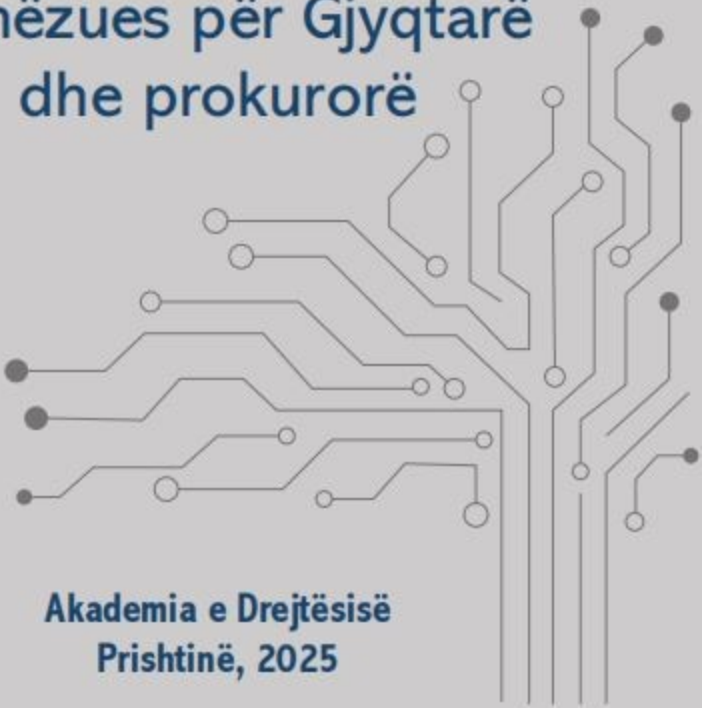
UDHËZUES PËR PROVAT ELEKTRONIKE

Udhëzues për Gjyqtarë dhe prokurorë



Akademia e Drejtësisë
Prishtinë, 2025

Republika e Kosovës
Republika Kosova/Republic of Kosovo
Akademia e Drejtësisë/Akademija Pravde/Academy of Justice

UDHËZUES PËR PROVAT ELEKTRONIKE

Prishtinë, 2025

Nëntor 2025

Shtypur në Prishtinë

Hartimi, publikimi dhe shtypja e botimit me titull: "Udhëzues për provat elektronike" është mundësuar nga Akademia e Drejtësisë.

MOHIMI I PËREGJEGJËSISË

Pikëpamjet e autorëve nuk pasqyrojnë medoemos pikëpamjet e Akademisë së Drejtësisë.

Tabela e përmbajtjes

Hyrje

Në ditët e sotme zhvillimet e shpejta teknologjike kanë ndikuar ndjeshëm në mënyrën se si kryhen veprat penale dhe si trajtohen ato në sistemin e drejtësisë. Sot, përveç formave tradicionale të kriminalitetit, po përballemi me fenomene të reja që lidhen ngushtë me teknologjinë informative, përfshirë krimet kibernetike dhe sfidat që ato paraqesin në procesin e hetimit dhe të provuarit gjyqësor.

Në përmbushje të mandatit të saj, Akademia e Drejtësisë në vazhdimësi ndjek zhvillimet ligjore dhe praktikat gjyqësore, duke vlerësuar vazhdimisht nevojat profesionale të gjyqtarëve dhe prokurorëve. Krahas zhvillimit dhe organizimit të trajnimeve, Akademia e Drejtësisë përmes hulumtimeve dhe botimeve të reja juridike vazhdon të mbështesë zhvillimin dhe shpërndarjen e njohurive që ndihmojnë gjyqtarët dhe prokurorët në ushtrimin e drejtë, të pavarur dhe efikas të funksioneve të tyre e që mbështesin zbatimin e drejtë dhe efikas të ligjit në praktikë. Për më tepër zbatimi i legjislacionit e veçanërisht pjesa e rregullave në sigurimin e provave elektronike, procesin e vlerësimit dhe të provuarit e fakteve përmes tyre, mbështetjen e provave elektronike me provat tjera, sigurimin e provave elektronike në rrugën e bashkëpunimit juridik ndërkombëtarë, kushtet e pranueshmërisë së tyre si dhe ndërhyrja në të drejtën e privatësisë si e drejtë e garantuar me Kushtetutë, instituti i heqjes dorë nga të drejtat e caktuara sipas praktikes se GJEDNJ-se, janë disa nga temat qe janë përcaktuar si nevoja të sistemit të drejtësisë në fushën e publikimeve dhe botimeve.

Andaj, Akademia e Drejtësisë përmes këtij botimi, jo vetëm që synon të ofrojë një mjet praktik pune për gjyqtaret, prokuroret dhe profesionistët tjerë të drejtësisë, por edhe të nxisë reflektimin mbi përvojën e fituar, shkëmbimin e praktikave më të mira dhe ndërtimin e një kulture të qëndrueshme dhe profesionale.

Ky udhëzues vjen si një kontribut konkret në procesin e forcimit të praktikës gjyqësore dhe të unifikimit të saj, me qëllim që të rritet siguria juridike dhe besimi i qytetarëve në sistemin e drejtësisë. Prandaj me rastin e këtij publikimi Akademi e Drejtësisë shprehë mirënjohjen dhe vlerësimin e lartë për punimet

e autoreve si të përmbledhura në këtë udhëzues, gjyqtaret nga Gjykata Supreme z. Agim Maliqi, z. Afrim Shala, z. Burim Ademi , z.Vaton Durguti, nga Departamenti Special ne Gjykatën Apelit, si dhe Prokurorin z. Naim Abazi në Prokurorinë Speciale të Republikës se Kosovës. Puna e tyre profesionale, përkushtimi dhe bashkëpunimi me Akademinë e Drejtësisë përbëjnë një shembull të vlefshëm se si ekspertiza dhe përvoja gjyqësore mund të përkthehen në dije të dobishme për sistemin tonë të drejtësisë.

Në emër të Akademisë së Drejtësisë, shpreh falënderimin dhe mirënjohjen për të gjithë ata që kanë dhënë kontribut në hartimin dhe publikimin e këtij udhëzuesi, me bindjen se ai do të shërbejë si një burim i rëndësishëm për gjyqtarët dhe prokurorët në praktikën e tyre të përditshme.

Prishtinë, 2025

Enver Fejzullahu,
Drejtor Ekzekutiv
Akademia e Drejtësisë

KAPITULLI I

HISTORIKU I ZHVILLIMIT TË LEGJISLACIONIT MATERIAL DHE PROCEDURAL PËR LUFTIMIN E VEPRAVE PENALE NGA KRIMI KOMPJUTERIK

Naim Abazi, Prokuror në Prokurorinë Speciale

Naim Abazi, Prokuror në Prokurorinë Speciale

1. HISTORIKU I ZHVILLIMIT TË LEGJISLACIONIT MATERIAL DHE PROCEDURAL PËR LUFTIMIN E VEPRAVE PENALE NGA KRIMI KOMPJUTERIK

Krimi kompjuterik është një sfidë në rritje për shoqëritë moderne, përfshirë Kosovën. Me avancimin e teknologjisë dhe digjitalizimin e shumë proceseve, nevoja për një legjislacion të përshtatshëm për të luftuar këtë lloj kriminaliteti është bërë e domosdoshme.

Në Kosovë, fillimet e luftës kundër krimit kompjuterik lidhen me procesin e ndërtimit të sistemit ligjor pas pavarësisë së vitit 2008. Fillimisht, Kodi Penal i Kosovës i miratuar në vitin 2004 nga administrata e UNMIK-ut nuk përmbante dispozita specifike për krimin kibernetik. Megjithatë, me evoluimin e teknologjisë dhe nevojën për një rregullim më të detajuar, në vitin 2012 u miratua Kodi i ri Penal i Kosovës (Ligji Nr. 04/L-082), i cili për herë të parë përcaktoi një kornizë të qartë ligjore për veprat penale që lidhen me teknologjinë dhe informacionin. Në këtë Kod Penal janë përfshirë vepra të tilla si:

- Qasja e paautorizuar në sisteme kompjuterike,
- Dëmtimi i të dhënave kompjuterike,
- Mashtrimi kompjuterik,
- Përdorimi i paautorizuar i pajisjeve kompjuterike.

Në vazhdën e përpjekjeve për të përmirësuar legjislacionin në këtë fushë, në vitin 2019 Kosova miratoi ndryshime të rëndësishme në Kodin Penal, duke reflektuar tendencat globale dhe detyrimet ndërkombëtare, veçanërisht përputhjen me Konventën e Budapestit për Krimin Kibernetik, të cilën Kosova e ka ratifikuar.

Përveç Kodit Penal, Kosova ka miratuar disa ligje dhe udhëzime administrative për të përmirësuar kuadrin ligjor në këtë fushë, duke përfshirë Ligjin për Mbrojtjen e të Dhënave Personale (Ligji Nr. 06/L-082) dhe Ligjin për Sigurinë Kibernetike (Ligji Nr. 08/L-066). Këto ligje përcaktojnë përgjegjësitë e institucioneve shtetërore për parandalimin dhe ndjekjen e krimeve kibernetike, si dhe për mbrojtjen e të dhënave digjitale të qytetarëve.

Po ashtu, Policia e Kosovës ka krijuar Njësinë për Krime Kibernetike, e cila është e specializuar në hetimin e veprave penale që lidhen me teknologjinë, ndërsa Prokuroria dhe gjykatat kanë marrë trajnime specifike për përpunimin dhe trajtimin e provave elektronike në gjykime.1

Krimi kibernetik shpesh ka natyrë ndërkombëtare, duke kërkuar një kornizë juridike të përbashkët për luftimin e tij. Organizatat ndërkombëtare, si Kombet e Bashkuara, Bashkimi Evropian dhe Këshilli i Evropës, kanë zhvilluar rregulla dhe rekomandime për shtetet anëtare për të standardizuar trajtimin ligjor të krimeve në fushën e kibernetikës.

Krimi kompjuterik shpesh përfshin individë dhe organizata në juridiksione të ndryshme, duke e bërë të nevojshëm bashkëpunimin juridik ndërkombëtar. Kjo përfshin shkëmbimin e informacionit, ekstradimin e të dyshuarve dhe ndihmën e ndërsjellë juridike.

Konventa e Budapestit, e miratuar nga Këshilli i Evropës në vitin 2001, është dokumenti më i rëndësishëm ndërkombëtar për luftimin e krimit kibernetik. Ajo siguron një kornizë të harmonizuar për shtetet anëtare, duke përcaktuar standardet për kriminalizimin e veprave penale kibernetike, mbledhjen e provave elektronike dhe bashkëpunimin ndërkombëtar.

Lufta kundër krimit kompjuterik kërkon një qasje të integruar që përfshin legjislacionin, politikat dhe bashkëpunimin mes institucioneve të ndryshme. Ligjet dhe praktikat hetimore duhet të përshtaten me zhvillimet teknologjike për të garantuar mbrojtjen e të dhënave dhe të drejtat e qytetarëve.

Konventa e Budapestit përcakton rregulla specifike për mbledhjen, ruajtjen dhe pranueshmërinë e provave elektronike në gjykata. Ajo kërkon që shtetet anëtare të krijojnë mekanizma efektivë për të siguruar që të dhënat e ndjeshme të mos manipulohen dhe të jenë të përdorshme në proceset gjyqësore.

Zbatimi i dispozitave të Konventës së Budapestit në nivel kombëtar paraqet sfida të ndryshme, përfshirë mungesën e ekspertizës teknike dhe nevojën për pajisje të specializuara. Për të siguruar prova elektronike në mënyrë efektive, bashkëpunimi mes autoriteteve kombëtare dhe ndërkombëtare është jetik. Kjo

1 Kodi Penal i Republikës së Kosovës (Ligji Nr. 06/L-074), 2019
Ligji për Mbrojtjen e të Dhënave Personale (Ligji Nr. 06/L-082), 2019
Ligji për Sigurinë Kibernetike (Ligji Nr. 08/L-066), 2022
Konventa e Budapestit për Krimin Kibernetik, ratifikuar nga Kosova në 2018

përfshin krijimin e protokolleve për shkëmbimin e informacionit, harmonizimin e ligjeve dhe trajnimin e personelit.

1. Korniza Juridike Ndërkombëtare

Trajtimi i provave elektronike në nivel ndërkombëtar rregullohet nga disa instrumente ligjore kyçe si në vijim:

1.1 Konventa e Budapestit për Krimin Kibernetik (2001)

Konventa e Budapestit për Krimin Kibernetik, e miratuar nga Këshilli i Evropës më 23 nëntor 2001, është instrumenti i parë ndërkombëtar që synon të harmonizojë ligjet për luftimin e krimit kibernetik dhe trajtimin e provave elektronike. Konventa synon:

- Harmonizimin e legjislacionit penal mbi veprat penale kibernetike;
- Krijimin e mekanizmave të hetimit dhe ndjekjes penale për prova elektronike;
- Lehtësimin e bashkëpunimit ndërkombëtar mes shteteve për hetimin dhe ndjekjen penale të krimeve kibernetike.

Ky traktat njihet si standardi kryesor ndërkombëtar për krimin kibernetik dhe ka shërbyer si model për legjislacionin e shumë vendeve në mbarë botën.

Konventa është e ndarë në disa kapituj kryesorë që mbulojnë veprat penale kibernetike, masat procedurale dhe bashkëpunimin ndërkombëtar.

Konventa detyron shtetet nënshkruese të kriminalizojnë një sërë veprash penale të lidhura me përdorimin e kompjuterëve dhe internetit, duke përfshirë:

Krimet kundër konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave dhe sistemeve, Qasja e paautorizuar (hacking) → Hyrja në sisteme kompjuterike pa leje, Ndërhyrja e paautorizuar në të dhëna (data interference) → Fshirja, modifikimi ose ndryshimi i të dhënave në mënyrë të paautorizuar, Ndërhyrja në sisteme kompjuterike (system interference) → Bllokimi ose pengimi i funksionimit të një sistemi informatik, Keqpërdorimi i pajisjeve (misuse of devices) → Prodhimi ose shpërndarja e pajisjeve (p.sh. viruseve kompjuterike) për të kryer krime kibernetike, Krimet kompjuterike të lidhura me mashtrimin dhe falsifikimin, Mashtrimi kompjuterik (computer-related fraud), Përdorimi i sistemeve kompjuterike për përfitime financiare me anë të

mashtrimit, Falsifikimi kompjuterik (computer-related forgery) → Manipulimi i të dhënave për qëllime mashtrimi, si krijimi i dokumenteve të rreme dixhitale.

Krimet e lidhura me përmbajtjen e paligjshme, Pornografia e fëmijëve online → Prodhimi, shpërndarja ose posedimi i materialeve të paligjshme që përfshijnë fëmijët. Krimet që lidhen me shkeljen e të drejtave të autorit dhe pronësisë intelektuale, Piratimi dhe shpërndarja e paligjshme e përmbajtjes dixhitale → Shkelja e të drejtave të autorit përmes internetit.

Përveç përcaktimit të veprave penale, Konventa kërkon nga shtetet pjesëmarrëse të vendosin mekanizma të fortë proceduralë për hetimin dhe mbledhjen e provave elektronike.

Ruajtja e të dhënave (data preservation) → Autoritetet mund të kërkojnë nga ofruesit e shërbimeve të ruajnë të dhëna të caktuara për një periudhë të caktuar kohore për qëllime hetimi; Qasja në të dhëna të ruajtura (data access) → Hetuesit mund të kenë qasje në të dhënat e ruajtura që lidhen me një krim të dyshuar, Ndërprerja e veprimtarive të paligjshme (real-time collection) → Monitorimi i të dhënave në kohë reale për hetimin e krimeve të rënda, Bllokimi ose heqja e përmbajtjes së paligjshme nga interneti → Shtetet mund të kërkojnë që përmbajtja e paligjshme të fshihet ose bllokohet.

