paraqitje e fakteve, informacioneve ose koncepteve në një formë të përshtatshme për përpunim në një sistem kompjuterik[1]. Në preambulën e saj, krimi kibernetik përkufizohet si: "aktivitete të drejtuara direkt kundër konfidencialitetit, integritetit dhe qasjes së sistemeve kompjuterike dhe rrjeteve të të dhënave, si dhe keqpërdorimit të mundshëm të këtyre rrjeteve të sistemit dhe të dhënave kompjuterike"[2].

Punimi i parë shkencor mbi kriminalitetin kompjuterik është shkruar nga Von zur Muhlen (1973), i cili krimin kibernetik e definon si dukuri që përfshin të gjitha sjelljet në të cilat kompjuteri është mjet dhe qëllim i veprimtarisë kriminale[3].

Lidhur me definimin e krimit kibernetik, rëndësi të madhe ka edhe Kongresi i tetë i Kombeve të Bashkuara për parandalimin e krimit dhe trajtimit të kryerësve, ku ky term përkufizohet në dy kuptime:

-në kuptimin e ngushtë, me krim kibernetik kuptohet çdo sjellje e kryer nëpërmjet veprimeve elektronike të cilat drejtohen ndaj sigurisë së sistemeve kompjuterike dhe të dhënave të përpunuara prej tyre;

-në kuptim të gjërë, me krim kibernetik kuptohet çdo sjellje e kryer nëpërmjet një kompjuteri apo sistemi kompjuterik[4].

Edhe përkundër tentativave të shumta të autorëve të ndryshëm rreth përcaktimit të definicionit të krimit kibernetik, deri më tani nuk ekziston një definicion i pranuar universal. Sipas profesorit Dragan Jovasheviq, "kjo formë e krimit, ndryshe nga format e tjera, nuk është ende një kategori fenomenologjike dhe prandaj është e pamundur të përcaktohet definicioni precis. Krimi kibernetik është vetëm një formë e përgjithshme përmes së cilës shfaqen lloje të ndryshme të veprave penale"[5].

---

[1] Convention on Cybercrime: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (qasja e fundit 10.02.2020)
[2] Convention on Cybercrime, Këshilli i Evropës, Budapest, 2001.
[3] Latifi, Vesel, "Kriminalistika", Prishtinë, 2014, fq.473
[4] United Nations "Definiton of cybercrime" 2014: https://idn-wi.com/united-nations-definition-cybercrime/ (qasja e fundit 10.02.2020)
[5] Jovaševič D., Leksikon krivicnog prava, JP Sluzbeni list, Beograd, 2002

Shumëllojshmëria e formave të krimit kibernetik dhe shpejtësia me të cilën përhapet, e kanë vështirësuar definimin e këtij krimi. Në këtë drejtim, autori Don Parker arriti në përfundim se "Krimi i kompjuterit është një formë përmes së cilës shfaqen lloje të ndryshme krimesh, të cilat në të ardhmen do të jenë mbizotëruese"[6].

Teoricienti Michael Cross krimin kibernetik e definon si vepër penale që kryhet me përdorimin e internetit ose një rrjeti tjetër kompjuterik[7]. Sipas tij kompjuterët dhe rrjetet mund të përfshihen në krime në disa mënyra të ndryshme:

- Kompjuteri ose rrjeti mund të jenë mjeti i krimit (përdoret për kryerjen e krimit).
- Kompjuteri ose rrjeti mund të jenë shënjestra të krimit ("viktima").
- Kompjuteri ose rrjeti mund të përdoren për qëllime të rastësishme që lidhen me krimin (për shembull, për të mbajtur të dhëna për shitje ilegale të drogës)

Autori gjerman, Hans Gopinger thekson se krimi kibernetik është veçanërisht i dukshëm gjatë kryerjes së veprave të caktuara penale, të cilat ai i ndan në disa veprime. Në rend të parë, ai përmend manipulimet kompjuterike. Veprim tjetër është i ashtuquajturi spiunazh kompjuterik, i cili kryhet me ndihmën e programeve të caktuara, duke filluar nga lojërat deri te programet e fushave të ndryshme shkencore, të cilat u sjellin fitime të mëdha financiare autorëve. Formë tjetër është i ashtuquajturi sabotim kompjuterik, me të cilin bëhen ndërhyrje jolegale dhe të paligjshme në sisteme dhe programe të ndryshme kompjuterike, me qëllim që të shkatërrohen ose të shkaktohen dëme të mëdha materiale për pronarët e tyre[8].

Gjithashtu, kriminologu italian Gianluigi Ponti, flet se si kompjuterit si një mjet ekzekutimi shfrytëzohet për kryerjen krimet më të shpeshta, e të cilat janë: mashtrimi, pirateria, vjedhja e programeve, qasja e paautorizuar në programe, qasja në programe private dhe zbulimi i sekreteve intime, spiunazhi politik dhe industrial dhe format e tjera të krimit. Sipas

[6] Parker, Don, "Fighting computer crime", New York, 1985, fq.7

[7] Shinder, Debra Littlejohn, and Michael Cross. "Scene of the Cybercrime", 2008, fq.2

[8] Goppinger, Hans, "Kriminologie", Munchen, 1997, fq. 545

tij, krimi kibernetik është shumë i përhapur, por edhe shumë i vështirë për tu zbuluar. Ashtuqë, numri i errët është shumë i lartë[9].

Në përpjekje për të dhënë një mendim autonom mbi krimin kibernetik, ne theksojmë se kjo është një formë e veçantë e krimit, në të cilën kompjuteri paraqitet si një mjet për të kryer veprim të paligjshëm ose si një objekt sulmi të drejtuar nga njerëz që kanë njohuri për sistemet kompjuterike, me qëllim që të sjellin përfitime për veten ose të tjerët. Definicionet e lartëpërmendura bëjnë të kuptojmë se krimi kibernetik ka karakteristika të veçanta me të cilat dallon nga veprat e tjera penale. Disa nga këto veçori që e karakterizojnë janë shpejtësia e kryejes së këtij veprimi, mungesa e kryerësit së vepres penale në vendin e ngjarjes, vështirësia për ta zbuluar këtë lloj krimi përshkak të mosekzistimit të gjurmëve, mungesa e dëshmitarëve, e kështu me radhë. Gjithashtu, nuk duhet anashkaluar edhe një fakt tjetër që e karakterizon këtë vepër penale, e që duhet pasur parasysh, se kryerësit e krimeve kibernetike janë individë me inteligjencë dhe aftësi të larta në këtë drejtim. Shpesh ndërmarrin veprime që janë një hap para punës së institucioneve që merren me zbulimin e tyre. Kjo e vështirëson shumë situatën dhe si krim e bën shumë të dallueshëm nga llojet e tjera të krimeve në përgjithësi.

1.2. Historiku i krimit kibernetik

1.2.1 Paraqitja e krimit kibernetik

Për paraqitjen e krimit kibernetik ekzistojnë mendime të ndryshme. Janë të shumtë autorët që vitet fillestare dhe arsyet e shfaqjes të këtij krimi i kanë të ndryshme nga njëri tjetri.

Disa teoricientë theksojnë se ideja për disa lloje të krimit kibernetik u ngrit në të njejtën kohë kur kompjuteret filluan të përdoreshin më shumë. Jonathan Clough thotë se që nga vitet e

[9] Ponti, Gianluigi, "Compendio di Criminologia", Milano, 1997, fq. 161

60 filluan të raportohen veprime si manipulim i kompjuterëve, sabotimit të kompjuterëve, spiunazh i kompjuterëve dhe përdorimi i paligjshëm i sistemeve kompjuterike[10].

Sipas Majid Yar, krimi kibernetik fillet e veta i ka në kohën kur është paraqitur interneti. Ai thekson se "pa internetin, krimi kibernetik nuk do të kishte ekzistuar"[11]. Mëtej, Yar vazhdon me analizën e tij duke sqaruar se janë të dhënat e ndryshme që ne njerëzit fusim në internet, ato të cilat krijojnë mundësi për veprimtari kriminale. Shembull konkret, nëse njerëzit nuk do i kishin kryer blerjet e ndryshme nga interneti, atëherë nuk do kishte mundësi të bëheshin keqpërdorime apo veprime kriminale me kredit kartelat. E njejtë me të është edhe situata, ku për shkak se ne përdorim internetin për të komunikuar me miq tanë, janë krijuar virusa të ndryshëm të cilët shkatërrojnë sistemet e postës elektronikedhe shkaktojnë dëme të mëdha. Origjina e internetit lidhet me zhvillimin e një rrjeti, të quajtur ARPANET, i sponsorizuar nga ushtria amerikane në vitet 1960[12]. Qëllimi ishte të përcaktohej një mjet me të cilin mund të bëhet i mundur komunikimi i sigurt dhe koordinimi i aktiviteteve ushtarake.

Gjithashtu, edhe autorja Sussan W. Brenner paraqitjen e krimit kibernetik e lidh me vitet e 60-ta kur kompjuterët kishin sisteme "mainframe"[13]. Ajo këtë mendim e mbështet në faktin se, përderisa në vitin 1960, në SHBA, kishte në përdorim rreth 5000 "mainframe", në vitin 1970 ky numër u rrit deri në 80000 përdorues në SHBA dhe 50000 të tjerë jashtë vendit dhe duke pasur parasysh rritjen e jashtëzakonshme të këtij numri të kompjuterëve, nuk është për t'u habitur që krimi i kompjuterave filloi të bëhej problem në vitet e 60-ta[14]. Sipas saj historija e informatikës moderne daton që nga shekulli i XIX, por zhvillimi i kompjuterit nuk filloi deri pas Luftës së Dytë Botërore

[10] Clough, Jonathan, "Principles of Cybercrime." New York, 2010, fq.3
[11] Yar, Majid, "Cybercrime and Society" London, 2006, fq.6;
[12] Po aty ;
[13] Kompjuter i madh, i fuqishëm, që mund të trajtojë shumë detyra njëkohësisht dhe zakonisht është përdorur për tregti.
[14] Brenner, Susan W., "Cybercrime Criminal Threats from Cyberspace" California, 2010, fq.10;

1.2.2 Historiku i zhvillimit të krimit kibernetik

Derisa teoricientet e lartëpërmendur, paraqitjen e krimit kibernetik, e lidhin kryesisht me vitet e 60-ta, disa autorë dhe publikime tjera shkojnë edhe më larg, duke theksuar kështu se elemtetet e para të krimit kibernetik ekzistojnë edhe më herët.

Zhvillimin e krimit kibernetik në të kaluarën do ta shtjellojmë përmes rasteve të paraqitura nga redaktorët e revistës për krim kibernetik "Cybercrime Magazine", të cilët në korrik të vitit 2019, publikuan një listë të këtyre krimeve që datojnë nga viti 1834[15]. Këto janë disa prej tyre:

1834 - Sistemi francez "Telegrafi" - Disa hajdutë kanë hakuar sistemin francez "Telegrafi" dhe kanë vjedhur informacionin e tregut financiar, duke kryer kështu sulmin e parë kibernetik në botë;

1870 - Switchboard Hack – Një djal i ri i punësuar si një operator i linjës telefonike ka qenë në gjendje të shkëpusë dhe ridrejtojë thirrjet si dhe të përdorë linjën për përdorim personal;

1878 - Telefonatat e hershme - Dy vjet pasi Aleksandër Graham Bell shpik telefonin, kompania "Bell Telephone" përjashton një grup të adoleshentëve nga sistemi telefonik në New York sepse ata vazhdimisht dhe qëllimisht kanë keqpërdorur dhe shkëputur lidhjet e klientëve;

1939 — "Military Codebreaking" Alan Turing dhe Gordon Welchman zhvillojnë një makinë elektro-mekanike- "BOMBE", gjatë Luftës së Dytë Botërore derisa punonin si persona që thyenin kode në Bletchley Park. Kjo u ndihmoi për të prishur kodet enigme të gjermanëve;

1940 - Haker i parë - Rene Carmille, një anëtar i rezistencës në Francën e okupuar naziste dhe një ekspert kompjuteri që zotëronte makinat që qeveria e Francës i përdorte për të përpunuar informacione, zbulon se nazistët po përdorin makineritë "punch-card" për të gjurmuar hebrenjtë;

1957 - Joe Engressia (Joybubbles), një djalë i verbër, 7-vjeçar, dëgjon një tingull në një linjë telefonike dhe fillon të fishkëllen përgjatë tij me një frekuencë prej 2600Hz, duke i mundësuar

[15] Cybersecurity CEO: The history of cybercrime, from 1834 to Present: https://cybersecurityventures.com/cybersecurity-ceo-the-history-of-cybercrime-from-1834-to-present/ (qasja e fundit më 16.02.2020)

atij të komunikojë me linja telefonike dhe bëhet hakeri i parë i telefonit në SHBA;
1969 - RABBITS Virus - Një person anonim instalon një program në një kompjuter në Qendrën Kompjuterike të Universitetit të Washingtonit. Programi i paqartë bën kopjet e vetes derisa kompjuteri të mbingarkohet dhe të ndalojë punën. Mendohet se është virusi i parë i kompjuterave;
1973 - në një bankë lokale në New York përdoret një kompjuter për të përvetësuar mbi 2 milion dollarë;
1982 – "The Logic Bomb"- CIA shpërthen një tubacion të gazit siberian pa përdorimin e një bombe ose një rakete, duke futur një kod në rrjet dhe sistemin kompjuterik që kontrollon tubacionin e gazit. Kodi ishte vendosur në pajisjet e blera nga Bashkimi Sovjetik;
1988 — "The Morris Worm" – Robert Morris krijoi virusin e parë në internet;
1995 - Vladmir Levin – Inxhinieri rus i softuerëve Vladimir Levin hakon sistemin e IT-së të Citibank në New York, nga banesa e tij në Shën Petersburg dhe autorizon një seri transaksionesh mashtruese, duke përfunduar kështu instalimin e rreth 10 milion dollarëve në llogari;
2000 – "Mafiaboy" – kanadezi 15-vjeçar Michael Calce, nxënës i shkollës së mesme, lëshon një sulm DDoS në disa faqe interneti me profit të lartë, përfshirë Amazon, CNN, eBay dhe Yahoo! Një ekspert i industrisë, vlerëson se sulmet rezultuan në dëmtime prej 1.2 miliardë dollarësh;
2010 - Zeus Trojan Virus - Një rreth i kryerësve të krimit kibernetik në Evropën lindore vjedhin 70 milion dollarë nga bankat amerikane duke përdorur virusin Zeus Trojan për të goditur llogaritë bankare të hapura dhe për të tërhequr paratë në Evropën Lindore. Dhjetëra individë u akuzuan;
2011 – "Sony Pictures" - Një haker që ka ruajtur të dhënat e Sony-t, ekspozon të dhënat e mbi 100 milion konsumatorëve që përdorin shërbimet e PlayStation në internet. Hakerët fitojnë qasje në të gjitha informacionet e kredit kartelave të përdoruesve. Shkelja i kushton Sony-t më shumë se 171 milion dollarë; ;
2014 – "eBay" - Një sulm në internet ekspozon emrat, adresat, datat e lindjes dhe fjalëkalimet e koduara të të gjithë, 145 milion përdoruesve të eBay.

Revista e lartëpërmendur, në vitet pasuese duke filluar nga 2014 e deri më 2019, ka publikuar një numër dukshëm më të madh të rasteve apo e krimeve kibernetike. Përveç kësaj, nëse në vitet e hershme krimet kibernetike kanë qenë më të ”lehta” në ditët e sotshme vërehet se kanë ndryshuar dhe kanë përparuar mënyrat e kryerjes, duke sjellur kështu fitime të mëdha për kryerësit. Kjo na len të kuptojmë se krimi kibernetik po zhvillohet në të njëjtin hap, për të mos thënë një hap më para, se zhvillimet e tjera teknologjike. Zhvillimi i shpejtë teknologjik vazhdon dhe do të vazhdojë, duke paraqitur kështu sfida të reja për ata të cilët e luftojnë.

1.3 Llojet e krimit kibernetik

1.3.1 Kategoritë e krimit kibernetik

Krimi kibernetik është bërë një shqetësim i gjithanshëm duke bërë kështu që shumë persona të mirren me studimin dhe hulumtimin e tij. Ai shpesh cilësohet si formë e krimit të organizuar që mund të paraqitet në lloje të ndryshme. Sa i përket llojeve të krimit kibernetik ekzistojnë ndarje të ndryshme nga autorë të shumtë. Por, një nga ndarjet që është pranuar nga shumica e autorëve është ajo e David Wall. Ai krijoi një nga tipologjitë më të njohura të krimit kibernetik duke e ndarë në katër kategori[16] :

1. Cyber-trespass – (shkeljet kibernetike) – kalimi i kufijve duke hyrë në pronën e njerëzve të tjerë dhe/ose duke dëmtuar atë, psh. virusat, hakimi;
2. Cyber-deceptions and thefts – (mashtrimet dhe vjedhjet kibernetike) – vjedhje e parave, pronës psh. vjedhje e të dhënave të kredit kartelave, shkeljet e pronësisë intelektuale;
3. Cyber-pornography – (pornografia kibernetike) – shkelja e ligjeve mbi moralin;
4. Cyber-violence – (dhuna kibernetike) – shkaktimi i dëmit psikologjik ose nxitja e dëmit fizik ndaj të tjerëve, psh. gjuha e urrejtjes.

[16] Wall, David, ”Crime and the Internet”, London, 2001, fq.3-7

Nga klasifikimi i tillë mund të shihet se ndarja e krimit kibernetik bëhet sipas objektit apo cakut të veprës penale. Dy kategoritë e para përmbajnë krime kundër pronës, pasurisë, e treta mbulon krime kundër moralit dhe e katërt ka të bëjë me krime kundër personit.

Disa vite më vonë, më saktësisht në vitin 2007, David Wall në botimin e tij të radhës mbi krimin kibernetik, bëri një tjetër klasifikim[17]:

1. Computer integrity crimes – (krimet e integritetit të kompjuterit) - që cilësohen si "krimet kundër makinës përkatësisht kompjuterit", më saktësisht krimet që kryhen për të dëmtuar një kompjuter tjetër;
2. Computer assisted crimes- (krimet e asistuara nga kompjuteri) që cilësohen si "krimet që përdorin makinën", më saktësisht krimet që kryhen duke përdorur kompjuterin;
3. Computer content crimes (violence, pornography) – krime nga përmbajtja kompjuterike (dhuna, pornografia) që cilësohen si “krimet në makinë”, më saktësisht krimet që bëhen në kompjuter.

Ekziston edhe një ndarje tjetër nga Debra Littlejohn Shinder, që është bërë në kategori shumë më të gjëra. Sipas kësaj ndarje krimet kibernetike ndahen në krime të kryera nga kriminelë të dhunshëm ose potencialisht të dhunshëm, dhe krime jo të dhunshme[18]. Krimet kibernetike të dhunshme ose potencialisht të dhunshme përfshijnë:

1. Terrorizmin kibernetin (Cyberterrorism)
2. Sulme kërcënuese (Assault by threat)
3. Cyberstalking
4. Pornografia me fëmijë (Child pornography)

Krimet kibernetike jo të dhunshme ndahen në:

1. Shkeljet kibernetike (Cybertrespass)
2. Vjedhjet kibernetike (Cyberthef)
3. Mashtrimet kibernetike (Cyberfraud)
4. Krime të tjera në internet

[17] Wall, David, “Cybercrime: The transformation of crime in the information age”, Cambridge, 2007
[18] Shinder, Debra Littlejohn, and Michael Cross. “Scene of the Cybercrime”, 2008, fq.15

1.3.2 Aktet e kryerjes së krimit kibernetik

Në anën tjetër, aktet më të shpeshta nëpërmjet të cilave kryhet krimi kibernetik janë: mashtrimet përmes internetit, vjedhja e identitetit, hakingu (hacking), fishingu (phishing), viruset e ndryshme, ngacmimet kibernetike (cyber bulling) etj.

1.3.2.1 Mashtrimet përmes internetit

Mashtrimi është një term i përgjithshëm. Përdoret për të përshkruar një krim në internet që synon të mashtrojë person të caktuar, në mënyrë që të sigurojë të dhëna ose informacione të rëndësishme. Mashtrimi mund të bëhet duke ndryshuar, shkatërruar, vjedhur çdo informacion për të siguruar një përfitim të paligjshëm ose të padrejtë[19].

1.3.2.2 Vjedhja e identitetit

Vjedhja e identitetit është një formë specifike e mashtrimit, në të cilën kriminelët kibernetikë vjedhin të dhëna personale, duke përfshirë fjalëkalimet, të dhënat në lidhje me llogaritë bankare, kredit kartelat, sigurimet shoqërore dhe informacione të tjera. Përmes vjedhjes së identitetit, kriminelët në fakt vjedhin para. Sipas një studimi të vitit 2017, nga 19 vende Evropiane, humbjet e shkaktuara nga vjedhjet e identitetit kanë arritur rekord prej 1.8 miliardë euro[20].

[19] The 16 most common types of cybercrime acts, 2018: https://www.voipshield.com/the-16-most-common-types-of-cybercrime-acts/ (qasja e fundit më 18.02.2020)
[20] Identity theft is more rampant now than ever—here's how to prevent It: https://www.readersdigest.ca/home-garden/money/identity-theft-europe/ (qasja e fundit më 18.02.2020)

1.3.2.3 Hakingu (hacking)

Hacking përfshin përvetësimin e pjesshëm ose të plotë të funksioneve të caktuara brenda një sistemi, rrjeti ose websajti. Ai gjithashtu synon të ketë akses në të dhëna dhe informacione të rëndësishme, duke shkelur privatësinë. Shumica e "hakerave" sulmojnë llogaritë e korporatave dhe qeverive. Ekzistojnë lloje të ndryshme të metodave dhe procedurave të hakingut. Në vitin 2018 u zbulua se disa hakerë, me vite kishin depërtuar në rrjetin e komunikimeve diplomatike të Bashkimit Evropian[21].

