DORACAK
PËR KRIMIN
KOMPJUTERIK

Janar 2014

Autorë:

Marko Zvërlevski, *Prokuror publik i Republikës së Maqedonisë*

Spasenka Andonova, *Prokurore publike në Prokurorinë themelore publike për ndjekjen e krimit të organizuar dhe korrupsionit*

Vladimir Millosheski, *Prokuror publik në Prokurorinë themelore publike për ndjekjen e krimit të organizuar dhe korrupsionit*

Redaktorë:

Ana Novakova Zhikova, *Zyrtare nacionale për sundimin e të drejtës, Misioni i OSBE-së në Shkup*

Igor Risteski, *Asistent programor, Misioni i OSBE-së në Shkup*

Tirazhi: *200 kopje*

Shtypi: *Skenpoint, Shkup*

CIP - Каталогизација во публикација
Национална и универзитетска библиотека „Св. Климент Охридски", Скопје
343.533.9:009.7(035)

ZVËRLEVSKI, Marko

Doracak për krimin kompjuterik / [autorë Marko Zvërlevski, Spasenka Andonova, Vladimir Millosheski]. - Shkup : OSBE, 2014. - 60 стр. : илустр. ; 24 см
Фусноти кон текстот. - Содржи и: Shtojca 1-2

ISBN 978-608-4630-72-2
1. Andonova, Spasenka [автор] 2. Millosheski, Vladimir [автор]
а) Компјутерски криминалитет - Софтверски измами - Прирачници
COBISS.MK-ID 96196618

Поддржано од:

OSCE Organization for Security and Co-operation in Europe
Mission to Skopje

PËRMBAJTJA

HYRJE

Prokuroria ka rol të rëndësishëm në hulumtimin, zbulimin dhe nxjerrjen para drejtësisë së individëve ose grupeve që kanë kryer vepra penale. Në kushte kur ka rritje të shpejtë të veprimeve kundërligjore, veçanërisht të atyre që përmbajnë elemente kompjuterike (cyber), gjithnjë e më e domosdoshme është nevoja për edukim adekuat që të mund të kuptohet natyra e vërtetë e këtij lloji të krimit.

Në një kohë kur përdorimi i kompjuterëve dhe i aparateve elektronike në jetën e përditshme është gjithnjë e më i madh, jurisprudenca, në nivel global, gjithnjë e më shumë fillon t'i kushtojë rëndësi kësaj dukurie.

Fokusi i këtij Doracaku është i orientuar në disa aspekte, e para së gjithash në fenomenologjinë e komunikimit elektronik dhe në zëvendësimin e sistemit konvencional të ndjekjes së informatave me një sistem të ri, i cili mundëson transfer të sasive të mëdha të të dhënave në distancë të madhe në mënyrë më të shpejtë dhe më efikase. E gjithë kjo, pa dyshim, e përmirëson kualitetin e jetesës, por nga ana tjetër paraqet fushë në të cilën, në mënyrë shumë më të thjeshtë, mund të kryhen veprime joligjore. Pikërisht ky segment i dytë zgjon interes të madh te publiku që merret me materien juridike penale. Në fakt, tani hapen çështje të tjera që në fazat më të hershme të procedurës penale dhe të mbledhjes së provave. Kryerësit e këtij lloji të krimit aspak nuk janë të kufizuar në kufinjtë shtetërorë, e me këtë edhe kompetenca e çdo vendi vihet në pikëpyetje në momentin e mbledhjes së të dhënave. E gjithë kjo paraqet një sfidë shumë më të vështirë për prokurorët publikë gjatë realizimit të procedurës. Ndërlikueshmëria e këtij lloji të krimit, veçanërisht evoluimi i vazhdueshëm i mënyrave dhe i formave të kryerjes së veprimeve kundërligjore kërkon zhdërvjelltësi dhe gatishmëri të vazhdueshme të prokurorëve gjatë veprimit të përditshëm praktik.

Ky Doracak nuk ka për qëllim të japë udhëzime për veprim hap pas hapi, por ideja është që të ofrohet një vegël e dobishme – udhëzues që do të përmbajë terme që do ta lehtësojnë identifikimin e mjeteve me të cilat kryhet ky lloj i kriminit, lloji i provave që duhet të sigurohen, si dhe mënyra e drejtë e sigurimit të tyre, me çka do të lehtësohet procesi i vërtetimit të provave.

Provat tradicionale kanë formë fizike, për shembull: dokumente të ndryshme, fotografi, sende dhe gjurmë të tjera që janë dukshme fizikisht dhe që lehtë mund të gjenden dhe të mblidhen si prova. Nga ana tjetër, provat elektronike, edhe pse nuk kanë ndonjë formë të dukshme, për nga fuqia e tyre dëshmuese nuk dallojnë shumë nga ato që konsiderohen si tradicionale. Ato shumë shpesh gjenden në vende në të cilat, vetëm njerëz që janë të trajnuar në mënyrë të veçantë mund t'i zbulojnë dhe t'i sigurojnë ato, dhe në atë mënyrë të fitojnë vlerë relevante para organeve të gjyqësisë. Njëra nga veçoritë e të dhënave digjitale është mundësia që ato të sigurohen në numër të pakufizuar dhe gjatë kësaj çdo kopje në fakt është origjinal. Çdo pajisje elektronike ka karakteristika të saja të veçanta që e imponon nevojën të zbatohet edhe procedurë specifike me qëllim që të sigurohet

hyrje në memorjen ku ruhen provat elektronike, dhe gjatë kësaj ato të mbeten të pakompremetuara.

Bashkëpunimi ndërinstitucional paraqet segment të rëndësishëm të cilit duhet t'i kushtohet rëndësi e veçantë, para së gjithash për shkak të thjeshtësimit dhe operacionalizimit të nevojave të prokurorit publik për t'i mbledhur provat relevante dhe mundësisë që ato t'i dorëzohen atij në afat sa më të shkurtër.

Prej këtu doli edhe motivi kryesor për përgatitjen e një Doracaku të këtillë, ku do të futen parametrat kryesorë që duhet të merren parasysh gjatë shqyrtimit të lëndëve juridike penale, ku trajtohen vepra penale nga fusha e krimit kompjuterik, por edhe për të gjitha veprat e tjera penale ku duhet të sigurohen prova të cilat, në formë burimore ose derivate, janë në formë elektronike.

1. ZHVILLIMI HISTORIK I LEGJISLACIONIT

Nevoja për barazimin dhe sistematizimin në nivel global të normave materiale dhe procedurale nga fusha e krimit kompjuterik dhe provave elektronike, është shprehur edhe në Konventën për krimin kompjuterik[1] të Këshillit të Evropës (në vazhdim të tekstit: Konventa). Edhe pse më parë ka pasur përpjekje për definimin e normave materiale që e rregullojnë bashkëpunimin juridik ndërkombëtar, megjithatë Konventa, për nga përfshirja e gjerë, fleksibiliteti dhe mundësia për inkorporim të lehtë në legjislacionet nacionale, edhe pse fillimisht e dedikuar për vendet evropiane, u bë mekanizëm për komunikim të lehtë ndërmjet vendeve nga e gjithë bota.

Me Konventën për krimin kompjuterik më vonë u ndërlidhën edhe Konventa për mbrojtjen e të dhënave personale gjatë procesit të automatizuar për përpunimin e të dhënave personale[2] me amandamentet e saj dhe Protokolli shtesë për qarkullim të autorizuar të të dhënave personale jashtë vendit[3], Protokolli shtesë i Konventës për krimin kompjuterik për mbrojtje nga racizmi dhe ksenofobia[4], Konventa për mbrojtjen e fëmijëve nga eksploatimi seksual dhe keqtrajtimi seksual[5] dhe Direktivat e BE-së.

Këshilli i Evropës e miratoi Konventën për krimin kompjuterik në Budapest më 23.11.2001. Gjithsej 58 vende e kanë nënshkruar Konventën, prej të cilave 28 me ratifikim. Konventa u nënshkrua nga ana e vendit tonë më 23.11.2001, u ratifikua më 15.09.2004, ndërsa hyri në fuqi më 01.01.2005.

Konventa përmban norma materiale, procedurale dhe norma për bashkëpunim ndërkombëtar. Dispozitat nga fusha e të drejtës materiale kanë të bëjnë me: hyrjen e paligjshme, interceptimin e paligjshëm, interferencën e të dhënave, interferencën e sistemeve, 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.

Dispozitat e definuara në këtë mënyrë janë futur edhe në legjislacionin material të Maqedonisë, edhe atë në pjesën e dispozitave të përgjithshme ku janë përkufizuar termet kryesore për këtë lloj të krimit, si dhe veprat konkrete penale. Korniza juridike e vendit që e rregullon fushën e krimit kompjuterik e përfshin:

[1] Shih: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[2] Shih: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
[3] Shih: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&CM=8&NT=181
[4] Shih: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm
[5] Shih: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=201

- Kodin Penal (KP)[6]
- Ligjin për procedurë penale (LPP)[7]
- Ligjin për komunikime elektronike[8]
- Ligjin për ndjekje të komunikimeve[9]
- Ligjin për tregtinë elektronike[10]
- Ligjin për udhëheqjen elektronike[11]
- Ligjin për shërbimin gjyqësor[12]
- Ligjin për të dhënat në formë elektronike dhe nënshkrimin elek tronik[13]
- Deklaratën për internet më të sigurt

Në suaza botërore ekzistojnë disa parime të inkorporimit të këtyre normave në legjislacionet vendore, për shembull në Rumani dhe në Tahiti normimi i kësaj problematike është bërë me ligj të veçantë ku janë përfshirë edhe dispozita juridike materiale dhe procedurale, plotësisht të ndara nga ligjet konvencionale ndëshkuese.

Legjislacioni vendor e ruan qasjen kontinentale dhe normat që e rregullojnë këtë materie janë përfshirë në ligjet ekzistuese, duke mbajtur llogari gjatë kësaj për mbrojtjen e të drejtave themelore të njeriut në lidhje me të drejtën për lirinë e të shprehurit dhe lirinë e të menduarit dhe të drejtën e privatësisë.

Edhe përkundër asaj se krimi kompjuterik paraqet materie që vazhdimisht ndryshon dhe ka risi që nuk mund të përkufizohen në mënyrë të thjeshtë (teknologjitë e reja në telefoninë celulare, zbatimi i masave të veçanta hetuese etj.), edhe atë veçanërisht kur bëhet fjalë për komunikimin tradicional, megjithatë Konventa në tërësi është inkorporuar në legjislacionin tonë. Në këtë mënyrë mundësohet bashkëpunim më i lehtë ndërkombëtar, si dhe krijohen mundësi për përshtatjen e lehtë të dispozitave përkatëse me format e reja të këtij lloji të krimit.

[6] Gazeta zyrtare e RM-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
[7] Gazeta zyrtare e RM-së nr.150/2010, 100/2012
[8] Gazeta zyrtare e RM-së nr.13/2005, 14/2007, 55/2007, 98/2008, 83/2010, 13/2012, 59/2012, 123/2012, 23/2013.
[9] Gazeta zyrtare e RM-së nr.121/2006, 110/2008, 4/2009, 116/2012
[10] Gazeta zyrtare e RM-së nr.133/2007, 17/2011
[11] Gazeta zyrtare e RM-së nr.105/2009, 47/2011
[12] Gazeta zyrtare e RM-së nr. 79/2005, 110/2008, 83/2009, 116/2010
[13] Gazeta zyrtare e RM-së nr.34/2001, 98/2008

➢ ***E drejta materiale***

- *Kodi penal*[14]

Dispozitat materiale për veprat penale nga fusha e krimit kompjuterik janë të përfshira në KP dhe kanë të bëjnë me:

- nenin 144 - Rrezikimi i sigurisë
- nenin 147 - Dhunimi i fshehtësisë së letrave ose i dërgesave të tjera
- nenin 149 - Keqpërdorimi i të dhënave personale
- nenin149-a - Pengimi i hyrjes në sistem informatik publik
- nenin 157 - Dhunimi i të drejtës së autorit dhe i të drejtave të tjera të lidhura me të
- nenin 157-a - Dhunimi i të drejtës së distributorit të sinjalit satelitor të mbrojtur në mënyrë të veçantë
- nenin 157-b - Piratëria e një vepre audiovizuale
- nenin 157-c - Piratëria e fonogramit
- nenin 193 - Tregimi i materialit pornografik ndonjë fëmije
- nenin 193-a - Prodhimi dhe shpërndarja e pornografisë së fëmijëve
- nenin 193-b – Mashtrimi i të miturit që nuk ka mbushur 14 vjet për të kryer marrëdhënie seksuale ose ndonjë veprimi tjetër seksual me të
- nenin 251 - Dëmtimi ose hyrja e paligjshme në sistem kompjuterik
- nenin 251-a – Përgatitja dhe futja e virusëve kompjuterikë
- nenin 251-b - Mashtrimi kompjuterik
- nenin 271 - Përgatitja, blerja ose tëhuajësimi i mjeteve për falsifikim

[14] Teksti integral i dispozitave të Kodit Penal që kanë të bëjnë me krimin kompjuterik është bashkangjitur me këtë Doracak si Shtojcë e veçantë 1 (shih faqen 34)

- nenin 274-b - Përgatitja dhe përdorimi i kartelës së rrjeshme për pagesë
- nenin 279-a - Falsifikimi kompjuterik
- nenin 286 - Dhunimi i të drejtës për ndonjë zbulim të regjistruar ose të mbrojtur dhe topografia e qarqeve integrale
- nenin 394-d - Shpërndarja e materialit racist dhe ksenofob nëpërmjet sistemit kompjuterik
- nenin 122 - Përkufizimi i segmenteve kryesore të krimit kompjuterik:

  pika 15 **kartelat për pagesë** - Me kartelë për pagesë nënkuptohet çdo lloj i mjeteve për pagesë, e cila është lëshuar nga institucionet bankare ose ndonjë institucion tjetër financiar, që përmban të dhëna elektronike për njerëzit dhe numra të gjeneruar në mënyrë elektronike, me të cilat mundësohet kryerja e çfarëdo lloji të transaksionit financiar;

  pika 24 **pornografia e fëmijëve** – Me pornografi të fëmijëve nënkuptohet materiali pornografik, i cili në mënyrë vizuale tregon veprime të qarta seksuale me ndonjë të mitur ose person të rritur që duket si i mitur, ose e paraqesin të miturin ose personin e rritur që duket si i mitur në pozitë të qartë të seksuale, ose fotografi reale që tregojnë veprime të qarta seksuale me të mitur ose e paraqesin të miturin ose të rriturin që duket si i mitur në pozitë të qartë seksuale;

  pika 26 **sistemi kompjuterik –** Me sistem kompjuterik nënkuptohet çfarëdo pajisje ose grup i pajisjeve të lidhura ndërmjet vete, nga të cilat, njëra ose më tepër prej tyre bën përpunimin automatik të të dhënave sipas një programi të caktuar;

  pika 27 **të dhënat kompjuterike –** Me të dhëna kompjuterike nënkuptohet prezantimi i fakteve, informatave ose i koncepteve në formë të përshtatshme për përpunim nëpërmjet sistemit kompjuterik, duke e përfshirë edhe programin përkatës që e vë në funksion sistemin kompjuterik

Përveç KP-së, e drejta materiale që i rregullon aspektet e ndryshme ndëshkuese të krimit kompjuterik, poashtu haset edhe në ligjet e tjera, të cilat më shpesh përmbajnë një kapitull të veçantë që ka të bëjë me dispozitat kundërvajtëse. Ligjet e tilla të veçanta *(lex specialis)* që rregullojnë çështje të veçanta nga fusha e komunikimeve elektronike, janë theksuar më lartë.