Për shkak të natyrës ndërkufitare të krimit kibernetik, Konventa e Budapestit vendos mekanizma të bashkëpunimit ndërkombëtar, si*: Ekstradimi i të dyshuarve → Shtetet palë angazhohen për të ekstraduar personat e akuzuar për krime të rënda kibernetike; Shkëmbimi i informacionit mes autoriteteve hetimore → Vendet duhet të ofrojnë ndihmë të shpejtë për hetimin e provave elektronike; Krijimi i ekipeve të përbashkëta hetimore → Shtetet mund të krijojnë njësi të përbashkëta për të luftuar krimin kibernetik.*

Pavarësisht rëndësisë së saj, Konventa e Budapestit përballet me disa sfida, si mos ratifikimi nga disa shtete të mëdha → Disa vende, si Kina dhe Rusia, nuk e kanë ratifikuar konventën dhe refuzojnë të ndajnë të dhëna me vendet e tjera, harmonizimi i legjislacioneve kombëtare → Disa shtete kanë ligje të ndryshme mbi privatësinë, duke e bërë të vështirë shkëmbimin e të dhënave, kriptimi dhe privatësia → Përdorimi i kriptimit fundor (end-to-end encryption) nga platformat si Whats App dhe Signal e bën të vështirë qasjen në komunikimet e kriminelëve kibernetikë, Krimi kibernetik në zhvillim → Teknologjitë e reja, si deep fake dhe inteligjenca artificiale, po krijojnë forma të reja të mashtrimit që nuk mbulohen plotësisht nga konventa.

Konventa e Budapestit mbetet instrumenti më i rëndësishëm ndërkombëtar për luftimin e krimit kibernetikë dhe është modeli bazë për shumicën e ligjeve kombëtare mbi këtë fushë. Ajo lehtëson bashkëpunimin ndërkombëtar, duke ndihmuar shtetet në shkëmbimin e provave dhe ekstradimin e të dyshuarve.

Megjithatë, sfidat e lidhura me privatësinë, teknologjitë e reja dhe mungesën e një bashkëpunimi të plotë global mbeten problematike.

1.2 Konventa e Këshillit të Evropës mbi Ndihmën e Ndërsjellë Juridike (1959) dhe Protokollet Shtesë

Konventa e Këshillit të Evropës mbi Ndihmën e Ndërsjellë Juridike në Çështjet Penale (European Convention on Mutual Assistance in Criminal Matters – ECMACM), e miratuar më 20 prill 1959, është një nga instrumentet më të rëndësishme ndërkombëtare për bashkëpunimin juridik midis shteteve evropiane në çështjet penale.
Kjo konventë u krijua me qëllim lehtësimin e bashkëpunimit gjyqësor ndërkombëtar midis shteteve anëtare të Këshillit të Evropës duke pas për bazë përmirësimin e mekanizmave për shkëmbimin e informacioneve dhe provave në hetimet penale, rritjen e efektivitetit të hetimeve dhe ndjekjeve penale ndërkombëtare, sidomos për krimet ndërkufitare dhe të organizuara.

Konventa ka ratifikime nga 50 vende, duke përfshirë shumicën e shteteve evropiane dhe disa shtete jashtë Evropës. Konventa e vitit 1959 vendos rregulla bazë mbi mënyrën se si shtetet mund të ndihmojnë njëra-tjetrën në hetimin dhe ndjekjen penale të rasteve kriminale.

Konventa rregullon mënyrën se si shtetet anëtare duhet të bashkëpunojnë në hetime penale, përfshirë shkëmbimin e Informacionit mbi Krimet → Shtetet mund të kërkojnë informacion mbi precedentët penalë të një personi ose mbi të dhënat që lidhen me një hetim penal, dërgimi i Dokumenteve Gjyqësore → Letër porositë ose dokumentet ligjore mund të dërgohen drejtpërdrejt autoriteteve të drejtësisë së një shteti tjetër, marrja e Dëshmive dhe Deklaratave → Shtetet mund të kërkojnë nga një shtet tjetër të marrë dëshmi ose të intervistojë dëshmitarë në lidhje me një rast penal, ekzaminimi i Proveve dhe Objektit të Krimit → Mund të kërkohet analiza e provave materiale ose dokumenteve, dërgimi i Provave dhe Dokumenteve → Provat që janë sekuestruar në një shtet mund të dërgohen në një shtet tjetër për qëllime hetimore.

Konventa bazohet në disa parime themelore, të cilat ndihmojnë në rregullimin e ndihmës juridike ndërmjet shteteve:

Parimi i Reciprocitetit → Ndihma mund të ofrohet vetëm nëse ekziston garancia se shteti tjetër do të veprojë në të njëjtën mënyrë;

Parimi i Specialitetit → Provat ose informacionet e marra përmes kësaj konvente mund të përdoren vetëm për çështjen specifike për të cilën janë kërkuar, përveç rasteve kur lejohet nga shteti që i ka ofruar;

Refuzimi i Ndihmës në Raste të Caktuara → Shtetet kanë të drejtë të refuzojnë ndihmën nëse ajo bie në kundërshtim me sovranitetin, sigurinë kombëtare ose parimet themelore të rendit juridik të tyre.

Protokollet Shtesë të Konventës

Me kalimin e viteve, është vërejtur nevoja për modernizimin dhe zgjerimin e Konventës së vitit 1959, duke sjellë dy protokolle shtesë që e kanë plotësuar dhe përmirësuar konventën fillestare.

Protokolli i Parë Shtesë (1978)

Ky protokoll u miratua për të adresuar disa boshllëqe në konventën fillestare, duke përfshirë, marrja e Dëshmive përmes Video konferencës → Ky protokoll për herë të parë lejonte marrjen e dëshmive nga dëshmitarët ose të dyshuarit përmes lidhjeve të largëta, sidomos kur ata nuk mund të udhëtonin për arsye sigurie ose shëndetësore, përdorimi i Zinxhirit të Provave → Shtetet u obliguan të ruajnë autenticitetin e provave elektronike dhe të sigurojnë zinxhirin e tyre ligjor, kufizimi i Arsyeve për Refuzimin e Ndihmës → Shtetet nuk mund të refuzonin ndihmën për arsye që nuk ishin të qarta në tekstin origjinal të konventës.

Protokolli i Dytë Shtesë (2001)

Protokolli i Dytë Shtesë i Konventës Evropiane për Ndihmën e Ndërsjelltë Juridike në Fushën Penale (ETS No. 182), është një instrument ligjor i përgatitur nga Këshilli i Evropës, me qëllim modernizimin dhe zgjerimin e fushës së bashkëpunimit juridik ndërkombëtar. Këtë dokument e ka hartuar Komiteti i Ekspertëve për Veprimin e Konventave Evropiane në Fushën Penale (PC-OC) dhe u miratua nga Komiteti Evropian për Problemet e Krimit (CDPC) në vitin 2001.

Konventa e vitit 1959 dhe Protokolli i Parë Shtesë (1978) nuk ishin të mjaftueshme për të trajtuar sfidat e reja të drejtësisë penale ndërkombëtare,

veçanërisht në lidhje me modernizimin e rregullave të ndihmës juridike, lehtësimin dhe përshpejtimin e procesit të ndihmës, integrimin e teknologjive të reja dhe zhvillimeve sociale, mbrojtjen e të dhënave personale gjatë procesit të ndihmës si dhe dispozitat Kryesore të Protokollit.

Objektivi i Protokollit të Dytë Shtesë përcakton synimet e tij kryesore:

- Sigurimi i ndihmës juridike më efikase dhe të shpejtë,
- Zgjerimi i fushës së veprimit të Konventës së vitit 1959,
- Mbështetja e procedurave administrative me ndikim penal,
- Sigurimi i ndihmës në raste të përfshirjes së personave juridikë.

Kërkesat për ndihmë duhet të bëhen me shkrim dhe përmes Ministrive të Drejtësisë, mire po lejohet komunikimi i drejtpërdrejtë midis autoriteteve gjyqësore, si dhe përdorimi i mjeteve telekomunikuese si fax, e-mail ose sisteme të tjera dixhitale.

Lejohet transferimi i përkohshëm i personave në paraburgim për qëllime hetimore, pala e kërkuar duhet të sigurojë kthimin e personit të transferuar pas përmbushjes së detyrimeve hetimore.

Konventa thekson nevojën për përshpejtim të procedurave të ndihmës juridike, në rastet urgjente, Pala pritëse mund të pezullojë ose kufizojë ndihmën.

Përpunimi i të dhënave personale sipas Konventës Evropiane për Mbrojtjen e Të Dhënave, kjo konvente trajton dhe kufizimin e përdorimit të të dhënave personale sipas kushteve të vendosura nga Pala dërguese.

Konventa gjithashtu parasheh krijimin e Ekipeve të Përbashkëta Hetimore (JIT) për bashkëpunim ndërkufitar, duke lejuar vëzhgimin ndërkufitar për hetimet e krimit të organizuar, duke mundësuar dhe përdorimin e video-konferencave për marrjen në pyetje të dëshmitarëve dhe të akuzuarve.

Pala kërkuese mund të kërkojë masa mbrojtëse për dëshmitarët dhe viktimat, duke lejuar që të behet transferimi i tyre në një shtet tjetër nëse ka rrezik të lartë për jetën e tyre.

Përfitimet e Protokollit të Dytë Shtesë të konventës:

- Modernizimi i procesit të ndihmës juridike (Efikasitet më i lartë).
- Lehtësimi i procedurave dhe zgjerimi i kanaleve të komunikimit (Fleksibilitet).

- Përputhshmëria me Konventat e BE-së, si Marrëveshja Schengen (Harmonizimi me BE-në).
- Sigurimi i respektimit të të drejtave të individit dhe mbrojtja e privatësisë (Mbrojtja e të drejtave).

Protokolli i Dytë Shtesë i Konventës Evropiane për Ndihmën e Ndërsjelltë Juridike në Fushën Penale paraqet një hap të rëndësishëm për modernizimin e bashkëpunimit ndërkombëtar në fushën e drejtësisë penale. Duke u bazuar në teknologjinë dhe zhvillimet sociale, ai synon të forcojë luftën kundër krimit të organizuar, korrupsionit dhe terrorizmit, duke lehtësuar shkëmbimin e informacioneve mes shteteve. Me këto përmirësime, Europa siguron një sistem më efektiv dhe të përditësuar të drejtësisë ndërkombëtare.

1.3 Rregullorja e BE-së për Mbrojtjen e të Dhënave (GDPR)

Në një botë gjithnjë e më të ndërlidhur, ku informacioni personal është bërë një mjet i fuqishëm në duart e kompanive dhe institucioneve, Rregullorja e Përgjithshme për Mbrojtjen e të Dhënave, ose siç njihet ndryshe GDPR, u shfaq si një fener shprese për privatësinë dhe sigurinë e individëve. Hyri në fuqi më 25 maj 2018, duke vendosur një standard të ri për mënyrën se si të dhënat personale duhet të trajtohen në Bashkimin Evropian. Me këtë rregullore, BE-ja shpalosi ambicien e saj për të garantuar mbrojtjen e të drejtave themelore të qytetarëve të saj në një epokë dixhitale.
GDPR-ja ishte më shumë sesa një rregullore – ishte një thirrje për respekt dhe përgjegjësi në përpunimin e të dhënave personale. Qëllimi i saj ishte i qartë: të mbrojë të drejtat e individëve, të krijojë një standard të unifikuar në të gjithë BE-në dhe të detyrojë kompanitë që të jenë transparente në mënyrën se si përpunojnë informacionin personal. Për herë të parë, qytetarët e BE-së do të kishin kontroll të plotë mbi të dhënat e tyre, një e drejtë që deri atëherë ishte shpeshherë e anashkaluar.

Ajo prek të gjitha kompanitë dhe organizatat që përpunojnë të dhënat e qytetarëve të BE-së, duke mos marrë parasysh vendndodhjen e tyre gjeografike. Bizneset e mëdha apo të vogla, institucionet publike apo private, të gjitha duhej të përshtatnin politikat dhe praktikat e tyre për të respektuar këtë rregullore të re. Në thelb të GDPR-së qëndrojnë shtatë parime kyçe: ligjshmëria, ndershmëria dhe transparenca; kufizimi i qëllimit; minimizimi i të dhënave; saktësia; kufizimi i ruajtjes; integriteti dhe konfidencialiteti; dhe

përgjegjshmëria. Këto parime nuk ishin thjesht fjalë në letër – ato përfaqësonin një ndryshim rrënjësor në mënyrën se si duhet të trajtoheshin të dhënat personale. Ndërkohë që kompanitë përballeshin me sfida të reja në përmbushjen e këtyre kërkesave, individët për herë të parë ndjenë fuqinë për të kërkuar transparencë, për të korrigjuar të dhënat e tyre dhe për të kërkuar që ato të fshihen kur nuk ishin më të nevojshme.

Gjithsesi, GDPR nuk ishte pa kritika. Disa argumentonin se ajo ishte e ndërlikuar për t'u zbatuar, sidomos për bizneset e vogla, dhe se vendoste pengesa për inovacionin, veçanërisht në fushën e inteligjencës artificiale. Të tjerë e shihnin si një standard të artë që do të frymëzonte ligje të ngjashme në mbarë botën. Por një gjë ishte e qartë – GDPR-ja kishte sjellë një ndryshim të pakthyeshëm në marrëdhënien mes individëve dhe organizatave që përpunonin të dhënat e tyre.

Nën dritën e kësaj rregulloreje, kompanitë filluan të përballen me një realitet të ri, ku një gabim i vogël mund të kushtonte miliona euro gjoba. Rasti i Google, i gjobitur me 50 milionë euro për mungesë transparence, apo Meta, me një gjobë prej 1.2 miliardë eurosh për transferimin e të dhënave në SHBA pa masa të duhura mbrojtëse, treguan se GDPR-ja nuk ishte thjesht një kërcënim bosh.

Në fund, GDPR-ja përfaqëson një ndërmarrje ambicioze për të rikthyer balancën në favor të individit në një botë të dominuar nga të dhënat. Ishte një përpjekje për të siguruar se edhe në epokën dixhitale, të drejtat e njeriut dhe dinjiteti personal do të mbeteshin të paprekura. Dhe ndërsa sfidat vazhdojnë të shfaqen, GDPR-ja mbetet një simbol i fuqishëm i asaj që mund të arrihet kur ligji vihet në shërbim të qytetarit.

1.4 Rregullat Model të Kombeve të Bashkuara për Provën Elektronike në Arbitrazh (UNCITRAL, 2017)

Në epokën moderne të dixhitalizimit, ku shumica e transaksioneve dhe komunikimeve kryhen përmes mjeteve elektronike, edhe sistemi ligjor është detyruar të përshtatet me realitetin e ri të provave dixhitale. Një nga nismat më të rëndësishme në këtë drejtim është Rregullorja Model për Provën Elektronike në Arbitrazh, e hartuar nga Komisioni i Kombeve të Bashkuara për Ligjin e Tregtisë Ndërkombëtare (UNCITRAL) në vitin 2017.

UNCITRAL është një organ i Kombeve të Bashkuara, përgjegjës për harmonizimin dhe modernizimin e ligjeve të tregtisë ndërkombëtare. Me kalimin e viteve, ai ka hartuar standarde ligjore për arbitrazhin, kontratat tregtare, pagesat ndërkombëtare dhe e-commerce. Kjo rregullore model përqendrohet në rregullat për trajtimin e provave elektronike në proceset e arbitrazhit ndërkombëtar, duke krijuar një kornizë të qartë për pranueshmërinë, autenticitetin dhe ruajtjen e këtyre provave.