1.3.2.4 Fishingu (phishing)

"Phishers" veprojnë si një kompani ose organizatë legjitime. "Phishing" është krim në internet me të cilin objektivi ose personi që dëshirohet të dëmtohet, kontaktohet me postë elektronike, telefon ose mesazh. Kjo zakonisht bëhet nga ndonjë person që shtiret se ka cilësinë e një "institucion i ligjshëm". Përdoruesit zakonisht besojnë se këto janë të ligjshme, duke futur kështu informacionet e tyre personale. Në këtë mënyrë nxjerren shumë informacione lidhur me fjalëkalimet, të dhënat personale, të dhëna të kredit kartelave etj. Më 28 mars 2018 nëntë persona u arrestuan në Rumani dhe njëmbëdhjetë në Itali për mashtrim bankar që kapën rreth 1 milion euro nga qindra klientë. Një hetim dy-vjeçar i krimit kibernetik midis Drejtorisë rumune për hetimin e krimit të organizuar dhe terrorizmin, policisë kombëtare rumune, prokurorisë së Milanos dhe policisë kombëtare italiane, me mbështetjen e Eurojust, Europol dhe Taskforce ka çuar në arrestimin e 20 të dyshuarve[22].

[21]Hacked European Cables, 2018: https://www.nytimes.com/2018/12/18/us/politics/european-diplomats-cables-hacked.html (qasja e fundit më 19.02.2020)
[22] EUROJUST:20 hackers arrested in EUR 1 million bank phishing scam,2018: http://www.eurojust.europa.eu/press/PressReleases/Pages/2018/2018-03-29.aspx (qasja e fundit më 19.02.2020)

1.3.2.5 Viruset e ndryshme

Shumica e kriminelëve përfitojnë shumë nga viruset. Nëpërmjet viruseve fitojnë qasje të paautorizuar në sisteme dhe vjedhin të dhëna të rëndësishme. Kryesisht, programet shumë të zhvilluara i dërgojnë viruset e ndryshme tek të tjerët, për të dëmtuar dhe shkatërruar kompjuterë, rrjete dhe sisteme. Viruset mund të përhapet përmes pajisjeve që shkëmbejnë të dhëna dhe përmes internetit. Pasi që depërtojnë në pajisje ato vazhdojnë të përhapen nga një kompjuter në tjetrin apo nga një telefon në tjetrin[23]. Autori Veton Vula thotë se "karakteristikë themelore e kësaj vepre është krijimi dhe përhapja e këtyre programeve destruktive, mundësitë e të cilave janë nxitja dhe bartja e formave të ndryshme të dëmtimeve në sistemet ku gjenden ato viruse"[24].

1.3.2.6 Ngacmimet kibernetike (cyberbullying)

Bulizmi apo ngacmimi në përgjithësi është një problematikë mjaft e përhapur sidomos tek të rinjtë. Cyberbullying (ngacmimi kibernetik) paraqet formë moderne të bulizmit apo ngacmimit. Faktin se të rinjtë sot kanë qasje të drejtpërdrejtë në internet qoftë nga kompjuterët personal apo celularët, kudo që ato ndodhen, në shtëpi, shkollë apo në vende publike, tregon shumë rreth kësaj problematike. Ky lloj sulmi apo agresioni elektronik paraqet kërcënim serioz për shëndetin psiqik të shumë të rinjëve. Në një studim shkencor, Tokunaga këtë krim e definon si "Çdo sjellje e kryer përmes mediave elektronike ose dixhitale, nga individë ose grupe që adresojnë në kontinuitet mesazhe armiqësore ose agresive, të cilat synojnë të shkaktojnë dëm për të tjerët"[25]. Ky lloj bulizmi (ngacmimi) dallon nga ai tradicional nga fakti se këtu viktima dhe kryerësi nuk janë ballë për ballë njëri tjetrit. Në këto raste

[23]ENISA "What is malware?": https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/malware (qasja e fundit më 19.02.2020)
[24] Vula, Veton,"Krimi kompjuterik", Prishtinë, 2010, fq.105
[25] Tokunaga, Robert S. "A critical review and synthesis of research on cyberbullying victimization." -Computers in human behavior- 2010, fq. 277-287.

ngacmuesi nuk dihet, ai kryen këtë akt nëpërmjet internetit pa ju njohur identiteti. Cyberbullying (ngacmimi kibernetik) ka rezutlate shumë më negative sepse ai qëndron në internet dhe mund të shihet në çdo kohë, e të përhapet me shpejtësi marramendëse.

1.3.2.7 Abuzimet seksuale të fëmijëve në internet

Pornografia me fëmijë është krim shumë i rëndë që paraqet shkelje serioze të të drejtave fundamentale të njeriut. Disa nga organizatat dhe agjencionet ndërkombëtare që merren me këtë çështje (siç janë Europol, Interpol) përdorin një term tjetër "child sexual exploitation" (shfrytëzim seksual i fëmijëve)[26]. Pornografia e fëmijëve në internet paraqet çdo shfrytëzim të ndonjë të mituri apo fëmije që detyrohet për sjellje seksuale dhe e cila paraqitet si video online apo fotografi e publikuar në internet. Ky lloj keqpërdorimi është vepër penale që dënohet si me legjislacionet shtetërore ashtu edhe me aktet e ndryshme ndërkombëtare. Sipas legjislacionit vendas, Republika e Maqedonisë së Veriut, pornografinë fëmijërore e rregullon me nenin 193-a të Kodit Penal[27], sipas të cilit parashihet dënim me së paku pesë vjet burgim. Ky krim në ditët e sotshme zakonisht kryhet nëpërmjet internetit.

Angazhimi i parë ndërkombëtar lidhur me këtë çështje është Konferenca ndërkombëtare për luftimin e pornografisë së fëmijëve në internet, e mbajtur në Vienë në vitin 1999, ku u deklarua se: "pornografia e fëmijëve në internet është një problem në rritje, dhe derisa bota do të fillojë të përdor më shumë internetin, ajo do të vazhdojë të rritet në të ardhmen pasi nuk njeh apo nuk respekton kufijtë"[28]. Sot, ekzistojnë edhe shumë akte të tjera që e inkriminojnë këtë dukuri.

[26] EUROPOL ," Child Sexual Exploitation Fact Sheet 2011"
[27] Kodi Penal i Republikës së Maqedonisë së Veriut
[28] EUROPOL ," Child Sexual Exploitation Fact Sheet 2011"

1.3.2.8 Pirateria e softuerëve (Software Piracy)

Interneti është i mbushur me programe që kopjojnë në mënyrë të paligjshme përmbajtjen origjinale të këngëve, librave, filmave, albumeve dhe softuerëve. Kjo paraqet shkelje të së drejtës së autorit. Pirateria e softuerëve është akti i vjedhjes së softuerëve që është i mbrojtur me ligj, e cila përfshin kopjimin, shpërndarjen, modifikimin ose shitjen e softuerit[29].

1.4 Shkaqet e paraqitjes së krimit kibernetik

Etiologjija kriminale është shkenca e cila analizon dhe studion shkaqet e paraqitjes së të gjitha veprave penale. Ajo ka të bëjë me njohjen e burimeve, rrënjëve dhe rrethanave përcaktuese të kriminalitetit[30]. Lidhur me shkaqet, rrënjët, burimet që ndikojnë në kryerjen e krimeve, në literaturë të ndryshme përdoret emërtimi faktorë kriminogjen. Njohja e këtyre faktorëve apo shkaqeve luan rol të madh në luftimin dhe parandalimin e kriminalitetit. E njejta gjë vlen edhe për krimin kibernetik.

Epoka dixhitale në të cilën jetojmë, ka ndryshuar mënyrën e jetesës e në veçanti mënyrën e socializimit. I gjithë ky përparim është shoqëruar nga ana tjetër, edhe nga shfrytëzimi për qëllime kriminale. Për një person që kryen krim apo mashtrim, përdorimi i internetit, postës elektronike ose një faqe të internetit, i mundëson që potencialisht të arrijë tek më tepër njerëz. Kompjuteri dhe interneti bëhen një mjet tejet i dobishëm dhe i përshtatshëm për nevojat e kriminelit në drejtim të mundësimit të kryerjes së krimit, madje ndihmon që ky krim të kryhet edhe më lehtë. Shpeshherë kjo mënyrë veprimi nuk len asnjë gjurmë për kryerësin. Çështja që ngjall kureshtje tek shumë teoricientë dhe studiues ka të bëjë me shkaqet që i shtyjnë individët e caktuar të kryejnë krim kibernetik.

[29] Panda Security "What is software piracy?": https://www.pandasecurity.com/mediacenter/panda-security/software-piracy/ (qasja e fundit më 19.02.2020)
[30] Halili,Ragip, "Kriminologjia", Prishtinë, 2011,fq.235

Arsyet pse dikush kryen një krim kibernetik mund të jenë po aq të ndryshme siç janë të ndryshëm vet njerëzit që kryejnë krimet.

Disa nga shkaqet e ndryshme që ndikojnë në kryerjen e krimeve kibernetike janë:

- Shkaqet financiare, si në rastet që përfshijnë mashtrim, përvetësim, me qëllim të përfitimeve pasurore etj.
- Shkaqet emocionale, si në rastet e kërcënimeve të dërguara me postë elektronike, programues të pakënaqur që përdorin bomba logjike për të shpërndarë viruse ose për të hedhur poshtë një rrjet për arsye të hakmarrjes ndaj një punëdhënësi;
- Shkaqet intelektuale, siç është rasti kur hakerë të caktuar përpiqen të fitojnë qasje në një web faqe të sigurt me qëllim të përpjekjes për të thyer fjalëkalimet;
- Kurioziteti, si shkak, mund të vjen në shprehje kur njerëzit vizitojnë web faqet ose shkarkojnë materiale që e dinë se përmbajnë përmbajtje të jashtëligjshme, dhe megjithatë e bëjnë atë;
- Ndërkaq, sjellja devijuese, për shembull vjen në shprehje kur një person publikon pornografi të fëmijëve ose imazhe të tjera të jashtëligjshme, video, ose materiale të tjera[31].

Sipas Azeez Nureni Ayofe dhe Barry Irwin ka shumë arsye pse kriminelët kibernetik kryejnë këto krime, në mesin e tyre si më të rëndësishme janë:

1. Krimet në internet mund të kryhen për hir të afirmimit. Në fakt, në këtë rast krimi kryhet nga të rinjtë që duan të vihen re dhe të ndjehen pjesë e grupit të djemve problematik dhe të ashpër në shoqëri. Ata nuk duan të lëndojnë dikë në veçanti. Zakonisht ato hyjnë në kategorinë e idealistëve të cilët thjeshtë duan të jenë në qendër të vëmendjes;

2. Një tjetër shkak i krimit në internet është fitimi i parave të shpejta. Ky grup është i motivuar nga lakmia dhe janë kriminel karriere, të cilët rregullojnë të dhënat në rrjet ose sistem, veçanërisht e-commerce, informacione për të dhënat e-banking me qëllimin e vetëm

[31] Shinder, Debra Littlejohn, and Michael Cross. "Scene of the Cybercrime", 2008, fq.29

për të kryer mashtrim të klientëve, që nuk dyshojnë ose nuk kanë mjaftueshëm njohuri, dhe në këtë mënyrë duke ua marrë paratë;

3. Së treti, krimi kibernetik mund të kryhet për të luftuar një kauzë për të cilën krimineli mendon dhe e beson. Pra këtë e bëjnë për të shkaktuar kërcënim dhe më së shpeshti dëme që ndikojnë negativisht tek viktima. Kjo është më e rrezikshmja nga të gjitha shkaqet e krimit në internet. Të implikuarit besojnë se ata janë duke luftuar një kauzë të drejtë dhe kështu nuk brengosen se kë ose çfarë shkatërrojnë në përpjekjen e tyre për të arritur qëllimet e tyre. Këta janë terroristët kibernetikë[32].

Një ndarje tjetër të shkaqeve apo faktorëve që ndikojnë në kryerjen e krimit kibernetik, bëhet duke i ndarë ato në faktorë objektiv të kriminalitetit kompjuterik dhe faktorë subjektiv të kriminalitetit kompjuterik[33]. Në faktorët objektiv të kriminalitetit, në mënyrë të veçantë përmendet zhvillimi teknologjik. Ndërsa tek faktorët subjektiv bëjnë pjesë motivet (duke përmendur kështu motivet financiare, emocionale, politike, ideologjike etj), mundësinë dhe gatishmërinë.

Nga kjo, mund të shihet se krimet kibernetike janë të qëllimshme dhe jo të rastësishme. Pavarësisht nga lloji i krimit, personi është i organizuar dhe veprën e bën me paramendim. Nëse e analizojmë në nivelin më bazik të kryerjes së krimit kibernetik, personi duhet ta ndez kompjuterin, të logohet dhe të kryej veprime specifike për të kryer këtë vepër penale dhe kjo mjafton për të konstatuar se krimi është kryer me paramendim.

[32] Ayofe, Azeez Nureni, and Barry Irwin. "CYBER SECURITY: CHALLENGES AND THE WAY FORWARD." Computer Science & Telecommunications 29, 2010

[33] Vula, Veton, “Kriminaliteti kompjuterik”, Prishtinë, 2010, fq.142

KAPITULLI I DYTË

Krimi kibernetik në Republikën e Maqedonisë së Veriut

2.1 Harmonizimi i legjislacionit të RMV-së me legjislacionin ndërkombëtar

Sa i përket rregullimit ndërkombëtar të krimit kibernetik, që nga vitet e 90-ta, shumë organizata dhe institucione ndërkombëtare i kanë kushtuar vëmendje të madhe këtij lloji të krimit, duke miratuar akte të ndryshme për rregullimin e tij juridik. Në vitin 2001 u miratua akti më domethënës për krimin kibernetik. Kjo është Konventa për Krimin Kompjuterik, e miratuar nga Këshilli i Evropës, në Budapest. Kjo konventë është marrëveshja e parë ndërkombëtare me të cilën rregullohet lufta kundër krimit kibernetik, duke harmonizuar legjislacionin kombëtar, duke përmirësuar teknikat e hetimit dhe duke rritur bashkëpunimin midis shteteve. Konventa është nënshkruar nga 60 shtete dhe është ratifikuar nga 56 shtete dhe ka hyrë në fuqi në korrik të vitit 2004[34]. RMV ka nënshkruar dhe ratifikuar Konventën për Krimin Kompjuterik. Konventa u nënshkrua nga vendi ynë më 23.11.2001, u ratifikua më 15.09.2004, dhe e njejta hyri në fuqi më 01.01.2005[35]. Konventa përmban norma materiale, norma procedurale dhe norma për bashkëpunimin ndërkombëtar. Dispozitat nga fusha e të drejtës materiale kanë të bëjnë me: hyrjen e paligjshme, ndërhyrjen në të dhëna, ndërhyrjen në sisteme, keqpërdorimin e pajisjeve, falsifikimet e lidhura me kompjuterët, mashtrimet e lidhura me kompjuterët, veprat penale të lidhura me pornografinë e fëmijëve, veprat penale të lidhura me dhunimin e të drejtës së autorit dhe të të drejtave të tjera të lidhura me të[36].

Konventa, e cila hyri në fuqi në korrik 2004, shoqërohet me një numër dokumentesh të miratuara nga Këshilli, e të cilat janë:

[34]Chart of signatures and ratifications of Treaty 185: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (qasja e fundit më 24.02.2020)
[35] Ligji për ratifikimin e Konventës për krimin e Kompjuterëve, nr. 07-2623 / 1, Shkup, 2004
[36] Doracak për krimin kompjuterik: https://www.osce.org/sq/skopje/121225?download=true (qasja e fundit më 24.02.2020)

- Trust and Security in Cyberspace: The Legal and Policy Framework for Addressing Cybercrime (2002);
- Cyber-Rights & Cyber-Liberties, Advocacy Handbook for NGOs (2003);
- Racism Protocol to the Convention on Cybercrime (2003);
- The Protocol to the Cybercrime Treaty (2002);
- Additional Protocol to the Cybercrime Convention Regarding "Criminalization of Acts of a Racist or Xenophobic Nature Committed through Computer Networks " (2006);
- Report Revised draft of the Protocol on Racist Speech (2002);
- Background Materials on the Racist Speech Protocol;
- Draft Protocol on Racist and Zenophobic Speech: Prelimiary draft (2001);
- Second Protocol on Terrorism (2002)[37].

Unioni Evropian, gjithashtu ka ndërmarrur edhe disa veprime legjislative për të luftuar krimin kibernetik, si psh:

- Vendimi kornizë në luftimin e mashtrimit dhe falsifikimit të mjeteve pagesore, me të cilën definohet sjellja mashtruese që vendet anëtare të BE-së duhet të konsiderojnë një vepër penale (2001);[38]
- Direktiva e privatësisë elektronike, në të cilën ofruesit e shërbimeve të komunikimit elektronik duhet të sigurojnë sigurinë e shërbimeve të tyre dhe të ruajnë konfidencialitetin e informacionit për klientin. Në vitin 2017, Komisioni propozoi të shfuqizojë Direktivën dhe ta zëvendësojë atë me një rregullore për respektimin e privatësisë dhe mbrojtjen e të dhënave personale në komunikimet elektronike (2002);[39]

[37] Ачковски Југослав, "Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам", Shkup, 2012, fq. 33
[38]EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001F0413 (qasja e fundit më 24.02.2020)
[39]Official Journal of the European Union- Directives, 2009: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF (qasja e fundit më 24.02.2020)

- Direktiva e luftës kundër shfrytëzimit seksual të fëmijëve dhe pornografisë së fëmijëve (2011);[40]
- Direktiva për sulmet ndaj sistemeve të informacionite cila ka për qëllim të merret me sulmet kibernetike të shkallës më të lartë duke i nxitur vendet anëtare të forcojnë ligjet kombëtare të krimit kibernetik dhe të vendosin sanksione më të ashpra penale. Në vitin 2017, Komisioni publikoi një Raport që vlerëson shkallën në të cilën Shtetet Anëtare kanë ndërmarrë masat e nevojshme për t'u pajtuar me Direktivën.(2013);[41].

Në kuadër të EUROPOL-it, në vitin 2013, është formuar Qendra Evropiane për krim kibernetik që të përforcohet zbatimi i ligjit për krim kibernetik në BE dhe në atë mënyrë të ndihmon në mbrojten e qytetarëve evropian, bizneseve dhe qeverive nga krimi kibernetik. Që nga fillimet e saja kjo qendër evropiane ka kontribuar në mënyrë të konsiderueshme në luftimin e krimit kibernetik. U përfshi në dhjetëra operacione të profilit të lartë dhe qindra operacione të lidhjes operative, që rezultuan në arrestime dhe analiza të dosjeve, shumica e të cilave janë vërtetuar të jenë me qëllim të keq[42].

RMV gjithashtu ka ratifikuar Protokollin shtesë të konventës së krimit të kompjuterëve më 13 korrik 2005.

2.2 Legjislacioni ekzistues në Republikën e Maqedonisë së Veriut (RMV)

Krimi kibernetik rezulton të jetë kërcënim serioz për shoqërinë në përgjithësi. Ka raste kur paraqitet në formë lufte në mes shtetesh të ndryshme, apo raste kur paraqitet në formë lufte në mes të organizatave botërore, apo thjeshtë luftë në mes të individëve të caktuar. Paraqitja e tij si një problem në përmasa kaq të mëdha, ka shtyrë juristët e shteteve të ndryshme dhe të organizatave ndërkombëtare që merren me parandalimin dhe luftimin e tij, të

[40] EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093 (qasja e fundit më 24.02.2020)
[41] Official Journal of the European Union –Directive 2013/40/EU: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF (qasja e fundit më 24.02.2020)
[42] EUROPOL-EC3, (https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3) (qasja e fundit më 24.02.2020)

ndërmarrin masa adekuate duke miratuar ligje dhe konventa. Në RMV, edhepse ka mungesë të madhe të ekspertëve në këtë fushë e njëkohësisht edhe mungesë të një ligji të veçantë në këtë drejtim, ekzistojnë dispozita të veçanta në Kodin Penal dhe ligje të tjera që e inkriminojnë si vepër penale. Korniza juridike e vendit tonë që e rregullon fushën e krimit kompjuterik e përfshin[43]:

- Kodin Penal (KP);
- Ligjin për procedurë penale (LPP);
- Ligjin për komunikime elektronike;
- Ligjin për ndjekje të komunikimeve;
- Ligjin për tregtinë elektronike;
- Ligjin për udhëheqjen elektronike;
- Ligjin për shërbimin gjyqësor;
- Ligjin për të dhënat në formë elektronike dhe nënshkrimin elektronik;
- Deklaratën për internet më të sigurt;

Kodi Penal i RMV-së përcakton veprat penale që kryhen përmes kompjuterit, si dhe sanksionet penale për të njejtat krime. Mirëpo, përpara se të shtjellojmë këto vepra penale, fillimisht do t'i referohemi kuptimit të disa shprehjeve. Kështu, neni 122 i KP përcakton domethënien e shprehjeve themelore të këtij kodi, disa prej të cilave janë të lidhura me krimin kibernetik. Pika 15 e këtij neni definon kartelat pagesore: "Me kartelë pagesore nënkuptohet çdo lloj mjeti për pagesë, të lëshuar nga institucionet bankare apo institucionet tjera financiare që përmbajnë të dhëna elektronike për personat dhe numra të gjeneruar elektronik me të cilët mundësohet kryerja e çfarëdo lloj transaksionit financiar"[44].

Pika e 24 e nenit 122 sqaron kuptimin e shprehjes pornografi fëmijërore: "Me pornografi fëmijërore nënkuptohet materiali pornografik i cili në mënyrë vijuese tregon veprimen të dukshme seksuale me të mitur, apo veprime të dukshme seksuale me person i cili duket si i mitur, apo fotografi reale që tregojnë veprime të dukshme seksuale me të mitur apo e

[43] Doracak për krimin kompjuterik, 2014, (https://www.osce.org/sq/skopje/121225?download=true) (qasja e fundit më 26.02.2020)
[44] Neni 122 i Kodit Penal të RMV-së;

tregojnë të miturin ose personin e rritur i cili duket si i mitur në gjendjen e dukshme seksuale”[45].

Pika 26 e të njejtit nen definon sistemin komjuterik: “Me sistem kompjuterik nënkuptohet çfarëdo qoftë pajisje apo grup pajisjesh të ndërlidhura mes vete, nga të cilët, një apo më shumë prej tyre kryejnë përpunim automatik të të dhënave sipas programit të caktuar”[46].

Pika 27 e nenit 122 përkufizon shprehjen të dhëna kompjuterikesi në vazhdim: “Me të dhëna kompjuterike nënkuptohet prezantimi i fakteve, informatave apo koncepteve në formë të përshtatshme për përpunim përmes sistemit kompjuterik, duke përfshirë edhe program të përshtatshëm që sistemin kompjuterik ta vë në funksion”[47].