➢ ***E drejta procedurale***

- *Ligji për procedurë penale*

Aspekti procedural i çështjeve që ndërlidhen me krimin kompjuterik ka të bëjë me masat dhe veprimet që zbatohen në mënyrë të veçantë për këtë lloj krimi, si dhe me masat dhe veprimet që zbatohen gjatë krimit konvencional. Kështu, këtu mund t'i përmendim dispozitat e LPP-së për kërkim në sistemin kompjuterik dhe kërkimin e të dhënave kompjuterike (neni 184) dhe për konfiskimin e përkohshëm të të dhënave kompjuterike (neni 198), si dhe dispozitat e Kapitullit XVII – Masat për gjetjen dhe sigurimin e personave dhe të sendeve, pastaj qëllimi dhe llojet e masave të posaçme hetuese (neni 252), veçanërisht masat e posaçme, si kontrolli i fshehtë dhe kërkimi në sistemin kompjuterik dhe kontrolli i komunikimeve të realizuara telefonike dhe i komunikimeve të tjera elektronike etj.

Krimi kompjuterik, sikurse edhe krimi konvencional, parasheh mbledhjen e provave, të cilat edhe përkundër prezencës së tyre fizike, kanë nevojë edhe për mbledhjen e të dhënave që janë të padukshme[15] dhe që janë në formë që kërkon zbulimin dhe fiksimin e tyre paraprak nëpërmjet formës fizike (kompjuter, stacion pune, telefon etj.) e pastaj ndërmarrjen e veprimeve plotësuese procedurale, të cilat nënkuptojnë kontakt indirekt me provat në formë elektronike dhe vendet ku ato janë ruajtur.

Me rëndësi të veçantë gjatë mbledhjes së provave janë:

- Vërtetimi për konfiskimin e përkohshëm të sendeve
- Cilat sende mund të konfiskohen
- Mënyrat e konfiskimit të përkohshëm të sendeve
- Kushtet dhe parimet e ruajtjes së vërtetësisë së sendeve të konfiskuara

Në raste të veçanta, mbledhja e provave bëhet nga largësia, duke i zbatuar dispozitat e nenit 326 të Konventës për krimin kompjuterik.

Në situata kur duhet të bëhet kontroll në kompjuterë të cilët në atë moment janë duke punuar, me rëndësi të madhe është që të mos ketë ndërprerje të rrymës elektrike, për shkak se memorja RAM i ruan të dhënat deri sa ka furnizim me rrymë, përndryshe ato mund të humben.

[15] CASX – të dhënat që gjenden në memorjen aktive të kompjuterit

- *Konventa për krimin kompjuterik – normat procedurale*[16]

Siç u theksua më lartë, përveç normave materiale, Konventa për krimin kompjuterik përmban një sërë normash procedurale:

- Neni 14 –Sfera e zbatimit të dispozitave procedurale
- Neni 15 – Kushtet dhe garancitë
- Neni 16 – Ruajtja e përshpejtuar e të dhënave kompjuterike të memorizuara
- Neni 17 – Ruajtja e përshpejtuar dhe zbulimi i pjesshëm i të dhënave të trafikut
- Neni 18 – Urdhëri për prodhim
- Neni 19 – Kërkimi dhe konfiskimi i të dhënave kompjuterike të memorizuara
- Neni 20 – Mbledhja e të dhënave të trafikut në kohë reale
- Neni 21 – Interceptimi i të dhënave të përmbajtjes
- Neni 22 - Juridiksioni

[16] Teksti integral i dispozitave procedurale të Konventës për krimin kompjuterik është bashkangjitur me këtë Doracak si Shtojcë e veçantë 2 (shih faqen 42)

2. KORNIZA JURIDIKE NDËRKOMBËTARE DHE BASHKËPUNIMI

Mutual Legal Assistance (MLA, ndihma e ndërsjellë ligjore) – paraqet bazë të vetme për të siguruar prova që gjenden në ndonjë shtet tjetër, dhe të cilat mund të kenë fuqi adekuate dëshmuese para gjykatës kompetente.

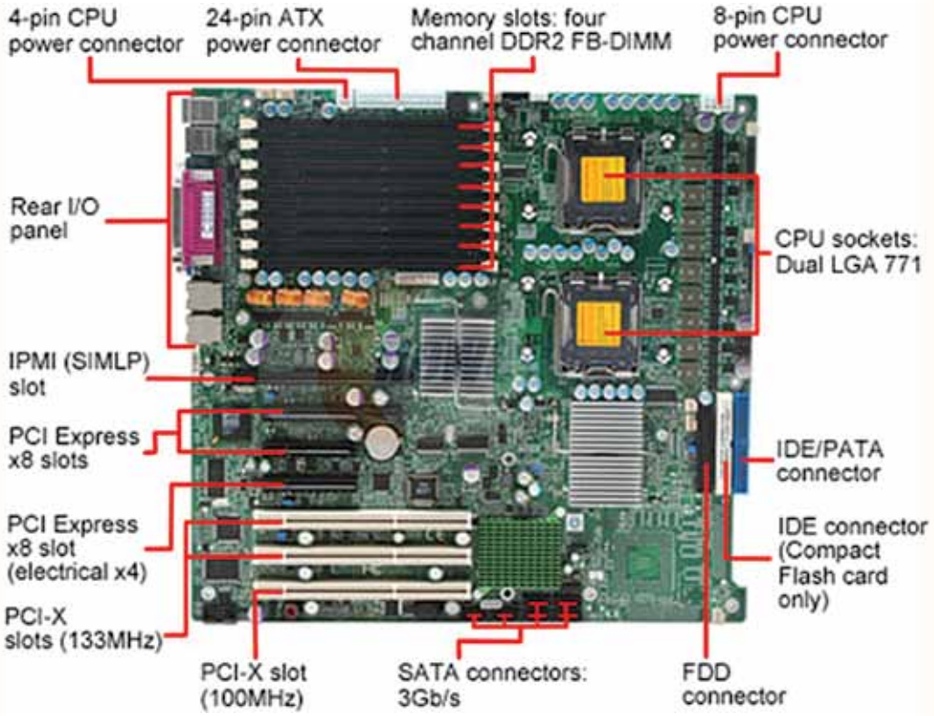
Second additional protocol of the European Convention Mutual Assistance in Criminal Matters (i datës 08.11.2001) – mundëson komunikim të shpejtë dhe të drejtpërdrejtë ndërmjet organeve të autorizuara shtetërore gjatë marrjes së informatave spontane që kanë të bëjnë me ndonjë ngjarje penale ligjore dhe në këtë mënyrë provat primare fitohen drejtpërdrejt, pa zbatimin e MLA-së. Në këtë mënyrë, arrihet efikasitet më i madh i procedurës penale, veçanërisht në ato raste kur dihet se provat elektronike mund të humben shumë lehtë dhe shpejtë, të ndryshohen ose në çfarëdo mënyre të kompromentohen.

Point 24/7(Pika 24/7) – sipas nenit 35, Konventa për krimin kompjuterik vendos një instrument të ri, i cili në mënyrë shumë efikase e rregullon ndihmën ligjore ndërkombëtare në nivel institucional. Kjo ofron mundësi që të mblidhen, gjegjësisht të bëhet ngrirja e të dhënave në periudhë që na mundëson zgjidhje efikase parahetuese të premisave kryesore për ndjekjen e qarkullimit të të dhënave nëpër Internet Service Providers (ISP, dhënës i shërbimeve të qasjes në internet) të ndryshëm, nëpër vende të ndryshme, por edhe të të dhënave që gjenden në organet shtetërore, institucionet, subjektet juridike dhe personat fizikë, dhe gjatë kësaj duke mos i shfrytëzuar metodat konvencionale dhe organet shtetërore (Ministrinë për Drejtësi dhe Ministrinë për Punë të Brendshme), të cilat do të mund ta ngadalësonin procedurën e gjetjes dhe të ngrirjes së të dhënave.

Pika 24/7 nuk do të thotë edhe zëvendësim i mënyrave konvencionale të ndihmës së ndërsjellë ligjore. Mënyra e këtillë është vetëm përkrahje për fillimin e ndihmës së ndërsjellë ligjore, me ç'rast nuk do të humbet kohë e çmuar për ruajtjen e të dhënave të kërkuara, të cilat, kur bëhet fjalë për provat elektronike, ka mundësi të ndryshohen shpejtë dhe të shkatërrohen. Kjo do të thotë se kalimi i kohës është faktor esencial për ta siguruar provën dhe për ta dëshmuar origjinalitetin e saj, si dhe për mundësinë që organi kompetent shtetëror me kohë ta ketë provën përkatëse që të mund të zhvillohet procedura penale.

3. TERMET QË PËRDOREN MË SHPESH NË FUSHËN E KRIMIT KOMPJUTERIK

Pllaka amë – Poashtu e njohur edhe si kryepllaka ose pllaka sistemore e kompjuterit. Pllaka amë është skema qendrore e kompjuterit. Të gjitha pjesët e tjera dhe pajisjet periferike lidhen në të. Detyra e pllakës amë është që t'i lidhë informatat ndërmjet të gjitha pajisjeve të tjera. Në pllakën amë gjendet BIOS-i (basic input/output system[17]) – sistemi themelor për hyrje/dalje, i cili e udhëheq kompjuterin kur ndizet fillimisht. Në pllakën amë lidhen drejtpërdrejt pjesët e tjera përbërëse, si për shembull: memorja, njësia qendrore për përpunim të të dhënave, kartela grafike, hard-disku, njësia e diskut, video-kartela, së bashku me portat e ndryshme dhe pajisjet e tjera periferike.



Fotografia 1 – pllaka amë

[17] Shkurtesa zakonisht lexohet "bye-oss".

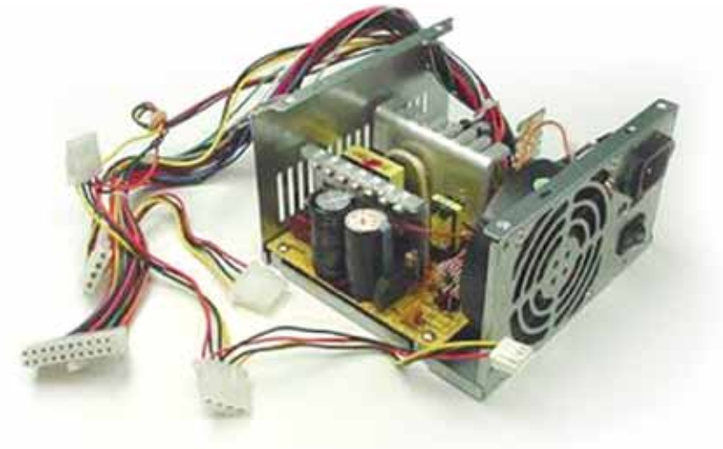
CMOS (Complementary Metal Oxide Semiconductor[18], gjysmëpërçuesi plotësues metal-oksid) – e paraqet harduerin e kompjuterit që kryen funksione në nivel të ulët (elementare) dhe rutina themelore kompjuterike gjatë startimit të tij. CMOS-i dhe BIOS-i shpeshherë përdoren në mënyrë alternative. BIOS-in mund ta konsiderojmë si softuer, ndërsa CMOS-in si harduer që e përdor atë.

Fotografia 2 – Vendi ku gjendet CMOS-i

BIOS (Basic Input/Output System, sistemi themelor për hyrje/dalje) – paraqet pajisje të ndërmjetme që i mundëson shfrytëzuesit të kryejë funksione elementare (low-level) në pllakën amë, CPU, memorje dhe në pajisjet e tjera. Vendet iniciale të BIOS-it zakonisht janë të vendosur ashtu siç duhet. Njëra nga ndryshimet më të shpeshta që i bëhen BIOS-it në kapacitet forenzik është kur ndryshohet renditja sipas së cilës kompjuteri i kërkon njësitë në të cilat mund të jetë i vendosur sistemi operativ (për shembull: një kompjuter mund të startohet nëpërmjet pajisjes USB, CDROM-it ose hard-diskut dhe renditja se me cilën prej tyre do të bëhet startimi mund të ndryshojë).

Furnizuesi me energji elektrike i kompjuterit - Njësia për furnizim me energji elektrike ose i ashtuquajturi Power Supply Unit (PSU) në kompjuter e rregullon dhe e përcjell energjinë te pjesët përbërëse në shtëpizë. Furnizimi standard elektrik e shndërron energjinë hyrëse prej 110V ose 220 të rrymës alternative në rrymë njëkahëshe, e cila pastaj është e përshtatshme për t'i furnizuar pjesët përbërëse të kompjuterit.

[18] Kjo shkurtesë zakonisht lexohet "see-moss".



Fotografia 3 – Furnizuesi me energji elektrike i kompjuterit

Central Processing Unit (CPU, njësia qendrore për përpunim/procesori) – është harduer në kuadër të kompjuterit që i ekzekuton instruksionet e programeve kompjuterike për kryerjen e operacioneve themelore aritmetike, logjike dhe hyrëse/dalëse në sistemin kompjuterik. Njerëzit shpeshherë e ngatërrojnë me shtëpizën ose shasinë e kompjuterit. Mirëpo, procesori paraqet komponentë të brendshme dhe nuk mund të shihet jashtë sistemit. Pa marrë parasysh se për çfarë lloj kompjuteri bëhet fjalë, procesori punon në ekzekutimin e një sërë instruksionesh të memorizuara, që janë të njohura si program.

Fotografia 4 – CPU/procesori

Random Access Memory (RAM, memorja me qasje të rastësishme) – Memorja kompjuterike paraqet formë të memorizimit të të dhënave, edhe pse më shpesh përshkruhet si formë e përkohshme e memorizimit të të dhënave që i shfrytëzojnë programet aktive, me qëllim që më shpejt të kenë qasje në to. Procesori kërkon të dhëna nga RAM-i, ato përpunohen dhe pasi të jenë përpunuar, shënohen në RAM. Kjo gjë ndodh disa miliona herë në sekondë.[19]

Fotografia 5 – RAM-i

Universal Serial Bus (USB) - USB konektorë muund të gjenden te shumica e kompjuterëve bashkëkohorë dhe ato mundësojnë që një numër i madh pajisjesh të lidhen në mënyrë të thjeshtë me kompjuterin, siç janë miu, shtypësit, pajisjet e jashtme memoruese dhe telefonat celularë. Në këtë moment, kjo është mënyra më e shpeshtë e lidhje së pajisjeve të jashtme me kompjuterin. Në praktikë ekziston mundësia që nëpërmjet USB-së të lidhen mbi 127 pajisje me një kompjuter. Lehtësia me të cilën mund të shfrytëzohen pajisjet USB, nënkupton se ato dallohen si pajisje që përdoren më shpesh në shumë hetime/ekspertiza digjitale forenzike[20].