Para vitit 2017, arbitrazhi ndërkombëtar nuk kishte një standardi të njësuar për trajtimin e provave elektronike. Gjykatat dhe tribunat arbitrale shpesh përballeshin me sfida të mëdha në pranimin dhe vlerësimin e dokumenteve dixhitale, duke përfshirë:

- Dokumentet elektronike, si emailet, mesazhet dhe databazat dixhitale;
- Regjistrimet e serverëve dhe të dhënat e përdoruesve nga kompanitë teknologjike;
- Provat nga rrjetet sociale dhe platformat online;
- Dëshmitë e bazuara në blockchain dhe inteligjencë artificiale.

Për të adresuar këto sfida, UNCITRAL krijoi një kornizë ligjore të qartë dhe uniforme, të cilën shtetet dhe institucionet arbitrare mund ta adoptojnë në sistemet e tyre.

1.5 Bashkëpunimi Juridik Ndërkombëtar

Në epokën moderne, ku informacioni qarkullon me shpejtësi të jashtëzakonshme dhe komunikimi dixhital është bërë pjesë e pandashme e jetës sonë, krimet kibernetike janë kthyer në një nga sfidat më të mëdha për sistemet ligjore në mbarë botën. Rrjetet globale të krimit të organizuar, përdorimi i anonimitetit në internet dhe sofistikimi i teknologjisë kanë krijuar një realitet të ri, ku ndjekja penale e këtyre krimeve nuk mund të bëhet pa një bashkëpunim të fortë ndërkombëtar.

Nëse një mashtrim financiar online kryhet nga një individ në një vend, përmes një serveri të vendosur në një kontinent tjetër, duke përdorur një platformë të regjistruar në një vend të tretë, hetimi dhe sigurimi i provave bëhet jashtëzakonisht kompleks. Kjo situatë ka bërë të nevojshme krijimin e

mekanizmave të ndihmës së ndërsjellë juridike, marrëveshjeve dypalëshe dhe bashkëpunimin me sektorin privat për të garantuar drejtësinë.

Në këtë drejtim, Konventa e Budapestit për Krimin Kibernetik (2001) mbetet traktati më i rëndësishëm ndërkombëtar për adresimin e krimeve dixhitale. Ajo jo vetëm që përcakton se cilat vepra penale përbëjnë krim kibernetik – si hyrja e paautorizuar në sisteme, ndërhyrja në të dhëna, mashtrimi kompjuterik dhe pornografia e fëmijëve – por gjithashtu krijon mekanizma për ndihmën juridike ndërkombëtare. Përmes kësaj konvente, shtetet pjesëmarrëse mund të bashkëpunojnë në shkëmbimin e informacionit, sigurimin e provave dixhitale dhe ekstradimin e të dyshuarve.

Në përmirësim të saj, Protokolli Shtesë i vitit 2022 ka zgjeruar mundësitë për qasje në të dhënat elektronike të mbajtura nga kompanitë teknologjike, duke krijuar procedura të përshpejtuara për mbledhjen dhe ndarjen e informacioneve në kohë reale.

Përveç kësaj konvente, Konventa e Këshillit të Evropës mbi Ndihmën e Ndërsjellë Juridike (1959) dhe protokollet e saj shtesë kanë luajtur një rol kyç në sigurimin e provave ndërkombëtare dhe lehtësimin e ekstradimeve. Këto instrumente kanë mundësuar shkëmbimin e dokumenteve, intervistimin e dëshmitarëve përmes videokonferencës dhe sekuestrimin e materialeve të paligjshme, duke i dhënë organeve hetimore mjete të reja për të luftuar krimet transnacionale.

Përveç traktateve ndërkombëtare, janë krijuar edhe mekanizma praktikë për bashkëpunimin ndërkombëtar. Ndihma e Ndërsjellë Juridike (MLA – Mutual Legal Assistance) është një nga mënyrat më të përdorura për të kërkuar ndihmë nga një shtet tjetër në mbledhjen e provave. Në të njëjtën kohë, shumë shtete kanë krijuar marrëveshje të drejtpërdrejta me kompanitë teknologjike, si Google, Meta dhe Apple, për të siguruar të dhënat e përdoruesve kur është e nevojshme për hetime penale.

Në këtë kuadër, CLOUD Act (Clarifying Lawful Overseas Use of Data Act) i miratuar në SHBA, ka mundësuar autoriteteve amerikane të kërkojnë të dhëna nga kompanitë teknologjike, edhe nëse ato janë të ruajtura jashtë kufijve të SHBA-së. Megjithatë, kjo ka sjellë shqetësime për privatësinë, veçanërisht në Bashkimin Evropian, ku GDPR rregullon mbrojtjen e të dhënave personale dhe kufizon ndarjen e tyre pa garanci të duhura ligjore.

Organizatat ndërkombëtare si Interpoli dhe Europoli gjithashtu luajnë një rol kyç në koordinimin e hetimeve për krimet kibernetike. Europoli, përmes

Qendrës Evropiane për Krimin Kibernetik (EC3), bashkëpunon me shtetet anëtare të BE-së për të ndjekur rrjetet kriminale dixhitale, ndërsa Interpoli përdor platformat e tij globale për të lehtësuar shkëmbimin e informacionit ndërmjet policive të ndryshme.

Pavarësisht përpjekjeve të shumta për të krijuar një sistem efektiv bashkëpunimi, ekzistojnë ende disa sfida madhore sa I perket bazez ligjore midis Shteteve → Jo të gjitha vendet kanë ratifikuar konventat ndërkombëtare mbi krimin kibernetik, duke krijuar boshllëqe ligjore dhe vështirësi në ndihmën juridike.

Burokracia dhe Vonesat në Shkëmbimin e Informacionit → Disa procedura janë ende të ngadalta, veçanërisht përmes marrëveshjeve tradicionale të ndihmës juridike ndërkombëtare.

Privatësia dhe Mbrojtja e të Dhënave → Ligje të ndryshme si GDPR dhe aktet e mbrojtjes së privatësisë në vende të ndryshme mund të kufizojnë shkëmbimin e informacioneve midis autoriteteve hetimore.

Përdorimi i Teknologjive të Avancuara nga Kriminelët → Teknologjitë si kriptimi fundor (end-to-end encryption), rrjetet anonime si Dark Web, dhe kriptovalutat i bëjnë hetimet më të ndërlikuara.

1.6 Shqyrtime të Përgjithshme

Në një botë ku teknologjia është e pranishme në çdo aspekt të jetës, mënyra se si njerëzit komunikojnë, bëjnë biznes dhe shkëmbejnë informacion ka ndryshuar rrënjësisht. Me këtë transformim dixhital, edhe sistemet ligjore janë detyruar të përshtaten, duke përfshirë në proceset e tyre provat elektronike.

Nga e-mailet dhe mesazhet telefonike deri te të dhënat e ruajtura në pajisje inteligjente, informacioni elektronik është kthyer në një burim kyç për drejtësinë.

Por, çfarë janë saktësisht provat elektronike? Si mund të përdoren në një proces gjyqësor? Dhe cilat janë sfidat kryesore në pranimin dhe trajtimin e tyre? Ky udhëzues synon të japë një pasqyrë të qartë mbi këto çështje, duke ofruar një kuptim të thelluar për avokatët, hetuesit dhe të gjithë ata që merren me drejtësinë në epokën dixhitale.

Çfarë Janë Provat Elektronike?

Provat elektronike përfshijnë çdo informacion të ruajtur ose të transmetuar përmes një pajisjeje kompjuterike, rrjeti dixhital apo platforme elektronike, i cili mund të përdoret si dëshmi në një proces ligjor.

Disa nga format më të zakonshme të provave elektronike janë:

- Dokumente dixhitale – e-mail, kontrata elektronike, fatura online;
- Regjistrime të komunikimeve – biseda në WhatsApp, SMS, telefonata të regjistruara;
- Metadata – të dhëna që tregojnë krijimin dhe modifikimin e skedarëve;
- Fotografi dhe video dixhitale – të ruajtura në telefona ose kamera mbikëqyrëse;
- Regjistrime të veprimtarive në internet – historiku i shfletimit, postime në rrjetet sociale;
- Të dhëna nga pajisjet inteligjente – regjistrime të GPS-it, aplikacionet e monitorimit të aktivitetit.

Në të kaluarën, provat mbështeteshin kryesisht në dokumentacion fizik, dëshmi verbale apo materiale të prekshme. Sot, provat elektronike kanë një avantazh të madh: ato mund të ruajnë një nivel të lartë saktësie dhe mund të analizohen për të zbuluar detaje të fshehura.

Provat elektronike janë bërë të domosdoshme në hetimet penale dhe proceset civile. Ato mund të ndihmojnë në zbardhjen e së vërtetës në raste të ndryshme, nga krimet ekonomike deri te shkeljet e të drejtave të autorit.

1.7 Provat Elektronike në Çështjet Penale

Në hetimet penale, provat elektronike përdoren për:

- Krimet kibernetike – mashtrime online, hakerime, vjedhje identiteti;
- Krimet financiare – gjurmimi i transaksioneve dixhitale për të zbuluar mashtrime;
- Dhunën familjare dhe kërcënimet – analizimi i mesazheve dhe postimeve në rrjetet sociale;
- Terrorizmin dhe krimin e organizuar – ndjekjen e komunikimeve të dyshimta dhe lëvizjeve financiare të paligjshme.

1.8 Provat Elektronike në Çështjet Civile

Në proceset civile, provat elektronike mund të jenë thelbësore për:

- Marrëveshjet dhe kontratat – e-mail-et dhe bisedat dixhitale si dëshmi të marrëveshjeve mes palëve;
- Shkeljet e të drejtave të autorit dhe pronësisë intelektuale – regjistrimi i faqeve të internetit që përdorin përmbajtje të mbrojtur nga ligji;
- Raste familjare – përdorimi i mesazheve elektronike si provë në çështjet e kujdestarisë ose divorceve.

1.9 Sfida në Përdorimin e Provave Elektronike

Pavarësisht rëndësisë së tyre, pranimi dhe trajtimi i provave elektronike sjell sfida të shumta, të cilat lidhen me autenticitetin, privatësinë dhe mundësinë e manipulimit.

Autenticiteti dhe Besueshmëria

Një nga sfidat më të mëdha është garantimi i autenticitetit të provave dixhitale. Pyetjet kryesore që duhet të marrin përgjigje janë:

- A është prova e ruajtur në mënyrë të sigurt?
- A ka pësuar manipulime?
- A mund të gjurmohet burimi i saj?

Për të siguruar besueshmërinë e një prove dixhitale, ruajtja e zinxhirit të provave (chain of custody) është thelbësore. Çdo ndryshim i të dhënave duhet të jetë i dokumentuar dhe i justifikueshëm, në mënyrë që të shmanget akuzimi për manipulim.

Një sfidë tjetër e madhe është balancimi mes hetimeve ligjore dhe privatësisë së individëve. Ligje si GDPR në Evropë përcaktojnë rregulla të rrepta për mbrojtjen e të dhënave personale, duke kufizuar përdorimin e disa informacioneve elektronike pa pëlqimin e personit të prekur.

Me avancimin e teknologjisë, provat elektronike po bëhen gjithnjë e më të ndërlikuara. Risi si inteligjenca artificiale, blockchain dhe analiza forenzike dixhitale po ndihmojnë në sigurimin e provave të sakta dhe të pa manipuluara.

Disa nga zhvillimet e pritshme përfshijnë:

- Përdorimin e inteligjencës artificiale për të analizuar provat elektronike më shpejt dhe më saktë;
- Forcimin e ligjeve për të parandaluar manipulimin e provave dixhitale;
- Zhvillimin e metodave të reja për të identifikuar deepfake dhe falsifikimet elektronike.

Provat elektronike kanë ndryshuar mënyrën se si drejtësia zbatohet në të gjithë botën. Ato janë bërë një mjet i fuqishëm për hetimet penale dhe zgjidhjen e mosmarrëveshjeve civile. Megjithatë, për të siguruar që këto prova të përdoren në mënyrë të drejtë dhe efektive, nevojiten rregulla të qarta për ruajtjen, analizimin dhe pranimin e tyre në gjykatë.
Teknologjia vazhdon të zhvillohet, por parimi themelor mbetet i njëjtë: drejtësia duhet të bazohet në prova të sigurta, të besueshme dhe të verifikuara. Për këtë arsye, njohja dhe trajtimi korrekt i provave elektronike është një detyrë e rëndësishme për të gjithë profesionistët ligjorë dhe institucionet e drejtësisë.

Pranueshmëria e Provave Elektronike në Raport me Kategorinë e Masave të Fshehta dhe Ekzaminimeve të Aparateve Elektronike

Provat elektronike, si të dhënat nga pajisjet elektronike, regjistrimet audio dhe video, mesazhet elektronike dhe të dhënat nga interneti, mund të sigurohen në bazë të masave të fshehta të hetimit ose ekzaminimeve të aparateve elektronike. Kodi i Procedurës Penale përcakton se masat e fshehta të hetimit mund të aplikohen vetëm kur ka dyshime të bazuara dhe kur metodat e tjera të hetimit janë të pamjaftueshme. Për pranueshmërinë e provës, duhet të respektohen kërkesat ligjore për autorizimin e gjykatës dhe për ruajtjen e integritetit të të dhënave.

Cilësia e Provës në Procedurën Penale Kur Sigurohet nga Organet e Ndjekjes

Provat e siguruara nga organet e ndjekjes penale duhet të jenë të ligjshme dhe të sigurta. Ky parim nënkupton që provat të mblidhen në përputhje me procedurat e përcaktuara në ligj, duke respektuar të drejtat e të dyshuarit dhe të dëmtuarit. Nëse një provë elektronike është siguruar në kundërshtim me ligjin, ajo mund të shpallet e papranueshme nga gjykata.

Cilësia e Provës Kur Sigurohet nga Ana e të Dëmtuarit Apo të Pandehurit si Palë në Procedurën Penale

Në rastet kur provat sigurohen nga të dëmtuarit ose të pandehurit, gjykata duhet të shqyrtojë vlefshmërinë dhe autenticitetin e tyre. Provat e tilla mund të jenë regjistrime audio, video, ose mesazhe të ruajtura nga palët, të cilat duhet të përmbushin kriteret e integritetit dhe të mos jenë të manipuluara. Gjykata vlerëson edhe mënyrën e sigurimit të provës për të shmangur ndërhyrjet në privatësi ose shkeljet e të drejtave themelore.

Refuzimi i të Pandehurit për Dhënien e Mundësisë për Sigurimin e Provës Elektronike dhe Mundësitë e Veprimeve Ligjore

Nëse i pandehuri refuzon të ofrojë akses në pajisjet e tij elektronike ose refuzon të japë kodet e hyrjes, organet e ndjekjes mund të kërkojnë një vendim gjyqësor për të autorizuar sekuestrimin dhe ekzaminimin e pajisjeve.

Refuzimi i të Dëmtuarit për Sigurimin e Provës Elektronike dhe Mundësitë e Veprimeve Ligjore

Nëse një i dëmtuar refuzon të ofrojë një provë elektronike që mund të ndihmojë në zbardhjen e çështjes, prokuroria mund të vlerësojë nëse ai ka një detyrim ligjor për ta dorëzuar atë. Në disa raste, gjykata mund të lëshojë një urdhër për sekuestrim nëse provohet se prova është thelbësore për ndjekjen e çështjes penale.