Veprat penale lidhur me krimin kibernetik, të parapara në Kodin Penal të RMV-së, janë:

- Neni 144 – Rrezikimi i sigurisë – paragrafi i katërt i nenit 144 thotë se “Ai i cili përmes sistemit informatik do të kanoset se do të kryej vepër penale për të cilën është paraparë dënim me burgim prej pesë vjet ose dënim më i rëndë kundër ndonjë personi pështkak të përkatësisë së tyre gjinore, races, ngjyrës së lëkurës, familjes, përkatësisë së grupit të margjinalizuar, përkatësisë etnike, gjuhës, shtetësisë, prejardhjes sociale, religjionit ose bindjes fetare, formave tjera të bindjes, arsimit… apo në çfarëdo qoftë baze tjetër e paraparë me ligj apo me marrëveshje të ratifikuar ndërkombëtare, do të dënohet me burgim prej një deri në pesë vjet.”
- Neni 147 – Cënimi i fshehtësisë së korrespodencës ose të dërgesave të tjera;
- Neni 149 – Keqpërdorimi i të dhënave personale – paragrafi i dytë thotë: “Me dënim nga paragrafi 1 (dënim me gjobë ose me burgim deri në 1 vjet) dënohet ai i cili do të hyjë në sistemin informatik kompjuterik të të dhënave personale me qëllim që duke i

[45] Neni 122 i Kodit Penal të RMV-së;
[46] Po aty;
[47] Po aty;

shfrytëzuar ato për vete apo për tjetër që të realizojë ndonjë dobi apo tjetër kujt t'i shkaktojë ndonjë dëm."

- Neni 149-a – Pengimi i qasjes në sistemin publik informatik;
- Neni 157 – Cënimi i të drejtës së autorit dhe të drejtave të përafërta;
- Neni 157-a – Cënimi i të drejtës së distributorit të sinjalit satelitor me mbrojtje të posaçme teknike;
- Neni 157-b – Pirateria e veprës audio-vizuale;
- Neni 157-v – Pirateria e fonogramit;
- Neni 193 – Ekspozimi i materialit pornografik fëmijës;
- Neni 193-a – Prodhimi dhe distribuimi i pornografisë me fëmijë – paragrafi i tretë i këtij neni ka paraparë dënim me më së paku tetë vjet burgim për kryerësin i cili prodhon pornografi fëmijërore me qëllim të distribuimit të saj apo e mbartjes të saj përmes sistemit kompjuterik apo ndonjë mjeti tjetër pë komunikim masiv;
- Neni 193-b – Joshja në akt seksual apo në veprim tjetër seksual e fëmijës i cili nuk ka mbushur 14 vjet;
- Neni 251 – Dëmtimi dhe hyrja e paautorizuar në sistemin kompjuterik – paragrafi i parë i këtij neni parasheh: "Ai i cili në mënyrë të paautorizuar do të shlyej, ndryshoj, dëmtoj, fsheh ose në mënyrë tjetër do të bëjë të dhëna ose programe të padobishme kompjuterike, ose do të pamundësojë ose vështirësoj shfrytëzimin e sistemit kompjuterik, të dhënave ose programeve të komunikimit kompjuterik, do të dënohet me dënim me gjobë ose me burgim deri në tre vjet."
- Neni 251-a – Bërja (programimi) dhe futja e viruseve kompjuterike – paragrafi i parë: "Ai i cili do të bëjë ose do të marrë nga tjetri virus kompjuterik me qëllim që ta fus në kompjuter të huaj ose në rrjet kompjuterik do të dënohet me dënim me gjobë ose me burgim deri në një vjet", paragrafi i dytë: "Ai i cilime përdorim të virusit kompjuterik do të shkaktoj dëm në kompjuter, sistem, të dhëna ose program të huaj, do të dënohet me burgim prej gjashtë muaj deri në tre vjet."
- Neni 251-b – Mashtrimi kompjuterik – paragrafi i parë: "Ai i cili me qëllim që për vete apo për ndonjë tjetër do të përfitojë dobi të kundërligjshme pasurore me futje në

kompjuter ose në sistem informatik të dhëna të pavërteta, me mosfutje të të dhënave të vërteta, me ndryshim, fshirje apo fshehje të të dhënave kompjuterike, me falsifikim të nënshkrimit elektronik ose në mënyrë tjetër do të shkaktojë rezultat të pavërtetë gjatë përpunimit elektronik dhe bartjes së të dhënave, do të dënohet medënim me gjobë ose me burgim deri në tre vjet."

- Neni 271 – Krijimi, furnizimi ose tjetërsimi i mjeteve për falsifikim – paragrafi i dytë: "Ai i cili në mënyrë të paautorizuar përpunon,furnizon, mban, shet apo jep në përdorim instrumente, sende, programe kompjuterike dhe mbrojtëse apo komponente tjera sigurimi që shërbejnë për mbrojtje kundër falsifikimit, si dhe mjete për furnizim të paautorizuar të të dhënave bankare për të bërë para të rrejshme apo shtrembërim të parave të vërteta apo instrumente tjera për pagesë, letra me vlerë apo kartela të rrejshme për pagesë, do të dënohet me burgim prej tre deri në dhjetë vjet."
- Neni 274-b – Përpunimi dhe përdorimi i kartelës së rrejshme pagesore – paragrafi i parë: "Ai i cili do të bëjë kartelë të rrejshme pagesore me qëllim që ta përdor si të vërtetë, apo pajis kartelë të rrejshme me qëllim të tillë, apo do t'ia jep në përdorim tjetërkujt apo ai i cili kartelën e rrejshme do ta përdorë si të vërtetë, do të dënohet me burgim prej gjashtë muaj deri në pesë vjet dhe me dënimme gjobë."
- Neni 394-d – Përhapja e materialit racist dhe ksenofob nëpërmjet sistemit kompjuterik – paragrafi i parë: "Ai i cili përmes sistemit kompjuterik në publik përhap material të shkruar racist dhe ksenofobik, fotografi apo reprezentim tjetër të idesë apo teorisë e cila ndihmon, promovon apo nxit urrejtje, diskriminim apo dhunë, kundër kujtdo qoftë personi apo grupi, në bazë të gjinisë, racës, ngjyrës së lëkurës, fisit, përkatësisë etnike … do të dënohet me burgim prej një deri në pesë vjet."

Nga ana tjetër, ligji për procedurë penale rregullon çështjet procedurale lidhur me zbatimin e dispozitave që ndërlidhen me krimin kibernetik e që kanë të bëjnë me masat dhe veprimet që zbatohen për këtë vepër penale. Kështu, në dispozitat e LPP-së lidhur me krimin kibernetik, bëjnë pjesë:

- Neni 184 - Kërkimi i sistemit kompjuterik dhe të dhënave kompjuterike – "(1) Me kërkesë të zbatuesit të urdhrit, personi i cili e përdor kompjuterin apo ka qasje te ai apo te pajisja apo mbajtësi tjetër i të dhënave, është i obliguar që të mundësojë qasje te ato dhe t'i japë informatat e nevojshme për realizimin pa pengesë të qëllimit të bastisjes. (2) Me kërkesë të zbatuesit të urdhrit, personi që e përdorë kompjuterin ose ka qasje te ai ose te pajisja tjetër apo mbajtës i të dhënave, është i obliguar që menjeherë të ndërmarre masa me të cilat pengohet shkatërrimi apo ndryshimi i të dhënave"[48].
- Neni 198 - Konfiskimi i përkohshem i të dhënave kompjuterike- "(1) Dispozitat nga neni 194 paragrafi (1), neni 195 paragrafi (1) dhe neni 197 të këtij ligji, i përkasin edhe të dhënave të ruajtura në kompjuter dhe pajsje të ngjashme për përpunim automatik, përkatesisht përpunim elektronik të të dhënave, pajisje të cilat shërbejnë për grumbullimin dhe transmetimin e të dhënave, bartës të të dhënave dhe informacioneve parapaguese me të cilat disponon dhënësi i shërbimeve. Me kërkesë me shkrim të prokurorit publik, këto të dhëna duhet t'i dorëzohen prokurorit publik në afatin që ai e përcakton. Në rast të refuzimit të dorëzimit, do të veprohet sipas nenit 196 paragrafi (1) të këtij ligji"[49].

Gjithashtu, për rregullimin procedural të krimit kibernetik vlejnë edhe dispozitat e kapitullit XVII – masat për gjetjen dhe sigurimin e personave dhe të sendeve. Me rëndësi janë edhe dispozitat e nenit 252 lidhur me qëllimin dhe llojet e masave të veçanta hetuese, sipas të cilit, kur ka gjasa që të sigurohen të dhëna dhe prova të domosdoshme për udhëheqjen e suksesshme të procedurës penale, të cilat në mënyrë tjetër nuk mund të mblidhen, mund të ndërmerren masat e veçanta hetuese në vijim:

- përcjellja dhe inçizimi i komunikimeve telefonike dhe komunikimeve tjera elektronike në procedurën e përcaktuar me ligj të veçantë;

[48] Ligji për procedurë penale të Republikës së Maqedonisë së Veriut (Gazeta Zyrtare e RMV nr:150/2010)
[49] Po aty

- përcjellja dhe inçizimi në shtepi, lokal të mbyllur ose të rrethuar që i takon asaj shtëpie ose lokal afarist të shënuar si privat ose në automjet dhe hyrje në ato lokale për krijimin e kushteve për përcjelljen e komunikimeve;
- përcjellja dhe inçizimi i fshehtë i personave dhe sendeve me mjete teknike jashtë shtëpisë ose lokalit afarist të shënuar si privat;
- shikimi i fshehtë dhe kontrollimi i sistemit kompjuterik;
- kërkimi automatik ose në mënyre tjetër, kërkimi dhe krahasimi i të dhënave personale;
- shikimi në komunikimet telefonike ose komunikimet tjera të realizuara elektronike;
- grumbullimi i simuluar i sendeve; etj[50].

2.3 Institucionet shtetërore kompetente për trajtimin e krimit kibernetik në RMV

Në shkurt të vitit 2005, me formimin e njësisë për krim kompjuterik dhe falsifikime, për herë të parë i hasim fillimet për themelimin e një departamenti për krim kompjuterik dhe forenzikë dixhitale. Tre vite më vonë u formua njësia e veçantë për luftimin e krimit kompjuterik, kurse në vitin 2014 kjo njësi u nda nga departamenti për krim të organizuar duke u shëndruar në departament për krim kompjuterik dhe forenzikë dixhitale në kuadër të shërbimit qendror të policisë.

Departamenti për krim kompjuterik dhe forenzikë dixhitale përbëhet nga dy njësi:

1. Njësia për hetimin e krimit kompjuterik, që ka dy seksione:
   -Seksioni për hetimin e keqpërdorimit të kartelave pagesore;
   -Seksioni për hetimin e incidenteve kompjuterike.

Kjo njësi merret me vepra penale që kanë të bëjnë me krimin kompjuterik, e të cilat janë të parapara në kodin penal të RMV-së. Këtu bëjnë pjesë: neni 251- dëmtimi dhe hyrja e

[50] Ligji për procedurë penale të Republikës së Maqedonisë së Veriut (Gazeta Zyrtare e RMV nr:150/2010)

paautorizuar në sistemin kompjuterik, neni 251-a –bërja (programimi) dhe futja e viruseve kompjuterike, neni 193- ekspozimi i materialit pornografik fëmijës, neni 193-a- prodhimi dhe distribuimi i pornografisë fëmijërore, neni 251-b - mashtrimi (kompjuterik), neni 149- keqpërdorimi i të dhënave personale. Njësia për hetimin e krimit kompjuterik bashkëpunon edhe me njësi të tjera organizative në kuadër të Ministrisë së punëve të brendshme[51].

2. Njësia për forenzikë dixhitale, e cila ka dy seksione:
   - Seksioni për ekzaminimin e pajisjeve kompjuterike;
   - Seksioni për ekzaminimin e pajisjeve telefonike.

Departamenti për krim kompjuterik dhe forenzikë dixhitale ka bashkëpunim të ngushtë me dy organizatat ndërkombëtare, EUROPOL dhe INTERPOL.

Në RMV ekzistojnë institucione kompetente shtetërore që merren në mënyrë indirekte me luftimin e krimit kibernetik. Disa nga këto institucione janë:

- Ministria për Shoqëri Informatike;
- Ministria e Ekonomisë;
- Ministria e Financave;
- Ministria e Drejtësisë (me gjykatat dhe prokuroritë publike);
- Biroja për siguri publike në kuadër të Ministrisë së punëve të brendshme;
- Ministria e Mbrojtjes;
- Qendra për menaxhimin e krizave;
- Agjencioni për komunikime elektronike[52].

[51] Të dhëna nga Ministria e punëve të brendshme

[52] Ачковски Југослав, “Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам”, Shkup, 2012.

KAPITULLI I TRETË

Krimi kibernetik në disa vende të Unionit Evropian – aspekte krahasimore

Zhvillimi i shpejtë kompjuterik dhe roli i madh i internetit kanë detyruar qeveritë kombëtare dhe agjensionet ndërkombëtare të ndërmarrin masa lidhur me rregullimin e kësaj çështje. Këto mjete shumë të sofistikuaara kanë shkatërruar pengesat e komunikimit dhe ndryshuan mënyrën se si një pjesë e madhe e botës bën biznes. Mundësitë e reja që u krijuan në "hapsirën kompjuterike" rritën edhe aftësitë e kriminelëve, që duke shfrytëzuar dobësitë që ka kjo "hapsirë" të kryejnë vepra penale. Rreziqet e reja që lidhen me këto ndryshime kërkojnë vëmendje të vazhdueshme në të gjitha frontet, duke përfshirë këtu ato: kombëtare, rajonale dhe ndërkombëtare. Derisa procesi i 'globalizimit' vazhdon të përshpejtohet, një përgjigje plotësisht globale ndaj këtyre problemeve të epokës dixhitale, ende nuk është shfaqur.

Kontrolli i krimit kibernetik, kërkon përdorimin e rrjeteve të reja: rrjete në mes policisë dhe agjencioneve të tjera brenda qeverisë, rrjete në mes policisë dhe institucioneve private dhe rrjeteve të policisë përtej kufijve kombëtarë. Gjatë dekadës së fundit, është bërë një përparim i konsiderueshëm brenda dhe mes shteteve për të zhvilluar punën e policisë në luftë kundër krimit kibernetik. Megjithatë, ritmi i ndryshimit teknologjik do të vazhdojë duke mos u pakësuar dhe veprimet e kriminelëve në kompjuter do të vazhdojnë të paraqesin sfida për zbatimin e ligjit. Deri vonë, nuk ishte e mundur të flitej për një konsensus ndërkombëtar për luftimin e krimit kibernetik. Në nivelin ndërkombëtar, dy instrumente të reja ofrojnë një bazë të shëndoshë për bashkëpunim ndërkufitar lidhur me zbatimin e ligjit për luftimin e krimit kibernetik. I pari nga këto instrumente është Konventa e Këshillit të Evropës për krimin kibernetik, megjithëse e dizajnuar si një mekanizëm rajonal ka rëndësi globale, e dyta është Konventa e Kombeve të Bashkuara kundër krimit të organizuar transnacional, e cila është globale.

Masat e ndryshme që veprojnë tani brenda Bashkimit Evropian, Konventa e Këshillit të Evropës, krijimi i EUROPOL dhe krijimi i një rrjeti evropian gjyqësor, japin shembuj të një

harmonizimi më të madh të ligjit dhe më pak mundësi për kriminelët që të shfrytëzojnë zbrazëtirat juridike. Themelimi i Agjensisë të Bashkimit Evropian për Siguri Kibernetike - "European Union Agency for Cybersecurity (ENISA)" në vitin 2004, është një tjetër masë e ndërmarrë për luftimin e krimit kibernetik. Ky agjension është një qendër e ekspertizës për sigurinë kibernetike në Evropë. ENISA ndihmon BE dhe vendet e BE-së të pajisen më mirë dhe të përgatiten për të parandaluar, zbuluar dhe reaguar ndaj problemeve që shfaqen lidhur me sigurinë e informacionit, njëkohësisht ofron këshilla dhe zgjidhje praktike për sektorin publik dhe privat në vendet e BE-së dhe institucionet e BE-së[53].

Në vazhdim do të paraqiten të dhëna të ndryshme lidhur me krimin kibernetik në disa vende të Evropës. Qëllimi i vetëm është fitimi i një pasqyre të legjislacioneve dhe strategjive të shteteve të ndryshme të Unionit Evropian.

3.1 Krimi kibernetik në Gjermani

3.1.1 Legjislacioni gjerman mbi krimin kibernetik

Gjermania bën pjesë në një nga vendet me teknologjinë e informacionit më të zhvilluar. Shërbimet e informacionit dhe komunikimit elektronik janë përhapur në të gjitha fushat ekonomike, e në të njejtën kohë janë bërë mënyrë e jetesës. Krimi kibernetik paraqet problem shumë serioz në Gjermani duke pasur parasysh se sipas një studimi të botuar nga Shoqata e Sektorit të IT në Gjermani, në shtator të 2018, dy të tretat e prodhuesve të Gjermanisë janë goditur nga sulmet e krimit kibernetik, duke i kushtuar ekonomisë të Evropës rreth 43 miliardë euro (50 miliardë dollarë)[54].

[53] European Union Agency for Cybersecurity (ENISA): https://europa.eu/european-union/about-eu/agencies/enisa_en (qasja e fundit më 05.03.2020)
[54]Cyber attacks cost German industry almost $50 billion: study: https://www.reuters.com/article/us-germany-security-cyber/cyber-attacks-cost-german-industry-almost-50-billion-study-idUSKCN1LT12T (qasja e fundit më 05.03.2020)

Edhe Gjermania është nënshkruese e Konventës së Budapestit, të cilën e ka ratifikuar në vitin 2009. Duke ju përmbajtur kësaj konvente, ajo ka miratuar në Kodin penal disa dispozita të caktuara. Kodi penal gjerman përfshin këto nene që kanë të bëjnë me krimin kibernetik:

- Neni 202a - hyrje e paligjshme;
- Neni 202b - përgjim i paligjshëm;
- Neni 202c - shpërndarja e viruseve;
- Neni 303a - manipulim i të dhënave;
- Neni 303b - sabotim kompjuterik;
- Neni 269 - falsifikimi kompjuterik;
- Neni 263 - mashtrim kompjuterik[55].

Sa i përket çështjeve procedurale lidhur me krimin kibernetik të gjitha masat procedurale dhe shtrënguese të përcaktuara nga Konventa e Krimit Kibernetik përfshihen në Kodin penal të Gjermanisë[56].

Përveç Kodit penal, siguria kibernetike në Gjermani, rregullohet edhe nga disa akte ligjore. Më i rëndësishmi, që ka të bëjë me sigurinë në internet është Akti ligjor gjerman për sigurinë e teknologjisë informative, i 25 korrikut 2015, i cili ndryshoi një numër ligjesh, në veçanti Aktin ligjor gjerman për telemedia, Aktin ligjor gjerman për telekomunikim, Akti ligjor federal për mbrojtjen e të dhënave, etj[57].

3.1.2 Institucionet e veçanta gjermane për luftimin e krimit kibernetik

Në secilin prej landeve gjermane ka një Landeskriminalamt (LKA) që është institucion operacional, përgjegjës për hetimet penale. Përshkak të numrit të rritur të krimit kibernetik,

[55] Cybercrime Laws:Germany: https://www.cybercrimelaw.net/Germany.html (qasja e fundit më 06.03.2020)
[56] Këshilli Evropës, " National legislation implementing the Convention on Cybercrime- Comparative analysis and good practices"
[57] Germany: Subersecurity 2020: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany (qasja e fundit më 06.03.2020)

disa Lande konsiderojnëse është i nevojshëm krijimi i një qendre të specializuar për krimin kibernetik. "Bundeskriminalamt" – Zyra Federale e Policisë Kriminale koordinon kontaktet e policisë kombëtare dhe ndërkombëtare. Përveç detyrës që ka për të hetuar krime të rënda (të organizuara), kjo zyrë është kompetente që të hetojë edhe raste të krimi të rëndë kibernetik[58].

Rëndësi të madhe në luftën kundër krimit kibernetik ka edhe Zyra Federale për Sigurinë e Informacionit. Zyra Federale për Sigurinë e Informacionit paraqitet si autoriteti kryesor që ka kompetenca të veprojë në lidhje me sigurinë kibernetike në Gjermani. Kjo zyrë është kontakti kryesor lidhur me pyetjet për masat parandaluese të sigurisë dhe është përgjegjëse për marrjen e njoftimeve për shkeljet e sigurisë [59].

Në Gjermani ekzistojnë edhe Autoritetet për Mbrojtjen e të Dhënave, të cilat zbatojnë të gjitha ligjet përkatëse për mbrojtjen e të dhënave. Çdo shtet federal gjerman ka një Autoritet të veçantë për mbrojtjen e të dhënave. Institucion tjetër që merret me formë të veçantë të krimit kibernetik është Agjensia Federale e Rrjetit, e cila zbaton ligjet e lidhura me telekomunikimin dhe është përgjegjës për marrjen e njoftimeve për shkeljet e sigurisë në lidhje me rrjetet dhe shërbimet e telekomunikimit[60].

3.1.3 Strategjia nacionale për siguri kibernetike në Gjermani

Ministria e punëve të brendshme në Gjermani, në vitin 2014 miratoi në mënyrë të përmbledhur Strategjine Nacionale për Siguri Kibernetike, për të përmirësuar sigurinë e IT në industri, për të siguruar mbrojtje të përdoruesve të internetit dhe për të forcuar mënyrën e veprimit të Zyrës Federale për Sigurinë e Informacionit dhe të Zyrës Federale të Policisë Kriminale. Strategji për krimin kibernetik ka pasur edhe më herët, respektivisht në vitin 2009.

Strategjia e viti 2014 për siguri kibernetike përfshin disa fusha, duke përfshirë

[58] Germany: Subersecurity 2020: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany (qasja e fundit më 06.03.2020)
[59] Po aty,
[60] Po aty,

- Mbrojtjen e infrastrukturave të informacionit;
- Sigurimin e sistemeve të teknologjisë informative në Gjermani;
- Forcimin e sigurisë së teknologjisë informative në administratën publike;
- Qendra Kombëtare e Kibernetikës;
- Kontroll efektiv i krimit - përfshirë hapësirën kibernetike;
- Zhvillimi i personelit në institucionet federale;
- Mjetet për t'iu përgjigjur sulmeve kibernetike[61].