Fotografia 6 – Konektori USB

[19] gjatë zbatimit të ligjit, më të shpeshta janë përpjekjet që të kapen të dhënat nga RAM-i, para se të ndërpritet furnizimi i energjisë elektrike, derisa kompjuteri është duke kërkuar

[20] Në kuadër të MPB-së, ekziston Sektori për krimin kompjuterik dhe forenzikë kompjuterike

Hard disk drive (HDD, hard disku) – Paraqet pajisje elektromekanike që përmban disqe rroutlluese dhe koka lëvizëse për shkrim/lexim të të dhënave. Disqet kanë pllaka ku janë shënuar informatat dhe të dhënat lehtë mund të fshihen ose të rishkruhen, me ç'rast ruhet struktura e diskut që i bën të dhënat të jenë të qëndrueshme në afat më të gjatë kohor. Të dhënat vendosen në sipërfaqen e pllakës, në të ashtuquajtur sektorë dhe shtigje. Shtigjet janë rrathë koncentrikë, ndërsa sektorët janë segmente të shtegut. Të dhënat në hard-disk ruhen në formë të skedarëve (fajllave), të cilat në formë të thjeshtë janë "bit-e"[21]. Programet paraqesin skedarë dhe procesori i trajton si të tilla që të mund t'i shfrytëzojë. Shumica e kompjuterëve kanë së paku një hard-disk, mirëpo ka edhe shumë kompjuterë të tjerë që kanë më shumë se një hard-disk. Për kompjuterët më të mëdhenj, siç janë kompjuterët "main frame"[22], është normale që të kenë më tepër hard-disqe. Sot, është e zakonshme që edhe pajisje të tjera, përveç kompjuterëve, siç janë CCTV (sistemet e mbyllura televizive) dhe pajisjet muzikore, të kenë hard-disqe, që të mund të ruajnë sasi të mëdha të të dhënave.

Fotografia 7 – Hard-disku

[21] Shih më poshtë, "Memorja dhe ruajtja e të dhënave"

[22] Kompjuterët "main frame" kryesisht i shfrytëzojnë kompanitë e mëdha ose institucionet qeveritare për ekzekutimin e aplikacioneve esenciale, për përpunimin e sasive të mëdha të të dhënave (për shembull, të dhënat statistikore) dhe për përpunimin e transaksioneve

Solid-state drive (SSD) – paraqet pajisje për ruajtjen e të dhënave që shfrytëzon memorje gjysmëpërçuese, gjegjësisht mikroçipe që përmbajnë pjesë mobile. Kjo pajisje i ruan të dhënat e përhershme me qëllim që të sigurohet qasje në to në të njëjtën mënyrë sikurse dhe në rastin e hard-diskut tradicional. Ndonjëherë quhet edhe "solid-state disk" ose disk elektronik. Në krahasim me disqet elektromekanike, SSD-të janë më pak të ndjeshme ndaj goditjeve fizike, nuk bëjnë zhurmë, kanë kohë më të shkurtë të qasjes te të dhënat dhe fshehtësi më të madhe, por kanë çmim më të lartë. SSD-të shfrytëzojnë pajisje të njëjta për t'u lidhur sikurse edhe hard-disqet, prandaj lehtë zëvendësohen në shumicën e aplikacioneve. Për shkak se te pajisjet SSD të dhënat ruhen në mënyrë krejtësisht tjetër, ato bartin me vete edhe sfida të reja për ekspertizat digjitale.

Fotografia 8 – Pajisja SSD

Disqet CD/DVD/BD[23] **-** Këto disqe mund të përmbajnë sasi të ndryshme të të dhënave dhe zakonisht përdoren për të ruajtur muzikë, video ose skedarë kompjuterikë për përdorim në pajisje të ndryshme. Për shembull, DVD-ja ka dimensione të njëjta sikurse edhe CD-ja, mirëpo mund të përmbajë shtatë herë më tepër të dhëna se sa CD-ja. BD-ja është disk optik për ruajtjen e të dhënave dhe ka kapacitet deri në dhjetë herë më të madh se sa DVD-ja. Me fjalë të tjera, këto disqe mund të ruajnë më shumë të dhëna se sa që kanë mundur të ruajnë hard-disqet e para disa viteve. Të gjitha ato i ruajnë të dhënat në mënyrë të ndryshme nga hard-disku dhe të dhënat që ruhen në to janë më të përhershme se sa ato që ruhen në hard-disk.

[23] CD – Compact Disc (kompakt disk), DVD – Digital Versatile Disc (disk digjital i gjithanshëm), BD – Blu ray Disc (disk me rreze të kaltër)

Fotografia 9 - CD/DVD/BD

Sistemi operativ (OS) – paraqet program softuerik (platformë) e cila i mundëson harduerit të komunikojë me programet/aplikacionet softuerike. Pa sistem operativ, kompjuteri nuk mund të funksionojë. Ka lloje të ndryshme të sistemeve operative (Windows, iOS, Android) varësisht nga lloji i kompjuterit ose i pajisjes digjitale (tablet, celular). Shumica e aplikacioneve kompjuterike janë të krijuara në mënyrë veçantë për ndonjë sistem operativ, edhe pse tani është e zakonshme që ato të jenë në dispozicion në disa platforma.

4. MEMORJA DHE MEMORIZIMI I TË DHËNAVE

4.1. Njësitë matëse të të dhënave

Bit – biti është njësia themelore e informatës te kompjuterët dhe komunikimet digjitale. Mund të ketë vetëm një nga dy vlera të mundshme, dhe për këtë arsye mund të zbatohet fizikisht në pajisje që kanë dy gjendje (për shembull, "ndezur" dhe "fikur"). Më shpesh, këto vlera shënohen me 0 dhe 1. Termi "bit" është shkurtesë prej "**bi**nary digi**t**" (shifër binare).

Byte – bajti është njësi për informatat digjitale në teknologjinë kompjuterike dhe te telekomunikimet, e cila zakonisht përbëhet nga tetë bita.

Është me rëndësi të theksohet se prefiksat metrikë që përdoren me njësinë e bajtit janë identike me prefiksat metrikë të sistemit SI[24], por dallimi qëndron në atë se memorja kompjuterike është e dizajnuar në bazë të logjikës binare, gjegjësisht vlerat e shumëzuara janë me bazë 2 (p.sh. 2^{10}, 2^{20}), e jo me bazë 10 (p.sh. 10^3, 10^6).

Emri (shqiptimi)	Vlera	Shkurtesa
Bit (bajt)	0 ose 1	/
Byte (bajt)	8 bita (2^3)	B
Kilobyte (kilobajt)	1,024 B (2^{10})	KB
Megabyte (megabajt)	1,048,576 B ($2^{20} = 1024^2$)	MB
Gigabyte (gigabajt)	1,073,741,824 B ($2^{30}=1024^3$)	GB
Terabyte (terabajt)	1,099,511,628,000 B ($2^{40}=1024^4$)	TB

[24] Le Système international d'unités – sistemi ndërkombëtar i njësive matëse

4.2. Memorizimi i të dhënave

Kapacitetet e bartësve të dhënave:

- *CD* – zakonisht kanë kapacitet prej 650MB ose 700MB
- *DVD* – momentalisht kanë kapacitet prej 4.7GB ose 8.5GB, ndërsa HVD është dizajnuar me kapacitet prej 3.9TB (830 herë kapacitet më i madh se sa i DVD-ve të zakonshme)
- *Hard drive* – momentalisht janë në dispozicion me 4 TB
- *Interneti* – termi INTERNET paraqet bashkim të pjesëve të fjalëve INTERconnected NETwork (Rrjet i ndërlidhur).

Memorizimi onlajn

- *I lejuar – Memorizimi onlajn ofron shërbim që është shumë i* dobishëm gjatë zhvillimit të biznesit dhe të udhëtimeve, për shkak se hyrja në të dhënat e memorizuara onlajn mund të bëhet nëpërmjet internetit, si dhe mund të gjenden dhe të shpërndahen skedarët.

- *I palejuar* –Zbatohet për skedarët, follderët, fotografitë ose çfarëdo qoftë lloji të të dhënave që mund të gjenden në çdo kompjuter që është i lidhur në internet dhe ato mund të shpërndahen nga çdokush që i ka të dhënat për t'u regjistruar (login).

Shembull të memorizimit të palejuar onlajn paraqet "dead letter box". Kjo do të thotë se llapet llogari në cilindo qoftë web-mail pa pagesë, pastaj shkruhet një porosi që përmban edhe përmbajtje "të fshehtë" dhe pastaj bashkangjiten shtojcat (attachment) – nëse ka nevojë për to. Porosia nuk dërgohet, por vetëm ruhet si version draft (i papërfunduar). Pastaj të dhënat për t'u futur (login) në llogari i tregohen dikujt tjetër. Personi i cili i di të dhënat për t'u futur në llogari, e lexon porosinë dhe pastaj e fshin atë. Porosia asnjëherë nuk është dërguar, por vetëm është ruajtur versioni i saj draft në ndonjërin nga follderët e llogarisë së shfrytëzuesit – pa pasur mundësi që porosia të ndiqet në mënyrë virtuale.

5. RRJETI

5.1. Kuptimi i rrjetit

Local Area Network (LAN, rrjeti lokal) – Rrjet kompjuterik që mbulon një zonë të vogël gjeografike, siç është shtëpia, zyra, një grup ndërtesash, si për shembull shkolla. Në karakteristikat që e definojnë *LAN*-in bëjnë pjesë shpejtësia e madhe e transferit të të dhënave, diapazoni i vogël gjeografik dhe mungesa e linjave të huazuara telekomunikuese.

Wide Area Network (WAN, rrjeti për zona më të gjera) – Rrjet kompjuterik që mbulon një zonë të gjerë (gjegjësisht çdo rrjet, linket komunikuese të të cilit i kalojnë kufinjtë e metropoleve, ato rajonalë ose nacionalë) ose thënë në mënyrë më të thjeshtë-joformale, rrjet që shfrytëzon ruterë dhe linke publike për komunikim. INTERNETI paraqet një shembull të këtij rrjeti.

Rrjetet mund të jenë të kufizuara:

- Sipas numrit të shfrytëzuesve që u takojnë,
- Sipas diapazonit maksimal gjeografik të mbulimit të rrjetit, siç janë për shembull, rrjetet Ethernet ose Wireless.

Interneti lejon/mundëson lidhje të këtyre rrjeteve të vogla në një rrjet, madhësia e të cilit është e pakufizuar. Poashtu, nuk është me rëndësi se për çfarë lloj rrjeti bëhet fjalë, përderisa protokolli TCP/IP është pranuar si ndërmjetësues për komunikim.

World Wide Web (www, rrjeti botëror) – Për herë të parë u paraqit në vitin 1991, kur Sër Tim Berners-Li e zbuloi HTML (Hyper Text Markup Language). HTML krijoi platformë për kombinimin e fjalëve, fotografive dhe zërave në ueb-faqe. Standardet e ueb-it zhvillohen nga ana e **World Wide Web Consortium (W3C)**, i cili paraqet komunitet ndërkombëtar që zhvillon standarde për të siguruar zhvillim afatgjatë të Rrjetit. Për shfletim të rrjetit shfrytëzohen të ashtuquajturit **Web Browser-ë (shfletues),** që janë programe të veçanta softuerike të zhvilluara për t'i gjetur dhe për t'i paraqitur ueb-faqet e ndryshme. Si shfletues më të njohur janë: Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opera etj. Që shfletuesit dhe serverët të mund të komunikojnë ndërmjet tyre në internet, ato shfrytëzojnë protokoll të përbashkët që quhet **HTTP (Hyper Text Transfer Protocol)**.

5.2. Terme të tjera të rrjetit

Ports - janë pika të skajshme (dalje) ose kanale për komunikim nëpër rrjet. Më tepër dalje në një makinë llogaritëse mundësojnë që në të njëjtën kohë të fitohen të dhëna nga rrjetet e ndryshme ose bartës të ndryshëm të të dhënave, pa pasur konflikt gjatë pranimit dhe dërgimit të informatave. Portet janë pika virtuale dhe nuk janë hyrje në makinën llogaritëse në të cilën lidhen njësi të jashtme ose kabllo komunikuese.

Media Access Control (MAC) address – është numër i vetëm identifikimi që e kanë numri më i madh i adapterëve ose i kartelave të rrjetit, që janë futur nga ana e prodhuesit dhe ato japin të dhëna të vetme për ekzistimin e komunikimit nëpër ndonjë adapter ose kartelë të rrjetit. Ky numër identifikimi haset te të gjitha pajisjet që mund të jenë bartëse të të dhënave (kompjuterët, shtypësit, skenerët, pajisjet shumëfunksionale që janë të lidhura me kompjuterin, foto-aparatet, video-kamerat etj.)

Botnet – ky term është i lidhur me një numër programesh kompjuterike të automatizuara me IRC për komunikim në internet, që janë të lidhura dhe mund të komunikojnë ndërmjet vete pa u penguar nga shfrytëzues të padëshiruar. Ky është kuptimi themelor për botnet-in që përdoret për komunikim legal. Nga ana tjetër, komunikimi joligjor nëpërmjet sistemit botnet për komunikim të automatizuar ndërmjet kompjuterëve, siguria e të cilëve është kompromet uar me ndihmën e programeve keqdashëse, paraqet mënyrë për transferin e informatave nëpër ndonjë kompjuter pa dijeninë e shfrytëzuesit të kompjuterit.

Encryption – është program i veçantë që mundëson të mbrohen disa të dhëna të caktuara. Mbrojtja bëhet me futjen e shifrave të veçanta, të cilat pamundësojnë qasje në përmbajtjen e një pjese të caktuar të memorjes së kompjuterit. Programe që përdoren më shpesh për enkriptimin e të dhënave janë: Microsoft Bitlocker, Truecrypt dhe Steganos.

Network Interface Controller (NIC) – i njohur edhe si "network adapter" ose "LAN adapter", është pjesë e harduerit (si pjesë përbërse e pllakës amë ose në formë të kartelës së rrjetit që është instaluar në kompjuter) nëpërmjet të të cilit kompjuteri komunikon me pajisjet e tjera në një rrjet kompjuterik.

Network Switch – është pajisje për rrjetëzim që mundëson më tepër pajisje të lidhen në rrjetin kompjuterik.

Router – është pajisje që e përcakton pikën e ardhshme në rrjet, ku duhet të dërgohet pakoja me të dhëna, si destinacion i saj i ardhshëm ose i fundit.

Server – është kompjuter ose pajisje që ofron informata ose shërbime për ndonjë kompjuter ose drejt ndonjë kompjuteri tjetër në rrjet. Me shfrytëzimin e pro-

gramit përkatës, çdo kompjuter i lidhur në rrjet mund bëhet server. Në numrin më të madh të rasteve, ai është një kompjuter "i dedikuar", i cili gjithë kohën është në dispozicion të kompjuterëve të tjerë. Një kompjuter i tillë mund të kryejë më tepër shërbime, edhe atë si: web server, e-mail server, print server e të ngjashme.

Priza e rrjetit – pajisje kompjuterike e rrjetit që i lidh pjesët e rrjetit.

Bandwidth (gjerësia e bandës) – Sasia e informatave që mund të barten nëpërmjet linjës telefonike, linjës kabllovike, satelitit etj. Sa më e madhe të jetë gjerësia e bandës, aq më e madhe do të jetë shpejtësia e lidhjes, si dhe qasja në internet, transferet do të jenë më të shpejta, përvoja televizive më e mirë.

Network Interface Controller (NIC, Kartela e rrjetit) - paraqet tabelë rrethore ose kartelë që është instaluar në kompjuter dhe mundëson lidhje në ndonjë rrjet të caktuar.