Sigurimi i Provave Elektronike në Kohë Reale të Ndodhjes së Veprës Penale

Për disa vepra penale, sigurimi i provave elektronike në kohë reale është i domosdoshëm. Ligji mundëson monitorimin e komunikimeve në kohë reale me autorizim gjyqësor në raste të rënda, të tilla si terrorizmi, krimi i organizuar, apo vepra të tjera serioze. Kjo përfshin interceptimet telefonike, ndjekjen e mesazheve të internetit, dhe përdorimin e mjeteve të tjera teknologjike.

Obligimi i Prokurorisë për Sigurimin e Provave për Ndjekjen Efektive Penale në Raport me Ruajtjen e të Drejtës së Privatësisë

Prokuroria ka për detyrë të mbledhë dhe sigurojë prova në mënyrë efektive, duke ruajtur një ekuilibër mes nevojës për ndjekjen penale dhe të drejtës së privatësisë së individëve. Për këtë arsye, përdorimi i metodave të sigurimit të provave duhet të jetë proporcional dhe i mbështetur në ligj. Nëse provat mblidhen në mënyrë të paligjshme, ato mund të përjashtohen nga procedura dhe të cenojnë vlefshmërinë e ndjekjes penale.

KAPITULLI II

VËSHTRIME TË PËRGJITHSHME TË MASAVE TË VEÇANTA HETIMORE DHE

MASAT E VEÇANTA HETIMORE SIPAS KODIT TË PROCEDURËS PENALE

Agim Maliqi, Gjyqtar në Gjykatën Supreme të Kosovës

Agim Maliqi, Gjyqtar në Gjykatën Supreme të Kosovës

Pjesa e Parë

1. VËSHTRIME TË PËRGJITHSHME TË MASAVE TË VEÇANTA HETIMORE

1.1 Vështrime të përgjithshme

Është evidente se në botën bashkëkohore janë të pranishme forma të ndryshme të kriminalitetit me rrezikshmëri të lartë. Në këtë drejtim, vlen të përmenden format e ndryshime të krimit të organizuar, vrasjet me pagesë, pastrimi i parave, terrorizimi, trafikimi me njerëz, kontrabandimi me migrantë, spiunazhi, krimi kibernetik, kontrabandimi ndërkombëtar i armëve, format e ndryshme të korrupsionit dhe keqpërdorimit të detyrës zyrtare, etj., për zbulimin dhe luftimin e të cilave është parë e nevojshme që të parashihen dhe të përdorën masa të veçanta hetimore nga ana e organeve të ndjekjes.

Në këtë mënyrë, me qëllim të arritjes së synimeve të lartcekura, si në Kosovë, ashtu edhe në shtetet tjera bashkëkohore janë parashikuar një sërë masash të veçanta hetimore të cilat i kanë në dispozicion organet e ndjekjes. Kështu, në dispozitat ligjore të Kodit të Procedurës Penale[2] janë parashikuar këto masa të veçanta hetimore: vëzhgim i fshehtë fotografik ose me video; monitorim i fshehtë i bisedave; kontrollim i dërgesave postare; përgjim i telekomunikimeve dhe përdorimi i lexuesit – IMSI – identifikimi ndërkombëtar i shfrytëzuesit mobil; dërgim i kontrolluar i dërgesave postare; dërgesa e kontrolluar; shfrytëzim i mjeteve për përcjellje të vendndodhjes; shitja dhe blerja e simuluar e artikujve, shërbimeve apo sendeve; dhënia dhe marrja e simuluar e ryshfetit; regjistrimi i simuluar i personave juridik ose përdorimi i personave ekzistues juridik për mbledhjen e të dhënave; hetim i fshehtë; regjistrim i thirrjeve telefonike dhe zbulim i të dhënave financiare.

Këto masa të veçanta, siç do të shohim, mund të përdorën jo vetëm me qëllim të sigurimit të të dhënave të nevojshme në procedurë penale, por edhe kur janë në pyetje nevojat e sigurisë së Kosovës dhe qytetarëve të saj.

[2] Kodi nr.08/L-032 i Procedurës Penale, datë 14.07.2022 (në vijim: KPP).

Është e qartë se parashikimi dhe zbatimi i këtyre masave ndikon edhe në kufizimin e ushtrimit të disa të drejtave themelore të njeriut. Andaj, me qëllim të evitimit të çdo lloj keqpërdorimi eventual të tyre apo arbitrariteti, si në legjislacionet e shteteve tjera, ashtu edhe në legjislacionin e aplikueshëm në Kosovë janë parashikuar disa kushte të domosdoshme që duhet plotësuar dhe procedura që duhet ndjekur me rastin e autorizimit dhe zbatimit të masave të veçanta hetimore.

Duhet theksuar se këto masa mund të autorizohen vetëm për vepra penale të caktuara, në rastet kur informatat që pretendohet të sigurohen janë të tejet të nevojshme dhe nuk mund të sigurohen përmes masave tjera hetimore.

1.2 Parimet bazë për zbatimin e masave të veçanta hetimore

Parimet bazë për zbatimin e masave të veçanta hetimore burojnë në radhë të parë nga dokumentet më të rëndësishme të të drejtave të njeriut, si në nivel ndërkombëtar, ashtu edhe në nivel kombëtar. Këto parime, si të tilla janë në proces të zhvillimit dhe avancimit të vazhdueshëm, ndërsa një rëndësi të madhe në këtë drejtim e luan edhe Gjykata Evropiane e të Drejtave të Njeriut. Fillimisht, duhet theksuar se sipas parimeve ndërkombëtare të të drejtave të njeriut, masat e veçanta hetimore duhet të zbatohen si mjet i fundit **("*Ultima ratio*")**, kur të dhënat dhe provat e domosdoshme për zhvillimin e suksesshëm të procedurës penale nuk mund të mblidhen në mënyra tjera.[3] Njëherit, këto masa mund të zbatohen vetëm nëse bëhet fjalë për vepra penale të rënda, vetëm në bazë të një urdhri të lëshuar nga organi shtetëror kompetent dhe në bazë të procedurës së përcaktuar me ligj.

Përndryshe me rastin e dhënien e urdhrit të këtyre masave duhet pasur parasysh disa parime themelore të cilat duhet të aplikohen dhe atë:

- Parimin e ligjshmërisë
- Parimin e subsidiaritetit
- Parimin e proporcionalitetit

[3] *Zbatimi i masave të veçanta hetimore 2024,* Raste nga praktika e jurisprudencës në Republikën e Maqedonisë së Veriut, Shkup, 2024, fq. 19.

- Parimin e konfidencialitetit
- Parimin e miratimit gjyqësor
- Parimin e kufizimit në kohë.

1.2.1 Parimi i ligjshmërisë

Parimi i ligjshmërisë i detyron shtetet që procedurën, kushtet dhe rrethanat tjera që kanë të bëjnë me zbatimin e masave të veçanta hetimore, t'i kenë të përcaktuara me dispozita precize ligjore, me qëllim që t'i shmanget ndonjë lloj arbitrariteti i shtetit në zbatimin e këtyre masave.[4]

Përndryshe, parimi i ligjshmërisë konsiderohet parim kryesor mbi bazën e të cilit mund të autorizohen masat e veçanta hetimore. Sipas këtij parimi, masat e veçanta hetimore mund të autorizohen vetëm nëse janë të përcaktuara me ligj. Ky parim në vetvete imponon krijimin e dispozitave ligjore të qarta dhe të sakta në lidhje me kushtet, procedurën dhe çështje tjera të rëndësishme që ndërlidhen me autorizimin e masave të veçanta hetimore. Në këtë drejtim, dispozitat ligjore duhet që ta përcaktojnë në mënyrë të qartë kategorinë e veprave penale për të cilat mund të autorizohen këto masa, personat që mund të jenë subjekt i këtyre masave, kohëzgjatjen dhe mënyrën e zbatimit të tyre, kontrollin e zbatimit, organi kompetent për autorizimin e tyre, ruajtjen dhe asgjësimin e materialeve, etj. Rrjedhimisht, parimi i ligjshmërisë në caktimin dhe zbatimin e masave të veçanta hetimore është një parakusht për sigurinë juridike të qytetarëve dhe ofron një garanci juridike se këto masa mund të autorizohen vetëm në rastet dhe kushtet e përcaktuara me ligj.

Edhe në nenin 8, paragrafi 2 të Konventën Evropiane për të Drejtat dhe Liritë e Njeriut,[5] është parashikuar mundësia e shtetit që ta derogoj të drejtën në privatësi, të paraparë në paragrafin 1 të nenit të njëjtë, nëse në mënyrë kumulative janë plotësuar dy (2) kushte: "në shkallën e parashikuar nga ligji dhe kur është e nevojshme në një shoqëri demokratike, në interes të sigurisë publike, për mbrojtjen e rendit publik, shëndetit ose moralit ose për mbrojtjen e të drejtave dhe lirive të të tjerëve".

[4] Po aty, fq. 31.
5 Konventën Evropiane për të Drejtat e Njeriut (në vijim: KEDNj) mund ta gjeni duke klikuar në këtë link: https://gzk.rks-gov.net/ActDetail.aspx?ActID=73773

Kushti, **"në shkallën e parashikuar nga ligji"** paraqet kërkesë eksplicite dhe promovim i parimit të ligjshmërisë. Me fjalë të tjera, siç u theksua edhe më lart, masat e veçanta hetimore duhet të jenë të parashikuara dhe rregulluara me ligj, i cili duhet në mënyrë koncize ta përkufizojë rrethin, respektivisht kategorinë e personave të cilët mund të jenë subjekt i zbatimit të masave; llojin e veprave penale për të cilat lejohet zbatimi i këtyre masave; kohëzgjatjen e masave, që duhet të jetë një kornizë e pranueshme kohore; mënyrën e zbatimit të këtyre masave; mënyrën e kontrollit dhe mbikëqyrjes së zbatimit të këtyre masave; regjimin e përdorimit dhe ruajtjes së incizimeve të siguruara nga zbatimi i masave dhe rrethanave tjera që janë të rëndësishme për zbatimin e tyre, e që reflektohen në liritë dhe të drejtat e individit.

Në linjë me këto që u theksuan, me dispozitat ligjore të KPP-së janë përcaktuar në mënyrë strikte masat e veçanta hetimore dhe qëllimi i tyre (nenet 85-86); ekzistimi i dyshimit të bazuar[6] se është kryer një vepër penale nga neni 89 i KPP-së, po kryhet apo së shpejti do të kryhet, si kriter i domosodoshëm për autorizimin e këtyre masave; organi kompetent që mund të autorizojë këto masa; personat ndaj të cilëve mund të autorizohen këto masa (neni 88); veprat penale për të cilat mund të autorizohen këto masa (neni 89); procedura për autorizimin e këtyre masave (neni 90); zbatimi i urdhrit për masat e veçanta hetimore (neni 91); afatet, zgjatja dhe ripërtëritja e urdhrit për masat e veçanta hetimore (neni 92) dhe shumë çështje tjera të rëndësishme.

1.2.2 Parimi i subsidiaritetit

Parimi i subsidiaritetit do të thotë se masat e veçanta hetimore mund të autorizohen vetëm si një mjet i fundit për t'u përdorur dhe vetëm nëse me

[6] "**Dyshim i bazuar"** nënkupton njohuri për informacionin që do të bindte një vëzhgues objektiv që një vepër penale ka ndodhur, po ndodh ose ka mundësi të konsiderueshme që do të ndodhë dhe se personi në fjalë ka më shumë gjasa që të ketë kryer veprën penale se sa që të mos e ketë kryer atë. Dyshimi i bazuar duhet të mbështetet në prova të artikulueshme (neni 19, paragrafi 1, nën-paragrafi 9 i KPP-së). Në dispozitat ligjore të KPP-së janë parashikuar disa nivele të dyshimeve në drejtim posedimit të njohurive dhe informacioneve lidhur me kryerjen e veprës penale dhe kryesit të saj, siç janë: "dyshimi i arsyeshëm"; "dyshimi i bazuar"; "shkaku i bazuar"; "gjasa reale" dhe "dyshimi i bazuar mirë" (neni 19, paragrafi 1, nën-paragrafët 8-12 të KPP-së). "Dyshimi i bazuar mirë" konsiderohet standardi më i lartë në raport me të gjitha këto nivele tjera, mirëpo për autorizimin e masave të veçanta hetimore kërkohet standardi i "dyshimit të bazuar".

masat apo me veprimet tjera hetimore nuk mund të arrihet qëllimi legjitim, përkatësisht që të sigurohet informacioni i kërkuar i cili do të kishte gjasa që të ndihmonte hetimin e veprave penale të caktuara. Ky parim si i tillë, është parashikuar, përveç tjerash, edhe në nenin 86, paragrafët 1 dhe 2 të KPP-së.

Në këtë mënyrë, në nenin 86, paragrafi 1 të KPP-së është parashikuar se "Nëse ekziston dyshimi i bazuar se është kryer një vepër penale nga neni 89 i këtij Kodi, po kryhet apo së shpejti do të kryhet, nëse informacioni i kërkuar për t'u marrë do të kishte gjasa të ndihmonte në hetimin dhe nëse informacioni nuk do të ishte i mundur për t'u marrë përmes ndonjë veprimi tjetër hetimor, pa vështirësi të paarsyeshme ose rrezik potencial për të tjerët...".

Gjithashtu, edhe në nenin 86, paragrafi 2 të KPP-së është parashikuar se "Nëse ekziston dyshimi i bazuar se është kryer një vepër penale nga neni 89 i këtij Kodi, po kryhet apo së shpejti do të kryhet dhe në qoftë se hetimi i veprës penale nuk mund të kryhet në ndonjë mënyrë tjetër, ose do të jetë shumë i vështirë...". Nga këto dispozita ligjore, rezulton në mënyrë të qartë, se masat e veçanta hetimore mund të autorizohen **"vetëm nëse hetimi i veprës penale nuk mund të kryhet në ndonjë mënyrë tjetër, ose do të jetë shumë i vështirë"**.

Ndërsa, se në cilat raste nuk mund që hetimi i veprës penale të kryhet në ndonjë mënyrë tjetër ose do të ishte shumë i vështirë, kjo është çështje që duhet të vlerësohet nga rrethanat specifike të secilit rast veç e veç dhe është përgjegjësi e gjyqtarit të procedurës paraprake apo prokurorit të shtetit. Përndryshe, nëse gjyqtari i procedurës paraprake apo prokurori i shtetit, konsiderojnë se hetimi i veprës penale mund të kryhet edhe në ndonjë mënyrë tjetër, përkatësisht duke ndërmarrë veprime tjera hetimore ose nuk do të jetë i vështirë, atëherë nuk duhet që të autorizojë masat e veçanta hetimore të kërkuara nga prokurori i shtetit.

Po ashtu, edhe nenin 88, paragrafi 1, nën-paragrafi 1.2. të KPP-së, është parashikuar se njëri prej kushteve që duhet të përmbushet në mënyrë që të autorizohen masat e veçanta hetimore është se "informacioni i kërkuar nuk do të kishte mundësi të merrej me masa të tjera hetimore, pa shkaktuar vështirësi të paarsyeshme ose rrezik potencial për të tjerët". Pra, siç shihet njëri prej kushteve ligjore, për autorizimin e masave të veçanta hetimore është që **"informacioni nuk do të ishte i mundur për t'u marrë përmes ndonjë**

veprimi tjetër hetimor, pa vështirësi të paarsyeshme ose rrezik potencial për të tjerët", e që në thelb nënkupton se këto masa vijnë në shprehje, vetëm nëse informacioni nuk është i mundur që të sigurohet përmes ndonjë veprimi tjetër hetimor, pa vështirësi të paarsyeshme ose rrezik potencial për të tjerët.