3.2 Krimi kibernetik në Austri

3.2.1 Korniza ligjore për rregullimin e krimit kibernetik në Austri

Statistikat më të fundit kriminale të publikuara nga Ministria e Punëve të Brendshme e Austrisë, tregojnë një rritje të madhe të krimit kibernetik. Në gjysmën e parë të 2019, policia austriake regjistroi mbi 13,000 vepra të krimit kibernetik, krahasuar me rreth 8.700 në të njejtën periudhë të vitit të kaluar[62]. Prandaj, lufta kundër krimit kibernetik po bëhet gjithnjë e më e rëndësishme, veçanërisht për kompanitë që të mbrojnë sekretet e tyre të biznesit.

Sipas Raportit për Siguri Kibernetike të Austrisë të vitit 2019, zhvillimet teknologjike dhe rrjeti dixhital global nënkupton që hapësira kibernetike, si një fushë e paprekshme, është bërë shumë më e rëndësishme në sektorin ushtarak. Në raport theksohet se në konfliktet e tanishme dhe të ardhshme ushtarake do të bëhen përpjekje për të arritur efekte në hapësirën kibernetike.

[61] Këshilli Evropian, "The practical implementation and operation of European policies on prevention and combating cybercrime - Report on Germany", Bruksel, 2017

[62] Austria: Cybercrime And Protection Under Criminal Law, 2019: https://www.mondaq.com/austria/crime/874318/cybercrime-and-protection-under-criminal-law (qasja e fundit më 10.03.2020)

Për ratifikim e Konventës për Krim Kibernetik, republika e Austrisë ka miratuar ndryshime në Kodin Penal në vitin 2002 dhe Kodin Procedural Penal. Kodi Penal i Austrisë përfshin veprat penale të mëposhtme:

- Neni 118a - qasje e paligjshme;
- Neni 119a - përgjimi i paligjshëm;
- Neni 126a - manipulimi i të dhënave;
- Neni 126b - ndërhyrja në system;
- Neni 126c - keqpërdorim i pajisjeve;
- Neni 225a - falsifikimi kompjuterik;
- Neni 148a - mashtrimi kompjuterik[63].

3.2.2 Institucionet kompetente për luftimin e krimit kibernetik në Austri

Brenda prokurorisë të Austrisë, nuk ka një zyrë të specializuar për krimin kibernetik. Si qëllim i Strategjisë për Krimin Kibernetik, Qendra Kompetente për Krim Kibernetik (C4) është themeluar si pjesë e Zyrës Federale të Hetimeve Penale (Bundeskriminalamt). C4 është urë lidhëse mes Austrisë me Qendrën Evropiane të Krimit Kibernetik të Europol (EC3) dhe Qendrës së Krimeve Digjitale (IDCC) të Interpolit. C4 është e përbërë nga ekspertë teknikë dhe persona shumë të specializuar në fushat e zbulimit, mjekësisë ligjore dhe teknologjisë. Nga Ministria e Punëve të Brendshme është hapur një numër direkt telefonik ku mund të paraqiten rastet e krimit kibernetik. Numër i veçantë ekziston edhe për denoncimin e pornografisë me fëmijë.

Gjithashtu, në Austri funksionon edhe Qendra Ushtarake e Sigurisë Kibernetike (MilCySihZ) që mbron sitemet dhe rrjetet e ushtrisë nga kërcënimet dhe sulmet kibernetike[64].

[63] Austria: Cybercrime: (https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/austria/pop_up?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=print&_101_INSTANCE_hFPA5fbKjyCJ_languageId=fi_FI) (qasja e fundit më 12.03.2020)

[64] Austrina: Report Cyber Security 2019,(file:///C:/Users/User/Downloads/EN-Cybersicherheit_Bericht_2019.pdf) (qasja e fundit më 12.03.2020)

3.2.3 Strategjia nacionale e sigurisë kibernetike austriake

Strategjia Nacionale e Sigurisë Kibernetike austriake është implementuar më 20 mars 2013. Në kuadër të Strategjisë së saj për Siguri Kibernetike, Austria ndjek qëllimet e mëposhtme strategjike:

1. Disponueshmëria, besueshmëria dhe konfidencialiteti i shkëmbimit të të dhënave, garantohen vetëm në një hapësirë të sigurt dhe të besueshme kibernetike;
2. Bazuar në qasjen nacionale të ministrive federale kompetente, Austria do të sigurojë mbrojtje të teknologjisë informative, që të jetë e sigurt dhe rezistente ndaj kërcënimeve;
3. Siguria kibernetike do të mbrohet nga autoritetet austriake - në bashkëpunim me partnerë jo-qeveritarë;
4. Duke ndërmarrur një numër masash ndërgjegjësimi, Austria do të ndërton një "kulturë të sigurisë kibernetike";
5. Austria do të luajë një rol aktiv në bashkëpunimin ndërkombëtar në nivelin evropian dhe global, veçanërisht duke shkëmbyer informacione, duke formuluar strategji ndërkombëtare, duke hartuar skema vullnetare dhe rregullore ligjërisht të detyrueshme, duke ndjekur çështje penale, duke mbajtur ushtrime transnacionale dhe duke realizuar projekte bashkëpunimi;
6. Të gjitha ndërmarrjet austriake do të mbrojnë integritetin e aplikacioneve të tyre, si dhe identitetin dhe privatësinë e klientëve të tyre. Bashkëpunimi i ngushtë dhe sistematik midis ndërmarrjeve luan një rol vendimtar në këtë process;
7. Popullsia austriake duhet të jetë e vetëdijshme për përgjegjësinë personale lidhur me hapësirën kibernetike. Të gjithë qytetarët duhet të sigurojnë mbrojtje adekuate të aktiviteteve të tyre në internet[65].

[65]Austria: Report Cyber Security 2019, (file:///C:/Users/User/Downloads/EN-Cybersicherheit_Bericht_2019.pdf) (qasja e fundit më 13.03.2020)

3.3 Krimi kibernetik në Francë

3.3.1 Legjislacioni francez mbi krimin kibernetik

Franca gjithmonë ka qenë në vijë të parë për zhvillime teknologjike mbi sigurinë kibernetike. Ajo është bazuar në ofrimin e mbrojtjes dhe paraqitjen e një perspektive unike mbi sigurinë kibernetike. Studiuesit francezë, duke u bazuar në legjislacionin francez kundër krimit kibernetik, këto krime i ndajnë në dy kategori të mëdha: krimet që synojnë drejtpërdrejt sistemet kompjuterike dhe rrjetet e informacionit, të quajtura si "krime të pastra kompjuterike", dhe krimet e kryera përmes përdorimit të kompjuterave dhe rrjeteve të tyre, me fjalë të tjera përdorimi i kompjuterëve në kryerjen e krimeve "konvencionale", të cilat quhen edhe "krime konvencionale të lidhura me kompjuterin"

Ransomware, malware bankar dhe mashtrimet kibernetike janë disa nga kërcënimet kryesore me të cilat përballen mbrojtësit e krimit kibernetik në Francë, sipas një raporti të fundit nga Ministria e Punëve të Brendshme të Francës[66]. "Ransomware" paraqet lloj të virusit që kërcënon se do të publikohen të dhënat e viktimës ose bllokon qasjen e përdoruesit në pajisjen e tij, nëse nuk paguhet një shpërblim.

Franca ka adoptuar një kornizë të gjerë ligjore mbi krimin kibernetik dhe veprat penale të lidhura me kompjuterin, duke filluar me Ligjin Nr. 88-19, 5 Janar 1988, për mashtrimin kompjuterik ("Godfrain Law ") dhe ndryshimet e tij, i cili u kodifikua në nenet 323-1 deri 323-7 të Kodit Penal[67].

Ligjet më të rëndësishme të Francës në fushën e sigurisë kibernetike janë:

1. The Godfrain Law (Ligji Godfrain) - 88-19, i 15 janarit 1988;
2. The Law for a Digital Republic (Ligji për një republikë dixhitale) – 2016-1321, i 7 tetorit 2016;

[66] Cybersecurity news and views: Ransomware is a real problem in France, (https://portswigger.net/daily-swig/ransomware-is-a-real-problem-in-france) (qasja e fundit më 18.03.2020)
[67]France-Cybercrime, (https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/france/pop_up?inheritRedirect=false) (qasja e fundit më 18.03.2020)

3. The Network and Information Systems Security Act (Akti ligjor i sigurisë së rrjetit dhe sistemeve të informacionit) – 2018-133, i 26 shkurtit 2018[68].

Kodi penal francez, krimin kibernetik e rregullon në këtë mënyrë: nenet prej 323-1 deri 323-7 përcaktojnë si krime të gjitha veprat penale kundër konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave dhe sistemeve kompjuterike, duke përfshirë qasjen e paligjshme (neni 323-1 p.1), ndërhyrjen në të dhëna (neni 323-1 p.2 dhe 323-3), ndërhyrjen në sistem (neni 323-2), si dhe keqpërdorimi i pajisjeve (neni 323-3). Veprat penale lidhur me pornografinë e fëmijëve mbulohen nga neni 222-23 deri 222-31.

Vëmendjen më të madhe tërheqin dënimet që janë të parapara për këto vepra penale. Përveç dënimeve me burg, Franca parasheh edhe dënime me të holla për të cilat shumat janë tepër të larta. Kështu psh. për rastet kur kryhet hakingu, dënimi me gjobë zen vlerën e 60,000€, ndërkaq nëse e njejta vepër është kryer ndaj ndonjë sistemi publik apo qeveritar dënimi me gjobë është 150,000 €. Për sulmet ndaj sistemeve informative janë paraparë dënime me burgim me pesë vjet burg dhe me gjobë deri në 150,000€. Kur vepra penale përfshin një sistem publik ose qeveritar, sanksionet ngrihen në shtatë vjet burgim dhe gjobë deri në 300,000€. Pra mund të shihet qartë se Franca ka paraqitur dënime kaq të larta me qëllim të preventivës, duke "frikësuar" personat që dëshirojnë të kryejnë krime kibernetike.

3.3.2 Institucionet kompetente franceze për luftim të krimit kibernetik

Në dhjetor të vitit 2014, në Ministrinë e Punëve të Brendshme u emërua këshilltar special qeveritar për luftën kundër krimit kibernetik. Ai është përgjegjës për koordinimin e strategjisë së ministrisë në këtë fushë.

Qendra Franceze e Ekspertëve kundër Krimit Kibernetik (CECyF) është një qendër për të luftuar krimin kibernetik në Francë. Paraqet partneritet midis agjencioneve qeveritare,

[68]France:Cybersecurity 2020, (https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/france) (qasja e fundit më 20.03.2020)

komunitetit akademik, shoqatave jofitimprurëse dhe industrisë, i vendosur për të parë mënyra të reja dhe më efektive për të luftuar kërcënimet nga krimit kibernetik[69].

Gjithashtu, dy sektore që janë kompetente për kërkesën ligjore në lidhje me sigurinë kibernetike janë:

- Sektori i Shërbimeve Financiare – i cili merret me kërkesa të tilla si auditimi i sistemit informatik, forcimi i rezistencës ndaj rreziqeve në internet, zhvillimi i mbrojtjes që i përshtatet kompleksitetit të sulmeve kibernetike, etj;
- Sektori i Telekomunikimit – i cili merret me respektimin rregullave që lidhen me kushtet e qëndrueshmërisë, cilësisë, sigurisë të rrjetit dhe shërbimit.

Një tjetër institucion me rëndësi është Agjensioni Nacional për Siguri Kibernetike të Francës (ANSSI) që është themeluar në vitin 2009. Roli i agjensionit është të nxisë një reagim të koordinuar, ambicioz, pro-aktiv për çështjet e sigurisë kibernetike në Francë. ANSSI raporton tek Sekretariati i Përgjithshëm për Mbrojtjen dhe Sigurinë Nacionale (SGDSN) duke ndihmuar kështu kryeministrin në ushtrimin e përgjegjësive të tij për mbrojtjen dhe sigurinë nacionale[70].

3.3.3 Strategjia nacionale për krim kibernetik në Francë

Në shkurt të vitit 2011, Agjensioni Nacional i Sigurisë Kibernetike të Francës (ANSSI) botoi strategjinë e Francës për kibernetikë dhe siguri kibernetike. Për tu mbrojtur nga sulmet kibernetike dhe për të mbrojtur sigurinë e qytetarëve francezë, bizneseve, strategjia e Francës përcakton katër objektiva strategjikë:

- të jetë një fuqi globale për mbrojtje kibernetike;
- të mbrojë lirinë e Francës për vendimmarrje duke mbrojtur informacionin sovran;

[69] French Expert Center Against Cybercrime (CECyF) (https://www.cybersecurityintelligence.com/french-expert-center-against-cybercrime-cecyf-2816.html)(qasja e fundit më 21.03.2020)
[70]ANSSI: A WORD FROM THE DIRECTOR GENERAL, (https://www.ssi.gouv.fr/en/mission/word-from-director-general/) (qasja e fundit më 21.03.2020)

- të forcojë sigurinë kibernetike;
- të ruaj sigurinë në hapësirën kibernetike[71].

Përveç kësaj, Franca ka miratuar një strategji tjetër nacionale për sigurinë kibernetike në vitin 2015. Kjo strategji synon të përcjell tranzicionin dixhital të shoqërisë franceze dhe të drejtojë sfidat e reja të ndryshimit të përdorimeve të teknologjisë dixhitale dhe kërcënimeve që shoqërohen me këto ndryshime. Strategjia përqendrohet në pesë qëllime:

- garantimi i sovranitetit kombëtar;
- sigurimi i reagimit të fortë ndaj akteve të krimit kibernetik;
- informimi i publikut;
- bërja e sigurisë dixhitale një avantazh konkurrues për bizneset franceze;
- rritja e zërit të Francës në skenën ndërkombëtare[72].

3.4 Krimi kibernetik në Spanjë

3.4.1 Legjislacioni spanjol mbi krimin kibernetik

Spanja si shtet hyn në grupin e vendeve më të mëdha dhe më të pasura në Evropë. Ajo vazhdimisht ka bërë përpjekje të qëllimshme për të luftuar krimin kibernetik, duke investuar kohë, para dhe burime në sistemet dhe organizatat e saj kompetente për këtë qëllim. Përdorimi i internetit nga më shumë se 70% e popullatës spanjole, paraqet rrezikim të tyre nga krimi kibernetik[73]. Të dhënat statistikore të publikuara në vitin 2018, tregojnë totalin e rasteve të krimit kibernetik që kanë ndodhur në Spanjë në vitin 2017. Këto të dhëna u bazuan në raportet e prokurorisë së shtetit spanjoll. Mashtrimi përmes teknologjisë së informacionit dhe komunikimit ishte renditur më i larti, me gjithësej 3.714 raste, nërkaq menjëherë pas tij, me

[71]ANSSI:Cybersecurity strategy, (https://www.ssi.gouv.fr/en/cybersecurity-in-france/cybersecurity-strategy/) (qasja e fundit më 23.03.2020)
[72]France and Cyber security, (https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/) (qasja e fundit më 23.03.2020)
[73]Cybersecurity in Spain,2019, (https://cybernews.com/security/cybersecurity-in-spain/) (qasja e fundit më 24.03.2020)

numër më të lartë të rasteve (825 raste) u rendit pornografia me fëmijë dhe korrupsioni i të miturve ose personave me aftësi të kufizuara[74]. Kështu u bënë ndryshime në Kodin Penal të Spanjës, duke inkriminuar lloje të reja të veprave penale dhe duke ndryshuar klasifikimet e mëparshme të krimit kibernetik.

Spanja ka një numër të madh të rregullave pë siguri kibernetike, duke përfshirë mbi 50 ligje të ndryshme që zbatohen, prej të cilave disa prej më të rëndësishmeve janë:

1. Ligji 38/2015, i 28 shtatorit 2015, për sigurinë kombëtare;
2. Dekret- ligji mbretëror 12/2018, i 7 shtatorit 2018, duke përfshirë Direktivën e BE, në lidhje me masat për një nivel të lartë të sigurisë së sistemit të rrjetit dhe informacionit në të gjithë Bashkimin Evropian;
3. Ligji 34/2002, i 11 korrikut, për shërbimet e informacionit dhe tregtinë elektronike;
4. Ligji 59/2003, i 19 dhjetorit, për nënshkrimet elektronike;
5. Ligji 9/2014, i 9 majit, për telekomunikimin e përgjithshëm, etj[75].

Kodi Penal spanjol rregullon krimin kibernetik me këto nene:

- Neni 197 - zbulim i sekretit;
- Neni 199 – vjedhje elektronike;
- Neni 248 - mashtrimi kompjuterik;
- Neni 256 – dëmtimi i telekomunikimi;
- Neni 264 - shpërndarja e viruseve;
- Neni 270 – shkelja e të drejtës të autorit;[76].

[74] Statista: Court proceedings of cybercrime in Spain in 2017, (https://www.statista.com/statistics/463628/cybercrime-type-figures-spain/) (qasja e fundit më 25.03.2020)
[75] Spain: Cybersecurity laws and regulations, (https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/spain) (qasja e fundit më 26.03.2020)
[76] Spain: Cybercrime laws, (https://www.cybercrimelaw.net/Spain.html) (qasja e fundit më 27.03.2020)

3.4.2 Institucionet e specializuara për luftimin e krimit kibernetik në Spanjë

Spanja ka dy ekipe të ndryshme për reagim urgjent ndaj krimeve kibernetike, nën emrat INCIBE-CERT dhe CCN-CERT. INCIBE-CERT është themeluar në vitin 2008 dhe juridiksionii tij shtrihet në të gjithë Spanjën, që do të thotë se ky është ekip përgjegjës për publikun e gjerë, bizneset dhe grupet e tjera spanjole, ndërsa CCN-CERT është përqendruar vetëm në institucionet qeveritare.[77]

Institucioni kryesor për siguri kibernetike në Spanjë, është Centro Nacional de Protección de las Infraestructuras Críticas (CNPIC).[78] Për detyrë kryesore ka forcimin e sigurisë kibernetike të Spanjës duke rritur ndërgjegjësimin për çështjet përkatëse dhe duke iu përgjigjur sulmeve kibernetike. INCIBE-CERT është nën kontrollin e CNPIC dhe mund të përdoret për t'iu përgjigjur sulmeve të ndryshme kibernetike.

Gjithashtu, Spanja është pjesë e rrjetit Fourteen Eyes. Fourteen Eyes është një aleancë inteligjence midis shteteve të mëdha të botës, ku bëjnë pjesë edhe Shtetet e Bashkuara të Amerikës, Mbretëria e Bashkuar, Franca dhe Australia. Kjo aleancë i lejon agjencitë e inteligjencës nga këto vende të përdorin teknika të ndryshme për të monitoruar të dhënat kibernetike. Shtetet e përfshira në këtë aleancë, këto të dhëna mund t'i shkëmbejnë me njëra-tjetrën, me qëllim që të parandalojnë sulmet terroriste dhe të mbrojnë qytetarët.

3.4.3 Strtegjitë nacionale të Spanjës për krim kibernetik

Si shumë vende evropiane, edhe Spanja ka miratuar strategji për siguri kibernetike. Strategjia e parë daton nga viti 2013, paraqitet si dokument gjithëpërfshirës me objektiva të veçanta, qëllimi kryesor i të cilës ishte forcimi i institucioneve dhe rrjeteve të sigurisë

[77] Cybernews: Cybersecurity in Spain, (https://cybernews.com/security/cybersecurity-in-spain/) (qasja e fundit më 28.03.2020)
[78]CNPIC: Cybersecurity, (http://www.cnpic.es/en/Ciberseguridad/index.html) (qasja e fundit më 28.03.2020)

kibernetike[79]. Ndërsa strategjia e dytë është miratuar më 1 prill 2019 duke përfshirë 15 objektiva, disa prej të cilave janë:

- Adresimi i krimit kibernetik;
- Bilanci mes sigurisë dhe privatësisë;
- Ndërgjegjësimi i qytetarëve;
- Mbrojtja e informacionit;
- Hartimi i planeve kombëtare për krim kibernetik;
- Angazhimi në bashkëpunim ndërkombëtar;
- Vendosja e partneritetit publik-privat;
- Themelimi i një forme të institucionalizuar bashkëpunimi mes agjencioneve publike;
- Themelimi i mekanizmave për raportimin e rasteve;
- Organizimi i ushtrimeve për siguri kibernetike;
- Nxitja e sektorit privat që të investojë në masa të sigurisë;
- Forcimi i programeve trajnuese dhe educative[80].

3.5 Krimi kibernetik në Holandë

3.5.1 Rregullimi legjislativ i krimit kibernetik në Holandë

Në historinë e rregullimit të legjislacionit për krimin kibernetik në Holandë, Konventa e Këshillit të Evropës për Krimin Kibernetik paraqet një përpjekje të rëndësishme për të harmonizuar ligjin penal kombëtar në këtë fushë. Për të kuptuar mirë legjislacionin e krimit kibernetik, disa karakteristika të përgjithshme të së drejtës penale holandeze mund të jenë të

[79]Bsa: Cybersecurity Spain, (http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_spain.pdf) (qasja e fundit më 28.03.2020)
[80]Enisa:Spanish National cybersecurity strategy, (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy) (qasja e fundit më 28.03.2020)

dobishme për t'u përmendur. E drejta penale është kodifikuar kryesisht në Kodin Penal dhe në Kodin e Procedurës Penale. Kodi Penal bën dallimin midis krimeve (te të cilat hyjnë pothuajse të gjitha krimet kompjuterike) dhe kundërvajtjeve. Një karakteristikë tjetër e rëndësishme e së drejtës penale holandeze është e drejta për të ushtruar diskrecionin prokurorial (oportuniteitsbeginsel). Kjo do të thotë që prokurori publik vendos nëse është apo jo e përshtatshme të ndiqni penalisht dikë për një vepër penale[81].