Network Hub (Ethernet Hub, pajisje rrjeti ose koncentrues) – paraqet pajisje për lidhje të më tepër pajisjeve Ethernet së bashku me ato që veprojnë si segment i vetëm në rrjet. Hab-et punojnë në shtresën fizike (shtresa e parë) të modelit OSI dhe termi "kyçje në shtresën e parë" shpeshherë përdoret si zëvendësim i termit hab. Me këtë, pajisja paraqet formë të përsëritësit multi-hyrës. Hab-et e rrjetit, poashtu janë përgjegjëse për ridërgimin e sinjalit te të gjitha portet në qoftë se konstatohet konflikt.

5.3. Rrjetet me komutim të kanaleve kundrejt rrjeteve me komutim të pakove

Në rrjetet me "komutim (zëvendësim) të kanaleve", ekziston një lidhje e definuar ndërmjet dërguesit dhe pranuesit të të dhënave gjatë sesionit komunikues. Shembull i rrjetit me komutim të kanaleve është rrjeti telefonik.

Pjesa më e madhe e rrjeteve moderne të të dhënave, siç është interneti, janë rrjete me "komutim të pakove". Në to, të dhënat që transmetohen ndahen në pako të vogla, pa marrë parasysh përmbajtjen, llojin ose strukturën, në blloqe me madhësi përkatëse, të cilat quhen pako, dhe që e gjejnë rrugën e tyre deri te pranuesi nëpërmjet një protokolli të veçantë.

5.4. Protokolli i internetit (Internet Protocol - IP)

Aplikacionet dhe shërbimet e ndryshme shfrytëzojnë protokolle që të komunikojnë nëpërmjet rrjeteve. Disa nga protokollet më të rëndësishme janë: HTTP – HyperText Transfer Protocol; SMTP – Simple Mail Transfer Protocol; FTP – File Transfer Protocol; NNTP – Network News Transfer Protocol, TCP – Transmission Control Protocol, IP – Internet Protocol.

Protokolli i internetit është njëri nga dy protokollet kryesore në modelin e internetit (i njohur si TCP/IP). Ai është protokolli kryesor për komunikim, gjegjësisht për transmetim të datagrameve (njësia themelore e të dhënave që transmetohet në një rrjet me pako). Funksioni i tij kryesor e mundëson rrjetëzimin, dhe, në esencë, e cakton internetin. Detyra e IP-së si protokoll kryesor në modelin e internetit, është të dërgojë pako nga burimi deri te destinacioni, në bazë të adresave IP në kreun e pakos me të dhëna që transmetohet. Ai i definon edhe metodat e adresimit që shfrytëzohen për shënimin e datagramit, me informata për burimin dhe destinacionin.

Adresa e protokollit të internetit (adresa IP) është shënim numerik që i jepet çdo pajisjeje (kompjuterit, shtypësit) që është e lidhur në rrjetin kompjuterik dhe të cilat e përdorin protokollin IP. Adresa IP ka dy funksione kryesore: identifikimin e interfejsit të rrjetit dhe adresimin e lokacionit. Roli i saj është përshkruar në këtë mënyrë: "emri tregon se çka kërkojmë, adresa tregon se ku gjendet ajo, rruga tregon se si arrihet deri te qëllimi". Adresa IP, në fakt, mund të kuptohet si "linjë telefonike" në internet. Pa adresë IP nuk mund të hyhet në internet. IP-ja nuk paraqet gjithmonë mënyrë të saktë për identifikim. Adresat IP ndahen në dy kategori, varësisht nga oferta e dhënësit të shërbimeve:

- Statike – mbeten të njëjta gjatë çdo hyrjeje në internet.
- Dinamike – ndryshojnë çdoherë kur shfrytëzuesi hyn në internet

Për ta përcaktuar shfrytëzuesin e adresës IP në momentin kritik, shumë me rëndësi është koha e saktë e hyrjes në internet. Të dhënat për kohën e saktë të hyrjes, si dhe zonën kohore, i siguron dhënësi i shërbimit të internetit.

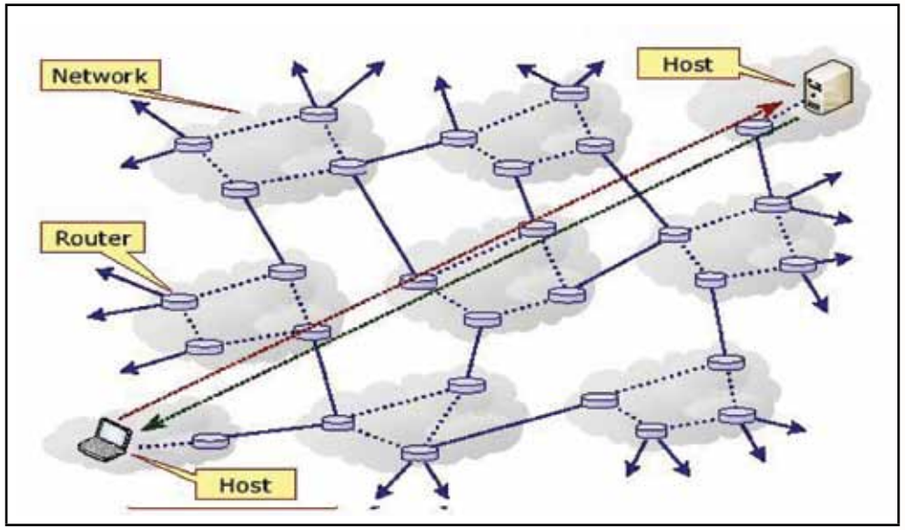
5.5. Lidhja në Internet

Shumica e shfrytëzuesve lidhen në internet duke i shfrytëzuar shërbimet e ndonjë dhënësi të shërbimeve të internetit (Internet Service Provider – ISP). Lidhja mund të jetë nëpërmjet linjës telefonike (Dial-up), lidhjes me bandë të gjerë (Broadband, ADSL), rrjetit digjital për shërbime të integruara (Integrated Services Digital Network – ISDN), ofruesit të televizionit kabllovik, rrjetit pa tel (WiFi), ose lidhjes satelitore.

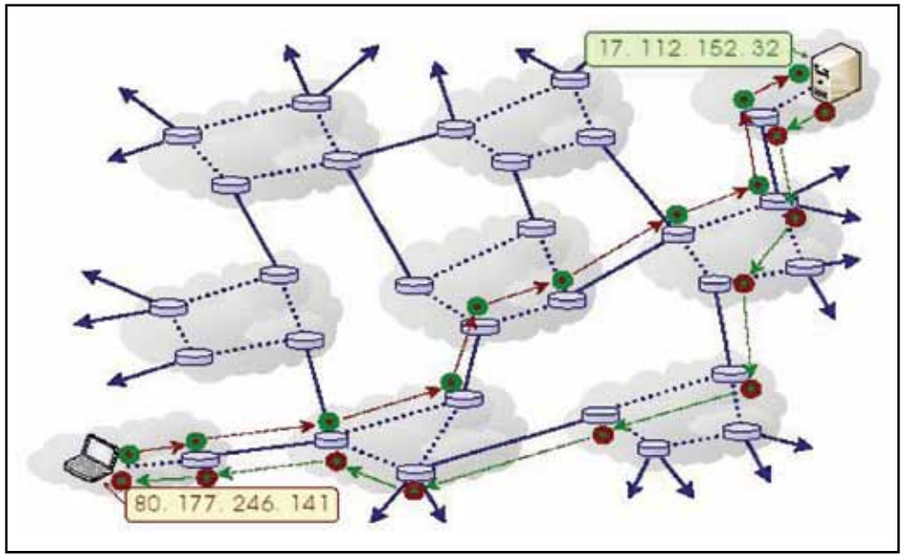
- *Dhënësit e shërbimeve të internetit*

Internet Service Provider (ISP) janë organizata komerciale që mundësojnë/huazojnë hyrje në internet. Vlerësohet se nëpër botë ka mbi 14,000 organizata të tilla. ISP-të mbajnë evidencë për shfrytëzimin e internetit nën kushte të cilat ndryshojnë në legjislacione të ndryshme nacionale. Sipas legjislacionit në Republikën e Maqedonisë, ISP-të janë të obliguara që të dhënat t'i ruajnë në afat prej dy vitesh.

Interneti – paraqitja ideale



Interneti – paraqitja reale



- *Identifikuesi uniform i resurseve - URL*

URL-ja paraqet një seri shenjash që është referencë për një resurs të caktuar. Për shembull, ueb-faqja http://www.jorm.org.mk

- *http://- Ka të bëjë me protokollin e internetit që shfrytëzohet (hypertext transfer protocol)*
- *www.- Ka të bëjë me serverin World Wide W*eb
- *jorm.– është emri i domenit dhe ka të bëjë me pronarin e ueb-faqes*
- *org.mk- Ka të bëjë me nivelin më të lartë të domenit (Top Level Domain - TLD) që shfrytëzohet (zakonisht emri i vendit)*

6. SERVERËT

Web servers (ueb serverët) – paraqesin kompjuterë që mundësojnë (ofrojnë shërbim për) qasje në ueb-faqe. Çdo ueb-server ka adresë IP dhe eventualisht edhe domen. Për shembull, në qoftë se e shkruani identifikuesin uniform të resurseve (URL) http://www.jorm.org.mk/index.html në shfletuesin tuaj, do të dërgohet kërkesë deri te ueb-serveri, domeni i të cilit është jorm.org.mk. Pastaj, serveri e merr faqen me titull index.html dhe ia dërgon shfletuesit tuaj.

Çdo kompjuter mund të bëhet ueb-server në qoftë se instalohet softuer për server dhe në qoftë se lidhet në internet. Ka disa aplikacione softuerike për ueb-serverë, si për shembull: pakot e ndryshme komerciale të Microsoft-it, Netscape etj.

Me qëllim që të lidheni me ndonjë ueb-faqe, ju duhet të logoheni. Të gjitha sistemet kompjuterike krijojnë dhe ruajnë shënime të lidhjeve (konekcioneve), të ashtuquajtura kuki (cookies), të cilat përmbajnë informata për:

- Identitetin e shfrytëzuesit (adresën IP)
- Datën dhe kohën e hyrjes
- Përmbajtjen që është kërkuar
- Sa gjatë është shikuar përmbajtja e kërkuar
- Shfletuesin prej ku është bërë hyrja
- Sistemin operativ që e ka shfrytëzuar kompjuteri
- Në çfarë mënyrë është hyrë në atë ueb-faqe

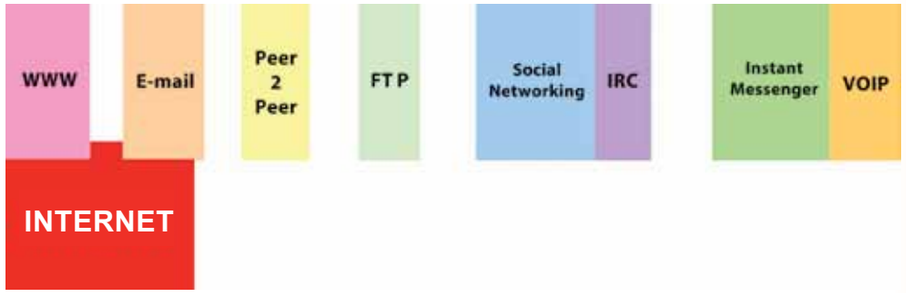
Proxy serveri – paraqet server (sisteme kompjuterik ose aplikacion) që vepron si ndërmjetësues për kërkesat e klientëve që kërkojnë resurse (të dhëna, informata, dokumente etj.) nga serverët e tjerë. Serverët e këtillë e kontrollojnë kërkesën dhe mundësojnë hyrje në resursin e kërkuar. Sot, shumica e proxy serverëve janë wwwproxy serverë që sigurojnë hyrje në përmbajtjet në *www* dhe gjatë kësaj shfrytëzuesit i ofrojnë anonimitet.

Shembull:

218.12.171.14 - [15/Feb/2009:16:08:43+0100] "GET/test.html HTTP/1.0" 200 1921 www.technologyrisklimited.co.uk "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)" "-"Nëse është "anonime" atëherë pranuesi e sheh 218.12.171.14 dhe – Nëse është 'transparente' atëherë pranuesi e sheh 218.12.171.14, por edhe 212.99.110.242.

Cloud Computing – paraqet një lloj të shërbimit që bazohet në resurset e përbashkëta (të ndara) kompjuterike, e jo në shërbimin e serverit lokal ose të pajisjes lokale gjatë shfrytëzimit të aplikacioneve. Te "cloud computing", fjala "cloud" përdoret si metaforë për "internetin", kështu që fraza *"cloud computing"* do të thotë "lloj i punës kompjuterike në internet", ku shërbimet e ndryshme (serverët, ruajtja e të dhënave dhe aplikacionet) transmetohen deri te kompjuterët dhe pajisjet e organizatës ose institucionit nëpërmjet internetit.

7. LLOJET E KOMUNIKIMIT NDËRMJET SHFRYTËZUESVE



Peer to Peer shërbimet një kohë të gjatë kanë ofruar transfer të skedarëve joligjorë, si dhe të skedarëve që i nënshtrohen të drejtës për pronësi intelektuale. Klientët "peer to peer" janë të njohur në mesin e grupeve kriminale që janë të përfshira në këto aktivitete. Gjenerata e parë e arkitekturës "peer-to-peer" ka funksionuar në bazë të parimit të shfrytëzimit të serverit të centralizuar, me të cilin njerëzit janë lidhur që të shkarkojnë skedarë. Në këtë mënyrë është bërë identifikimi i njerëzve që kanë ofruar shërbime joligjore, të cilat kanë mundur të gjenden shumë lehtë dhe të pengohen. Gjenerata e dytë e klientëve "peer to peer" kanë shfrytëzuar metoda të tjera të lidhjes nga ato që kanë pasur listë të skedarëve që kanë qenë në dispozicion, të cilët janë më të lehtë për t'u kërkuar në krahasim me ato që kanë vepruar si supernyje, me të cilat është bërë identifikimi për skedarët që kanë qenë në dispozicion.

File Transfer Protocol (FTP) është protokoll që mundëson transfer të skedarëve nga një kompjuter në kompjuter tjetër. Funksionon në bazë të logjikës klient/server, me ndonjë program për FTP që është instaluar te kompjuteri klient, që i mundëson shfrytëzuesit të komunikojë me serverin, me qëllim që të fitojë qasje te shërbimet dhe informatat e serverit. Kur shfrytëzuesi dëshiron të transferojë ndonjë skedar, krijohet lidhje TCP deri te sistemi i cakut (target). ID-ja e shfrytëzuesit dhe fjalëkalimi mund të transmetohen dhe shfrytëzuesi mund të bëjë specifikim të skedarëve dhe të aktivitetit të nevojshëm. Kur jepet leja për transfer të skedarëve, krijohet edhe një lidhje TCP për të dhënat që duhet të transmetohen.

Internet Relay Chat (IRC) është sistem për telekonferencë që akoma ekziston, por më shpesh përdoret nga ana e kriminelëve për komunikim dhe për këmbim të skedarëve. Funksionon në bazë të një serie serverësh që janë të lidhur ndërmjet vete dhe që ndajnë porosi tekstuale që dërgohen në "kanale" - dhoma

virtuale për takime. Janë shënuar temat për diskutim dhe shfrytëzuesit që kanë klient IRC mund të lidhen në një ose më tepër kanale dhe të fillojnë diskutim me bashkëmendimtarët. IRC-ja nuk është shërbimi më i shpeshtë që është i lehtë për përdorim ("user friendly") dhe që përdoret në internet, dhe atë më shpesh e përdorin shfrytëzuesit më të vjetër, me përvojë më të madhe.