Bazuar në dispozitat e lartcekura ligjore, por edhe në parimet ndërkombëtare të të drejtave të njeriut, masat e veçanta hetimore mund të autorizohen vetëm nëse informacioni i kërkuar ose hetimi i veprës penale nuk mund të kryhet me veprime tjera hetimore, do të ishte shumë i vështirë apo do të paraqiste rrezik potencial për të tjerët. Andaj, edhe në këtë drejtim, konstatohet se masat e veçanta hetimore janë të karakterit subsidiar, pasi që mund të autorizohen vetëm si mjet i fundit, nëse plotësohen kushtet ligjore të lartcekura.

Rrjedhimisht, parimi i subsidiaritet është një garanci juridike se këto masa nuk mund të zbatohen në mënyrë rutinë, përkatësisht si një mënyrë e zakonshme e sigurimit të informacioneve apo zbatimit të hetimeve.

1.2.3 Parimi i proporcionalitetit

Parimi i proporcionalitetit nënkupton sigurimin e proporcionit midis zbatimit të masave të veçanta hetimore dhe kufizimit të të drejtave individuale të personit, nga njëra anë, kundrejt interesit shoqëror dhe qëllimit legjitim mbi të cilin janë fokusuar këto masa, nga ana tjetër. Për të arritur këtë, nevojitet një ekuilibër midis qëllimit të zbatimit të tyre dhe mjeteve të përdorura për arritjen e këtij qëllimi, si dhe një ekuilibër midis interesave të përgjithshme (sigurisë publike) dhe mbrojtjes së të drejtave individuale të personit.[7] Me fjalë të tjera, subjektet që i kërkojnë ose aprovojnë këto masa, në çdo rast individual, duhet me kujdes ta vlerësojnë proporcionin midis peshës së veprës penale dhe të gjitha rrethanave të lëndës konkrete, nga njëra anë, kundrejt masave përkatëse, nga ana tjetër, për shkak se disa nga këto masa të veçanta hetimore janë të natyrës së tillë që **"prima facie"** mund të cenojnë të drejtat e privatësisë. Përndryshe, proporcioni në këtë kontekst synon një ekuilibër të barabartë midis mbrojtjes së të drejtave individuale nga njëra anë dhe interesave të shoqërisë, nga ana tjetër. Parimi i proporcionalitetit është i parashikuar në një mënyrë në dispozitat ligjore të theksuara më lart që i referohen e parimit të

[7] *Zbatimi i masave të veçanta hetimore 2024,* Raste nga praktika e jurisprudencës në Republikën e Maqedonisë së Veriut, Shkup, 2024, fq.20.

subsidiaritetit, nga të cilat shihet se masat e veçanta hetimore duhet të zbatohen vetëm në rastet e domosdoshme, me qëllim të sigurimit të informacioneve të rëndësishme për procedurën penale. Përtej kësaj, një parim i tillë buron edhe nga dispozitat kushtetuese. Kështu, në nenin 36.3. të Kushtetutës së Kosovës, në të cilën është garantuar "Fshehtësia e korrespondencës, telefonisë dhe komunikimit tjetër" si pjesë përbërëse e "Të Drejtës për Privatësi", është parashikuar se kjo e drejtë mund të kufizohet vetëm përkohësisht, në bazë të vendimit gjyqësor, **"nëse është e domosdoshme"** për ecurinë e procedurës penale ose për mbrojtjen e vendit, në mënyrën e parashikuar me ligj. Kurse, GjEDNj-ja, nocionin e **"domosdoshmërisë"** në raste të tilla e sqaron si ndërhyrje në jetën private të personit, vetëm si përgjigje ndaj një nevoje urgjente shoqërore. Në këtë mënyrë, shkalla dhe intensiteti i ndërhyrjes në privatësinë e një personi duhet të jetë në proporcion me nevojën për shkak të së cilës zbatohet masa e veçantë hetimore.

Po ashtu, ky parim i rëndësishëm është i parashikuar edhe në dispozitat ligjore të Ligjit për Përgjimin e Komunikimeve Elektronike, pavarësisht faktit ky parim trajtohet vetëm në kuptim të përgjimeve elektronike.[8] Kështu, në nenin 4, paragrafi 2 të këtij Ligji, është parashikuar se me rastin e marrjes së vendimit për përgjim, gjykata kompetente bartë detyrimin për t'u kujdesur për esencën e të drejtave dhe lirive të personave për të cilët është bërë kërkesë përgjimi; rëndësinë, nevojën e përgjimit dhe proporcionalitetin; natyrën, mjetet dhe vëllimin e përgjimit; raportin në mes të qëllimit që synohet të arrihet dhe mundësisë së realizimit të këtij qëllimi me metoda tjera hetuese dhe sekretin dhe objektivitetin gjatë kryerjes së përgjimit.

1.2.4 Parimi i konfidencialitetit

Parimi i konfidencialitetit nënkupton se masat e veçanta hetimore konsiderohen konfidenciale, derisa zbulimi i tyre të kërkohet në pajtim me dispozitat ligjore të KPP-së. Kështu, në nenin 87 të KPP-së ("Fshehtësia e mbledhjes së informatave") është parashikuar se "nëse prokurori i shtetit apo gjyqtari i procedurës paraprake autorizojnë masat veçanta hetimore në pajtim me paragrafët 1 ose 2 të nenit 86 të këtij Kodi, dosja mbyllet dhe mbahet e fshehur derisa zbulimi i saj të kërkohet në pajtim me këtë Kod". Gjithashtu,

[8] Ligji Nr. 05/L-030 për Përgjimin e Komunikimeve Elektronike, datë 28.05.2015.

në nenin 94, paragrafi 1 të KPP-së është parashikuar se "Personi i cili i nënshtrohet masave të veçanta hetimore nuk njoftohet për rrjedhën apo rezultatin deri në përfundimin e masës". Së këndejmi, për shkak të natyrës së tyre, zyrtarët që kanë përgjegjësi të caktuara në autorizimin dhe zbatimin e masave të veçanta hetimore detyrohen që të ruajnë si fshehtësi zyrtare zbatimin e këtyre masave.

Përndryshe, zbulimi i çfarëdo informate në këtë drejtim përbën vepër penale **"Shkelja e urdhrave për masat e fshehura ose teknike të vëzhgimit ose hetimit"** sipas nenit 203 Kodit Penal të Republikës së Kosovës.[9]

Kështu, në paragrafin 1 të këtij neni është parashikuar se "Zyrtari policor i autorizuar i cili zbaton një urdhër gjyqësor ose prokurorial për masat e fshehura ose teknike të vëzhgimit ose hetimit në shkelje të ligjit, dënohet me burgim prej tre (3) muaj deri në tre (3) vjet". Kurse, në paragrafin 2 të këtij neni është parashikuar se "Kushdo që zbulon informatën që do të dëmtojë efikasitetin e zbatimit të një urdhri për masat e fshehura ose teknike të vëzhgimit ose hetimit, dënohet me burgim prej gjashtë (6) muaj deri në tre (3) vjet". Gjithashtu, duke qenë se dosja e masave të veçanta të hetimeve konsiderohet fshehtësi zyrtare derisa të zbulohet sipas dispozitave të KPP-së,

[9] Kodi Penal i Kosovës, Nr.06/L-074, datë 23.11.2018 (në tekstin e mëtejmë: KPRK). KPRK mund të gjendet në këtë link: https://gzk.rks-gov.net/ActDetail.aspx?ActID=18413

atëherë zbulimi i paautorizuar i këtyre të dhënave mund të cilësohet edhe si vepër penale **"Zbulimi i fshehtësisë zyrtare"**,[10] nga neni 426 të KPRK-së.[11]

1.2.5 Parimi i miratimit gjyqësor

Për shkak të natyrës së tyre, në shumë shtete bashkëkohore është parashikuar edhe parimi i miratimit gjyqësor të masave të veçanta hetimore. Në fakt, ky parim i rëndësishëm i zbatimit të masave të veçanta hetimore, përveç nga dispozitat përkatëse ligjore, buron edhe nga vetë dispozitat kushtetuese. Në këtë mënyrë, në nenin 36.1. të Kushtetutës së Kosovës **(" E Drejta e Privatësisë")** është garantuar se "Çdokush gëzon të drejtën që t'i respektohet jeta private dhe familjare, pacenueshmëria e banesës dhe fshehtësia e korrespondencës, telefonisë dhe e komunikimeve të tjera". Kurse, "Kontrollet e cilësdo banesë ose cilitdo objekti privat, që mendohet se janë të

[10] Kështu, në paragrafin 1 të nenit 426 të KPRK-së është parashikuar forma themelore e kësaj vepre penale e cila kryhet në rastet kur "Personi zyrtar i cili pa autorizim kumton, dërgon ose në ndonjë mënyrë tjetër i vë në dispozicion personit tjetër informatën që përbën fshehtësi zyrtare ose siguron informatën e tillë me qëllim që t'ia përcjellë ndonjë personi të paautorizuar, për të cilën është parashikuar dënim me burgim prej gjashtë (6) muaj deri në tre (3) vjet". Kurse, në paragrafin 2 të këtij neni është parashikuar forma e rëndë e kësaj vepre penale e cila kryhet për përfitim personal ose me qëllim të publikimit apo shfrytëzimit të informacionit jashtë Republikës së Kosovës, për të cilën është parashikuar dënim me gjobë dhe me burgim prej një (1) deri në dhjetë (10) vjet. Ndërsa, në paragrafin 3 të këtij neni është parashikuar forma e lehtë e kësaj vepre penale e cila kryhet nga pakujdesia, për të cilën është parashikuar dënim me gjobë ose me burgim deri në tre (3) vjet. Gjithashtu, duhet theksuar sipas paragrafit 4, dispozitat e këtij neni zbatohen ndaj personit i cili zbulon fshehtësinë zyrtare edhe pasi që të ketë pushuar statusi i tij zyrtar. Dhe në fund, paragrafi 5 i këtij neni është dispozitë ligjore e karakterit shpjegues, pasi që sqaron domethënien e shprehjes "fshehtësi zyrtare" dhe rastet kur informatat e caktuara nuk konsiderohen "fshehtësi zyrtare". Kështu, sipas kësaj dispozitë ligjore, për qëllime të këtij neni, shprehja "fshehtësi zyrtare" nënkupton informatat ose dokumentet të shpallura si fshehtësi zyrtare me ligj, dispozita të tjera ose me vendim të organit kompetent të nxjerrë në bazë të ligjit dhe zbulimi i të cilave ka shkaktuar ose mund të shkaktojë pasoja të dëmshme. Sidoqoftë, informatat në vijim nuk konsiderohen fshehtësi zyrtare: informatat apo dokumentet të cilat janë të drejtuara në cenimin e rëndë të të drejtave themelore të njeriut ose mos zbulimi i të cilave do të mund të rrezikonte rendin kushtetues apo sigurinë e Republikës së Kosovës; ose informatat dhe dokumentet të cilat kanë për qëllim fshehjen e kryesit të veprës penale të dënueshme me së paku pesë (5) vjet burgim

[11] Vepër penale e natyrës së tillë është parashikuar edhe në nenin 125 të KPRK-së, e cila emërtohet "Zbulimi i informacioneve të klasifikuara dhe mos ruajtja e informacioneve të klasifikuara", të cilën e kryen kushdo që zbulon ose nuk ruan informacionin e klasifikuar, e për të cilën do të dënohet sipas Ligjit për klasifikimin e informacioneve dhe verifikimin e sigurisë.

domosdoshme për hetimin e krimit, mund të bëhen vetëm deri në shkallën e domosdoshme dhe "**vetëm pas miratimit nga ana e gjykatës",** pas shpjegimit të arsyeve pse një kontroll i tillë është i domosdoshëm. Shmangia nga kjo rregull lejohet, nëse është e domosdoshme për arrestim të ligjshëm, për mbledhjen e provave që ka rrezik të humbasin ose për mënjanimin e rrezikut të drejtpërdrejtë dhe serioz për njerëzit dhe për pasuri, në mënyrën e përcaktuar me ligj. Gjykata duhet që të miratoj veprimet e tilla në mënyrë retroaktive". Bazuar në këtë dispozitë kushtetuese, rezulton se kontrollimi i cilësdo banesë apo objekti privat, që janë të domosodoshme për hetimin e veprave penale mund të bëhet vetëm deri në shkallën e domoshdoshme dhe "vetëm pas miratimit nga ana e gjykatës". Kjo që u theksua, shihet se këto veprime hetimore mund të bëhet vetëm në bazë të "miratimit të gjykatës", kuptohet nëse plotësohen edhe kushtet tjera të paracaktuar.

Përveç kësaj, edhe "Fshehtësia e korrespondencës, telefonisë dhe komunikimit tjetër" që konsiderohen pjesë përbërëse e "Të Drejtës për Privatësi",[12] mund të kufizohet vetëm përkohësisht dhe në bazë **"të vendimit gjyqësor"**, nëse është e domosdoshme për ecurinë e procedurës penale ose për mbrojtjen e vendit, në mënyrën e parashikuar me ligj.[13]

1.2.6 Parimi i kufizimit në kohë

Parimi i kufizimit në kohë nënkupton se masat e veçanta hetimore kanë karakter të përkohshëm dhe duhet të kenë kohëzgjatje sa më të shkurtër të mundshme, përkatësisht vetëm sa është e domosodshme për arritjen e synimit të përcaktuar me ligj. Një parim i tillë, përveç me dispozitat ligjore të KPP-së,[14] është parashikuar edhe me dispozitat e Kushtetutës së Kosovës. Kështu,

[12] Neni 36.3. i Kushtetutës së Kosovës.

[13] Përndryshe, duhet sqaruar se përgjimi i paautorizuar konsiderohet vepër penale sipas dispozitave ligjore të KPRK-së. Kështu, në nenin 201 të KPRK-së ("Përgjimi i paautorizuar") është parashikuar se "Kushdo që pa autorizim, përgjon bisedën apo deklaratën ose i mundëson personit tjetër të jetë në dijeni për bisedën apo deklaratën e cila është përgjuar pa autorizim, dënohet me burgim prej një (1) deri në tre (3) vjet. Kur vepra penale nga paragrafi 1. i këtij neni kryhet nga personi zyrtar në keqpërdorim të pozitës apo autorizimeve të tij, kryesi dënohet me burgim prej dy (2) vjet deri në pesë (5) vjet. Pajisjet e përdorura për kryerjen e veprës penale nga paragrafi 1. i këtij neni konfiskohen".

[14]Në nenin 92, paragrafët 1 dhe 2 të KPP-së është parashikuar se "Prokurori i shtetit apo gjyqtari i procedurës paraprake mund të lëshojnë urdhrin për masat e veçanta hetimore për një afat prej nëntëdhjetë (90) ditësh nga dita e lëshimit të urdhrit. Prokurori i shtetit apo gjyqtari

në nenin 36.3 të Kushtetutës, në të është parashikuar se "Fshehtësia e korrespondencës, telefonisë dhe komunikimit tjetër, është e drejtë e pacenueshme", njëkohësisht është parashikuar se "Kjo e drejtë mund të kufizohet **vetëm përkohësisht,** në bazë të vendimit gjyqësor, nëse është e domosdoshme për ecurinë e procedurës penale ose për mbrojtjen e vendit, në mënyrën e parashikuar me ligj". Pra, siç shihet, fshehtësia e korrespondencës, telefonisë dhe komunikimeve tjera, nën supozimin e përmbushjeve edhe të kushteve tjera, mund të kufizohet "**vetëm përkohësisht",** ndërsa një aspekt i tillë mandej duhet që rregullohet me dispozita përkatëse ligjore dhe duhet të vlerësohet në dritën e rrethanave të secilit rast veç e veç.

i procedurës paraprake nuk mund të lëshojë urdhër tjetër me shkrim për zgjatjen e urdhrit sipas këtij kapitulli, përveç nëse vazhdojnë të vlejnë parakushtet e parapara në nenin 88 të këtij Kodi për urdhërimin e masës sipas këtij kapitulli dhe nëse për shkak të nevojës për grumbullimin e mëtejshëm të provave kërkohet zgjatja e urdhrit. Zgjatja e urdhrit të lëshuar sipas paragrafit 1 të këtij neni mund të bëhet edhe për një afat prej nëntëdhjetë (90) ditësh brenda periudhës kohore prej treqindegjashtëdhjetepesë (365) ditësh".