Në lidhje me legjislacionin e krimit kibernetik në Holandë, më të rëndësishme janë Akti ligjor i Krimit të Kompjuterave i vitit 1993 dhe Akti ligjor i Krimit të Kompjuterave II i vitit 2006. Këto akte ishin të pandara. Akti ligjor i krimit të kompjuterave ishte rezultat i një procesi të gjerë legjislativ, i cili filloi në vitin 1985 me krijimin e një Komiteti për krimin kompjuterik. Komiteti bëri një analizë të plotë të kodit penal dhe kodit të procedurës penale dhe paraqiti raportin dhe rekomandimet në vitin 1987. Kjo çoi në projektligjin për krimin kompjuterik që u dërgua në Parlament më 16 maj 1990. Amandamente të ndryshme dhe një debat i nxehtë në parlament dërguan në versionin përfundimtar të Aktit ligjor për krimin e kompjuterëve që hyri në fuqi më 1 mars 1993. Më 15 mars 2005, një projekt-ligj për ratifikimin e konventës u paraqit në parlament dhe në këtë mënyrë erdh në shprehje Akti ligjor i krimit të kompjuterave II i cili u pranua nga parlamenti më 1 qershor 2006 dhe hyri në fuqi më 1 shtator 2006[82]. Që të dy aktet ligjore janë të inkorporuara në Kodin Penal dhe Kodin e Procedurës Penale të Holandës. Në të njëjtën kohë Holanda ratifikoi Konventën për krim kibernetik e cila hyri në fuqi më 1 mars 2007.

Kodi Penal, në përputhje me Konventën e krimit kibernetik, përfshin krimet e mëposhtme:

- Neni 138 - qasje të paligjshme;
- Neni 139 - përgjim i paligjshëm;
- Neni 350a - manipulim i të dhënave;
- Neni 161 - sabotim kompjuterik;
- Neni 225 - falsifikimi i dokumenteve;
- Neni 232 – kartelat pagesore;

[81] Koops, Bert-Jaap, "Cybercrime Legislation in the Netherlands" 2010
[82] Po aty

- Neni 326-326c - Mashtrimi kompjuterik;
- Neni 240b – pornografia e fëmijëve[83].

Edhe Kodi i Procedurës Penale rregullon çështje me rëndësi lidhur me krimin kibernetik. Kështu në nenet 125i – 125o parashikohen rregulla mbi kërkimin e sistemeve kompjuterike gjatë kontrollit të lokaleve me qëllim të ruajtjes së të dhënave kompjuterike, neni 126la- 126mn rregullon kompetencat për mbikëqyrjen e komunikimeve elektronike, ndërkaq neni 126m ka të bëjë me përgjimet e komunikimeve[84].

3.5.2 Institucionet kompetente për luftimin e krimit kibernetik në Holandë

Hetimi i krimit kibernetik është e përqendruar në Njësinë Kombëtare të Policisë Kombëtare në Driebergen. Megjithatë, kompetenca ligjore për të filluar dhe drejtuar hetimet penale i përket prokurorisë, me mbështetjen teknike nga policia. Holanda i është përmbajtur detyrimit që parasheh Konventa e Budapestit, për të vendosur një pikë kontakti 24/7 kudo të mund tëparaqiten të gjitha rastet që kanë të bëjnë me krim kibernetik. Kjo realizohet nëpërmjet disa qendrave kompetente të cilat janë në kordinim me Ministinë e drejtësisë. Njëra nga këto është "Qendra Nacionale e Operacioneve për Siguri Kibernetike" (NCSOC) e cila është në dispozicion 24/7 si qendër raportimi. Zbulon kërcënime dhe cënimet e reja, si dhe siguron rrjetin e kontakteve[85]. Qendër tjetër kompetente për krim kibernetik është "Qendra Nacionale e Sigurisë Kibernetike (NCSC) e cila është themeluar në vitin 2012 dhe në vete përfshin edhe Ekipin holandez për reagimin ndaj emergjencave kompjuterike.

Gjithashtu, është formuar një institut i veçantë për krim kibernetik, i quajtur "Dutch Institute for Technology, Safety & Security" që është krijuar nga qeveria, institucionet arsimore dhe kompanitë për të shqyrtuar dhe zgjidhur çështjet e sigurisë. Fushat e fokusit përfshijnë

[83]Netherlands: Cybercrime, (https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/netherlands/pop_up?inheritRedirect=false) (qasja e fundit 02.04.2020)
[84] Po aty
[85] Cyberwiser: Netherlands (https://www.cyberwiser.eu/netherlands-nl) (qasja e fundit më 02.04.2020)

sigurinë kompjuterike[86]. Ky institut promovon, organizon dhe krijon programe kërkimi dhe inovacioni në lidhje me sigurinë.

3.5.2 Strategjia nacionale për siguri kibernetike në Holandë

Holanda ka një kornizë ligjore dhe politike mjaft të sofistikuar lidhur me sigurinë kibernetike, e cila çdo dy vjet avansohet dhe përmirësohet. Strategjitë nacionale të sigurisë kibernetike që i ka miratuar Holanda janë: njëra e vitit 2011 dhe tjetra e vitit 2014. Strategjia e parë, "Nga Injoranca në Ndërgjegjësim", u përqëndrua në krijimin e partneriteteve publike-private, krijimin e kapaciteteve dhe masat për rritjen e besimit. Strategjia e dytë, "Nga Ndërgjegjësimi në Kapacitet", bazohet në progresin që vjen nga strategjia e parë. Plani i veprimit, për vitet 2014-2016, sipas kësaj strategjie përfshin këto qëllime kryesore:

1. Holanda të jet rezistente ndaj sulmeve kibernetike dhe mbron interesat jetike në fushën dixhitale;
2. Holanda të merret me krimin kibernetik;
3. Holanda të investon në shërbime të sigurta që mbrojnë privatësinë;
4. Holanda të ndërton koalicione për liri, siguri dhe paqe në fushën dixhitale;
5. Holanda të ketë njohuri të mjaftueshme për sigurinë kibernetike dhe të investon në fushat e duhura për luftimin e këtij krimi[87].

3.6 Krimi kibernetik në Itali

3.6.1 Legjislacioni Italian mbi krimin kibernetik

Përhapja aktuale e rrjetit kompjuterik, e mediave sociale, tregtisë elektronike dhe të dhënave të ndryshme, po tregon ndikim gjithnjë e më të rëndë në sigurinë e sistemeve të

[86] CyberSecurity Intelligence: DITSS, (https://www.cybersecurityintelligence.com/dutch-institute-for-technology-safety-and-security-ditss-3038.html) (qasja e fundit më 02.04.2020)
[87] National Cyber Security Strategy 2, "From awareness to capability"

informacionit. Ashtu si pjesa tjetër e botës, sulmet kibernetike edhe në Itali përbëjnë një çështje aktuale. Në vitin 2018, kompanitë në Itali humbën mbi tetë milion dollarë nga sulmet kibernetike. Kjo përfaqësonte një rritje prej 20% në krahasim me shifrën e paraqitur për vitin 2017. Derisa kompanitë përqafojnë inovacionin dixhital, ato bëhen më të varura nga interneti. Sipas Indeksit Global të Cybersecurance ITU (2017), Italia u rendit në vendin e 31-të në botë përsa i përket angazhimit të saj ndaj sigurisë kibernetike. Edhepse Italia ekonomikisht është mjaft e pasur, mbeti prapa vendeve të tjera evropiane si Franca, Norvegjia dhe Estonia, të cilat ishin udhëheqës global në fushën e krimit kibernetik[88].

Italia ka qenë një nga vendet e para në Evropë që ka zbatuar Rekomandimin për Krimin Kompjuterik të miratuar më 13 shtator 1989 nga Komiteti i Ministrave të Këshillit të Evropës. Në të vërtetë, Ligji Nr. 547 i 23 dhjetorit 1993 hyri në fuqi disa vite më vonë me të cilin u bënë ndryshime me dispozita plotësuese të Kodit Penal dhe Kodit të Procedurës Penale për krimin kibernetik[89]. Kjo kornizë ligjore ka mbetur e pandryshuar deri në prezantimin e rregullave të reja sipas Ligjit Nr. 48 të 18 marsit 2008, me të cilin Italia zbatoi Konventën e Budapestit.

Prandaj, edhe pse Italia nuk ka rregulla të veçanta për krimin kibernetik, ajo ka ndryshuar dispozitat e ligjit ekzistues (të përfshira tashmë në Kodin Penal dhe Kodin e Procedurës Penale). Senati i Parlamentit Italian ka aprovuar dhe ratifikuar Konventën për Krimin Kibernetik më 27 shkurt 2008.

Përveç dispozitave të përfshira në Kodin Penal të Italisë, ekzistojnë edhe ligjet e posaçme që rregullojnë krimin kibernetik, e të cilat janë:

1. Ligji për të drejtat e autorit (22 Prill 1941, nr. 633);
2. Ligji penal i kartelave të kreditit (21 nëntor 2007 nr. 231);
3. Kodi Italian i Mbrojtjes së të Dhënave Personale (30 qershorit 2003);

[88] Statista: cybercrime in Italy in 2017 and 2018, (https://www.statista.com/statistics/1032488/cybercrime-cost-italy/) (qasja e fundit më 05.04.2020)
[89] Council of Europe: Cybercrime in Italy (https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/italy?inheritRedirect=false&redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Foctopus%2Fcountry-wiki%3Fp_p_id%3D101_INSTANCE_hFPA5fbKjyCJ%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-4%26p_p_col_count%3D1) (qasja e fundit më 05.04.2020)

4. Kodi i Komunikimeve Elektronike (1 gusht 2003, nr. 259)[90].

3.6.2 Institucionet e veçanta për luftimin e krimit kibernetik në Itali

Në prill të vitit 2008 me një dekret të veçantë është përcaktuar fusha specifike hetimore nën kompetencën e Policisë së Postës dhe Komunikimeve. Kohët e fundit, roli i Policisë së Postës dhe Komunikimit është përforcuar në parandalimin dhe luftimin e terrorizmit, përfshirë këtu edhe krimin kibernetik. Sa i përket rregullimit dhe mbikëqyrjes së kompanive italiane të telekomunikimit, autoriteti kompetent është Ministria e Zhvillimit Ekonomik[91].

Për mbrojtjen e të dhënave personale është kompetent Autoriteti Italian i Mbrojtjes së të Dhënave që është themeluar në bazë të ligjit nr. 675 i 31 dhjetorit 1996. Ky është një autoritet i pavarur administrativ, kompetencat e të cilit përcaktohen aktualisht nga Kodi për mbrojtjen e të dhënave personale.

Në lidhje me të drejtat e autorit në internet, që nga viti 2013 nën "Rregulloren për mbrojtjen e të drejtave të autorit në rrjetet e komunikimeve elektronike", Autoriteti për Ruajtjen e Komunikimeve (AGCOM) ka disa autorizime për të ndërmarrë veprime me qëllim të parandalimit të këtyre krimeve.

3.6.3 Strategjia Nacionale e sigurisë kibernetike në Itali

Strategjia Nacionale e Sigurisë Kibernetike dhe Plani Kombëtar lidhur me të, janë të parashikuara nga dekreti i kryeministrit që përmban Udhëzime Strategjike për Mbrojtjen Kibernetike Kombëtare dhe Sigurinë e TI (e 24 janarit 2013). Ato kanë për qëllim forcimin e

[90] Council of Europe: Cybercrime in Italy (https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/italy?inheritRedirect=false&redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Foctopus%2Fcountry-wiki%3Fp_p_id%3D101_INSTANCE_hFPA5fbKjyCJ%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-4%26p_p_col_count%3D1) (qasja e fundit më 05.04.2020)

[91] Italian Criminal legislation concerning ICTs, (http://www.studiolegalegaldieri.com/articoli-e-relazioni/italian-criminal-legislation-concerning-icts/) (qasja e fundit më 06.04.2020)

gatishmërisë nacionale për t'iu përgjigjur sfidave të së tashmes dhe të së ardhmes që prekin hapësirën kibernetike, dhe janë të përkushtuara në drejtimin e të gjitha përpjekjeve nacionale për të gjetur zgjidhje të përbashkëta, duke e ditur që siguria kibernetike dhe risitë teknike gjithmonë do të prezantojnë dobësi të reja në horizontin strategjik dhe operacional[92].

[92] Italy's National Strategic Framework for Cyberspace Security, (file:///C:/Users/User/Downloads/IT_NCSS_en%20(1).pdf) (qasja e fundit më 06.04.2020)

KAPITULLI I KATËRT

Shtrirja e krimit kibernetik në RMV - Studim empirik

4.1 Vështrime të përgjithshme

Në këtë pjesë të hulumtimit është konkretizuar prania e krimit kibernetik në RMV. Për të arritur në rezultate më të sakta, fillimisht janë marrë të dhëna nga Enti shtetëror statistikor, me të cilat është nxjerrur në pah se sa disa vepra penale që përbëjnë krimin kibernetik, janë gjykuar në RMV për periudhën kohore 2013-2017. Njëkohësisht, duke paraqitur kështu edhe dënimet që janë shqiptuar për këto vepra penale.

Analizimi dhe komentimi i aktgjykimeve nga Gjykata Themelore Shkupi I dhe Gjykata e Apelit Shkup lidhur me krimet kibernetike, rezulton me konludime sa i përket sanksioneve që më së shumti shqiptohen në RMV për këto vepra.

Ndërkaq, me të dhëna nga Prokuroria Themelore Shkup, fitohet pasqyrë lidhur me aktakuzat e ngritura nga kjo Prokurori për krimin kibernetik, për periudhën kohore 2016-2018, si dhe, pasqyrë lidhur me disa të dhëna mbi kallëzimet penale dhe veprat penale për vitin 2019.

Theks i veçantë është vendosur mbi anketën e realizuar me numër të caktuar të personave, e cila ka rëndësi shumë të madhe për këtë hulumtim. Rezultatet e kësaj ankete janë shtjelluar dhe analizuar në mënyrë të veçantë për të arritur kështu në konkluza shumë të sakta nga të cilat rrjedhin edhe rekomandimet.

4.2 Të dhëna nga Enti shtetëror për statistikë

TABELA PËR KRIM KOMPJUTERIK NË RMV - PERIUDHA KOHORE 2013 - 2017											
		2013		***2014***		***2015***		***2016***		***2017***	
		Të dënuar	Llojet e sanksioneve	Të dënuar	Llojet e sanksioneve	Të dënuar	Llojet e sanksioneve	Të dënuar	Llojet e sanksioneve	Të dënuar	Llojet e sanksioneve
Neni 193	Ekspozimi i materijalit pornografik fëmijës	1	**1** dënim me burg	1	**1** dënim me të holla	0		0		0	
Neni 251	Dëmtimi dhe hyrja e paautorizuar në sistemin kompjuterik	27	**7** dënime me burg, **1** dënim me të holla, **18** dënime me kusht, **1** vërejtje gjyqësore	14	**4** dënime me burg, **2** dënime me të holla, **8** dënime me kusht	20	**7** dënime me burg, **4** dënime me të holla, **9** dënime me kusht	16	**1** dënim me burg, **3** dënime me të holla, **12** dënime me kusht	17	**3** dënime me burg, **1** dënim me të holla, **13** dënime me kusht
Neni 251b	Mashtrimi kompjuterik	3	**2** dënime me burg, **1**dënim me kusht	0		0		0		1	**1** dënim me kusht
Neni 274b	Përpunimi dhe përdorimi i kartelës së rrejshme pagesore	0		0		25	**10** dënime me burg, **9** dënime me të holla, **6** dënime me kusht	4	**3** dënime me burg, **1** dënim me kusht	8	**7**dënime me burg, **1** dënim me kusht
Gjithsej		***31***		***15***		***45***		***20***		***26***	

Tabela 1: Krimi kompjuterik në RMV – Periudha kohore 2013-2017

Në hulumtimin e mësipërm që ka të bëjë me krimin kibernetik në RMV, të dhëna këto të siguruara në mënyrë zyrtare nga Enti shtetëror për statistikë, janë analizuar të dhënat për numrin e personave të dënuar dhe llojet e sanksioneve që u janë shqiptuar të dënuarve, për këto kategori të krimit kibernetik në RMV: ekspozimi i materijalit pornografik fëmijës; dëmtimi dhe hyrja e paautorizuarnë sistemin kompjuterik; mashtrimi kompjuterik; dhe përpunimi dhe përdorimi i kartelës së rrejshme pagesore. Të dhënat e analizuara janë nga periudha kohore 2013 – 2017.

Në të gjitha vitet në intervalin kohor 2013 – 2017, mund të konstatojmë se kategoria e krimit kibernetik që është më e përhapur në RMV, është dëmtimi dhe hyrja e paautorizuar në sistemin kompjuterik me rreth 70% të rasteve të gjykuara. Konstatim tjetër është se në vitin 2015 janë shqiptuar më së shumti dënime, 45 gjithsej.

Nga hulumtimi i bërë, mund të sjellim përfundim se lloji i sanskionit që më së shumti është shqiptuar në vitet në fjalë është dënimi me kusht.

4.3 Aktgjykime nga Gjykata Themelore Shkupi I dhe Gjykata e Apelit Shkup lidhur me krimet kibernetike në RMV (analizë dhe komentim i tyre)

4.3.1 Përmbledhje e aktgjykimeve të marra nga Gjykatat Themelore dhe Gjykata e Apelit Shkup

Në pamundësi për t'i inkorporuar të gjitha aktgjykimet në këtë punim, do bëhet përmbledhja dhe sjellja e konkluzioneve nga karakteristikat e përbashkëta të tyre.

Aktgjykimet që janë shqyrtuar dhe hulumtuar janë këto:

- GjThSh I, aktgjykimi –K.nr.3838/10 nga 09.02.2012, dhe aktgjykimi nga GjASh, KZH.nr.992/12 nga 11.07.2012 (Pirateria e veprës audio-vizuale, neni 157b i KP);

- GjThSh I, aktgjykimi – K.nr.582/10 nga 02.04.2012, dhe aktgjykimi nga GjASh, KZH.nr.1628/12 nga 07.12.2012 (Ekzpozimi i materialit pornografik të fëmijës, neni 193 i KP);
- GjThGj, aktgjykimi – K.nr.48/13 nga 04.03.2013, dhe aktgjykimi nga GjASh, KZH.nr. 48/14 nga 08.05.2014 (Cënimii të drejtës së distributorit të sinjalit satelitor me mbrojtje të posaçme teknike, neni 157a i KP);
- GjThK, aktgjykimi – K.nr.1211/08 nga 19.06.2014, dhe aktgjykimi nga GjASh, KZH.nr. 2224/14 nga 10.03.2015 (Mashtrim kompjuterik, neni 251b i KP);
- GjThSh, aktgjykimi – K.nr.1167/15 nga 27.08.2015 dhe aktgjykimi nga GjASh, KZH.nr. 1428/15 nga 09.12.2015 (Dëmtimi dhe hyrja e paautorizuar në sistemin kompjuterik, neni 251 i KP);
- GjThSh, aktgjykimi – K.nr.501/17 nga 22.09.2017 dhe aktgjykimi nga GjASh, KZH.nr.1002/17 nga 10.01.2018 (Keqpërdorimi i të dhënave personale, neni 149 i KP);
- GjThSh, aktgjykimi – K.nr.329/17 nga 16.11.2017 dhe akgjykimi nga GjASh, KZH.nr.288/18 nga 24.04.2018 (Cënimi i të drejtës së autorit dhe të drejtave të përafërta, neni 157 i KP);
- GjThK, aktgjykimi – K.nr. 225/18 nga 12.11.2018 dhe aktgjykimi nga GjASh, KZH.nr.23/19 nga 01.02.2019 (Cënimi i fshehtësisë së korrespodencës ose të dërgesave të tjera, neni 147 i KP);
- GjThV, aktgjykimi – K.nr.169/18 nga 26.02.2019 dhe aktgjykiminga GjASh, KZH.nr. 723/19 nga 12.11.2019 (Rrezikimi i sigurisë, neni 144 i KP)

Nga analizimi dhe shqyrtimi i këtyre aktgjykimeve erdhëm në përfundim se politika ndëshkimore për veprat penale në fushën e krimit kibernetik në RMV, është mjaft e ulët në krahasim me vendet Evropiane. Sidomos kur mirret parasysh fakti se këto vepra edhepse më të rejat, kanë pasoja shumë të rënda dhe paraqesin rrezikshmëri të lartë shoqërore.

Sipas hulumtimeve që kemi bërë, nga të gjitha aktgjykimet e lartëpërmendura dhe të analizuara, konkludojmë se në 90% të rasteve është shqiptuar masa alternative – dënim me kusht. Mendoj që me shqiptimin e sanksioneve të tilla për veprat e krimit kibernetik nuk ndikohet mjaftueshëm tek kryerësit e këtyre veprave që të mos paraqiten si recidivist si dhe nuk ndikohet pozitivisht në planin e preventimit gjeneral me të cilin arrihet qëllimi i ndëshkueshmërisë. Që do të thotë ndëshkimet ndajkrimeve kibernetike duhet të jenë më rigoroze dhe më të larta.

4.3.2 Aktgjykimi K.nr.2038/18

NË EMËR TË QYTETARËVE TË REPUBLIKËS SË MAQEDONISË

GJYKATA THEMELORE SHKUPI I - SHKUP, si gjykatë penale e shkallës së parë, përmes gjykatëses L.D. si gjykatëse individuale, me procesverbalist V.A. duke vepruar sipas aktakuzës së Prokurorisë Publike S. KO-2 Nr. 121/17 të datës 19.11.2018, kundër të pandehurës R.A. nga Shkupi, për vepër penale - **Dëmtim dhe hyrje e paautorizuar në sistem kompjuterik** nga neni 251 paragrafi 2, në lidhje me parag. 1, në lidhje me nenin 45 të KP, pas mbajtjes së seancës kryesore, publike dhe gojore,në prani të prokurorit publik nga Prokuroria Themelore Publike Shkup, I. H.V., të pandehurit R.A., avokatit mbrojtës B. G. dhe përfaqësuesi i personit juridik të dëmtuar "D." - avokati E.T. më 18.02.2019, bazuar në nenin 480 par. 2 në lidhje me nenin 381 të LPP-së, miratoi dhe shpalli publikisht këtë:

AKTGJYKIM

NË BAZË TË PRANIMIT TË FAJIT

E pandehura: R.A. me EMBG ..., nga babai V., nëna D., e lindur më ... në Sh., jeton në S. në Blvd. "..., me arsimin fillor të mbaruar, pensionist, e divorcuar, nënë e një fëmije të rritur, maqedonase, qytetare e Republikës së Maqedonisë, deri më tani e pagjykuar dhe pa asnjë procedurë tjetër penale të ngritur

ËSHTË FAJTORE

SEPSE:

Në periudhën nga 06.09.2016 deri në 09.09.2016, në S., me paramendim, kreu dymbëdhjetë veprime të lidhura kohore... duke përdorur të njëjtat rrethana, hyri në sistemin e dikujt tjetër pa autorizim, me qëllim përdorimin e të dhënave të tij, për të fituar pasuri të paligjshme për vete, në shumën totale prej 44,680.00 denarë, me të cilën është dëmtuar personi juridik "D." DOOEL S., ashtuqë pas datës 06.09.2016 në Qendrën Tregtare të Qytetit, në Shkup gjeti një kartë krediti "D.", në pronësi të dëshmitarit L.J., i cili e kishte humbur atë një ditë më parë, e përdori kartën dhe e përdori për të blerë mallra dhe shërbime në disa dyqane në Shkup

.....