VoIP (Voice over Internet Protocol) është vegël që ofron komunikim me zë nëpërmjet transferit të pakove me të dhëna, me ndihmën e komunikimit në internet (Skype, Viber etj.).

Social Networking Instant Messaging dhe Social Networking e kanë zënë vendin e veglave për komunikim gjatë viteve të fundit, me shembuj të njohur shumë mirë për qasje të shpejtë dhe të lehtë deri te shfrytëzuesit e tjerë nga mbarë bota. Funksioni kryesor i këtyre ueb-faqeve është mundësia për krijimin e profilit personal dhe mundësia për përbashkimin e informatave personale me të tjerët dhe njohja me njerëz të rinj. Ekziston mundësia edhe për përbashkimin e fotografive, muzikës dhe video-inçizimeve me të tjerët. Niveli i të dhënave personale të cilat njerëzit i përbashkojnë me të tjerët, mund t'i bëjë ata cak të kriminelëve, si për shembull të atyre që janë të përzier në vjedhjen e të dhënave personale dhe keqpërdorimin e fëmijëve. Ueb-faqet për rrjetëzim social janë një mjet shumë i dobishëm për zbatimin e ligjit duke mbledhur informata për të dyshuarit dhe për aktivitetet e tyre joligjore.

Instant messaging është formë e komunikimit të drejtpërdrejtë në kohë reale ndërmjet dy ose më tepër personave që shfrytëzojnë klientë të ndarë. Ky lloj i komunikimit përfshin kontakt ndërmjet njerëzve që njihen, për dallim nga llojet e tjera, që mundësojnë komunikim ndërmjet njerëzve të panjohur. Kriminelët njihen si shfrytëzues të "Instant messaging"-ut si metodë për komunikim.

Twitter paraqet rrjetëzim social dhe shërbim për "micro-blogging" që u mundëson shfrytëzuesve të tij të dërgojnë dhe t'i lexojnë porositë e shfrytëzuesve të tjerë (të njohura si tweet-e), të cilat paraqesin porosi tekstuale me gjatësi maksimale deri në 140 karaktere. Ka mbi 5 milionë shfrytëzues në SHBA, Kanada, Indi, Britani të Madhe dhe Japoni.

Loja onlajn është lojë që luhet nëpërmjet ndonjë lloji të rrjetit kompjuterik. Kjo, pothuajse gjithmonë, e nënkupton internetin ose ndonjë teknologji ekuivalente, por lojërat gjithmonë e shfrytëzojnë teknologjinë e fundit; modemet para internetit dhe terminalet me tel para modemeve. Ekspanzioni i lojërave onlajn është pasqyrë e ekspanzionit të gjithëmbarshëm të rrjeteve kompjuterike nga rrjetet e vogla lokale në internet dhe rritjes së qasjes në internet. Lojërat onlajn ndryshojnë, edhe atë duke filluar nga lojërat e thjeshta tekstuale e deri te lojërat ku përdoret grafikë e ndërlikuar dhe botëra virtuale me shumë lojtarë që luajnë njëkohësisht. Shumë lojëra onlajn janë të lidhura me shumë komunitete onlajn, duke i bërë lojërat onlajn si formë të veprimtarisë sociale.

Porosia elektronike (e-mail) – Zakonisht porosia elektronike kalon nëpër, së paku, katër kompjuterë gjatë kohë së jetesës së saj. Porosia përpilohet në kompjuterin e shfrytëzuesit, pastaj dërgohet deri te mail-serveri dalës SMTP (Simple Mail Transfer Protocol[25]) i ISP-së. ISP-ja dalëse e dërgon porosinë elektronike deri te mail-serveri ISP SMTP (SMTP – SMTP) i pranuesit. Mail-serveri i pranuesit e gjen mail-serverin dërgues të pranuesit (Post Office Protocol ose POP3) dhe e dërgon porosinë në "inbox-in (kutinë e porosive të pranuara) e pranuesit". Shfrytëzuesi logohet në llogarinë e tij të shfrytëzuesit dhe porosia gjendet në inbox-in (kutinë) e tij, e cila pastaj fshihet nga mail-serveri i cili ka ndërmjetësuar në këtë proces.

Porosia elektronike përbëhet nga **Header (zarfi) dhe Body (teksti).** Header-i përmban informata për dërguesin, pranuesin, adresat IP, mail-serverët, shënimet e kohës etj. Body është përmbajtja e porosisë elektronike dhe e shtojcave të bashkangjitura.

- *Llojet e ndryshme të postës elektronike:*

Traditional e-mail (lloji tradicional i postës elektronike) – karakteristike është ajo se hapet me ndonjë program/aplikacion (p.sh. Microsoft Outlook) menjëherë pas shkarkimit, gjendet në kompjuter dhe në të mund të hyjmë prej ndonjë kompjuteri tjetër.

Web based e-mail (Posta elektronike e bazuar në ueb) – shihet nëpërmjet kompjuterit, por gjendet në ndonjë server të largët (remote). Posta e këtillë elektronike mund të organizohet në follderë, por ka mundësi të shihet vetëm kur shfrytëzuesi është onlajn.

Shërbimet anonime të e-mail-it – Ofrojnë mundësi për të dërguar porosi elektronike anonime. Ky shërbim është pa pagesë dhe plotësisht anonim, nuk i kontrollon dhe nuk i ruan të dhënat tuaja, por ruhen kopje të skedarëve në server. Shembuj të shërbimeve të këtilla janë: cotse.com; anonymizer.com; hushmail.com etj.

[25] Mail-server – kompjuter i dedikuar për menaxhim të e-mail-eve

8. LLOJET E MASHTRIMEVE NË INTERNET

Skemat investuese – përdorimi i internetit për të dhënë përkrahje financiare për skema të larta teknike, siç janë ueb-faqet për shopping (blerje) virtuale ose ofruesit e shërbimeve të reja;

Skemat për kartelat kreditore – shfrytëzimi i detajeve të kartelave kreditore që janë marrë në mënyrë joligjore për blerjen nëpërmjet internetit të produkteve me vlerë të lartë;

Mundësitë për biznes/skemat për të punuar prej në shtëpi – shfrytëzimi i internetit për reklamimin e mundësive për biznes, me ç'rast viktima paguan që më parë për informatën ose produktin për punë;

Mashtrimi nigerian (të ashtuquajturat Mashtrimet 419) – mashtrime të Afrikës Perëndimore me mënyrë të ndryshuar të dërgesës. Tani përdoret porosia elektronike në vend të postës tradicionale ose faksit. Pjesa tjetër e qasjes është e njëjtë dhe ka rrezik potencialisht të madh për spaming.

Puna bankare në internet – kopjohet ueb-faqja e ndonjë banke, pak ndryshohet ueb-adresa, sigurohen linke deri te shërbimet ligjore bankare dhe vetëm një ose dy linke janë për investime të mëdha, që kërkojnë transfer të shumave të konsiderueshme, me qëllim që të sigurohet përfshirje në mundësi vërtet të pabesueshme për investime.

Thirrje për kontribute vullnetare për katastrofat – pjesa më e madhe e ueb-faqeve që kërkojnë ndihmë për vikimat e cunamit në Lindjen e Largët janë të rrejshme;

Herbal Viagra- në fushën e trajtimeve alternative mjekësore onlajn me të cilat spam-ohen shfrytëzuesit, pjesa më e madhe e produkteve nuk kanë efekte pozitive (poqese dërgohen fare) ose janë të rrezikshme për shëndetin e njeriut;

Nuset ruse – ueb-faqe që ofrojnë kontakte me femra të bukura nga Evropa Lindore dhe vizita të lira në vendet e ish-Bashkimit Sovjetik;

Fitimet në lotari – kërkesë për pagesën e fitimeve nga lotaria ose ndihmë për të fituar (zakonisht lotari të huaja);

Phishing – postë eletronike që ngjan sikur është nga ndonjë burim që njihet mirë (për shembull bankë ose dhënës i shërbimeve të internetit) me të cilën kërkohet të vërtetohen të dhënat personale.

9. SOFTUERËT E DËMSHËM

Malware – shkurtesë nga softuer keqdashës (malicious software) - është term i përgjithshëm me të cilin emërtohet një spektër i gjerë i softuerit armiqësor ose invaziv, gjegjësisht softuerit që përdoret me qëllim që të pengohet funksionimi i kompjuterit, të merren informata të ndjeshme, ose të hyhet në sisteme private kompjuterike. Mund të jetë në formë të kodit, skriptës, përmbajtjes aktive dhe llojeve të tjera të softuerit.

Në softuerin keqdashës bëjnë pjesë viruset kompjuterike, krimbat, trojanët, rootkit-ët, spyware-ët, adware-ët dhe programet e tjera keqdashëse. Pjesa më e madhe e kërcënimeve aktive nga softuerët keqdashës, zakonisht, janë trojanë ose krimba, kurse më pak viruse. Disa softuerë keqdashës mund të maskohen që të duken si softuer legjitim dhe madje mund të vijnë nga ueb-faqja zyrtare e ndonjë kompanie, në formë të programit të dobishëm ose tërheqës, ku është futur softueri keqdashës së bashku me softuerin për ndjekje, që mbledh të dhëna statistikore për qëllime të marketingut.

- *Llojet më të shpeshta të softuerit keqdashës janë:*

Virusi kompjuterik është një lloj i softuerit keqdashës, i cili, kur të ekzekutohet, replikohet duke futur kopje të veta (ndoshta të modifikuara) në programet e tjera kompjuterike, skedarë me të dhëna, ose në boot sektorin e hard-diskut. Kur ky replikim ka sukses, për pjesët që i ka përfshirë ai thuhet se janë të "infektuara". Viruset shpeshherë paraqesin aktivitet të dëmshëm te nikoqiri i infektuar, si për shembull, vjedhje të hapësirës së hard-diskut ose procesorit, hyrje në informatat private, komprometim të të dhënave, paraqitje të porosive politike ose humoristike në ekranin e shfrytëzuesit, spaming të kontakteve të tyre ose hyrje në shkurtesat e tyre. Megjithatë, jo të gjithë viruset kanë element destruktiv. Karakteristika definuese e viruseve është se ato janë programe kompjuterike që vetë-replikohen, që instalohen pa pëlqimin e shfrytëzuesit.

Kali i Trojës (Trojan horse) ose "trojani" është softuer keqdashës që nuk replikohet vetë dhe i cili kryen vepra që janë të caktuara me natyrën e tij, që zakonisht rezulton me humbje ose vjedhje të të dhënave dhe, sipas të gjitha gjasave, dëmtim të sistemit. Ky lloj i softuerit keqdashës shpeshherë funksionon nëpërmjet të ashtuquajturit "inxhinjering social", duke u paraqitur si program ose kod rutinor, i dobishëm ose interesant, me qëllim që të binden viktimat ta instalojnë atë në kompjuterët e tyre. Shpesh, trojani vepron si hyrje e prapme, dhe më pas krijuesi i tij mund të hyjë në mënyrë të paautorizuar te kompjuteri i infektuar. Trojanët nuk mund të dallohen lehtë, por, në qoftë se zhvillojnë aktivitete të konsiderueshme kompjuterike ose komunikative, munden ta ngadalësojnë dukshëm punën e kompjuterit. Trojanët nuk përpiqen të futen në programe ose të dhëna të tjera si viruset dhe nuk replikohen si krimbat.

Sulmi i distribuar për refuzim të shërbimit (DISTRIBUTED DENIAL-OF-SERVICES - DDoS) ose sulmi DdoS është përpjekje që kompjuteri ose ndonjë resurs i caktuar i rrjetit të bëhet i paqasshëm për shfrytëzuesit e fundit. Edhe pse mjetet për kryerjen e sulmit DDoS, e poashtu edhe motivet dhe qëllimet mund të ndryshojnë, ky lloj i sulmit zakonisht përbëhet nga përpjekjet që përkohësisht ose në kohë të pacaktuar ta ndërpresin ose ta suspendojnë ofrimin e shërbimeve të pajisjes që është e lidhur në internet. Kryerësit e sulmeve DdoS, zakonisht, i kanë si cak ueb-faqet ose shërbimet që janë vendosur në ueb-serverë me profil të lartë, siç janë bankat, portalet për pagesa nga kartelat bankare, e madje edhe serverët që janë përgjegjës për TLD. Kjo teknikë, sot më gjerësisht përdoret te disa lojëra ose përdoret nga ana e pronarëve të serverëve, ose, nga ana e konkurrentëve të pakënaqur. Gjithnjë e më shpesh, sulmet DoS, poashtu, shfrytëzohen edhe si formë e rezistencës. Për DoS thuhet se është vegël për shprehjen e mospajtimit ose, sipas disa analistëve, DoS është formë e "protestave rrugore në internet". Termi, në përgjithësi shfrytëzohet në lidhje me rrjetet kompjuterike, por nuk është i kufizuar vetëm në këtë fushë. Për shembull, ai përdoret edhe për menaxhimin me resurset e procesorit kryesor. Metoda e zakonshme e sulmit përfshin "ngopjen" (saturimin) e makinës që është cak i sulmit me kërkesa të jashtme për komunikim, në atë masë sa që nuk mund t'u përgjigjet kërkesave legjitime për trafik, ose, nga ana tjetër, reagon aq ngadalë sa që, në fakt, ajo bëhet e paqasshme. Sulmet DoS, zakonisht, çojnë deri në stërngarkimin e serverit. Në vija të përgjithshme, sulmet DoS kryhen në atë mënyrë që kompjuteri që është cak i sulmit detyrohet të resetohet ose t'i konsumojë resurset e tij në atë mënyrë sa që më nuk mund t'i sigurojë shërbimet e tij për të cilat është i dedikuar, ose pengohet mjeti për komunikim ndërmjet shfrytëzuesve legjitimë dhe viktimës, ashtu që ata nuk mund të komunikojnë ashtu siç duhet. Sulmet "Denial-of-service" konsiderohen si dhunim i politikës për shfrytëzimin e internetit që është krijuar nga ana e Këshillit për arkitekturën e internetit (Internet Architecture Board - IAB), e poashtu i shkelin edhe politikat për shfrytëzimin e arsyeshëm të, pothuajse të gjithë dhënësve të shërbimit të internetit. Ato, poashtu, zakonisht paraqesin edhe shkelje të ligjeve në disa vende.

Worms (Krimbat) – janë programe keqdashëse që shumëzohen në sistem. Qëllimi i tyre është të mundësojnë punë jo të rregullt të sistemit, sipas dëshirës së personit që e ka krijuar këtë kod keqdashës, gjegjësisht ta lëshojnë të kalojë ndonjë informatë e cila do të hynte dhe do të dilte nga sistemi pa lejen e tij.

Firewall - është pajisje harduerike ose program softuerik që mundëson të fitohet shkallë më e lartë e sigurisë në rrjet. Detyra e tij është ta bllokojë ose ta pamundësojë qarkullimin e të dhënave nëpër rrjet. Detyra e tij më e shpeshtë është ta bllokojë hyrjen e të dhënave nëpër porte që nuk janë të dedikuara për ato të dhëna, gjegjësisht të mundësojë që qarkullimi i të dhënave të bëhet nëpër portet e sakta, ndërsa trafiku tjetër të bllokohet.