Pjesa e dytë

2. MASAT E VEÇANTA HETIMORE SIPAS KODIT TË PROCEDURËS PENALE

2.1 Vështrime të përgjithshme

Kushtetuta e Republikës së Kosovës në Kapitullin e dytë të saj ka përcaktuar të drejtat dhe liritë themelore të cilat përfshijnë një gamë të këtyre të drejtave që janë në harmoni të plotë edhe me një numër të madh të marrëveshjeve ndërkombëtare, deklaratash, konventash dhe instrumentesh ndërkombëtare e të cilat rrjedhimisht garantohen përmes kushtetutës. Vend të veçantë zë Deklarata Universale për të Drejtat e Njeriut, Konventa Evropiane për Mbrojtjen e të Drejtave të Njeriut dhe Lirive Themelore, Konventa Evropiane për të Drejtat Civile dhe Politike, Konventa për të Drejtat e Fëmijës Konventa për Eliminimin e të gjitha formave të Diskriminimit Racor dhe akte tjera ndërkombëtare.

Gjithashtu, me nenin 36 të Kushtetutës së Republikës së Kosovës është rregulluar e drejta e privatësisë dhe e cila dispozitë ofron mbrojtje të privatësisë si një ndër të drejtat themelore, përkatësisht gëzimi i të drejtës për respektim të jetës private dhe familjare, pacenueshmërinë e banesës dhe fshehtësisë së korrespodencës, telefonisë dhe komunikimeve tjera, si të drejta të patjetërsueshme. Megjithatë, Kushtetuta e rregullon edhe mundësinë e kufizimit të këtyre të drejtave dhe atë në bazë të vendimit gjyqësor dhe përkohësisht dhe kjo në rastet kur është e domosdoshme për zhvillimin e procedurës penale dhe nëse mohimi i përmendur është i domosdoshëm për mbrojtjen e vendit. mirëpo vendimi për këto kufizime duhet të jetë i kufizuar në kohë, pra duhet të ketë karakter të përkohshëm dhe duhet të zgjas në kohë sa më shkurtër, pra vetëm aq sa është e domosdoshme për zhvillimin e procedurës penale apo mbrojtjen e vendit.

Kufizimi i të drejtave kushtetuese bëhet vetëm sipas mënyrës së përcaktuar me ligj dhe konkretisht Kodi i Procedurës Penale të Kosovës ka përcaktuar kufizimin përmes aplikimit të masave të veçanta hetimore që janë veprime procedurale përmes të cilave të cilat përkohësisht kufizojnë të drejtat kushtetuese dhe liritë e njeriut. Përndryshe kushtet ligjore për aplikimin e

masave të veçanta hetimore përcaktojnë kufirin mes Kushtetutës, dokumenteve ndërkombëtare për të drejtat e njeriut dhe të cilat janë ngushtësisht të ndërlidhura me parimin e ligjshmërisë, subsidiaritetit, proporcionalitetit, konfidencialitetit, miratimit gjyqësor dhe kufizimit në kohë.

Në nënkapitullin e tretë të KPP-së janë përcaktuar masat e veçanta hetimore të cilat mund të përdoren nga ana e prokurorisë dhe gjykatës dhe të cilat janë të sistemuara në disa nene të veçanta, me ç'rast janë paraqitur përkufizimet sqaruese të këtyre masave, qëllimet e aplikimit të tyre, kushtet ligjore dhe llojet e veprave për të cilat mund të urdhërohen këto masa.

Tutje dispozitat ligjore në mënyrë të hollësishme kanë paraqitur organet e autorizuara për lëshimin e masave, organet për zbatimin e tyre, afatet dhe kohëzgjatja e tyre materialet e siguruara. Kurse dispozitat e neneve 93-97 të KPP-së, kanë përcaktuar veprimet pas sigurimit të materialeve të siguruara përmes masave të veçanta hetimore, njoftimi i personave që i janë nënshtruar këtyre masave dhe pranueshmëria e tyre, si dhe shqyrtimet e ankesave nga ana e panelit të posaçëm i cili shqyrton ankesat që personat i paraqesin duke konsideruar se pa të drejtë i janë nënshtruar masave të veçanta hetimore.

2.2 Përkufizimet e masave të veçanta hetimore

Me qëllim të shmangies së intepretimeve të ndryshme lidhur me masat e veçanta hetimore, ligjvënësi me dispozitë të posaçme ka përcaktuar përkufizime për secilën masë të veçantë hetimore[15]. Konsiderojmë se përkufizimi i shprehjeve të masave të veçanta hetimore kanë për qëllim parësor shmangien e interpretimeve të ndryshme dhe njëkohësisht paraqet një aspekt sqarues se cilat janë këto masa të veçanta hetimore të cilat mund të urdhërohen.

Përkufizimet e masave të veçanta hetimore janë dhënë për secilën masë si në vijim:
1. Shprehja "vëzhgim i fshehtë fotografik ose me video" do të thotë monitorim, vëzhgim ose incizim i personave, i lëvizjeve të tyre ose i

[15] Neni 85 i KPP-së.

aktiviteteve të tjera nga zyrtari i autorizuar i policisë ose personi i cili vepron nën mbikëqyrjen e zyrtarit të autorizuar të policisë, me anë të fotografimit ose me video mjete, pa dijeninë apo pëlqimin e së paku njërit prej personave që i nënshtrohen kësaj mase.

2. Shprehja "monitorim i fshehtë i bisedave" do të thotë monitorimi, incizimi ose transkriptimi i bisedave nga zyrtari i autorizuar i policisë ose personi i cili vepron nën mbikëqyrjen e zyrtarit të autorizuar të policisë, me anë të mjeteve teknike, pa dijeninë ose pëlqimin e së paku njërit prej personave që i nënshtrohen kësaj mase. Monitorimi i fshehtë i bisedave mund të kryhet edhe kur njëri nga dy personat që do të monitorohen është i gatshëm të kryejë dhe të regjistroj veprimin përkatës, nën mbikëqyrjen e zyrtarit të autorizuar të policisë.

3. Shprehja "kontrollim i dërgesave postare" do të thotë kontrollim i letrave dhe i dërgesave të tjera postare nga zyrtari i autorizuar i policisë, që mund të përfshijë edhe përdorimin e pajisjeve rëntgen.

4. Shprehja "përgjim i telekomunikimeve dhe përdorimi i lexuesit – IMSI – identifikimi ndërkombëtar i shfrytëzuesit mobil" do të thotë përgjim i komunikimeve zanore, komunikimeve tekstuale ose komunikimeve tjera përmes rrjeteve të telefonive fikse apo mobile. Kjo përfshinë çfarëdo mjeti apo sistemi tjetër të ngjashëm teknologjik që bartë të dhëna që kryesisht kanë për qëllim të jenë private.

5. Shprehja "dërgim i kontrolluar i dërgesave postare" do të thotë dërgim i letrave dhe i materialeve të tjera postare nga zyrtari i autorizuar i policisë.

6. Shprehja "dërgesa e kontrolluar" nënkupton teknikën e lejimit të dërgesave të paligjshme ose të dyshuara për të kaluar nga, përmes ose në territorin e një ose të më shumë shteteve, me njohurinë dhe nën mbikëqyrjen e autoriteteve kompetente, me qëllim hetimin e veprave penale dhe identifikimin e personave të përfshirë në kryerjen e veprës penale.

7. Shprehja "shfrytëzim i mjeteve për përcjellje të vendndodhjes" do të thotë shfrytëzim nga zyrtari i autorizuar i policisë i mjeteve të cilat identifikojnë vendndodhjen e personit ose të objektit në të cilin është ngjitur mjeti.

8. Shprehja “shitja dhe blerja e simuluar e artikujve, shërbimeve apo sendeve” do të thotë akt i shitjes apo blerjes së ndonjë artikulli, shërbimi apo sendi nga personi i dyshuar se ka kryer vepër penale, që mund të shërbejë si provë në procedurën penale, ose nga personi për të cilin dyshohet të jetë viktimë e veprës penale të “Trafikimit me njerëz”, siç përcaktohet në nenin 165 të Kodit Penal. Ky veprim mund të kryhet nga zyrtari i autorizuar i policisë ose personi i cili vepron nën mbikëqyrjen e zyrtarit të autorizuar të policisë.

9. Shprehja “dhënia dhe marrja e simuluar e ryshfetit” do të thotë një veprim që është i njëjtë me veprën penale të ndërlidhur me korrupsion, por që ndryshon për shkak se kryhet me qëllim të mbledhjes së informacionit dhe provave gjatë hetimit penal.

10. Shprehja “regjistrimi i simuluar i personave juridik ose përdorimi i personave ekzistues juridik për mbledhjen e të dhënave” do të thotë krijim i subjekteve juridike me qëllim të ofrimit të shërbimeve të simuluara të biznesit ose përdorimi i personave ekzistues juridik për mbledhjen e të dhënave. Ofrimi i shërbimeve të simuluara të biznesit mund të kryhen me përdorimin e masave të veçanta hetimore lidhur me identitetin e personit, pronësinë ndaj sendeve apo pasurisë dhe personave juridik.

11. Shprehja “hetim i fshehtë” do të thotë përdorimi i hetuesve të fshehtë dhe bashkëpunëtorëve, përkatësisht një ndërveprim i planifikuar i zyrtarit të autorizuar të policisë ose bashkëpunëtorit, i cili nuk është i identifikueshëm si zyrtar i autorizuar i policisë, ose i personit i cili vepron nën mbikëqyrjen e zyrtarit të autorizuar të policisë me personat e dyshuar se kanë kryer vepër penale.

12. Shprehja “regjistrim i thirrjeve telefonike” do të thotë sigurim i të dhënave të thirrjeve telefonike të bëra nga një numër i caktuar i telefonit, duke përfshirë por pa u kufizuar në vërtetimin e identifikimit të numrit të caktuar, verifikimin e numrit të telefonit, vendndodhjen gjeografike, lokacionin e pajisjes, vërtetimin e abonentit të telefonit, ose shenjat e identifikimit të pajisjes (IMEI).

13. Shprehja "zbulim i të dhënave financiare" do të thotë sigurim i informacionit nga banka apo ndonjë institucion tjetër financiar mbi depozitat, llogaritë ose transaksionet financiare.

Bazuar në shprehjet e kufizuara del se legjislacioni ynë ka përcaktuar trembëdhjetë masa të veçanta hetimore të cilat mund të aplikohen e që kjo paraqet një gamë mjaft të gjerë të këtyre masave. Sa për të bërë një komperacion del se legjislacionet tjera në rajon kanë përcaktuar numër më të vogël të këtyre masave, kjo për faktin se Kodi i Procedurës Penale të Shqipëtisë ka përcaktuar numër më të vogël të masave të veçanta hetimore[16], kurse Kodi i Procedurës Penale të Kroacisë nuk kuadër të masave që kufizojnë përkohësisht të drejtat kushtetuese dhe liritë e njeriut janë paraprë vetëm tetë masa të tilla.[17] Po ashtu edhe Kodi i Procedurës Penale të Malit të Zi ka paraparë dhjetë masa të hetimit të fshehtë të cilat aplikohen.[18] Kurse Kodi i Procedurës Penale të Bosnjes dhe Hercegovinës ka paraparë vetëm shtatë masa të veçanta hetimore.[19]

2.3 Qëllimi dhe llojet e masave të veçanta hetimore

Dispozita e nenit 86 të KPP-së ka përcaktuar qëllimin dhe llojet e masave të veçanta hetimore dhe përmes kësaj dispozite ligjore është përcaktuar se urdhrin për këto masa mund të autorizohet nga ana e vet prokurorit të shtetit në rastet kur këto masa janë të karakterit publik, kurse kur masat e veçanta hetimore duhet të lëshohen në vende ku cenohet privatësia, atëherë urdhrat e tillë lëshohen nga ana e gjyqtarit të procedurës paraprake. Kjo zgjidhje e bërë që disa nga masat e veçanta hetimore të urdhërohen nga ana e prokurorit të shtetit padyshim se ngre disa dilema të cilat mund të paraqiten lidhur me faktin se kjo dispozitë a është në frymën e dispoziatave kushtetuese të vendit tonë, meqë dispozita e nenit 36 par.3 të Kushtetutës së Republikës së Kosovës ka përcaktuar se:

"*Fshehtësia e korrespondencës, telefonisë dhe komunikimit tjetër, është e drejtë e pacenueshme. Kjo e drejtë mund të kufizohet vetëm përkohësisht, në*

[16] Shih Kodin e Procedurës Penale të Republikës së Shqipërisë
[17] Neni 332 i Kodit të Procedurës Penale të Kroacisë
[18] Neni 157 i Kodit të Procedurës Penale të Malit të Zi
[19] Neni 116 i Kodit të Procedurës Penale të Bosnjes dhe Hercegovinës

bazë të vendimit gjyqësor, nëse është e domosdoshme për ecurinë e procedurës penale ose për mbrojtjen e vendit, në mënyrën e parashikuar me ligj". E që sipas interpretimit të kësaj dispozite kushtetuese përkufizimet e përcaktuara mund të kufizohen vetëm përkohësisht dhe bazuar në një vendim gjyqësor. Pra si autoritet të vetëm për kufizimet e këtyre të drejtave e ka përcaktuar gjykatën, përkatësisht gjyqtarin kompetent. Për më tepër, kjo zgjidhje e legjislacionit tonë që disa nga këto masa të urdhërohen edhe nga ana e prokurorisë së shtetit janë vetëm në legjislacionin tonë. Meqë legjislacionet e shteteve tjera, Shqipëria, Kroacia dhe Mali i Zi, si autoritet të vetëm për urdhrin e këtyre masave e kanë përcaktuar gjykatën kompetente.

Tutje me dispozitën e nenit 86 të KPP-së janë përcaktuar dy kushtet ligjore të domosdoshme që të mund të urdhërohen masat e veçanta hetimore dhe që si kusht primar është përcaktuar ekzistimi i dyshimit të bazuar se është kryer një vepër penale, po kryhet apo së shpejti do të kryhet dhe që kjo vepër penale të jetë në veprat penale të përcaktuara me dispozitën e nenit 89 të KPP-së. Kurse kushti tjetër është që informacioni i kërkuar për t'u marrë do të kishte gjasa të ndihmonte në hetimin dhe nëse informacioni nuk do të ishte i mundur për t'u marrë përmes ndonjë veprimi tjetër hetimor pa vështirësi të paarsyeshme ose rrezik potencial për të tjerët.

Duke analizuar këto kushte gjithsesi fillimisht është e nevojshme të theksohet fakti se urdhërimi i këtyre masave mund të bëhet në tri faza në fazën kur vepra penale tani më është kryer, mirëpo ende nuk kemi informacione lidhur me kryerësin e saj dhe për zbulimin e identitetit të kryerësve nevojitet lëshimi i masave. Faza tjetër e urdhrit është në rastet kur vepra penale është duke u kryer, kjo për faktin se shumë vepra penale mund të kryhen në një kontinuitet të caktuar dhe në faza të ndryshme të kryerjes, kurse faza e tretë e mundësisë së lëshimit të urdhrit është në rastet kur vepra penale së shpejti do të kryhet.