Me veprimet e mësipërme, e pandehura R.A. nga Shkupi, ka kryer një vepër penale - Dëmtim dhe hyrje e paautorizuar në sistem kompjuterik nga neni 251 paragrafi 2 i Kodit Penal në lidhje me paragrafin 1, në lidhje me nenin 45 të KP, gjykata të pandehurës i shqipton masën alternative:

DËNIM ME KUSHT

Kështu, përcakton dënimin me burgim për një periudhë prej 6 -gjashtë muajsh dhe në të njëjtën kohë përcakton që dënimi me burgim nuk do të ekzekutohet nëse i pandehuri nuk kryen vepër penale tjetër brenda 2- dy vitesh pasi aktgjykimi të bëhet i formës së prerë, dhe gjithashtu si kusht i veçantë në përputhje me nenin 49 paragrafi 2 të Kodit Penal, i pandehuri urdhërohet brenda 1 - një viti pas aktgjykimit të plotëfuqishëm, personit juridik të dëmtuar "D." DOOEL S. t'i kompensojë dëmin e shkaktuar

.....

ARSYETIMI

Prokuroria Themelore Publike Shkup pranë kësaj gjykate, ngriti aktakuzë KO-2 nr.121 / 17

nga 19.11.2018, kundër të pandehurës R.A. nga Shkupi, për vepër penale - Dëmtim dhe hyrje të paautorizuar në sistem kompjuterik nga neni 251 paragrafi 2 i Kodit Penal në lidhje me paragrafin 1 të nenin 45 të KP.

Në rastin konkret, gjykata, në bazë të pranimit të fajit, përcaktoi se është vërtetuar kryerja e veprës penale nga e pandehura, në kohën, vendin dhe mënyrën, siç përshkruhet në aktgjykim...

Në përcaktimin e llojit të sanksionit penal, gjykata mori parasysh të gjitha rrethanat lehtësuese dhe rënduese të parapara në nenin 39 të Kodit Penal...

Duke vlerësuar të gjitha këto rrethana si dhe me pranimin e fajit e pandehura u shpall fajtore nga gjykata dhe u dënua me masë alternative.

.....

GJYKATA THEMELORE SHKUPI I SHKUP,

XVII K.br.2038 / 18 nga 18.02.2019

Regjistrues, Gjykatësi

V. A. L. D.

Ky aktgjykim është ankimuar nga ana e të dënuarës R.A. nga Shkupi deri tek Gjykata e Apelit Shkup. Në vazhdim është paraqitur edhe aktgjykimi i shkallës së dytë.

4.3.3 Aktgjykimi KZH -345/19

NË EMËR TË QYTETARËVE TË REPUBLIKËS SË MAQEDONISË

Gjykata e Apelit Shkup ne këshillin e përbërë nga gjykatësit C.P. kryetare e këshillit, T.M. dhe E.B. anëtarë të këshillit, me procesverbalist A.B. në lëndën penale kundër të pandehurës R.A. nga Shkupi për veprën penale të Dëmtim dhe hyrje e paautorizuar në sistem kompjuterik nga neni 251 paragrafi 2 i Kodit Penal në lidhje me paragrafin 1 dhe në lidhje me nenin 45 të Kodit Penal, duke vepruar sipas ankimit të të pandehurës R. A. nga Shkupi, e deklaruar personalisht, kundër aktgjykimit të Gjykatës Themelore Shkup I S. K.br.2038 / 18 nga 18.02.2019, në seancën publike të mbajtur më 22.05.2019, në përputhje me nenin 434 të Ligjit për Procedurën Penale, miratoi:

AKTGJYKIM

Ankesa e të akuzuarës R.A. nga Shkupi, e deklaruar personalisht, HUDHET SI E PABAZË

AKTGJYKIMI i Gjykatës Themelore Shkup I K.br.2038 / 18 nga 18.02.2019 ËSHTË VËRTETUAR

ARSYETIM

Gjykata Themelore Shkup I me aktgjykimin e ankimuar e shpalli fajtore të pandehurrën R.A. për veprën penale Dëmtim dhe hyrje e paautorizuar në sistem kompjuterik nga neni 251 paragrafi 2 i Kodit Penal ne lidhje me paragrafin 1 dhe me nenin 45 të Kodit Penal duke shqiptuar masë alternative-dënim me kusht në mënyrë që ka përcaktuar dënimin me burg në kohëzgjatje prej 6 muaj dhe në të njëjtën kohë përcaktoi që dënimi i shqiptuar në këtë mënyrë nuk do të ekzekutohet nëse i pandehuri nuk kryen një vepër të re penale brenda dy vitesh pas aktgjykimit të plotëfuqishëm ……..

Gjykata e Apelit duke vepruar sipas ankesës, pasi shqyrtoi të gjitha shkresat e lëndës, aktgjykimin e ankimuar, ankesën dhe propozimin me shkrim të Prokurorisë së lartë publike Shkup, vërtetoi se:

Ankesa është e pabazë

……

GJYKATA E APELIT SHKUP, "KZ-345/19" nga "22.05.2019".

Procesverbalist: Kryetari i Këshillit Gjyqësor

A.B. C.P.

Nëse analizojmë këto aktgjykime, mund të vërehet se ka shkaqe të mjaftueshme për shqiptimin e dënimit me kusht duke pasur parasysh se në rastin konkret gjendja faktike është vendosur në bazë të pranimit të fajit nga ana e të pandehurës. Përveç kësaj, në shqiptimin e këtij dënimi mendoj se ka ndikuar edhe gjendja e saj familjare, materijale, statusi i saj social, mosha e saj (e pensionuar), si dhe fakti që kundër saj nuk është e ngritur ndonjë procedurë tjetër penale dhe deri në atë kohë nuk ka qenë e dënuar më herët.

Ky aktgjykim është sjellur në bazë të paragrafit 2 të nenit 251 të KP i cili thotë: “Me veprën nga paragrafi 1 do të dënohet edhe ai i cili në mënyrë të paautorizuar hyn në kompjuter apo sistem të huaj me qëllim të shfrytëzimit të të dhënave apo programeve të tij përshkak të përfitimit të paligshëm të pasurisë ose dobisë tjetër për vete apo për tjetër kënd ose shkaktonte dëm të pasurisë, ose përshkak të bartjes së të dhënave kompjuterike që nuk janë kushtuar tij dhe në mënyrë të paautorizuar ka ardhur deri te personi jo i thirrur”, dhe në lidhje me paragrafin 1 të nenit të njejtë, i cili thotë “Ai i cili në mënyrë të paautorizuar do të shlyej, ndryshojë, dëmtojë, fshehë, ose në mënyrë tjetër do të bëjë të dhënë ose program ttë padobishëm kompjuterik... do të dënohet me dënim me gjobë ose burgim deri në tre vjet”

4.4 Të dhëna nga Prokuroria Themelore Shkup

Në këtë pjesë të hulumtimit, janë të prezentuara të dhëna tabelare të marra nga Prokuroria Themelore Shkup lidhur me aktakuzat e ngritura nga kjo Prokurori për krimin

kibernetik, për periudhën kohore 2016-2018. Paraqitja strukturale e këtij kriminaliteti sipas veprave penale të sistemuara në KP të RMV-së do të prezentohet ne tabelën në vijim.

KRIMI KOMPJUTERIK - PERIUDHA KOHORE 2016 - 2018							
		2016		***2017***		***2018***	
		VP	kryerës	VP	kryerës	VP	kryerës
Neni 144 p.4	Rrezikimi i sigurisë	3	1	5	2	21	22
Neni 149 p. 2	Keqpërdorimi i të dhënave personale	1	1	1	1	2	0
Neni157 p.2	Cënimi i të drejtës së autorit dhe të drejtave të përafërta	0	0	0	0	0	0
Neni 157a	Cënimi i të drejtës së distributorit të sinjalit satelitor me mbrojte të posaçme teknike	0	0	0	0	1	1
Neni 157b	Piraterija e veprës audio-vizuale	0	0	0	0	0	0
Neni 193	Ekspozimi i materijalit pornografik fëmijës	9	6	0	0	2	1
Neni 193a	Prodhimi dhe distribuimi i pornografisë fëmijërore	7	5	4	6	2	1
Neni 251	Dëmtimi dhe hyrja e paautorizuar në sistemin kompjuterik	70	40	43	34	53	28
Neni 251a	Bërja(programimi) dhefutja e viruseve kompjuterike	0	0	0	0	0	0
Neni 251b	Mashtrimi kompjuterik	12	3	13	12	14	10
Neni 271 p. 3	Ndreqja, furnizimi ose tjetërsimi i mjeteve për falsifikim	2	2	1	1	0	0
Neni 394ç	Përhapja e materijalit racist dhe ksenofobik permes sistemit kompjuterik	0	0	0	0	5	5
Neni 274b	Përpunimi dhe përdorimi i kartelës së rrejshme pagesore	13	25	12	14	4	2
Neni 379a	Falsifikimi kompjuterik	0	0	0	0	1	3
Gjithësej		**117**	***83***	***79***	***70***	***105***	***73***

Tabela 2: Aktakuzat për krim kompjuterik në Prokurorinë Themelore Shkup - periudha kohore 2016-2018

Nga tabela e mësipërme për aktakuzat për krim kibernetik të ngritura nga Prokuroria Themelore Shkup, mund të vërehet qartë se numri më i madh i tyre janë thyerjet e nenit 251 nga Kodi Penal që ka të bëjë me dëmtimin dhe hyrjen e paautorizuar në sistemin kompjuterik. Gjithashtu prezente janë edhe aktakuzat lidhur me thyerjen e neneve 274b që ka te bëjë me përpunimin dhe përdorimin e kartelës së rrejshme pagesore, nenit 251b që ka të bëjë me mashtrimin kompjuterik, etj.

Në pamundësi për të siguruar statistikë të kompletuar për krimet kibernetike të vitit 2019 përshkak se janë në përgatitje e sipër, në vazhdim është paraqitur një tabelë me disa të dhëna rreth kallëzimeve penale dhe veprave penale për vitin 2019. Kjo tabelë është fituar nga Prokuroria Themelore Shkup.

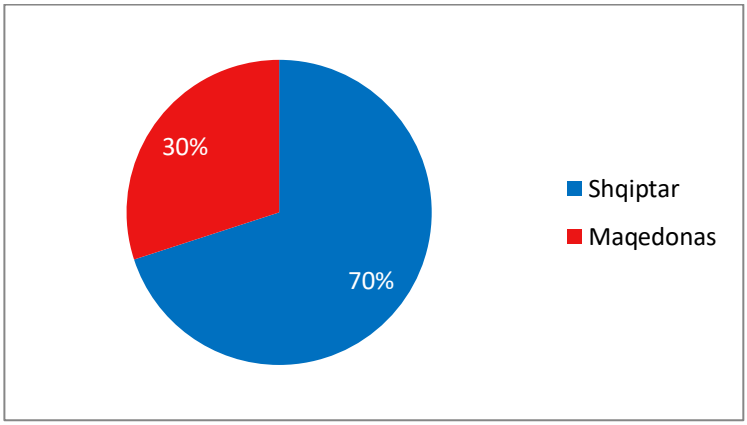
Viti	**2019**		
Nenet	**251**	**251b**	**247**
Kallëzimepenale	2	5	1
Veprapenale	2	5	1

Tabela 3: Të dhëna rreth kallëzimeve penale dhe veprave penale në PThSh për vitin 2019

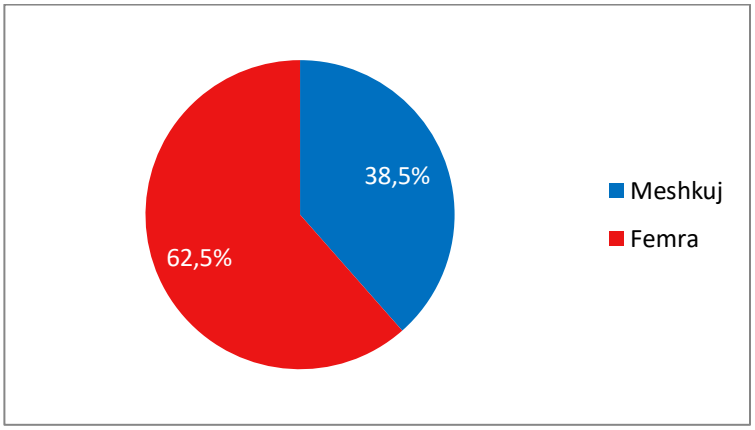
4.5 Zhvillimi dhe rezultatet e anketës

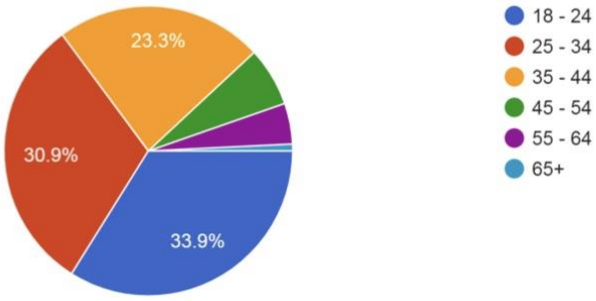
Për nevojat e këtij hulumtimi lidhur me faktin se sa është i përhapur krimi kibernetik në RMV, cilat lloje të këtij krimi janë më shumë prezente, sa qytetarët i denoncojnë këto krime në institucione kompetente, çfarë masa duhet të ndërmirren që krimi kibernetik të luftohet në mënyrë më efikase dhe për shumë pyetje tjera, autori ka realizuar një anketë (online) të cilës i janë përgjigjur një numër prej rreth 400 personave. Anketa ka përmbajtur gjithësej 20 pyetje në të cilat janë përfshirë kryerja e krimeve kibernetike përmes kartelave bankare, përmes postës elektronike (e-mail) si dhe përmes rrjeteve sociale.

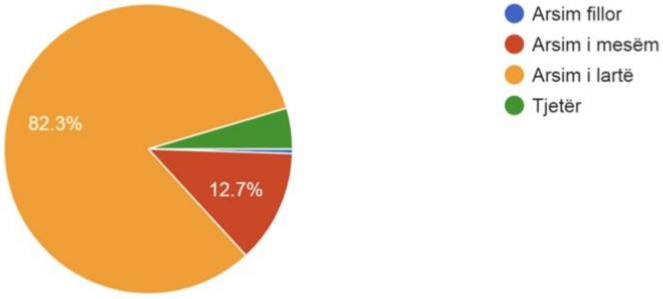
Anketa është zhvilluar me persona të ndryshëm, të cilët dallojnë për nga mosha, gjinia, nacionaliteti, niveli i arsimimit, profili etj. Ajo u realizua në dy gjuhë, shqipe dhe maqedonase, nga të cilët 70% ishin shqiptar dhe 30% maqedonas.



- Në tre pyetjet e para të anketës, që kanë të bëjnë me gjininë, moshën dhe nivelin arsimor, të anketuarit janë deklaruar kështu:





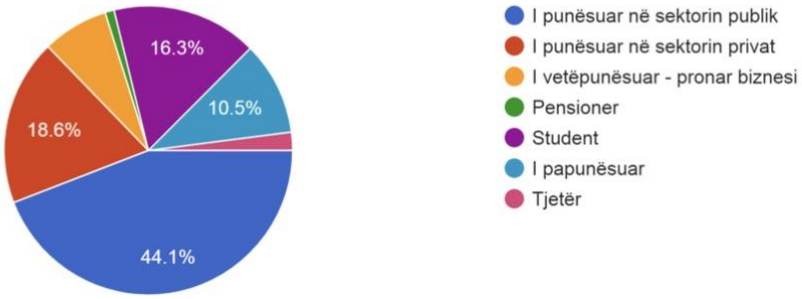


Nga të gjithë të anketuarit, gjinisë femërore i përkasin 61.5%, ndërsa gjinisë mashkullore 38.5%. Sa i përket grupmoshave të ndryshme, dominuese është mosha prej 18-24 vjeç (me33.9%) dhe ajo 25 – 34 vjeç (me 30.9%), kurse grupmosha më pak e përfshirë në anketë është mosha mbi 65 vjeç (0.8%). Ndërkaq lidhur me nivelin arsimor të personave që janë përgjigjur, përqindjen më të lartë (82.3%) e zënë ata që kanë mbaruar arsimin e lartë përderisa

përqindjen më të ulët (0.5%) e zënë ata me arsim fillor.

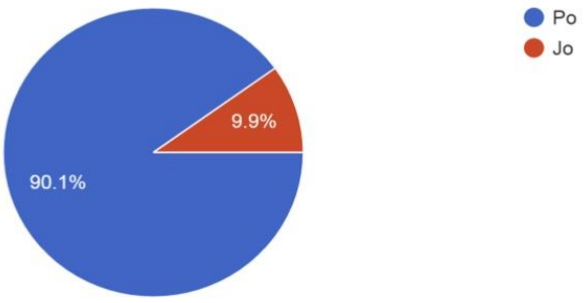
Ajo që mund të vërehet që në fillim është se anketa është bërë me një numër të madh të personave të profileve të ndryshme, nga pikëpamja gjinore, e moshës dhe shkollimit, me qëllimin e vetëm që rezultatet të jenë sa më gjithëpërfshirëse dhe kredibile.

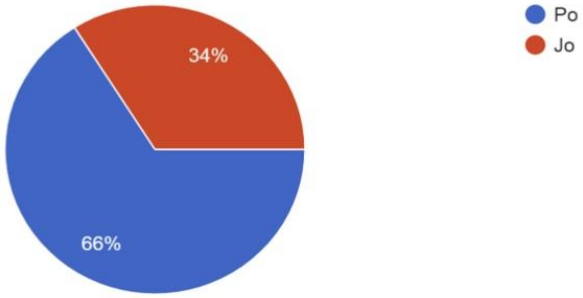
- Në pyetjen lidhur me statusin e punës, përgjigjet janë si vijojnë:



Rezulton se në përqindje më të lartë të të anketuarve, janë të punësuarit në sektorin publik me 44.1%, menjëherë pas tyre vijojnë të punësuarit në sektorin privat me 18.6%, studentët me 16.3%, kurse përqindjen mëtë ulët kanë pensionerët me 1%.

- Lidhur me pyetjet se “A posedoni kartelë bankare dhe a e shfrytëzoni atë?” si dhe “Nëse posedoni dhe e shfrytëzoni, me kartelën bankare a kryeni pagesa online?” në dy grafikonet e paraqitura tregohet se si janë shprehur të anketuarit:

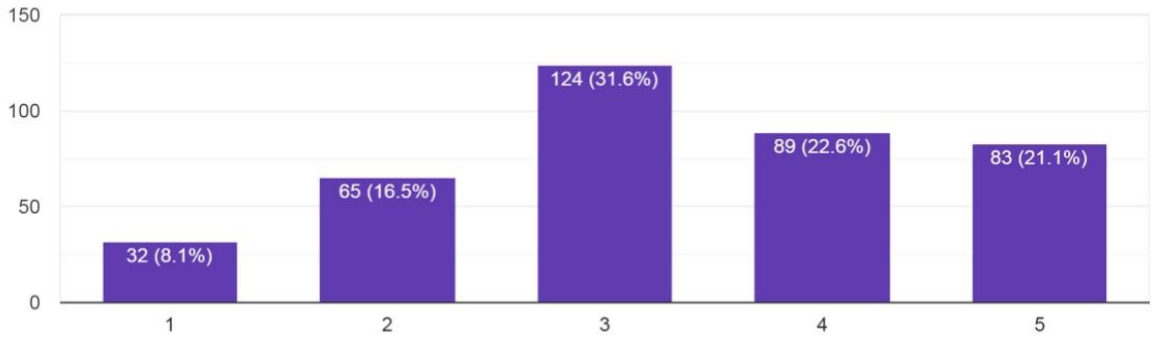




Nga rezultatet e paraqitura vërehet se një numër mjaft i madh janë përdorues të kartelave bankare shumica prej të cilëve kryejnë edhe pagesa online. Me këtë fakt ata në një mënyrë hyjnë në grupin e personave që janë target potencial apo më të “rrezikuar” nga kryerësit e krimeve kibernetike.

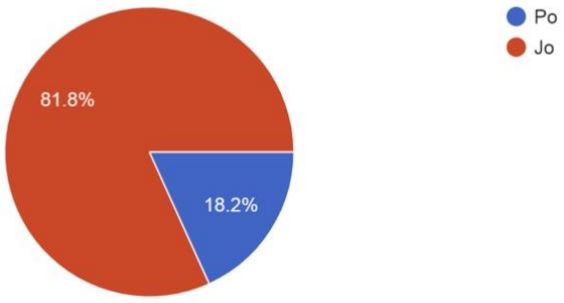
Nga këto dy pyetje vërtetohet edhe ajo se në përgjithsi një përqindje e lartë e qytetarëve posedojnë kartelë bankare dhe se të njejtit i përdorin ato në jetën e përditshme për pagesa të ndryshme. Në fakt, vërtetohet se online pagesat janë bërë pjesë e pandashme e jetës tonë.