- *Termet që përdoren më shpesh për kartelat për pagesë*

Skimers janë aparate që shfrytëzohen për mbledhjen e paautorizuar të të dhënave nga kartelat për pagesë, edhe atë të të dhënave që gjenden në shiritin magnetik të kartelës për pagesë dhe të të dhënave për PIN (Personal identification number) kodin e kartelës. Ka dy lloje të skimerëve: a) fiksë, që montohen në ATM (bankomate) dhe b) mobilë, që e lexojnë vetëm shënimin që gjendet në shiritin magnetik. Skimerët në vete përmbajnë disa komponente edhe atë:

- lexues të të dhënave nga shiriti magnetik,
- video kamerë për video-inçizim nga video-mbikëqyrja në pjesën e aparatit ku shfrytëzohet kartela për pagesë, e që gjendet në pjesën ku futet PIN kodi (çelësi autorizues) për përdorimin e kartelës për pagesë.

Skimerët në vete përmbajnë mjet për memorizimin e të dhënave që janë marrë nga pjesët e tjera të tij. Lexuesi i të dhënave nga shiriti magnetik i kartelës për pagesë është në formë të segmentit hyrës të ATM-së dhe nëpër të, në mënyrë të pahetueshme, kalon kartela për pagesë. Leximi i të dhënave mund të jetë:

- audio lexim (kur gjatë hyrjes së kartelës për pagesë në ATM, dëgjon zë të leximit, që në fakt paraqet audio komunikim ndërmjet ATM-së dhe kartelës për pagesë dhe në atë moment dëgjohet kodi që është regjistruar në kartelën për pagesë) dhe
- kur në skimer drejtpërdrejt regjistrohet përmbajtja nga kartela për pagesë dhe ruhet në mjetin për memorizim që është pjesë përbërëse e skimerit. Pjesa e dytë është video-kamerë ku futet kodi për autorizim, me ç'rast ky kod detektohet vizualisht dhe shkruhet në mjetin për memorizim.

Pastaj, këto të dhëna futen në kompjuter dhe me program të veçantë, të dhënat na shiriti magnetik marrin format të përshtatshëm në shirit tjetër magnetik si shënim magnetik. Hapi i ardhshëm është krahasimi me video-inçizimin për numrin që është futur si autorizim.

Mbledhësit mobilë të të dhënave (mobile skimmers) janë pajisje të cilat kriminelët i instalojnë në terminalet për pagesë (point of sale – POSterminal) ose në bankomate dhe të cilat i kopjojnë të dhënat për llogarinë e shfrytëzuesit në kartelën e futur për pagesë të shiritit magnetik, në anën e pasme të kartelës. Në qoftë se shfrytëzuesi përdor kartelë debitore për pagesë, së bashku me të dhënat e përmendura kopjohet edhe numri personal për identifikim i shfrytëzuesit (personal identification number - PIN). Të dhënat e kopjuara më vonë shfrytëzohen

për përgatitjen e kartelave të falsifikuara kreditore ose debitore për pagesë, për tërheqjen e parave nga bankomatet.

Plastic është çdo kartelë plastike që ka madhësi standarde dhe në të cilën është futur shirit magnetik, ku mund të futet shënimi magnetik. Nuk është me rëndësi që ana e përparme e kartelave plastike të jetë e plotësuar dhe e dizajnuar në qoftë se ato shfrytëzohen për ATM.

MSR 206 është aparat në të cilin futen të dhëna nga kartela për pagesë në shiritin magnetik të kartelës plastike.

Shiriti magnetik i kartelës për pagesë është shirit në të cilin vendosen të dhënat e bankës që e ka dhënë kartelën për pagesë, numri i llogarisë së bankës dhe emri i personit që është bartës i kartelës për pagesë. Interesante për të është se mund të shkruhen dhe të fshihen të dhëna pakufi shumë herë.

10. PIKËPAMJET PËRFUNDIMTARE TË AUTORËVE

E drejta për gjykim korrekt dhe të drejtë është e pacenueshme dhe për këtë arsye prokurori ka obligim dhe përgjegjësi që t'i sigurojë me kohë, t'i mbrojë dhe t'i prezantojë provat elektronike para gjykatës. Kjo e përcakton rolin proaktiv të prokurorit, i cili tani, duke e pasur parasysh pozitën e re gjatë hetimit, duhet të posedojë njohuri adekuate edhe nga fusha e krimit kompjuterik.

Prokurori duhet ta dijë se si funksionon kompjuteri dhe rrjetet e internetit, si t'i kuptojë raportet e ekspertëve nga kjo fushë dhe duhet ta dijë se në ç'drejtim dhe në çfarë mënyre do ta zhvillojë hetimin dhe çfarë obligimesh do t'i japë policisë gjyqësore. Gjatë gjithë procedurës, prokurori duhe të ketë njohuri dhe shkathtësi për mënyrën në të cilën do të bëjë mbikëqyrje të provave të mbledhura, si t'i mbledhë dhe si t'i sigurojë ato, veçanërisht nëse provat janë siguruar jashtë juridiksionit tonë. Nga përgatitja dhe profesionalizmi i prokurorit do të varet edhe rezultati i procedurës.

Mu për këtë arsye, prokurori, së bashku me policinë gjyqësore, duhet të bëjë përpjekje maksimale për mbledhjen e provave elektronike, të cilat do të jenë bazë për ndërtimin e rastit të fuqishëm dhe të prezantuar mirë në gjykatë.

Teknologjia e avancuar nënkupton edhe rritje të numrit të pajisjeve që mund të përmbajnë prova elektronike. Prandaj, çdokush që është i kyçur në procesin e zbulimit të këtij lloji të krimit duhet ta dijë se për çdo ditë zgjerohet lista e provave dhe e pajisjeve potenciale që përmbajnë informata elektronike dhe të cilat mund të funksionojnë individualisht ose të bashkuara me sistemin kompjuterik.

Procesi i këtillë nënkupton përditësimin e vazhdueshëm të dispozitave ligjore, të cilat duhet ta ndjekin tempon e shpejtë të zhvillimit të formave të reja të këtij lloji të krimit, e me këtë edhe normimin dhe sanksionimin e tyre adekuat.

Ky doracak është mjet themelor ndihmës gjatë veprimit të përditshëm, që në aspekt përmbajtësor i përfshin termet kryesore – të përgjithshme nga fusha e krimit kompjuterik, por kjo do të thotë edhe obligim i vazhdueshëm për edukimin e prokurorit.

Shtojca 1

Dispozita nga Kodi Penal që kanë të bëjnë me krimin kompjuterik

Neni 144

Ai që nëpërmjet sistemit informatik do të kërcënohet se do të bëjë vepër penale për të cilën është paraparë dënim me burg prej pesë vitesh ose dënim më i rëndë, kundër ndonjë personi, për shkak të përkatësisë së tij nacionale, etnike, fetare ose grupi racor.

Neni 149

(1) Ai që në kundërshtim me kushtet e përcaktuara me ligj, pa pëlqim të qytetarit, i mbledh, i përpunon ose i shfrytëzon të dhënat e tij personale, do të dënohet me dënim me para ose me dënim me burg deri në një vjet.

(2) Me dënimin nga paragrafi 1 dënohet ai që do të hyjë në sistemin informatik kompjuterik me të dhëna personale, me qëllim që duke i shfrytëzuar ato për vete ose për dikë tjetër, të realizojë ndonjë dobi ose dikujt tjetër t'i shkaktojë ndonjë dëm.

Neni 149-a

(1) Ai që në mënyrë të paautorizuar e pengon ose e kufizon dikë tjetër të hyjë në një sistem publik informatik, do të dënohet me dënim me para ose me dënim me burg deri në një vjet.

(2) Nëse veprën nga paragrafi 1 e kryen personi zyrtar gjatë ushtrimit të detyrës ose personi përgjegjës në një sistem publik informatik, do të dënohet me dënim me para ose me dënim me burg prej tre muaj deri në tre vjet.

(3) Nëse veprën nga paragrafi 1 e kryen personi juridik, do të dënohet me dënim me para.

(4) Ndjekja bëhet në bazë të padisë private.

Neni 157

(1) Ai që në emrin e tij ose në emrin e dikujt tjetër, në mënyrë të paautorizuar do të publikojë, paraqesë, reprodukojë, shfaqë, emitojë ose në ndonjë mënyrë

tjetër të paautorizuar do t'ia marrë dikujt tjetër të drejtën e autorit ose ndonjë të drejtë tjetër të lidhur me të, gjegjësisht veprën autoriale, shfaqjen ose diçka që i takon të drejtës tjetër të lidhur me të, do të dënohet me dënim me para ose me dënim me burg deri në një vjet.

(2) Ai që me veprën nga paragrafi 1 ka përfituar dobi më të madhe pronësore, do të dënohet me dënim me burg prej tre muaj deri në tre vjet.

(3) Ai që me veprën nga paragrafi 1 ka përfituar dobi të konsiderueshme pronësore, do të dënohet me dënim me burg prej gjashtë muaj deri në pesë vjet.

(4) Tentimi është i dënueshëm.

(5) Kopjet e veprave autoriale dhe sendet që u takojnë të drejtave të lidhura me veprat autoriale, si dhe mjetet për reprodukim, konfiskohen.

(6) Nëse veprën nga paragrafi 1 e kryen personi juridik, do të dënohet me dënim me para.

Neni 157-a

(1) Ai që pa lejen e distributorit të autorizuar të sinjalit satelitor të mbrojtur në mënyrë të veçantë teknike, prodhon, importon, distribuon, huazon ose në ndonjë mënyrë tjetër e vë në dispozicion të publikut, gjegjësisht ofron shërbime të vendosjes së pajisjes ose sistemit material ose jomaterial, me qëllim të zbërthimit të sinjalit të tillë, do të dënohet me burg prej gjashtë muaj deri në tre vjet.

(2) Nëse me veprën nga paragrafi 1 është përfituar dobi e konsiderueshme pronësore ose është shkaktuar dëm i konsiderueshëm, do të dënohet me burg prej një deri në pesë vjet.

(3) Ai që pranon sinjal satelitor të mbrojtur në mënyrë të veçantë teknike, mbrotja e të cilit është zbërthyer pa lejen e distributorit të tij të autorizuar ose bën distribuim të mëtutjeshëm të sinjalit të tillë, do të dënohet me burg prej gjashtë muaj deri në tre vjet.

(4) Nëse me veprën nga paragrafi 3 është përfituar dobi e konsiderueshme pronësore ose është shkaktuar dëm i konsiderueshëm, do të dënohet me burg prej një deri në pesë vjet.

(5) Nëse veprën nga ky nen e kryen personi juridik, do të dënohet me dënim me para.

(6) Sendet që kanë qenë të dedikuara ose që janë shfrytëzuar për kryerjen e veprës ose që janë krijuar gjatë kryerjes së veprës, konfiskohen.

Neni 157-b

(1) Ai që pa lejen e producentit filmik ose distributorit të autorizuar, të cilit producenti filmik ia ka bartur të drejtën e tij të veprës audiovizuale, prodhon, importon, reprodukon, distribuon, memorizon, huazon, lëshon në qarkullim ose në ndonjë mënyrë tjetër e vë në dispozicion të publikut ose ndërmerr veprime të tjera për distribuim, huazim, shfaqje publike, lëshim në qarkullim, vënie në dispozicion të publikut ose në ndonjë mënyrë tjetër e shfrytëzon në mënyrë kundërligjore veprën audiovizuale, gjegjësisht videogramin ose kopjet e tij të shumëzuara në mënyrë të paautorizuar, do të dënohet me burg prej gjashtë muajsh deri në tre vjet.

(2) Nëse me veprën nga paragrafi 1 është përfituar dobi e konsiderueshme pronësore ose është shkaktuar dëm i konsiderueshëm, do të dënohet me burg prej një deri në pesë vjet.

(3) Nëse veprën nga ky nen e kryen personi juridik, do të dënohet me dënim me para.

(4) Sendet që kanë qenë të dedikuara ose që janë shfrytëzuar për kryerjen e veprës ose që janë krijuar gjatë kryerjes së veprës, konfiskohen.

Neni 157-c

(1) Ai që pa lejen e prodhuesit të fonogramit ose të shoqatës për realizimin e të të drejtave të prodhuesve të fonogrameve prodhon, reprodukon, distribuon, memorizon, huazon, lëshon në qarkullim ose në ndonjë mënyrë tjetër e vë në dispozicion të publikut ose ndërmerr veprime të tjera për distribuim, huazim, shfaqje publike, lëshim në qarkullim, vënie në dispozicion të publikut ose në ndonjë mënyrë tjetër e shfrytëzon në mënyrë kundërligjore fonogramin ose kopjet e tij të shumëzuara në mënyrë të paautorizuar, do të dënohet me burg prej gjashtë muajsh deri në tre vjet.

(2) Nëse me veprën nga paragrafi 1 është përfituar dobi e konsiderueshme pronësore ose është shkaktuar dëm i konsiderueshëm, do të dënohet me burg prej një deri në pesë vjet.

(3) Nëse veprën nga ky nen e kryen personi juridik, do të dënohet me dënim me para.

(4) Sendet që kanë qenë të dedikuara ose që janë shfrytëzuar për kryerjen e veprës ose që janë krijuar gjatë kryerjes së veprës, konfiskohen.

Neni 193-a

(1) Ai që prodhon pornografi të fëmijëve me qëllim të distribuimit të saj ose që e transmeton ose e ofron ose në ndonjë mënyrë tjetër e vë në dispozicion pornografinë e fëmijëve, do të dënohet me së paku pesë vjet burg.

(2) Ai që siguron pornografi të fëmijëve për vete ose për dikë tjetër ose që posedon pornografi të fëmijëve, do të dënohet me burg prej pesë deri në tetë vjet.

(3) Nëse vepra nga paragrafet (1) dhe (2) të këtij neni është kryer nëpërmjet sistemit kompjuterik ose ndonjë mjeti tjetër për komunikim masiv, kryerësi do të dënohet me së paku tetë vjet burg.

(4) Nëse veprën nga ky nen e kryen personi juridik, do të dënohet me dënim me para.

Neni 193-b

Ai që nëpërmjet mjeteve kompjuterike-komunikuese për caktim të takimit ose në ndonjë mënyrë tjetër e mashtron ndonjë të mitur që nuk ka mbushur 14 vjet për të kryer marrëdhënie seksuale ose ndonjë akt tjetër seksual ose për të prodhuar pornografi të fëmijëve dhe nëse me këtë qëllim është realizuar takim i drejtpërdrejtë me të miturin, do të dënohet me burg prej një deri në pesë vjet.

Neni 251

(1) Ai që në mënyrë të paautorizuar do të fshijë, ndryshojë, dëmtojë, fshehë ose në ndonjë mënyrë tjetër do ta bëjë të papërdorshëm ndonjë të dhënë kompjuterike ose program kompjuterik ose pajisje për mirëmbajtjen e sistemit informatik ose do ta pamundësojë ose do ta vështirësojë shfrytëzimin e sistemit kompjuterik, informatës ose programit ose të komunikimit kompjuterik, do të dënohet me dënim me para ose me burg deri në tre vjet.

(2) Me dënimin nga paragrafi 1 do të dënohet edhe ai që në mënyrë të paautorizuar do të hyjë në ndonjë kompjuter ose sistem të huaj, me qëllim të shfrytëzimit të të dhënave ose programeve të tij, për të përvetësuar dobi pronësore ose ndonjë dobi tjetër në mënyrë kundërligjore, për veten e tij ose për dikë tjetër, ose për të shkaktuar dëm pronësor ose ndonjë dëm tjetër ose për t'i transferuar të dhënat kompjuterike që nuk janë të dedikuara për të dhe deri te të cilat ka ardhur në mënyrë të paautorizuar si person i paftuar.