Gjithashtu, për lëshimin e urdhrave për masa të veçanta janë përcaktuar edhe disa kushte specifike që janë të karakterit përjashtues që nënkupton se mund të urdhërohen vetëm në raste të veçanta dhe atë **se informacioni do të kishte gjasa të ndihmonte në hetimin dhe nëse informacioni nuk do të ishte i mundur për t'u marrë përmes ndonjë veprimi tjetër hetimor pa vështirësi të paarsyeshme ose rrezik potencial për të tjerët**. Pra në mënyrë kumulative duhet të përmbushen edhe kushtet e sipër cekura që në fakt në vete ngërthejnë

më së miri parimin e proporcionalitetit se masat e veçanta hetimore mund të lëshohen vetëm në rastet kur përmes këtyre masave do të ndihmohej hetimi, e që kjo nënkupton se hetimi nuk duhet bazuar ekskluzivisht vetëm në këto masa. Po ashtu si kushte përcaktohen edhe fakti se informacioni nuk do të mund të merret përmes veprimeve të tjera hetimore pa vështirësi të paarsyeshme, si dhe që mos aplikimi i këtyre masave, përkatësisht hetimet përmes metodave të zakonshme do të paraqitnin rrezik potencial për të tjerët.

Duke analizuar kushtet specifike *se informacioni nuk do të mund të merret përmes veprimeve të tjera hetimore pa vështirësi të paarsyeshme, si dhe që mos aplikimi i këtyre masave, përkatësisht hetimet përmes metodave të zakonshme do të paraqitnin rrezik potencial për të tjerët*, duke u referuar në praktikën gjyqësore del se ndër arsyet që theksohen në urdhrat e lëshuar janë të natyrave të ndryshme dhe kjo mund të ndërlidhet me personalitetin e kryerësit, dhe rrezikshmërinë e tij, natyra e veprës penale për të cilën ekziston dyshimi bazuar, mënyra e marrjes së veprimeve, numri më i madh i pjesëmarrësve dhe bashkëpunimi i tyre, roli kyç i ndonjërit prej personave, shkalla e lartë e organizimit. Aspekti i rrezikut potencial për të tjerët është rreziku që mund të i nështrohen zbatuesit e masave të veçanta hetimore qoftë të shëndetit apo jetës së tyre, rrezikimi pasurisë në përmasa të mëdha, mundësia e rrjedhjes së informacioneve që do të mundësonin asgjësimin e provave, pra këto janë disa nga rrethanat që mund të përdoren me rastin e arsyetimit të urdhrit për masat e veçanta hetimore, por gjithsesi këto nuk janë të natyrës shteruese pasi që mund të përdoren edhe rrethana të tjera, mirpo gjithmonë duhet dhënë një arsyetim i detajuar për faktin se marrja e informacionit nuk mund të merret përmes hetimeve të zakonshme.

Deri sa në nenin 86 paragrafin 1 të KPP-së janë përcaktuar kushtet dhe llojet e masave të veçanta hetimore që mund të urdhërohen nga ana e prokurirsë së shtetit në paragrafin e dytë janë paraqitur kushtet dhe llojet e masave kur urdhërohen nga ana e gjyqtarit të procedurës paraprake.

Edhe me këtë rast janë përcaktuar kushtet e përgjithshme që është dyshimi i bazuar se është kryer, po kryhet apo së shpejti do të kryhet një vepër penale nge neni 89 i KPP-së. Duhet theksuar se këto masa urdhërohen vetëm bazuar në kërkesën e prokurorit të shtetit dhe me këtë rast gjithsesi prokurori i shtetit duhet të bëj të besueshëm faktin se janë plotësuar kushtet nga neni 86 par.2 i

KPP-së. Përndryshe, dyshimi i bazuar është bazë e posaçme për lëshimin e urdhrit për masë të veçantë hetimore dhe me qëllim të definit të kësaj ligjvënësi me dispozitën e nenit 19 par.1.9 të KPP-së, ka përcaktuar se: *"Dyshimi i bazuar paraqet njohuri për informacionin që do të bindte një vëzhgues objektiv që një vepër penale ka ndodhu, po ndodh ose ka mundësi të konsiderueshme që do të ndoshë dhe se personi në fjalë ka më shumë gjasa që të ketë kryer veprësn penale se sa të mos e ketë kryer. Dyshimi i bazuar duhet të mbështetet në prova të artikulueshme.".*

Megjithatë, përkitazi me përcaktimin e dyshimit të bazuar se i pandehuri ka kryer veprën penale është një çështje mjaft delikate pasi që kjo është një fazë mjaft e hershme e procedurës penale, përkatësisht zhvillimit të hetimeve. Nga kjo rrjedh se gjykatat në këtë fazë kanë mjaft vështirësi në definimin e dyshimit të bazuar, përkatësisht përcaktimin e kualitetit dhe kuantitetit të provave me qëllim të përcaktimit të ekzistimit apo jo të dyshimit të bazuar, meqenëse kjo paraqet një çështje faktike se deri në cilën masë është arritur të definohet kjo bazë e dyshimit të bazuar.

Përveç kësaj gjithsesi edhe përcaktimi i bazave tjera për të urdhëruar këto masa janë mjaft sfiduese në këtë stad të procedurës penale, përkatësisht përcaktimi i se **hetimi i veprës penale nuk mund të kryhet në ndonjë mënyrë tjetër, ose do të jetë shumë i vështirë.** Në këtë aspekt bie në sy dy standarde të përdorura te ligjvënësi në rastet kur urdhrat lëshohen nga ana e prokurorisë dhe gjykatës e që me këtë rast del se te prokuroria kërkohen kushte më specifike se sa te gjykata. Për më tepër, në mënyrë të pashpjegueshme te masat që urdhërohen nga ana e gjykatave nuk potencohet fakti i rrezikut potencial për të tjerët në rast se aplikoheshin hetimet e zakonshme. Konsiderojmë se edhe në rastet kur urdhrat lëshohen nga prokuroria, por edhe nga gjykata do të duhej të përdorej i njëjti standard të plotësohej, meqë në parim masat e veçanta hetimore do të duhej të përcillnin standardin e njëjtë me rastin e lëshimit të këtyre urdhrave të veçantë hetimor.

Për autorizimin e masave të veçanta hetimore nuk është e domosdoshme të ketë dyshim të arsyeshëm për identitetin e të dyshuarit apo të dyshuarve të cilët kanë kryer, janë duke kryer ose së shpejti do të kryejnë vepër penale. Që nënkupton se këto masa mund të urdhërohen edhe në rast se nuk kemi identitet të personave që janë të involvuar në rast. Kjo paraqet një situatë kur ende nuk

ka zbulim të identitetit të personave të involvuar dhe të cilët mund të operojnë edhe përmes nofkave të ndryshme apo identiteteve të rrejshme me qëllim të arritjes së qëllimeve të tyre. Andaj, me këtë rast nuk paraqet asnjë pengesë ligjore fakti se nuk është i njohur identiteti i këtyre personave për autorizimin e urdhrit përkatës. Për më tepër, ekziston mundësia që prokurori i shtetit kur të ketë dyshim të arsyeshëm për identitetin e të dyshuarit apo dyshuarve që kanë kryer vepër penale. Kjo paraqet një situatë kur përmes provave që deri në këtë fazë të procedurës penale ende nuk është mësuar identiteti i personave, mirëpo përmes zbatimit të këtyre masave do të mund të zbulohet identiteti i personave por edhe informacione të tjera të rëndësishme përkitazi me veprën penale. Pra me këtë rast janë dy aspekte të rëndësishme të theksohen e para se ekziston dyshimi i bazuar se vepra penale është duke u kryer, po kryhet apo kur vepra penale së shpejti do të kryhet dhe e dyta se në këto raste identiteti i kryerësit nuk është i njohur, mirëpo në këto raste hetohen veprimet që kryhen në çështjen penale pa marrë parasysh se kryerësit janë persona për të cilët nuk ekzistojnë të dhëna lidhur me identitetin e tyre.

2.4 Fshehtësia e mbledhjes së informatave

Me dispozitë të posaçme ligjore[20] është përkufizuar parimi i konfedencialitetit, përkatësisht fshehtësia e mbledhjes së informatave e që është mishëruar përmes faktit se pas mbledhjes së informatave përmes aplikimit të masave të veçanta hetimore dosja mbyllet dhe mbahet e fshehur derisa zbulimi i saj të kërkohet në pajtim me këtë Kod e që kjo nënkupton se në disa raste nëse bëhet mbyllja e hetimit apo provat e mbledhura nuk janë relevante për zhvillimin më tutje të rastit, atëherë dosja do të mbetet e mbyllur.

2.5 Kushtet ligjore për masat e veçanta hetimore

Masat e veçanta hetimore mund të urdhërohen kundër personit kur ekziston dyshimi i bazuar se: është kryer, po kryhet apo së shpejti do të kryhet vepër penale e parashikuar sipas nenit 89 të këtij Kodi; dhe informacioni i cili mund të merret nga masat e urdhëruara ka gjasë të ndihmojë në hetimin e veprës penale dhe nuk do të kishte mundësi të merrej me masa të tjera hetimore pa shkaktuar vështirësi të paarsyeshme ose rrezik potencial për të tjerët.

[20] Neni 87 i KPP-së.

Përkundër faktit se në dispozitën e nenit 86 të KPP-së, përkatësisht në pjesën e mësipërme të punimit janë potencuar qëllimet dhe llojet e masave të veçanta hetimore, gjithashtu edhe në nenin 88 të KPP-së janë specifikuar kushtet ligjore të përcaktuara për urdhërimin e këtyre masave dhe të cilat vlejnë edhe në rastet kur masat autorizohen nga ana e prokurorit të shtetit e po ashtu edhe nga ana e gjyqtarit të procedurës paraprake e që si dispozitë e përgjithshme përcaktohet se lëshohen kundër personit në rastet kur ekziston dyshimi i bazuar se ka kryer, po kryen apo së shpejti do të kryejë vepër penale. Gjithsesi kjo paraqet një situatë e cila është e përcaktuar në tri faza të kryerjes së veprës penale. Gjithashtu duhet të plotësohen edhe kushtet e posaçme dhe atë informacioni i cili mund të merret nga masat e urdhëruara ka gjasa të ndihmojë në hetimin e veprës penale dhe nuk do të kishte mundësi të merrej me masa të tjera hetimore pa shkaktuar vështirësi të paarsyeshme ose rrezik potencial për të tjerët.

Përmes kësaj dispozite ligjvënësi ka balancuar aplikimin e këtyre masave vetëm në raste të caktuara dhe që mundësitë e një hetimi të zakonshëm nuk do të mund të shpijnë deri te rezultati i kërkuar e gjithsesi masat e tjera hetimore do të shkaktonin vështirësi të paarsyeshme ose rrezik potencial për të tjerët. Përmes kësaj dispozite është arritur të bëhet balancimi mes një hetimi të zakonshëm dhe aplikimit të masave të veçanta hetimore, si zgjidhje alternative vetëm në rastet kur deri te rezultati nuk mund të arrihet përmes hetimeve të zakonshme. E që nga kjo duhet nënkuptuar faktin se këto masa duhet të aplikohen vetëm në raste kur hetimet e zakonshme nuk mund të aplikohen. Në praktikën tonë gjyqësore shpesh herë ka pasur mospajtime rreth faktit se kur mund të fillohet me zbatimin e masave të veçanta hetimore dhe kush është kompetent për lëshimin e tyre e me këtë rast janë përcaktuar disa mundësi e para fillimit të procedurës formale, në të njëjtën kohë kur të merret aktvendimi për fillimin e hetimeve apo pas fillimit të hetimeve. Andaj, me qëllim të shmangies së këtyre situatave dhe me qëllim të unifikimit të praktikës gjyqësore Gjykata Supreme e Kosovës ka nxjerrë një Qarkore lidhur me masat e vëzhgimit dhe hetimit[21] përmes të cilës ka konfirmuar faktin se para nxjerrjes së aktvendimit për fillimin e hetimeve kompetent për lëshimin e urdhrave është prokurori i shtetit, kurse pas fillimit të hetimeve urdhrat e tillë lëshohen vetëm nga ana e gjyqtarit të procedurës paraprake.

[21] Shih Qarkoren e Gjykatës Supreme të Kosovës nr.12/2015, datë 12.01.2015.

Përveç personit të dyshuar masat e veçanta hetimore mund të urdhërohen kundër personit, përpos të dyshuarit, kur kushtet nga paragrafi 1 i këtij neni vlejnë për të dyshuarin dhe ekziston dyshim i bazuar se: 2.1. personi i tillë pranon ose transmeton komunikime që burojnë prej të dyshuarit ose që i dedikohen të dyshuarit apo që merr pjesë në transaksionet financiare të të dyshuarit; 2.2. i dyshuari përdor telefonin e personit të tillë ose ka qasje në sistem kompjuterik të personit të tillë; 2.3. ka dyshim se numri i telefonit, adresa elektronike apo llogaria financiare e personit të tillë është përdorur për kryerjen e veprës penale; 2.4. pronari apo shfrytëzuesi i numrit telefonik, adresës elektronike, adresës IP, numrit IMEI apo llogarisë financiare nuk është i njohur, është person juridik ose ka dyshim të arsyeshëm se numri telefonik, adresa elektronike apo llogaria financiare po përdoret nga dikush tjetër e jo nga pronari; ose vëzhgimi i të cilit mund të çojë në zbulimin e vendndodhjes ose të identitetit të të dyshuarit.

Përmes kësaj dispozite janë përcaktuar kushte të veçanta që edhe kundër personave të tjerë dhe të cilët nuk e kanë statusin e të dyshuarit, por për shkak të dyshimit të bazuar se në ndonjë formë apo mënyrë janë në shërbim të të dyshuarit, atëherë edhe ndaj tyre mund të urdhërohen masat e veçanta hetimore. Kjo zgjidhje është e arsyeshme për faktin se gjithnjë e më tepër kryerësit e veprave penale përdorin mjetet e komunikimit të personave të tjerë me qëllim që të komunikojnë dhe të realizojnë qëllimet e tyre. Andaj, me qëllim të kësaj masat e veçanta hetimore mund të urdhërohen edhe ndaj personave të tjerë që në fakt si zgjidhje ligjore e kanë edhe shumë shtete të tjera me legjislacionin e tyre përkatës dhe atë: Kodi i Procedurës Penale të Kroacisë (dispozita e e nenit 332 par.7) dhe Kodi i Procedurës Penale të Malit të Zi (dispozita e e nenit 157 par.3). Mirëpo deri sa me nenin 88 paragrafi 2 të KPP-së të gjitha masat e veçanta mund të aplikohen edhe për personat tjerë, kurse legjislacionet e lartpërmendura këto masa i aplikojnë në mënyrë restriktive vetëm përkitazi me përgjimin dhe incizimin e bisedave telefonike dhe komunikimeve të tjera, kurse nuk aplikohen edhe për masat e tjera të përcaktuara.

Rezultati i masave të veçanta hetimore është i vlefshëm për të gjithë komunikuesit që nënkupton se masat e urdhëruara janë të vlefshme për të gjithë personat, pra edhe të personave që nuk i janë nënshtruar urdhrave, por

kanë komunikuar me personin, përkatësisht të pandehurit kundër të cilit është lëshuar urdhri për masa të veçanta hetimore.