- Sa i përket pyetjes se sa mënyra e pagesave online është e sigurtë për të anketuarit, duke pasur mundësinë për tu përgjigjur nga “aspak e sigurtë” deri në “shumë e sigurtë”, janë përgjigjur në këtë mënyrë:



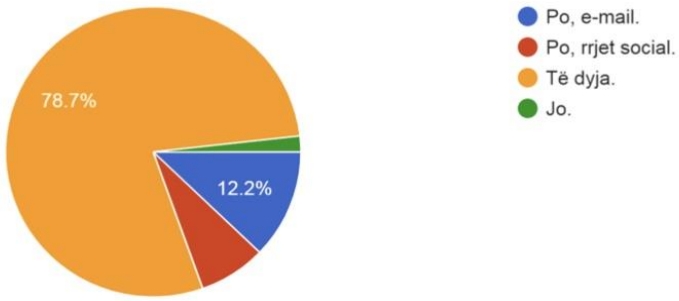
Ky grafikon tregon se mendimet e të anketuarve janë të ndara sa i përket perceptimit të tyre rreth sigurisë gjatë pagesave online. Derisa rreth 8.1% e të anketuarve mendojnë që nuk është aspak e sigurtë, 21.1% mendojnë që ky proces është tejet i sigurtë. Përqindja më e madhe e të anketuarve, rreth 31.6% janë përgjigjur që nuk mendojnë që ky proces është absolutisht jo i sigurtë, por nuk mendojnë që ky proces është edhe shumë i sigurtë, rrjedhimisht nënkuptohet se ata mendojnë që ky proces ka nevojë për përmirësim në drejtim të gjetjes së masave me të cilat përdoruesi do të ishte më i sigurtë gjatë shfrytëzimit të këtij shërbimi. Nga kjo mund të sillet përfundimi se në këtë fushë të pagesave online, institucionet përkatëse së bashku me bankat duhet të ndërmarrin masa shtesë, me qëllim që të rritet siguria e përdoruesve, duke e pasur parasysh faktin se kjo mënyrë e pagesës është shumë lehtësuese sidomos kur dëshirojmë t'iu shmangemi rradhëve të gjata për pagesën e faturave të ndryshme.

- Me sigurinë e mënyrës së kryerjes së pagesave online lidhet edhe fakti se sa dëme janë kryer duke përdorur këtë mënyrë. Prandaj pyetja e radhës e anketës ka të bëjë me atë se a ju ka ndodhur të anketuarve që të jenë viktimë e një mashtrimi potencial gjatë kryerjes së një pagese online?

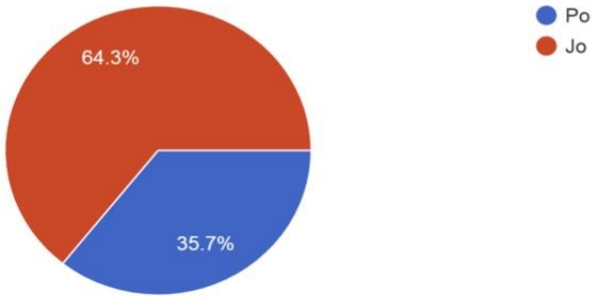


Nga numri total i të anketuarve, nga kjo pyetje arrihet tek një e dhënë shqetsuese ku një përqindje rreth 18.2% kanë deklaruar që në të kaluarën kanë qenë viktimë e një mashtrimi potencial gjatë kryerjes së një pagese online, fakt që dëshmon që institucionet kompetente duhet të merren në mënyrë thelbësore me këtë fenomen gjithnjë e më prezent.

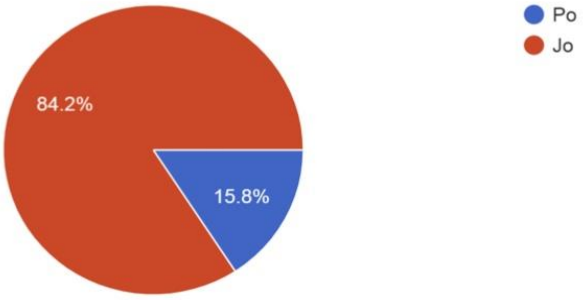
- Në pyetjen e parashtruar nga autori “A posedoni postë elektronike(e-mail)apo profil në rrjetet sociale (facebook, instagram...)?” 78.7% u përgjigjën që janë përdorues edhe të e-mailit edhe të rrjeteve sociale dhe pas tyre me një përqindje prej 12.2% janë personat që përdorin vetëm e-mail. Numrin më të ulët përfaqësojnë personat që nuk përdorin asnjërin nga këto. Nga këto përgjigje mund të konkludohet që një numër shumë i madh i të anketuarve janë përdorues të rrjeteve të ndryshme sociale dhe postës elektronike, të cilat janë pjesë e pandashme e përditshmërisë se tyre.



- Alarmues është fakti se në pyetjen e radhës “Personalisht juve, a ua kanë zbërthyer (thyer) fjalëkalimin (passwordi-in) e e-mailit apo profilit në rrjetet sociale,ose së paku a është tentuar një gjë e tillë?”, diku 35.7% janë përgjigjur pozitivisht, që na len të kuptojmë sa i përhapur është ky lloj i keqpërdorimit apo krimit dhe se target potencial mund të jetë gjithsecili individ. Në fakt, nga kjo përgjigje mund të nënkuptohet se më shumë se 1 në çdo 3 persona ka qenë viktimë apo është tentuar që t’i zbërthehet fjalëkalimi i e-mailit apo profilit në rrjetet sociale, që dëshmon që ky fenomen është gjithnjë më prezent dhe me trend rritës.

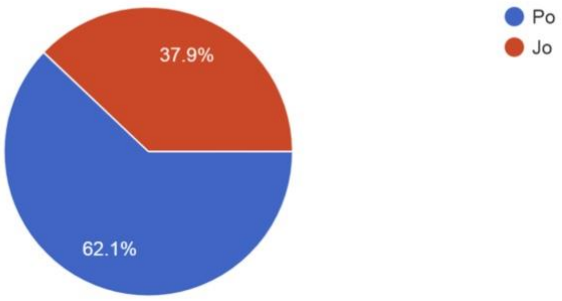


- Me pyetjen e lartëpërmendur lidhet edhe pyetja e radhës e anketës që ka për qëllim të hulumtojë se nëse veçmë personat kanë qenë viktimë e zbërthimit të fjalëkalimit të e-mailit apo profilit në rrjetet sociale, a u janë keqpërdorur të dhënat personale? Rezultatet dëshmojnë se 84.2% të rasteve nuk ka ndodhur një gjë e tillë, përderisa 15.8% të rasteve u janë keqpërdorur të dhënat personale, e dhënë që përdëfton vulnerabilitetin e secilit person përpara fenomenit të krimit kibernetik.

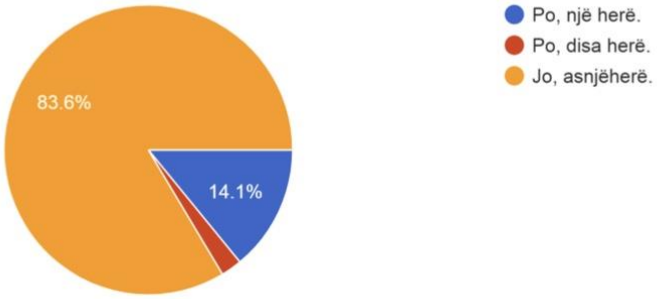


- Pyetja se “Përmes e-mailit apo rrjeteve sociale a ju ka ndodhur që identitete të panjohura (të paraqitura si lojëra shpërblyese, si mundësi investimi, si oferta...) të kërkojnë të

dhënat e juaja personale dhe bankare?" ka për qëllim që të arrihet tek rezultati se sa është i përhapur lloji i veçantë i krimit kribernetik – "phishing" dhe nga përgjigjet kuptohet se në masë të madhe është i përhapur tentimi për të kryer këtë vepër ndaj të anketuarve dhe se askush nuk është imun ndaj këtij lloj rreziku.



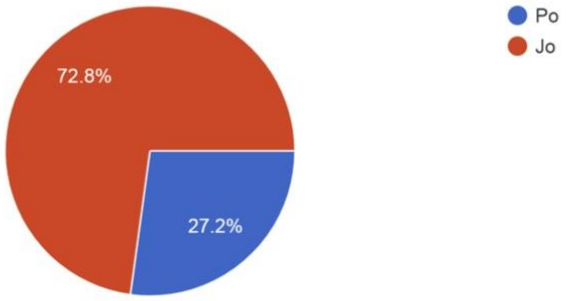
- Rrjedhimisht pason pyetja se sa prej të anketuarve bëhen viktimë e mashtrimeve të këtilla?



Konkluzat janë se 83.6% e të anketuarve nuk janë mashtruar, ndërsa 14.1% janë paraqitur si viktima një herë. Nuk duhet anashkaluar edhe personat që janë viktimizuar disa herë edhe pse janë në përqindje shumë të vogel (2.3%). Këto rezultate tregojnë se sa njerëzit biejnë pre e këtyre mashtrimeve për të cilat absolutisht duhet informim më i gjërë i qytetarëve që të mos

japin të dhënat personale dhe bankare pa u siguruar se për çka në të vërtetë bëhet fjalë, e kjo mund të arrihet përmes fushatave të ndryshme për ngritjen e vetëdijes kolektive.

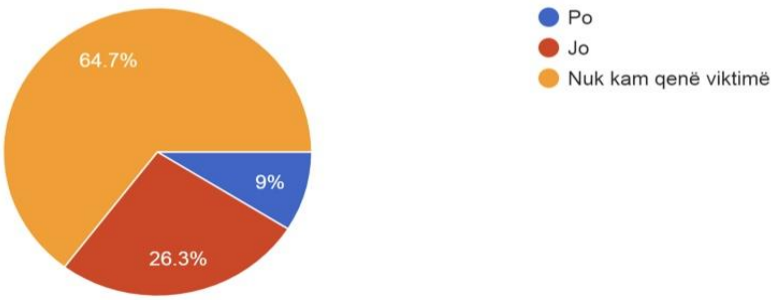
- Të anketuarit gjithashtu u pyetën sa i përket rrjeteve sociale, a ju ka ndodhur që me emrin apo fotografinë e tyre të hapen profile të rrejshme?



Përgjigjet e dhëna rezultuan që të kishin një numër të konsiderueshëm, e që përfshijnë 27.2% të personave, t'ju ketë ndodhur ky keqpërdorim që në mënyrë të drejtëpërdrejtë ka të bejë me vjedhjen e identitetit.

Pas konkludimit se llojet e krimeve kibernetike, disa më pak e disa më shumë, janë prezente në shoqërinë tonë, hulumtimi vazhdon të mirret me temën se si reagojnë të anketuarit ndaj këtyre krimeve dhe gjithashtu si reagojnë institucionet kompetente.

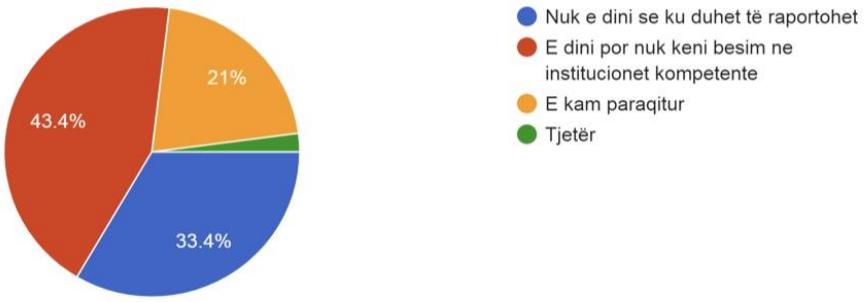
- Të anketuarit u pyetën se nëse eventualisht kanë qenë viktimë e cilit do lloj keqpërdorimi të lartëpërmendur, a e kanë paraqitur apo raportuar atë në institucionet kompetente? Përgjigjet e tyre ishin këto:



Sipas tyre 64.7% nuk kanë qenë viktimë, ndërsa 35.3% kanë qenë viktimë e këtij lloj krimi, prej të cilëve 9% e viktimave e kanë paraqitur veprën penale që ju ka ndodhur në organet kompetente, ndërsa alarmant është fakti që 26.3% e të anketuarve as nuk e kanë raportuar rastin që ju ka ndodhur. Kjo në njëjtën kohë tregon se numri i errët i krimeve kibernetike është mjaft i lartë.

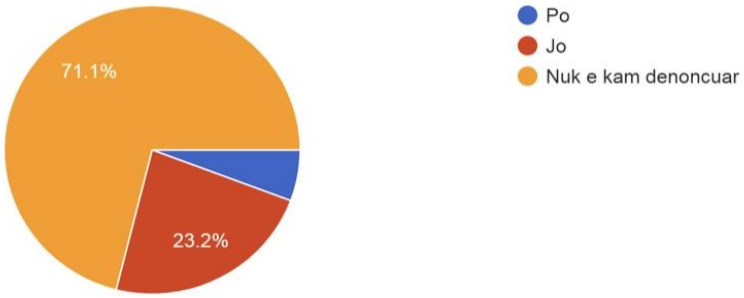
- Si rezultat i pyetjes paraprake, ne në pyetjen e rradhës u fokusuam në arsyen pse viktimat nuk e kanë denoncuar rastin në institucionet kompetente, duke ofruar si përgjigje: "nuk e dini se ku duhet të raportohet", "e dini por nuk keni besim në institucionet kompetente", "e kam paraqitur", dhe ndonjë "tjetër" arsye. Duhet të theksohet se këtë pyetje personat që nuk kanë qenë aspak viktima e kanë anashkaluar pa u përgjigjur, pra rezultatet rrjedhin vetëm nga numri i personave të dëmtuar.

.



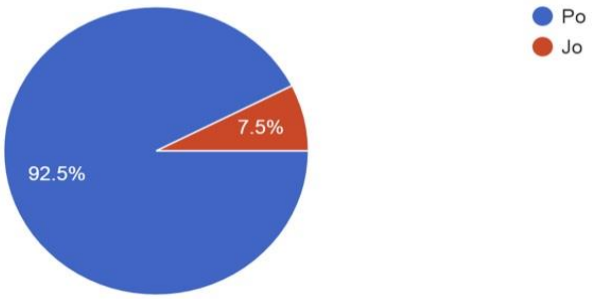
Siç shihet, përqindja më e lartë ka të bëjë me mosbesimin në institucionet kompetente(43.4%). Pas saj, 33.4% e të anketuarve viktima u përgjigjën se nuk kanë dijeni se ku duhet të raportohen rastet në fjalë, 21% e viktimave e kanë denoncuar rastin dhe përqindja më e ulët është për ata që nuk e kanë raportuar për ndonjë arsye tjetër. Përqindja e lartë e të anketuarve që kanë mosbesim në institucione dhe e atyre që nuk kanë dijeni se ku duhet të paraqiten krimet kibernetike, kërkojnë një trajtim të veçantë. Këto të dhëna qartë dëshmojnë se funksionimi i duhur të institucioneve lë për të dëshiruar, e nga ana tjetër mungon informimi i qytetarëve.

- Nga personat që e kanë denoncuar rastin në institucion kompetent, në anketë është kërkuar të përgjigjen se a kanë marrur përgjigje kthyese (a është trajtuar rasti nga ato organe, ose a janë kthyer të hollat apo a është fshirë profili i rrejshëm) ?



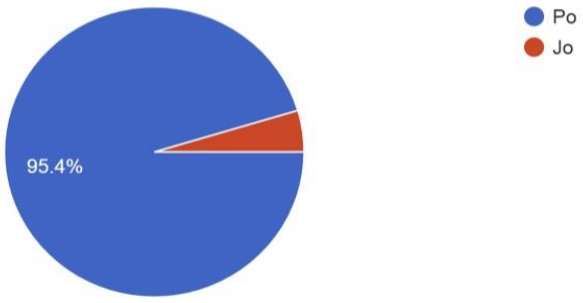
Rezultatet tregojnë që 71.1% nuk e kanë denoncuar fare rastin dhe pas saj me 23.2% janë deklaruar se nuk kanë marrur përgjigje kthyese. Ndërsa 5.7% kanë marrur përgjigje kthyese nga institucionet. Mos përgjigjja nga ana e institucioneve për rastet e krimit kibernetik, lejon të kuptohet se institucionet shtetërore nuk janë aq sa duhet të profesionalizuara në këtë drejtim dhe nuk i marrin me seriozitet këto lloje të krimeve, për të cilat nga deklarimet që u dhanë më lartë nga të anketuarit, shihet se janë në mjaft prezente dhe paraqesin rrezikshmëri për njerëzit.

- Për këto arsye në pyetjen se "A mendoni që institucionet kompetente duhet të jenë më të përgatitura në këtë drejtim (ligj i posaçëm, trajnim i posaçëm, punësim i ekspertëve në fushën e IT)?" të anketuarit u përgjigjën kështu:



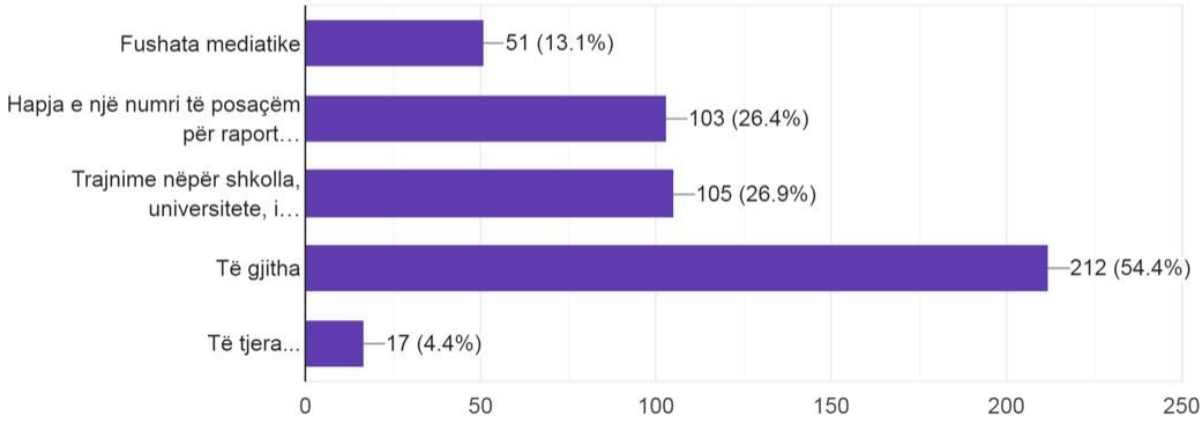
Shihet qartë se shumica prej 92.5% mendojnë dhe vlerësojnë se duhet të përmirësohet gjendja aktuale në vend lidhur me trajtimin e krimit kibernetik. Pra, duhet të miratohet ligj i veçantë, në departamentin për krim kibernetik të punësohen persona të profesionalizuar në këtë fushë, të mbahen trajnime me të punësuarit në institucionet kompetente për luftimin e krimit kibernetik etj.

- Në anketë u parashtrua pyetja se cili është mendimi i të anketuarve se a duhet të përpilohet fushatë e posaçme për informim dhe senzibilizim?



Përgjigjet e tyre, edhe në këtë pyetje ishin pozitive (95.4% po, 4.6% jo). Pra të anketuarit vlerësojnë se është e nevojshmë fushata për informim dhe senzibilizim të opinionit të gjërë.

- Në pyetjen e fundit të kësaj ankete, nga të anketuarit u kërkua të tregojnë, se nëse janë për përpilim të një fushate të posaçme, cilat nga veprimet e përmendura do ishin më të duhura: fushata mediatike, hapja e një numri të posaçëm për raportimin e rasteve të këtilla, trajnime nëpër shkolla, universitete, institucione për këto lloje të krimeve, të gjitha këto veprime, apo të tjera veprime?!



Në këtë pyetje, 212 persona apo 54.4% e të anketuarve kanë vlerësuar se të gjitha veprimet e përmendura duhet të ndërmirren, me 26.9% janë radhitur vetëm trajnimet nëpër shkolla, universitete dhe institucione, kurse me një diferencë shumë të vogël nga kjo është edhe vetëm hapja e numrit të posaçëm për raprtimin e krimeve kibernetike (26.4%).

Përfundime dhe rekomandime

Zhvillimet teknologjike, kompjuterët personal, telefonat e "mençur", interneti, sot luajnë një rol të madh në jetën e njerëzve. Ato kanë mundësuar lehtësim të dukshëm në shumë aspekte të ndryshme të përditshmërisë së çdo njeriu. Mirëpo, përveç të mirave të shumta siç janë kryerja e blerjeve të ndryshme nga web-faqet online, realizimi i pagesave të detyrueshme brenda sekondave, komunikimi më i lehtë dhe zhvillimi teknologjik, në të njejtën kohë paralelisht u paraqitën dhe u përhapën edhe forma të krimeve që nuk janë hasur më parë, një prej të cilëve është krimi kibernetik.

Për paraqitjen e krimit kibernetik ekzistojnë mendime të ndryshme. Mungon një qëndrim i unifikuar mes autorëve se në cilën periudhë shfaqet për së pari herë krimi kibernetik. Mirëpo, shumica e tyre theksojnë se krimi kibernetik më së shumti u përhap në kohën kur kompjuterët filluan të përdoreshin më shumë.

Në përpjekje për të dhënë një mendim autonom mbi krimin kibernetik, autori thekson se kjo është një formë e veçantë e krimit, në të cilën kompjuteri paraqitet si një mjet për të kryer veprim të paligjshëm ose si një objekt sulmi të drejtuar nga njerëz që kanë njohuri për sistemet kompjuterike, me qëllim që të sjellin përfitime për veten ose të tjerët.

Ne literaturë nuk ekziston një mendim i vetëm rreth tipologjisë së krimit kibernetik, mirëpo një ndarje që pranohet nga shumica e autorëve është ajo e teoreticientit David Wall, i cili krimin kibernetik e ndan në katër kategori, edhe atë: cyber-trespass apo shkeljet kibernetike, cyber-deceptions and thefts apo mashtrimet dhe vjedhjet kibernetike, cyber-pornography apo pornografia kibernetike dhe cyber-violence apo dhuna kibernetike. Në anën tjetër, aktet më të shpeshta nëpërmjet të cilave kryhet krimi kibernetik janë: mashtrimet përmes internetit, vjedhja e identitetit, hakingu (hacking), fishingu (phishing), viruset e ndryshme, ngacmimet kibernetike (cyber bulling) etj.

Arsyet pse dikush kryen një krim kibernetik mund të jenë po aq të ndryshme siç janë të ndryshëm vet njerëzit që kryejnë krimet. Disa nga shkaqet e ndryshme që ndikojnë në kryerjen

e krimeve kibernetike mund të jenë financiare, emocionale, intelektuale, kurioziteti, sjellja devijuese etj.

Në RMV, edhepse ka mungesë të madhe të ekspertëve në këtë fushë e njëkohësisht edhe mungesë të një ligji të veçantë në këtë drejtim, ekzistojnë dispozita të veçanta në Kodin Penal dhe ligje tjera që e inkriminojnë si vepër penale. Institucioni kompetent për ndjekjen e krimit kompjuterik është Departamenti për krim kompjuterik dhe forenzikë dixhitale i cili funkcionon në kuadër të Ministrisë së Punëve të Brendshme. Ky department përbëhet nga dy njësi, edhe atë: njësia për hetimin e krimit kompjuterik dhe njësia për forenzikë dixhitale.