(3) Me dënimin nga paragrafi (1) i këtij neni do të dënohet ai që në mënyrë të paautorizuar, me përdorimin e mjeteve teknike, do të interceptojë transfer të të dhënave kompjuterike që nuk kanë karakter publik, deri te, prej dhe brenda sistemit të caktuar kompjuterik, duke i përfshirë edhe emetimet elektromagnetike nga sistemi kompjuterik që mund të punojë me të dhënat e tilla kompjuterike.

(4) Ai që veprat nga paragrafet (1), (2) dhe (3) të këtij neni do t'i kryejë ndaj sistemit kompjuterik, të dhënave ose programeve që janë të mbrojtura me masa të veçanta mbrojtëse ose që shfrytëzohen në punën e organeve shtetërore, ndërmarrjeve publike ose institucioneve publike ose në komunikimet ndërkombëtare, ose si anëtar i grupit të krijuar për kryerjen e veprave të tilla, do të dënohet me burg prej një deri në pesë vjet.

(5) Nëse me veprën nga paragrafet (1), (2) dhe (3) të këtij neni është përfituar dobi e konsiderueshme pronësore ose është shkaktuar dëm i konsiderueshëm, do të dënohet me burg prej gjashtë muajsh deri në në pesë vjet.

(6) Nëse me veprën nga paragrafi (4) është përfituar dobi e konsiderueshme pronësore ose është shkaktuar dëm i konsiderueshëm, do të dënohet me burg prej një deri në dhjetë vjet.

(7) Ai që në mënyrë të paautorizuar përgatit, furnizon, shet, mban ose vë në dispozicion të të tjerëve pajisje, mjete, fjalëkalim kompjuterik, kod për qasje ose ndonjë të dhënë të ngjashme me të cilën tërësia ose një pjesë e sistemit kompjuterik aftësohet për qasje, programe kompjuterike ose të dhëna kompjuterike të dedikuara ose të përshtatshme për kryerjen e veprave nga paragrafet (1), (2) dhe (3) të këtij neni, do të dënohet me dënim me para ose me dënim me burg deri në një vjet.

(8) Tentimi për t'i kryer veprat nga paragrafet 1 dhe 2 është i dënueshëm.

(9) Nëse veprën nga ky nen e kryen personi juridik, do të dënohet me dënim me para.

(10) Pajisjet e veçanta, mjetet, programet kompjuterike ose të dhënat që janë dedikuar për kryerjen e veprës do të konfiskohen.

Neni 251-a

(1) Ai që do të bëjë ose do të marrë prej dikujt tjetër ndonjë virus kompjuterik me qëllim që ta fusë atë te ndonjë kompjuter i huaj ose rrjet i huaj kompjuterik, do të dënohet me dënim me para ose me dënim me burg deri në një vjet.

(2) Ai që me përdorimin e virusit kompjuterik do të shkaktojë dëm te ndonjë kompjuter, sistem, e dhënë ose program i huaj, do të dënohet me burg prej gjashtë muaj deri në tre vjet.

(3) Nëse me veprën nga paragrafi 2 është shkaktuar dëm më i madh ose nëse vepra është kryer në kuadër të grupit që është krijuar për kryerjen e veprës së tillë, kryerësi do të dënohet me burg prej një deri në pesë vjet.

(4) Tentimi për ta kryer veprën nga paragrafi 2 është i dënueshëm.

(5) Nëse veprën nga ky nen e kryen personi juridik, do të dënohet me dënim me para.

Neni 251-b

(1) Ai që ka për qëllim që për vete ose për dikë tjetër të përfitojë dobi të kundërligjshme pronësore duke futur në kompjuter ose në ndonjë sistem kompjuterik të dhëna të pavërteta, duke mos futur të dhëna të vërteta, duke ndryshuar, duke fshirë ose duke fshehur të dhëna të vërteta, duke ndryshuar, duke fshirë ose duke fshehur të dhëna kompjuterike, duke falsifikuar nënshkrimin elektronik ose në ndonjë mënyrë tjetër do të shkaktojë rezultat të pavërtetë gjatë përpunimit elektronik dhe transferimit të të dhënave, do të dënohet me dënim me para ose me dënim me burg deri në tre vjet.

(2) Nëse kryerësi ka përvetësuar dobi më të madhe pronësore, do të dënohet me burg prej tre muaj deri në pesë vjet.

(3) Nëse kryerësi ka përvetësuar dobi të konsiderueshme pronësore, do të dënohet me burg prej një deri në dhjetë vjet.

(4) Ai që veprën nga paragrafi 1 do ta kryejë me qëllim që ta dëmtojë dikë tjetër, do të dënohet me dënim me para ose me dënim me burg deri në një vjet.

(5) Nëse me veprën nga paragrafi 4 është shkaktuar dëm më i madh, autori do të dënohet me burg prej tre muaj deri në tre vjet.

(6) Ai që në mënyrë të paautorizuar përgatit, furnizon, shet, mban ose vë në dispozicion të të tjerëve pajisje të veçanta, mjete, programe kompjuterike ose të dhëna kompjuterike të dedikuara për kryerjen e veprës nga paragrafi 1, do të dënohet me dënim me para ose me dënim me burg deri në një vjet.

(7) Tentimi për t'i kryer veprat nga paragrafet 1 dhe 4 është i dënueshëm.

(8) Nëse veprën nga ky nen e kryen personi juridik, do të dënohet me dënim me para.

(9) Pajisjet e veçanta, mjetet, programet kompjuterike ose të dhënat që janë dedikuar për kryerjen e veprës do të konfiskohen.

(10) Për veprën nga paragrafi 4, ndjekja bëhet në bazë të padisë private.

Neni 271

(1) Ai që bën, furnizon, shet, ose jep në përdorim mjete për bërjen e shenjave të rrejshme për vlerë, do të dënohet me dënim me para ose me dënim me burg deri në një vjet.

(2) Ai që në mënyrë të paautorizuar përpunon, furnizon, mban, shet ose jep në përdorim instrumente, sende, programe kompjuterike dhe mbrojtje tjera të sigurimit ose komponente që shërbejnë për mbrojtje nga falsifikimi, si dhe mjete për marrje të paautorizuar të të dhënave bankare, me qëllim që të bëjë para të rrejshme ose t'i ndryshojë paratë e vërteta ose instrumentet e tjera për pagesë, letrat me vlerë ose kartelat e rrejshme për pagesë, do të dënohet me burg prej tre deri në dhjetë vjet.

Neni 274-b

(1) Ai që do të bëjë kartelë të rrejshme për pagesë me qëllim që ta shfrytëzojë atë si të vërtetë, ose pajiset me kartelë të rrejshme me qëllim të atillë, ose do t'ia japë dikujt tjetër për ta përdorur ose ai që kartelën e rrejshme do ta përdorë si të vërtetë, do të dënohet me burg prej gjashtë muaj deri në pesë vjet dhe me dënim me para.

(2) Me dënimin nga paragrafi (1) i këtij neni do të dënohet edhe ai që merr të dhëna bankare nga kartelat e vërteta për pagesë dhe të dhëna për bartësit e atyre kartelave për pagesë, me qëllim t'i shfrytëzojë ato që të bëjë dhe të përdorë kartelë të rrejshme për pagesë ose të dhënat që i ka marrë në këtë mënyrë ia jep dikujt tjetër me qëllim të atillë.

(3) Nëse kryerësi i veprës nga paragrafi (1) i këtij neni përfiton dobi më të madhe pronësore, do të dënohet me burg prej një deri në tetë vjet.

(4) Nëse vepra nga paragrafet (1), (2) dhe (3) të këtij neni është kryer nga anëtari i ndonjë grupi, bande ose shoqate tjetër kriminele, kryerësi do të dënohet me burg së paku prej katër vjetësh.

(5) Nëse veprën nga ky nen e kryen personi juridik, do të dënohet me dënim me para.

Neni 286

(1) Ai që, me qëllim që ta dëmtojë dikë tjetër ose të fitojë dobi të kundërligjshme pronësore, në mënyrë të paautorizuar do të dorëzojë fletëparaqitje për patentë ose në fletëparaqitje nuk do ta shënojë ose rrejshëm do ta shënojë shpikësin ose do ta vë në dispozicion të publikut thelbin e zbulimit, para se të shpallet në mënyrë të paraparë me ligj, do të dënohet me dënim me të holla ose me burg deri në tre vjet.

(2) Me dënimin nga paragrafi (1) të këtij neni do të dënohet ai i cili me qëllim që ta dëmtojë dikë tjetër ose të fitojë dobi të kundërligjshme pronësore, në mënyrë të paautorizuar do të prodhojë, do të lëshojë në qarkullim, do të eksportojë, do të importojë, do të ofrojë në shitje, do ta depozitojë ose do ta shfrytëzojë ndonjë prodhim ose procedurë që është e mbrojtur me patentë ose në mënyrë

të paautorizuar do të përdorë, riprodhojë, eksportojë, importojë ose distribuojë topografi të mbrojtur të qarkut integral ose softuerit.

(3) Ai që me veprën nga paragrafet (1) dhe (2) të këtij neni ka fituar dobi

të konsiderueshme pronësore ose ka shkaktuar dëm të konsiderueshëm pronësor, do të dënohet prej një deri në pesë vjet burg dhe dënim me para.

(4) Nëse vepra nga paragrafet (1) dhe (2) është kryer nga një grup i organizuar ose me veprën është shkaktuar rrezik për jetën dhe shëndetin e njerëzve, kryerësi do të dënohet me dënim me para ose me burg së paku prej tre vjetësh.

(5) Nëse veprën nga ky nen e kryen personi juridik, do të dënohet me dënim me para.

(6) Sendet që janë bërë apo që janë shfrytëzuar për kryerjen e veprës penale do të konfiskohen.

Neni 379-a

(1) Ai i cili me qëllim që t'i përdorë si të vërteta, në mënyrë të paautorizuar do të përpunojë, do të fusë, do të ndryshojë ose do të bëjë të papërdorshme të dhëna kompjuterike ose programe që janë caktuar ose që janë të përshtatshme të shërbejnë si prova për fakte që kanë vlerë për raportet juridike ose ai që të dhënat ose programet e tilla do t'i përdorë si të vërteta, do të dënohet me dënim me para ose me burg deri në tre vjet.

(2) Nëse vepra nga paragrafi 1 është kryer në lidhje me të dhëna kompjuterike ose programe që përdoren në punën e organeve shtetërore, insttitucioneve publike, ndërmarrjeve ose personave të tjerë juridikë dhe fizikë që kryejnë punë me interes publik ose në trafikun juridik me vendet e huaja ose nëse me përdorimin e tyre është shkaktuar dëm i konsiderueshëm, kryerësi do të dënohet me burg prej një deri në pesë vjet.

(3) Ai që në mënyrë të paautorizuar përgatit, furnizon, shet, mban ose vë në dispozicion të të tjerëve pajisje të veçanta, mjete, programe kompjuterike ose të dhëna kompjuterike që janë të dedikuara ose që janë të përshtatshme për kryerjen e veprës nga paragrafi 1, do të dënohet me dënim me para ose me dënim me burg deri në tre vjet.

(4) Tentimi për t'i kryer veprat nga paragrafet 1 dhe 2 është i dënueshëm.

(5) Pajisjet e veçanta, mjetet, programet kompjuterike ose të dhënat që janë dedikuar për kryerjen e veprës do të konfiskohen.

Neni 394-d

(1) Ai që nëpërmjet sistemit kompjuterik në publik shpërndan material të shkruar racist dhe ksenofob, fotografi ose ndonjë prezantim tjetër të idesë ose teorisë që ndihmon, promovon ose nxit urrejtje, diskriminim ose dhunë, kundër cilit do qoftë person apo grup, në bazë të racës, ngjyrës së lëkurës, prejardhjes nacionale ose etnike, si dhe bindjes fetare, do të dënohet me burg prej një deri në pesë vjet.

(2) Me dënimin nga paragrafi (1) i këtij neni do të dënohet edhe ai që do ta kryejë veprën nëpërmjet mjeteve tjera të informimit publik.

(3) Ai që veprën nga paragrafet (1) dhe (2) të këtij neni e kryen duke e keqpërdorur pozitën ose autorizimin ose nëse për shkak të atyre veprave kanë ndodhur trazira dhe dhunë mbi njerëzit ose është bërë dëm i pronës në përmasa të mëdha, do të dënohet me burg prej një deri në dhjetë vjet.

Shtojca 2

Dispozitat procedurale të Konventës për krimin kompjuterik

Seksioni 2 – E drejta procedurale

Titulli 1 – Dispozitat e përgjithshme

Neni 14 – Sfera e zbatimit të dispozitave procedurale

(1) Çdo Palë do të miratojë legjislacion të tillë dhe masa të tjera të nevojshme që të vendosen kompetencat dhe procedurat e parapara në këtë seksion me qëllim që të mundësohet ndërmarrja e veprimeve dhe procedurave të veçanta hetuese.

(2) Përveç në rastet kur në mënyrë eksplicite është paraparë procedurë tjetër, sikurse në rastet e parapara me dispozitën e nenit 21, çdo Palë do të vendosë kompetenca dhe procedura të parapara në paragrafin 1 të këtij neni, për:

a. veprat penale të parapara me nenet 2 deri në 11 të kësaj Konvente;

b. veprat të tjera penale të kryera me ndihmën e sistemit kompjuterik; dhe

c. mbledhjen e provave në formë elektronike për një vepër penale;

(3)

a. Çdo Palë mund ta rezervojë të drejtën t'i zbatojë masat e parapara në nenin 20 vetëm për veprat ose kategoritë e veprave të të specifikuara në rezervë, me kusht që fusha e veprave të tilla ose i kategorive të veprave të tilla të mos jetë më i kufizuar se sa fusha e veprave ndaj të cilave do të zbatohen masat e parapara me nenin 21. Çdo Palë do ta shqyrtojë mundësinë për ta kufizuar rezervimin e saj që të mundësojë zbatim sa më të gjerë të masave të parapara në nenin 20.

b. Kur një Palë, për shkak të kufizimeve të parapara në legjislacionin e vendit, të cilat janë në fuqi në momentin e miratimit të kësaj Konvente, nuk ka mundësi t'i zbatojë masat 20 dhe 21 sa i përket komunikimeve të transmetuara brenda sistemit kompjuterik të një dhënësi të shërbimeve, sistemi i të cilit:

i shërben dhe shfrytëzohet nga një grup i vogël shfrytëzuesish; dhe

ii nuk përdor rrjete publike të komunikimeve dhe nuk është i lidhur me ndonjë sistem kompjuterik, qoftë publik ose privat, atëherë kjo Palë mund ta rezervojë të drejtën të mos i zbatojë këto për komunikimet e tilla. Çdo Palë do ta shqyrtojë mundësinë për ta kufizuar rezervimin e saj që të mundësojë zbatim sa më të gjerë të masave të parapara në nenet 20 dhe 21.

Neni 15 – Kushtet dhe garancitë

(1) Çdo Palë siguron që themelimi, implementimi dhe zbatimi i kompetencave i procedurave të parapara në këtë seksion t'u nënshtrohen kushteve dhe garancive të parapara me legjislacionin e vendit, me të cilat sigurohet mbrojtje përkatëse e të drejtave dhe lirive të njeriut, duke i përfshirë edhe të drejtat që rrjedhin nga obligimet që Pala i ka marrë përsipër me nënshkrimin e Konventës së Këshillit të Evropës të vitit 1950 për Mbrojtjen e të Drejtave të Njeriut dhe Lirive Themelore, Marrëveshjes Ndërkombëtare të Kombeve të Bashkuara të vitit 1966 për të Drejtat Qytetare dhe Politike dhe instrumenteve të tjera ndërkombëtare për mbrojtjen e të drejtave të njeriut, të cilat do ta përfshijnë parimin e proporcionalitetit.

(2) Këto kushte dhe garanci, në varësi nga natyra e procedurës ose e kompetencës, ndër të tjera, e përfshijnë mbikëqyrjen gjyqësore ose ndonjë mbikëqyrje tjetër të pavarur, bazat që e arsyetojnë zbatimin e tyre dhe kufizimet e diapazonit dhe të kohëzgjatjes së kompetencave ose procedurave.

(3) Deri në masën që është në përputhje me interesin publik, e veçanërisht me interesin për zbatim të drejtë apo të shëndetshëm të drejtësisë, çdo Palë do ta marrë parasysh ndikimin e kompetencave dhe procedurave të parapara në këtë seksion, mbi të drejtat, përgjegjësitë dhe interesat legjitime të Palëve të treta.

Titulli 2 – Ruajtja e përshpejtuar e të dhënave kompjuterike të memorizuara

Neni 16 - Ruajtja e përshpejtuar e të dhënave kompjuterike të memorizuara

(1) Çdo Palë do të miratojë legjislacion të tillë dhe masa të tjera, që janë të nevojshme t'u mundësojë organeve të saj kompetente të urdhërojnë apo në mënyrë të ngjashme të sigurojnë ruajtje të menjëhershme të të dhënave specifike kompjuterike, duke i përfshirë të dhënat e trafikut që kanë qenë të memorizuara nëpërmjet një sistemi kompjuterik, e në veçanti atëherë kur ka bazë për të besuar se të dhënat kompjuterike janë të ekspozuara ndaj humbjeve apo modifikimeve.

(2) Kur një Palë e zbaton paragrafin 1 të këtij neni nëpërmjet një urdhëri ndaj një personi që t'i ruajë të dhënat kompjuterike specifike të memorizuara, të cilat i posedon apo janë nën kontrollin e tij, Pala do të miratojë legjislacion të tillë dhe masa të tjera që janë të nevojshme ta detyrojnë atë person që ta sigurojë dhe ta mirëmbajë integritetin e të dhënave kompjuterike për aq kohë sa të jetë e nevojshme, por jo më shumë se nëntëdhjetë ditë, që t'u mundësojë organeve kompetente ta kërkojnë hapjen e tyre. Pala mund të parashohë që urdhëri i tillë të rinovohet herë pas here.

(3) Çdo Palë do të miratojë legjislacion të tillë dhe masa të tjera, që janë të nevojshme ta detyrojnë mbikëqyrësin apo personin tjetër që duhet t'i ruajë të dhënat kompjuterike, që procedurat e ndërmarra t'i mbajë në fshehtësi për aq kohë sa është paraparë me legjislacionin e vendit.

(4) Kompetencat dhe procedurat e parapara me këtë nen u nënshtrohen dispozitave të neneve 14 dhe 15.

Neni 17 - Ruajtja e përshpejtuar dhe hapja e pjesshme e të dhënave të trafikut

(1) Çdo Palë do të miratojë, sa i përket të dhënave të trafikut që duhet të ruhen sipas nenit 16, legjislacion të tillë dhe masa të tjera që janë të nevojshme:

a. që të mundësohet ruajtja e përshpejtuar e të dhënave të trafikut, pavarësisht nëse një apo më tepër dhënës të shërbimeve kanë qenë të përfshirë në transmetimin e atij komunikimi; dhe

b. që të mundësohet hapja e përshpejtuar para organeve kompetente të Palës apo para personit të caktuar nga organi kompetent, të një sasie të mjaftueshme të të dhënave të trafikut, që Pala të mund ta identifikojë dhënësin e shërbimit dhe shtegun, nëpërmjet të cilit është transmetuar komunikimi.

(2) Kompetencat dhe procedurat e parapara me këtë nen u nënshtrohen dispozitave të neneve 14 dhe 15.

Titulli 3 – Urdhëri për prodhim

Neni 18 – Urdhëri për prodhim

(1) Çdo Palë do të miratojë një legjislacion të tillë dhe masa të tjera që janë të nevojshme që organet kompetente të saj të jenë të autorizuara t'i japin urdhër:

a. personit që gjendet në territorin e saj që të dorëzojë të dhëna kompjuterike të specifikuara që i posedon apo janë nën kontrollin e tij, e të cilat janë memorizuar në një sistem kompjuterik apo në një mjet që shërben për memorizimin e të dhënave kompjuterike; dhe

b. dhënësit të shërbimeve, i cili i ofron shërbimet e tij në territorin e Palës, që të dorëzojë informacion për parapaguesit, në lidhje me shërbimet që i posedon apo janë nën kontrollin e këtij dhënësi të shërbimeve.

(2) Kompetencat dhe procedurat e parapara me këtë nen u nënshtrohen dispozitave të neneve 14 dhe 15.

(3) Për qëllimet e këtij neni, shprehja "informacion për parapaguesin" nënkupton çfarëdo informacion të futur në formën e të dhënave kompjuterike apo çfarëdo forme tjetër, që mbahet nga dhënësi i shërbimit, e që ka të bëjë me parapaguesit e shërbimeve të tij, të ndryshme nga të dhënat e trafikut ose të përmbajtjes, nëpërmjet të cilave mund të përcaktohet:

a. lloji i shërbimit të komunikimit që përdoret, kushtet teknike dhe periudha në të cilën jepet shërbimi;

b. identiteti i parapaguesit, adresa e tij postale apo gjeografike, numri i tij i telefonit apo ndonjë numër tjetër për qasje, si dhe informacioni për faturat dhe pagesën, të cilat janë në dispozicion në bazë të marrëveshjes apo aranzhmanit për dhënien e shërbimit;

c. çdo informacion tjetër që mund të merret në vendin ku janë instaluar pajisjet e komunikimit, e që është në dispozicion në bazë të marrëveshjes apo aranzhmanit për dhënien e shërbimit.

Titulli 4 - Kërkimi dhe konfiskimi i të dhënave kompjuterike të memorizuara

Neni 19 - Kërkimi dhe konfiskimi i të dhënave kompjuterike të memorizuara

(1) Çdo Palë do të miratojë legjislacion të tillë dhe masa të tjera, që janë të nevojshme për t'u dhënë autorizim organeve kompetente të kërkojnë apo, në mënyrë të ngjashme, të hyjnë:

a. në një sistem kompjuterik apo në një pjesë të tij, si dhe në të dhënat kompjuterike të memorizuara aty; dhe

b. në një mjet memorizimi të të dhënave kompjuterike, ku mund të memorizohen të dhënat kompjuterike, dhe i cili gjendet në territorin e saj.

(2) Çdo Palë do të miratojë legjislacion të tillë dhe masa të tjera, që janë të nevojshme të sigurojnë që kur organet kompetente të saj kërkojnë apo në mënyrë të ngjashme hyjnë në një sistem kompjuterik specifik apo në një pjesë të tij sipas paragrafit 1.a. dhe kur kanë bazë për të besuar se të dhënat e kërkuara janë memorizuar në ndonjë sistem tjetër kompjuterik apo në një pjesë së tij, që gjendet në territorin e saj, të mund të hyjnë në të dhënat e tilla në mënyrë të ligjshme nëpërmjet sistemit fillestar kompjuterik dhe të mund mënyrë të përshpejtuar ta zgjerojnë kërkimin ose ndërmarrjen e veprimeve të ngjashme për të hyrë në sistemin tjetër.

(3) Çdo Palë do të miratojë legjislacion të tillë dhe masa të tjera që janë të nevojshme për t'u dhënë autorizim organeve kompetente të saj që t'i konfiskojnë ose në ndonjë mënyrë të ngjashme t'i sigurojnë të dhënat kompjuterike në të cilat kanë hyrë në përputhje me paragrafet 1 dhe 2. Këto masa do ta përfshijnë kompetencën:

a. për të konfiskuar ose në ndonjë mënyrë të ngjashme për të siguruar një sistem kompjuterik apo një pjesë të tij ose një mjet për memorizimin e të dhënave kompjuterike;

b. për të bërë ose për të mbajtur një kopje të këtyre të dhënave kompjuterike;

c. për ta mirëmbajtur integritetin e të dhënave relevante të memorizuara kompjuterike; dhe

d. për t'i bërë të paqasashme apo për t'i hequr këto të dhëna kompjuterike nga sistemi kompjuterik në të cilin ka qasje.

(4) Çdo Palë do të miratojë legjislacion të tillë dhe masa të tjera, që janë të nevojshme për t'u dhënë autorizim organeve kompetente që ta urdhërojnë çdo person i cili ka njohuri për mënyrën e funksionimit të sistemit kompjuterik apo masat që duhet të ndërmerren për mbrojtjen e të dhënave kompjuterike në të, që të japin, në masë të arsyeshme ose të nevojshme, informata që të mund të ndërmerren masat e parapara në paragrafet 1 dhe 2.

(5) Kompetencat dhe procedurat e parapara me këtë nen u nënshtrohen dispozitave të neneve 14 dhe 15.

Titulli 5 - Mbledhja e të dhënave kompjuterike në kohën reale

Neni 20 - Mbledhja e të dhënave kompjuterike në kohën reale

(1) Çdo Palë do të miratojë legjislacion të tillë dhe masa të tjera, që janë të nevojshme që organet kompetente të saj të kenë kompetencë:

a. të mbledhin ose të regjistrojnë me ndihmën e mjeteve teknike në territorin e saj; dhe

b. të detyrojnë një dhënës të shërbimeve, brenda mundësive të tij ekzistuese teknike:

i që të mbledhë apo të regjistrojë me ndihmën e mjeteve teknike në territorin e asaj Pale; ose

ii që të bashkëpunojë me ose t'u ndihmojë organeve kompetente në mbledhjen ose regjistrimin:

e të dhënave të trafikut në kohë reale (në kohën e ndodhjes), që janë të lidhura me komunikimet e specifikuara të cilat transmetohen në territorin e saj me ndihmën e një sistemi kompjuterik.

(2) Kur një Palë, për shkak të parimeve të përcaktuara në sistemin ligjor të vendit, nuk mund t'i miratojë masat e parapara në paragrafin 1.a., në vend të kësaj, ajo mund të miratojë legjislacion dhe masa të tjera që janë të nevojshme që të sigurohet mbledhja apo regjistrimi "në kohë reale-në kohën e ndodhjes" i të dhënave të trafikut, që janë të lidhura me komunikimet e specifikuara që transmetohen në territorin e saj, me ndihmën e mjeteve teknike.

(3) Çdo Palë do të miratojë legjislacion të tillë dhe masa të tjera që janë të nevojshme që ta detyrojnë një dhënës të shërbimeve ta mbajë konfidencial faktin e zbatimit të kompetencave të parapara me këtë nen, si dhe t'i mbajë si konfidenciale informacionet e fituara në atë mënyrë.

(4) Kompetencat dhe procedurat e parapara me këtë nen u nënshtrohen dispozitave të neneve 14 dhe 15.

Neni 21 - Interceptimi i të dhënave të përmbajtjes

(1) Çdo Palë do të miratojë legjislacion të tillë dhe masa të tjera, që janë të nevojshme në lidhje me një fushë veprash serioze, që duhet të parashihen me ligjin e vendit, me të cilat organeve kompetente do t'u jepet autorizim që:

a. të mbledhin dhe të regjistrojnë me ndihmën e mjeteve teknike në territorin e asaj Pale; dhe

b. të detyrojnë një dhënës të shërbimeve, brenda mundësive të tij ekzistuese teknike:

i që të mbledhë apo të regjistrojë me ndihmën e mjeteve teknike në territorin e asaj Pale; ose

ii që të bashkëpunojë me ose t'u ndihmojë organeve kompetente në mbledhjen ose regjistrimin:

e të dhënave të përmbajtjes që janë të lidhura me komunikimet e specifikuara, në kohë reale, që transmetohen nëpërmjet një sistemi kompjuterik në territorin e saj.

(2) Kur një Palë, për shkak të parimeve të përcaktuara në sistemin ligjor të vendit, nuk mund t'i miratojë masat e parapara në paragrafin 1.a., në vend të kësaj, ajo mund të miratojë legjislacion dhe masa të tjera që janë të nevojshme që të sigurohet mbledhja apo regjistrimi "në kohë reale-në kohën e ndodhjes" i të dhënave të përmbajtjes, që janë të lidhura me komunikimet e specifikuara që transmetohen në territorin e saj, me ndihmën e mjeteve teknike.

(3) Çdo Palë do të miratojë legjislacion të tillë dhe masa të tjera që janë të nevojshme që ta detyrojnë një dhënës të shërbimeve ta mbajë konfidencial faktin e zbatimit të kompetencave të parapara me këtë nen, si dhe t'i mbajë si konfidenciale informacionet e fituara në atë mënyrë.

(4) Kompetencat dhe procedurat e parapara me këtë nen u nënshtrohen dispozitave të neneve 14 dhe 15.

Seksioni 3 – Juridiksioni

Neni 22 – Juridiksioni

(1) Secila Palë do të miratojë masa të tilla legjislative dhe të tjera, që janë të nevojshme për ta caktuar juridiksionin për veprat që janë paraparë me nenet 2 deri në 11 të kësaj Konvente, në rastet kur një vepër e tillë është kryer:

a. në territorin e saj;

b. në një anije që mban flamurin e asaj Pale; ose

c. në një aeroplan të regjistruar sipas ligjit të asaj Pale; ose

d. nga një shtetas i saj, nëse vepra penale është e dënueshme sipas ligjit penal ku ajo është kryer, ose nëse vepra është kryer jashtë territorit që bie nën juridiksionin e cilësdo Palë.

(2) Çdo Palë mund ta rezervojë të drejtën që të mos i zbatojë ose t'i zbatojë rregullat për juridiksion të parapara në paragrafet 1.b deri në 1.d. të këtij neni ose të ndonjë pjese të tyre, vetëm në raste të caktuara ose në kushte të caktuara.

(3) Secila Palë do të miratojë masa të tilla legjislacioni që janë të nevojshme për të caktuar juridiksionin mbi veprat e parapara në nenin 24, paragrafi 1 të kësaj Konvente, në rastet kur kryerësi i supozuar i veprës penale gjendet në territorin e saj dhe ajo Palë nuk planifikon ta ekstradojë atë tek një Palë tjetër, vetëm për shkak të shtetësisë së tij, pas kërkesës së bërë për ekstradim.

(4) Kjo Konventë nuk e përjashton asnjë juridiksion penal të Palës, që ushtrohet në pajtim me ligjin e vendit.

(5) Nëse dy apo më shumë Palë thonë se kanë juridiksion mbi një vepër penale që është paraparë me këtë Konventë, kur për këtë ka mundësi, Palët e interesuara do të konsultohen për ta përcaktuar juridiksionin më të përshtatshëm për ta bërë ndjekjen e asaj vepre.