Sa i përket rregullimit ndërkombëtar të krimit kibernetik, që nga vitet e 90-ta, shumë organe ndërkombëtare i kanë kushtuar vëmendje të madhe këtij lloji të krimit, duke miratuar akte të ndryshme për rregullimin e tij juridik. Në vitin 2001 u miratua akti më domethënës për krimin kibernetik. Kjo është Konventa për Krimin Kompjuterik, e miratuar nga Këshilli i Evropës, në Budapest. Kjo konventë është marrëveshja e parë ndërkombëtare me të cilën rregullohet lufta kundër krimit kibernetik, duke harmonizuar legjislacionin kombëtar, duke përmirësuar teknikat e hetimit dhe duke rritur bashkëpunimin midis shteteve. Konventa është nënshkruar nga 60 shtete dhe është ratifikuar nga 56 shtete dhe ka hyrë në fuqi në korrik 2004. Republika e Maqedonisë së Veriut ka nënshkruar dhe ratifikuar konventën për krimin kompjuterik.

Gjatë këtij hulumtimi është realizuar analizë e detajuar e legjislacioneve të disa shteteve në UE që ka të bëjë me krimin kibernetik. Ajo që dukshëm vërehet është se në shtetet siç janë Gjermania, Austria, Franca, Spanja, Holanda dhe Italia, funksionojnë institucione të posaçme për luftimin e krimit kibernetik, gjë që mungon në RMV. Gjithashtu, ndërkohë u konstatua se të gjitha këto shtete të lartëpërmendura kanë strategji nacionale për parandalimin e krimit kibernetik, strategji që fatkeqsisht mungojnë në legjislacionin e RMV-së.

Analiza komparative dëshmon se të gjitha shtetet kanë të parapara sanksionime të rënda për të gjitha llojet e krimit kibernetik pa dallim, duke veçuar legjislacionin e Francës, që parasheh sanksione shumë rigoroze.

Për dallim nga shtetet e analizuara të UE, nga hulumtimi i autorit dhe shqyrtimi i shumë aktgjykimeve nga Gjykata Themelore Shkupi I, konstatohet se politika ndëshkimore për veprat penale në fushën e krimit kibernetik në RMV, është mjaft e ulët në krahasim me vendet Evropiane, sidomos kur mirret parasysh fakti se këto vepra penale edhepse janë paraqitur rishtazi, ata kanë pasoja shumë të rënda dhe paraqesin rrezikshmëri të lartë shoqërore.

Sipas hulumtimeve të autorit, nga analiza e aktgjykimeve vërtetohet se në 90% të rasteve është shqiptuar masa alternative – dënim me kusht. Mendoj që me shqiptimin e sanksioneve të tilla për veprat e krimit kibernetik nuk ndikohet mjaftueshëm tek kryerësit e këtyre veprave që të mos paraqiten si recidivist si dhe nuk ndikohet pozitivisht në planin e prevenimit gjeneral me të cilin arrihet qëllimi i ndëshkueshmërisë, që do të thotë ndëshkimet ndaj krimeve kibernetike duhet të jenë më rigoroze dhe më të larta.

Në anketën e realizuar nga autori, ku janë anketuar një numër i madh i të anketuarve të profileve të ndryshme profesioanle, etnike, të moshës etj., mund të vërehet qartë se një numër i madh i të anketuarve janë përdorues të kartelave bankare dhe me të njejtat shumica kryejnë pagesa online, gjithashtu 78.7% deklaruan që janë përdorues edhe të e-mailit edhe të rrjeteve sociale, që do të thotë që të njejtat janë bërë pjesë e përditshmërisë e një pjese të madhe të njerëzve, rrjedhimisht me këtë ata bëhen edhe target potencial për kryerësit e krimeve kibernetike. Vulnerabilitetin e të anketuarve në këtë drejtim e dëshmon fakti që diku 35.7% kanë qenë viktimë e zbërthimit të fjalëkalimit të e-mailit ose profilit në rrjetet sociale.

Personat e anketuar i shfrytëzojnë shërbimet e bankave për pagesa online, edhepse në pyetjen rreth sigurisë së këtyre pagesave, mendimet i kanë të ndara, ku 31.6% mendojnë që ky aktivitet nuk është aq i sigurt, derisa 24.6% i të anketuarve mendojnë se ky aktivitet nuk është fare i sigurtë. Këtë e vërteton fakti që rreth 18.2% e të anketuarve kanë deklaruar që në të kaluarën kanë qenë viktimë e një mashtrimi potencial gjatë kryerjes së një pagese online, fakt që dëshmon që institucionet kompetente duhet të merren në mënyrë thelbësore me këtë fenomen gjithnjë e më prezent.

Nga anketa e realizuar për qëllimet e këtij hulumtimi, qartë mund të konstatohet që mes llojeve të ndryshme të krimit kibernetik, më i përhapur në RMV rezulton të jetë vjedhja e identitetit. Këtë e vërteton e dhëna se rreth 27.2% të të anketuarve ju ka ndodhur që t`ju vidhet ose keqpërdoret identiteti në rrjetet sociale.

Shqetësues është rezultati që del nga anketimi, se nga viktimat e krimit kibernetik gatise ¾ e tyre as nuk e kanë raportuar në organet kompetente rastin që ju ka ndodhur, ndërsa vetëm ¼ e kanë raportuar. Me këtë mund të konstatohet se numri i errët i krimeve kibernetike është mjaft i lartë. Ajo që del në pah është se arsyeja pse të anketuarit nuk e raportojnë këtë lloj krimi është se 43.4% nuk kanë besim tek institucionet kompetente, që dëshmon kredibilitetin jashtëzakonisht të rrënuar të institucioneve, 33.4% fare nuk e dijnë se ku duhet të raportohet, dhe vetëm 21% rastet e tilla i kanë raportuar.

Nga të anketuarit të cilët kanë raportuar në institucionet kompetente se kanë qenë viktimë e krimit kibernetik, shumica e tyre nuk kanë marur përgjigje kthyese, rrjedhimisht afër 93% e të anketuarve nuk janë të kënaqur me punën e tanishme të institucioneve kompetente dhe kërkojnë të përpilohet ligj i posaçëm, trajnim i posaçëm, punësim i ekspertëve në fushën e IT etj., ndërsa 95.6% mendojnë që është e nevojshmë të fillojë fushatë speciale për informim dhe senzibilizim të opinionit të gjërë rreth kësaj tematike, ku do të përfshiheshin fushata mediatike, hapja e një numri të posaçëm për raportimin e rasteve të këtilla, trajnime nëpër shkolla, universitete, institucione etj.

Rezultatet nga hulumtimi i kryer rreth krimit kibernetik, bëjnë që të sjellet përfundimi se janë të nevojshme masa dhe aktivitete shtesë për përmirësimin e gjendjes aktuale, me të cilat sistemi do të funksionojë në mënyrë shumë më efikase dhe transparente. Masat dhe aktivitetet e propozuara i prezentojmë në disa drejtime, edhe atë:

- Edhepse ekzistojnë dispozita të veçanta në Kodin Penal dhe ligje tjera që e inkriminojnë krimin kibernetik si vepër penale, nevojitet ligj i veçantë për krimin kibernetik me qëllim që legjislacioni të jetë më i qartë dhe rrjedhimisht më rigoroz në përndjekjen e këtij fenomeni.

- Nevojitet institucion i posaçëm që do të merret me zbulimin e krimit kibernetik, pasiqë hulumtimi ka dëshmuar se ekzistimi i vetëm një departamenti në kuadër të MPB-së nuk është aspak i mjaftueshëm.
- Duke pasur parasysh se nga hulumtimi i aspekteve krahasimore të shteteve të UE-së, u konstatua se janë shumë më efikas në përndjekjen e krimit kibernetik, RMV duhet të përvetësojë praktikën dhe përvojën e tyre në drejtim të përpilimit të strategjive nacionale dhe shtërngimit të masave ndëshkuese ndaj kryerësve të krimit.
- Në bashkpunim me institucionet kompetente dhe sektorin bankar, të ngritet siguria në fushën e pagesave online.
- Sipas hulumtimit të autorit, duhet përkushtuar vëmendje të veçantë rasteve të raportuara në institucionet kompetente për vjedhje të identitetit në rrjetet sociale, si lloj i krimit kibernetik i cili është më së shumti prezent në RMV.
- Duke pasur parasysh faktin se shumica e viktimave të krimit kibernetik nuk e raportojnë rastin në organet kompetente, duhet të fillohet me fushatë të gjërë gjithëpërfshirëse në drejtim të informimit dhe senzibilizimit të opinionit për elaborim se sa i rëndësishëm është procesi i paraqitjes së këtyre rasteve.
- Pasiqë ky hulumtimi dëshmon se një përqindje e lartë e viktimave që nuk e kanë denoncuar krimin për shkak të mosbesimit në institucionet kompetente, ndërsa viktimat që e kanë denoncuar krimin në të shumtën e rasteve nuk kanë marur përgjigje kthyese nga institucioni, duhet që fillimisht të punësohen profesionistë të fushave përkatëse, punën e tyre ta kryejnë në mënyrë të përgjegjshme dhe profesionale, të ndërtohet sistem i detajizuar i funksionimit, e gjithë kjo me qëllimin e vetëm për ngritjen e besueshmerisë së rrënuar të qytetarit karshi insitucionit kompetent.
- Të ndërmerren aktivitete konkrete në këtë drejtim, si vijon: trajnime nëpër shkolla, universitete dhe insitucione, hapja dhe shpërndarja e një numri të posaçëm nga institucioni kompetent në të cilin viktimat lehtësisht do të mund ta paraqesin rastin e tyre, si dhe fushatë të gjërë mediatike për informimin dhe senzibilizimin e opinionit të gjërë për rrezikun që vjen nga ky lloj krimi.

Bibliografia

Ачковски Југослав, “Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам”, Shkup, 2012

Ayofe, Azeez Nureni, and Barry Irwin. "CYBER SECURITY: CHALLENGES AND THE WAY FORWARD." Computer Science & Telecommunications 29, 2010

Brenner, Susan W., “Cybercrime Criminal Threats from Cyberspace” California, 2010,

Calderoni, Francesco, “The European legal framework on cybercrime: striving for an effective implementation”. Crime, law and social change, 2010.

Clough, Jonathan, "Principles of Cybercrime." New York, 2010

Conteh, Nabie Y., and Paul J. Schmick. "Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks." *International Journal of Advanced Computer Research* 6, 2016.

EDWARDS , Graeme, “Cybercrime Investigators Handbook” New Jersey, 2020

EUROPOL ,” Child Sexual Exploitation Fact Sheet 2011”

Glenny, M. “Darkmarket: How ackers became the new mafia” 2012;

Goppinger, Hans, “Kriminologie”, Munchen, 1997

Halili, Ragip, “Kriminologjia”, Prishtinë, 2011

Ilves, L. K., Evans, T. J., Cilluffo, F. J., & Nadeau, A. A. “European Union and NATO Global Cybersecurity Challenges”. Prism, 2016.

Jovaševič D., Leksikon krivicnog prava, JP Sluzbeni list, Beograd

Kambovski, Vlado, E drejta penale – pjesa e përgjithshme (përkthim), 2004

Kambovski, Vlado, Komentar na Krivicniot Zakonik na Republika Makedonia,botimi i dytë, Shkup, 2015

Kambovski, Vlado, & Zejneli.I, E drejta penale-Tetovë, 2018

Keyser, M. “The Council of Europe Convention on Cybercrime. In Computer Crime”. Routledge; 2017.

Këshilli Evropian, “National legislation implementing the Convention on Cybercrime- Comparative analysis and good practices”

Këshilli Evropian, “The practical implementation and operation of European policies on prevention and combating cybercrime - Report on Germany”, Bruksel, 2017

Koops, Bert-Jaap, “Cybercrime Legislation in the Netherlands” 2010

Kshetri , Nir, “Cybercrime and Cybersecurity in the Global South” , SHBA, 2013

Latifi,Vesel, Kriminalistika- Zbulimi dhe të provuarit e krimit, Botimi i gjashtë, Prishtinë, 2009

Latifi, Vesel, “Kriminalistika”, Prishtinë, 2014

Mendez, F. “The European Union and cybercrime: insights from comparative federalism”. Journal of European Public Policy, 2005.

Moitra, S. Developing policies for cybercrime. European Journal of Crime, Criminal Law and Criminal Justice, 2005.

Parker, Don, ”Fighting computer crime”, New York, 1985

Pocar, F. “New challenges for international rules against cyber-crime”. European Journal on Criminal Policy and Research, 2004.

Ponti, Gianluigi, “Compendio di Criminologia”, Milano, 1997

Pradillo, J. C. O. Fighting against cybercrime in Europe: the admissibility of remote searches in Spain. Eur. J. Crime Crim. L. & Crim. Just., 2011.

Raporti për Siguri Kibernetike të Austrisë i vitit 2019, (file:///C:/Users/User/Downloads/EN-Cybersicherheit_Bericht_2019.pdf)

Schell ,Bernadette H. and Martin, Clemens, “CYBERCRIME” , SHBA, 2004

Shinder, Debra Littlejohn, and Michael Cross. “Scene of the Cybercrime”, 2008

Sulejmanov,Zoran, “Македонска Криминологија”, Shkup, 2000

Tokunaga, Robert S. "A critical review and synthesis of research on cyberbullying victimization." -Computers in human behavior- 2010

Virtanen, S. M. “Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities”. Psychiatry, Psychology and Law, 2017.

Vula, Veton,”Krimi kompjuterik”, Prishtinë, 2010

Yar, Majid, “Cybercrime and Society” London, 2006,

Wall, David, ”Crime and the Internet”, London, 2001,

Wall, David, “Cybercrime: The transformation of crime in the information age”, Cambridge, 2007

Zejneli, Ismail. Sahiti, Ejup. E drejta e procedurës penale e Republikës së Maqedonisë, Shkup, 2017

Tekste ligjore:

Kushtetuta e RMV-së;

Kodi Penal i RMV-së (Gazeta Zyrtare e RMV-së nr. 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 50/2006, 60/2006, 73/2006, 87/2007, 7/2008, 139/2008, 114/2009, 51/2011, 51/2011, 135/2011, 185/2011, 142/2012, 143/2012, 166/2012, 55/2013, 82/2013);

Ligji për procedurë penale të RMV-së (Gazeta Zyrtare e RMV-së nr. 150/2010, 100/2012);

Ligji për ratifikimin e Konventës për krimin e kompjuterëve;

Ligjin për komunikime elektronike (Gazeta Zyrtare e RMV-së nr.13/2005, 14/2007, 55/2007, 98/2008, 83/2010, 13/2012, 59/2012, 123/2012, 23/2013);

Ligjin për ndjekje të komunikimeve (Gazeta Zyrtare e RMV-së nr. 121/2006, 110/2008, 4/2009, 116/2012);

Ligjin për tregtinë elektronike (Gazeta Zyrtare e RMV-së nr. 133/2007, 17/2011);

Ligjin për udhëheqjen elektronike (Gazeta Zyrtare e RMV-së nr. 105/2009, 47/2011);

Ligjin për shërbimin gjyqësor (Gazeta Zyrtare e RMV-së nr. 79/2005, 110/2008, 83/2009, 116/2010);

Ligjin për të dhënat në formë elektronike dhe nënshkrimin elektronik (Gazeta Zyrtare e RMV-së nr. 34/2001, 98/2008);

Deklaratën për internet më të sigurt;

Doracak për krimin kompjuterik;

"Convention on Cybercrime", Këshilli i Evropës, Budapest, 2001.

Burime nga interneti:

Convention on Cybercrime: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (qasja e fundit 10.02.2020);

United Nations "Definiton of cybercrime" 2014: https://idn-wi.com/united-nations-definition-cybercrime/ (qasja e fundit 10.02.2020);

Cybersecurity CEO: The history of cybercrime, from 1834 to Present: https://cybersecurityventures.com/cybersecurity-ceo-the-history-of-cybercrime-from-1834-to-present/ (qasja e fundit më 16.02.2020);

The 16 most common types of cybercrime acts, 2018: https://www.voipshield.com/the-16-most-common-types-of-cybercrime-acts/ (qasja e fundit më 18.02.2020);

Identity theft is more rampant now than ever—here's how to prevent It: https://www.readersdigest.ca/home-garden/money/identity-theft-europe/ (qasja e fundit më 18.02.2020);

Hacked European Cables, 2018: https://www.nytimes.com/2018/12/18/us/politics/european-diplomats-cables-hacked.html (qasja e fundit më 19.02.2020);

EUROJUST:20 hackers arrested in EUR 1 million bank phishing scam,2018: http://www.eurojust.europa.eu/press/PressReleases/Pages/2018/2018-03-29.aspx (qasja e fundit më 19.02.2020);

ENISA "What is malware?": https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/malware (qasja e fundit më 19.02.2020);

Panda Security "What is software piracy?": https://www.pandasecurity.com/mediacenter/panda-security/software-piracy/ (qasja e fundit më 19.02.2020);

Chart of signatures and ratifications of Treaty 185: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (qasja e fundit më 24.02.2020);

Doracak për krimin kompjuterik: https://www.osce.org/sq/skopje/121225?download=true (qasja e fundit më 24.02.2020);

EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001F0413 (qasja e fundit më 24.02.2020);

Official Journal of the European Union- Directives, 2009: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF (qasja e fundit më 24.02.2020);

EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093 (qasja e fundit më 24.02.2020);

Official Journal of the European Union –Directive 2013/40/EU: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF (qasja e fundit më 24.02.2020);

EUROPOL-EC3, (https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3) (qasja e fundit më 24.02.2020);

European Union Agency for Cybersecurity (ENISA): https://europa.eu/european-union/about-eu/agencies/enisa_en (qasja e fundit më 05.03.2020);

Cyber attacks cost German industry almost $50 billion: study: https://www.reuters.com/article/us-germany-security-cyber/cyber-attacks-cost-german-industry-almost-50-billion-study-idUSKCN1LT12T (qasja e fundit më 05.03.2020);

Cybercrime Laws:Germany: https://www.cybercrimelaw.net/Germany.html (qasja e fundit më 06.03.2020);

Germany: Subersecurity 2020: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany (qasja e fundit më 06.03.2020);

Germany: Subersecurity 2020: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany (qasja e fundit më 06.03.2020);

Austria: Cybercrime And Protection Under Criminal Law, 2019: https://www.mondaq.com/austria/crime/874318/cybercrime-and-protection-under-criminal-law (qasja e fundit më 10.03.2020);

Austria: Cybercrime: (https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/austria/pop_up?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=print&_101_INSTANCE_hFPA5fbKjyCJ_languageId=fi_FI) (qasja e fundit më 12.03.2020);

Austrina: Report Cyber Security 2019,(file:///C:/Users/User/Downloads/EN-Cybersicherheit_Bericht_2019.pdf) (qasja e fundit më 12.03.2020);

Austrina: Report Cyber Security 2019, (file:///C:/Users/User/Downloads/EN-Cybersicherheit_Bericht_2019.pdf) (qasja e fundit më 13.03.2020);

Cybersecurity news and views: Ransomware is a real problem in France, (https://portswigger.net/daily-swig/ransomware-is-a-real-problem-in-france) (qasja e fundit më 18.03.2020);

France-Cybercrime, (https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/france/pop_up?inheritRedirect=false) (qasja e fundit më 18.03.2020);

France:Cybersecurity 2020, (https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/france) (qasja e fundit më 20.03.2020);

French Expert Center Against Cybercrime (CECyF) (https://www.cybersecurityintelligence.com/french-expert-center-against-cybercrime-cecyf-2816.html)(qasja e fundit më 21.03.2020);

ANSSI: A WORD FROM THE DIRECTOR GENERAL, (https://www.ssi.gouv.fr/en/mission/word-from-director-general/) (qasja e fundit më 21.03.2020);

ANSSI:Cybersecurity strategy, (https://www.ssi.gouv.fr/en/cybersecurity-in-france/cybersecurity-strategy/) (qasja e fundit më 23.03.2020);

France and Cyber security, (https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/) (qasja e fundit më 23.03.2020);

Cybersecurity in Spain,2019, (https://cybernews.com/security/cybersecurity-in-spain/) (qasja e fundit më 24.03.2020);

Statista: Court proceedings of cybercrime in Spain in 2017, (https://www.statista.com/statistics/463628/cybercrime-type-figures-spain/) (qasja e fundit më 25.03.2020);

Spain: Cybersecurity laws and regulations, (https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/spain) (qasja e fundit më 26.03.2020);

Spain: Cybercrime laws, (https://www.cybercrimelaw.net/Spain.html) (qasja e fundit më 27.03.2020);

Cybernews: Cybersecurity in Spain, (https://cybernews.com/security/cybersecurity-in-spain/) (qasja e fundit më 28.03.2020);

CNPIC: Cybersecurity, (http://www.cnpic.es/en/Ciberseguridad/index.html) (qasja e fundit më 28.03.2020);

Bsa: Cybersecurity Spain, (http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_spain.pdf) (qasja e fundit më 28.03.2020);

Enisa:Spanish National cybersecurity strategy, (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy) (qasja e fundit më 28.03.2020);

Netherlands: Cybercrime, (https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/netherlands/pop_up?inheritRedirect=false) (qasja e fundit 02.04.2020);

Cyberwiser: Netherlands (https://www.cyberwiser.eu/netherlands-nl) (qasja e fundit më 02.04.2020);

CyberSecurity Intelligence: DITSS, (https://www.cybersecurityintelligence.com/dutch-institute-for-technology-safety-and-security-ditss-3038.html) (qasja e fundit më 02.04.2020);

Statista: cybercrime in Italy in 2017 and 2018, (https://www.statista.com/statistics/1032488/cybercrime-cost-italy/) (qasja e fundit më 05.04.2020);

Council of Europe: Cybercrime in Italy (https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/italy?inheritRedirect=false&redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Foctopus%2Fcountry-wiki%3Fp_p_id%3D101_INSTANCE_hFPA5fbKjyCJ%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-4%26p_p_col_count%3D1) (qasja e fundit më 05.04.2020);

Italian Criminal legislation concerning ICTs, (http://www.studiolegalegaldieri.com/articoli-e-relazioni/italian-criminal-legislation-concerning-icts/) (qasja e fundit më 06.04.2020);

Italy's National Strategic Framework for Cyberspace Security, (file:///C:/Users/User/Downloads/IT_NCSS_en%20(1).pdf) (qasja e fundit më 06.04.2020);