2.6 Veprat penale për të cilat mund të lëshohen urdhrat

Kodi i Procedurës Penale ka përcaktuar në mënyrë taksative veprat penale për të cilat mund të urdhërohen masat e veçanta hetimore[22] dhe kjo është e ndarë në tri kategori dhe atë: për hetimin e së paku njërës nga këto vepra të dyshuara penale:
1.1. veprat penale për të cilat mund të shqiptohet dënim prej pesë (5) ose më shumë vjet burgim; ose

1.2. një apo më shumë nga veprat penale në vijim:

1.2.1. dhuna ndaj përfaqësuesve të lartë të Republikës së Kosovës; 1.2.2. rrezikimi i rendit kushtetues me shkatërrimin apo dëmtimin e instalimeve dhe pajisjeve publike; 1.2.3. sabotimi; 1.2.4. spiunazhi; 1.2.5. fshehja ose moslajmërimi i terroristëve dhe grupeve terroriste; 1.2.6. përgatitja e veprave terroriste ose veprave penale kundër rendit kushtetues dhe sigurisë së Republikës së Kosovës; 1.2.7. rrezikimi i negociatorëve; 1.2.8. organizimi i grupeve për kryerjen e gjenocidit, krimeve kundër njerëzimit dhe krimeve të luftës; 1.2.9. rrëmbimi i fluturakes; 1.2.10. rrezikimi i sigurisë së aviacionit civil; 1.2.11. skllavëria, kushtet e ngjashme me skllavërinë dhe puna e detyruar; 1.2.12. kontrabandimi me migrantë; 1.2.13. trafikimi me njerëz; 1.2.14. fshehja e dokumenteve të identifikimit të viktimave të skllavërisë ose trafikimit me njerëz; 1.2.15. rrezikimi i personave nën mbrojtje ndërkombëtare; 1.2.16. rrezikimi i personelit të Organizatës së Kombeve të Bashkuara dhe i personelit në marrëdhënie me to; 1.2.17. marrja e pengjeve; 1.2.18. kanosja për përdorimin ose kryerjen e vjedhjes apo të grabitjes së materialit nuklear ose radioaktiv; 1.2.19. sterilizimi i detyruar; 1.2.20. gjymtimi i organeve gjenitale femërore; 1.2.21. ngacmimi seksual; 1.2.22. rrëmbimi; 1.2.23. tortura; 1.2.24. cenimi i së drejtës për të kandiduar; 1.2.25. kanosja e kandidatit; 1.2.26. keqpërdorimi i detyrës zyrtare gjatë zgjedhjeve; 1.2.27. dhënia ose marrja e ryshfetit në lidhje me votimin; 1.2.28. falsifikimi i

[22] Neni 89 i KPP-së.

rezultateve të votimit; 1.2.29. asgjësimi i dokumenteve të votimit; 1.2.30. shërbimet seksuale të viktimës së trafikimit; 1.2.31. mundësimi ose detyrimi në prostitucion; 1.2.32. transplantimi i kundërligjshëm dhe trafikimi i organeve dhe qelizave njerëzore; 1.2.33. ndotja e ujit të pijshëm; 1.2.34. ndotja e artikujve ushqimorë që përdoren nga njerëzit apo kafshët; 1.2.35. blerja, posedimi, shpërndarja dhe shitja e paautorizuar e narkotikëve, substancave psikotrope dhe analoge; 1.2.36. prodhimi dhe përpunimi i paautorizuar i narkotikëve, substancave psikotrope, analoge apo veglave, pajisjeve apo materialeve narkotike; 1.2.37. organizimi, drejtimi apo financimi i trafikimit të narkotikëve apo substancave psikotrope; 1.2.38. cenimi i barazisë në ushtrimin e veprimtarisë ekonomike; 1.2.39. keqpërdorimi i autorizimeve ekonomike; 1.2.40. falsifikimi i letrave me vlerë dhe instrumenteve të pagesës; 1.2.41. organizimi i skemave piramidale dhe bixhozit të paligjshëm; 1.2.42. falsifikimi i parasë; 1.2.43. Prodhimi, furnizimi, shitja, posedimi ose dhënia në shfrytëzim e mjeteve për falsifikim; 1.2.44. shpërlarja e parave; 1.2.45. marrëveshjet për kufizimin e konkurrencës përmes ftesave për tender; 1.2.46. mashtrimi në shkëmbimin e letrave me vlerë; 1.2.47. marrëveshja dhe mashtrimi me letrat me vlerë të qeverisë; 1.2.48. shmangia nga tatimi; 1.2.49.pranimi i ryshfetit në sektorin privat; 1.2.50. dhënia e ryshfetit në sektorin privat; 1.2.51. kontrabandimi i mallrave; 1.2.52. shmangia nga pagesa e tarifave të detyrueshme doganore ose tarifave akcizore; 1.2.53. zjarrvënia; 1.2.54. mashtrimi; 1.2.55. mashtrimi me subvencione; 1.2.56. mashtrimi lidhur me pranimin e fondeve nga Komuniteti Ndërkombëtar; 1.2.57. kurdisja e ndeshjes ose e sportit; 1.2.58. keqpërdorimi i sigurimit; 1.2.59. hyrja në sistemet kompjuterike; 1.2.60. mbajtja e paligjshme e substancave dhe e mbeturinave të rrezikshme; 1.2.61. importi, eksporti, furnizimi, transportimi, prodhimi, këmbimi, ndërmjetësimi ose shitja e paautorizuar e armëve apo materieve plasëse; 1.2.62. shkretërimi i pyjeve; 1.2.63. vjedhja e pyllit; 1.2.64. tregtia e ndaluar.

1.3. një apo më shumë nga veprat e mëposhtme penale, nëse kryhen në lidhje me terrorizëm, korrupsion apo krim të organizuar:
1.3.1. kanosja; 1.3.2. ngacmimi; 1.3.3. sulmi; 1.3.4. lëndimi i rëndë trupor; 1.3.5. shtrëngimi; 1.3.6. detyrimi; 1.3.7. shantazhi; 1.3.8.shkaktimi i rrezikut të përgjithshëm; 1.3.9. asgjësimi, dëmtimi ose heqja e instalimeve publike; 1.3.10. asgjësimi, dëmtimi ose heqja e pajisjeve mbrojtëse dhe rrezikimi i sigurisë në vendin e punës; 1.3.11. dërgimi apo transportimi i kundërligjshëm

i lëndëve eksplozive ose lëndëve ndezëse; 1.3.12. përdorimi i armës apo mjetit të rrezikshëm; 1.3.13. pengimi i të provuarit apo procedurës zyrtare; 1.3.14. frikësimi gjatë procedurës penale; 1.3.15. keqpërdorimi i pozitës apo autoritetit zyrtar; 1.3.16.keqpërdorimi dhe mashtrimi në prokurim publik; 1.3.17. keqpërdorimi i informatës zyrtare; 1.3.18. konflikti i interesit; 1.3.19. përvetësimi në detyrë; 1.3.20. mashtrimi në detyrë; 1.3.21. marrja e ryshfetit; 1.3.22. dhënia e ryshfetit; 1.3.23. dhënia e ryshfetit zyrtarit publik të huaj; 1.3.24. ushtrimi i ndikimit; 1.3.25. zbulimi i fshehtësisë zyrtare.

Konsiderojmë se ndarja në këto tri kategori të veprave penale për të cilat lejohet lëshimi i urdhrave për masat e veçanta hetimore është mjaft gjithëpërfshirës dhe se ka përfshirë po thuajse të gjitha veprat penale që janë të rëndësishme. Gjithsesi për aspekt të komperacionit duhet theksuar faktin se Kodi i Procedurës Penale të Kroacisë (dispozita e nenit 334) ka përcaktuar po ashtu në mënyrë taksative se për cilat vepra penale mund të lëshohet urdhri për masa hetimore, pra për veprat penale për të cilat parashihet dënimi me burgim prej 5 (pesë) vite e më tepër dhe të gjitha veprat penale ku përcktohet dënimi me burgim afatgjatë e po ashtu edhe për shumë vepra të posaçme penale ka përcaktuar mundësinë e lëshimit të masave, kurse edhe Kodi i Procedurës Penale të Malit të Zi (dispozita e nenit 158), ka përcaktuar si minimum të dënimit veprat penale me dënime të përcaktuara në kohëzgjatje prej 10 (dhjetë) vite apo më tepër, si dhe veprat penale specifike të cilat në mënyrë taksative janë përcaktuar në këtë dispozitë ligjore.

Provat e siguruara ligjërisht në pajtim me masën e urdhëruar sipas nenit 88 të këtij Kodi janë të pranueshme në shqyrtim kryesor, pa marrë parasysh nëse janë apo jo të përfshira në aktakuzë për veprat penale të cekura në këtë nen. Përmes kësaj dispozite është përcaktuar se provat e siguruara përmes këtyre masave janë të pranueshme edhe për veprat penale të cilat nuk janë të përcaktuara me dispozitën ligjore.

2.7 Urdhrat për masat e veçanta hetimore

Duke marrë parasysh rëndësinë e masave të veçanta hetimore dhe karakterin e tyre se drejtpërdrejtë ndërhynë në të drejtat e karakterit kushtetues të personave që u nënshtrohen këtyre masave, atëherë është përcaktuar se

kompetent për lëshimin e masave të veçanta hetimore është gjyqtari i procedurës paraprake[23] dhe është e natyrshme që paraprakisht kërkohet që të ketë një kërkesë me shkrim të prokurorit të shtetit. Siç dihet dispozitat e KPP-së e po ashtu edhe Ligji për Prokurorinë e Shtetit i japin kompetenca dhe autorizime të plota prokurorit të shtetit në zhvillimin e hetimeve dhe ndjekjen penale, dhe duke u bazuar në këtë gjithashtu mund të paraqes kërkesë për lëshimin e urdhrave e nënkuptohet se kërkesa për lëshimin e urdhrit të tillë duhet të bëhet në formë të shkruar dhe të përfshijë të dhënat e nevojshme që të mund të veprohet në kuadër të kërkesës. Tutje është dhënë një kompetencë shtesë prokurorit të shtetit që përjashtimisht, pra që paraqet një shmangie nga rregullat e përgjithshme që në raste të caktuara edhe vet të urdhëroj të gjitha masat e përcaktuara me nenin 86 paragrafin 2 të KPP-së, pra masat që janë kompetencë e gjykatës, kjo nën kushte dhe rrethana të caktuara.

Mirëpo për të vepruar në këtë mënyrë duhet të plotësohen disa kushte të posaçme e posaçërisht për shkak të vonesave që mund të vinë në shprehje në këto situata. Duhet pasur parasysh se procedura hetimore shpesh herë mund të zhvillohet me dinamikë të shpejtë dhe që nuk varet drejtpërdrejt nga ana e prokurorit të shtetit, por edhe personave të tjerë e me qëllim të shmangies së vonesave dhe pamundësisë së marrjes me kohë të urdhrit nga ana e gjyqtarit për lëshimin e këtyre masave, atëherë këto mund të urdhërohen nga ana e prokurorit të shtetit. Mirëpo, lëshimi i këtyre masave ka karakter të përkohshëm dhe që prokurori i shteti duhet që jo më vonë se njëzet e katër orë (24) të e njoftoj gjykatën deri sa urdhri pushon të ketë efektin e tij nëse konfirmohet në formë të shkruar nga duhet të të konfirmohet nga ana e gjyqtarit të procedurës paraprake brenda shtatëdhjetë e dy (72) orëve nga lëshimi i tij. Pra me këtë rast urdhri i lëshuar nga ana e prokurorit të shtetit ka karakter të përkohshëm dhe në rast të mos konfirmimit të tij pushon të ketë efekt juridik. Dispozita ligjore është e heshtur përkitazi me faktin se si të veprohet me provat e mbledhura sipas urdhrit i cili nuk ka marrë konfirmim nga ana e gjyqtarit të procedurës paraprake, mirëpo bazuar në faktin se kemi të bëjmë me një urdhër i cili nuk është konfirmuar, atëherë pa dyshim se me këtë rast këto prova duhet të shpallen prova të papranueshme pasi që janë marrë në mënyrë të kundërligjshme. E rëndësishme është të theksohet fakti se në praktikën gjyqësore kemi pasur shpesh herë raste kur nuk është konfirmuar

[23] Neni 90 paragrafi 1 i KPP-së.

urdhri i prokurorit të shtetit dhe në këto raste përmes aktvendimit me të cilin nuk konfirmohet urdhri i prokurorit gjithashtu edhe vendoset se provat e siguruara përmes aplikimit të këtyre masave janë prova të papranueshme dhe si të tilla duhet të largohen nga shkresat e lëndës.

Po ashtu është përcaktuar përmbajtja e urdhrit i cili përveç që është e domosdoshme të përpilohet në formë të shkruar gjithashtu ka përcaktuar edhe përmbajtjen e saj[24], kjo me qëllim që të mos lihet ndonjë zbrazëti me rastin e zbatimit të tij. Fillimisht duhet theksuar faktin se në parim urdhrat nuk përmbajnë arsyetim, mirëpo për shkak se masat e veçanta hetimore cenojnë të drejtat kushtetuese dhe të drejtat e njeriut, atëherë urdhri i lëshuar duhet të përmbaj arsyetim të hollësishëm se cilat janë arsyet e ndërhyrjes në këto të drejta kushtetuese e që për këtë arsye në rend të parë në urdhër duhet të detajohet dyshimi i bazuar se është kryer apo mund të kryhet vepra penale. Fakti se arsyetimi i urdhrit për masat e veçanta hetimore duhet të jetë i standardit të lartë është potencuar edhe përmes vendimeve të gjykatave vendore por edhe në shumë vendime të GJELDNj, me ç'rast në çështjen Dragojeviç kundër Kroacisë kanë konstatuar se arsyetimi i këtyre masave nga ana e gjykatave të Kroacisë nuk ka qenë i mjaftueshëm dhe për këtë arsye ka gjetur shkelje të nenit 8 të KELDNj dhe me këtë rast është cenuar e drejta e jetës private, jetës familjare dhe korrespodencës. Për më tepër, GJELDNj ka konstatuar faktin se gjykatat kroate ka interpetuar dhe zbatuar aplikimin e këtyre masave përkundër faktit se ligji nuk është mjaftueshëm i qartë dhe preciz kur është fjala për diskrecionin e gjykatave me rastin e dhënies së urdhrit për aplikimin e këtyre masave dhe në praktikë nuk është siguruar garancion i mjaftueshëm që nuk do të bëhet keqpërdorimi i aplikimit të këtyre masave.[25]

Duke analizuar dispozitën e nenit 90 paragrafi 3 nën paragrafi 3.1 të KPP-së, pa dyshim se bie në sy një mos koherencë e dispozitave që rregullojnë këtë pjesë, kjo për faktin se deri sa me dispozitën e nenit 86 paragrafi 1 të KPP-së janë përcaktuar tri faza kur mund të lëshohen urdhrat dhe atë: se është kryer vepra penale, po kryhet apo së shpejti do të kryhet, kurse me këtë dispozitë janë përcaktuar vetëm dy faza, pra se është kryer apo mund të kryhet dhe në fakt nuk potencohet edhe kur vepra penale është duke u kryer. Kjo gjithsesi

[24] Neni 90 paragrafi 3 i KPP-së.

[25] Shih rastin e GJEDLNJ Dragojeviç kundër Kroacisë nr.68955/11

mund të shkakton konfuzion dhe për hir të qartësisë së normës juridike konsiderojmë se duhet në mënyrë konsistence të rregullohet kjo çështje dhe kjo paqartësi mes dispozitave në fjalë.

Megjithatë përcaktimi i dyshimit të bazuar është një çështje mjaft delikate pasi që kjo është një fazë mjaft e hershme e zhvillimit të hetimeve, për më tepër, në shumicën e rasteve në praktikën gjyqësore vërehet se paralelisht me kërkesën për lëshimin e masës së kërkuar nxjerrët aktvendimi për fillimin e hetimit apo edhe ende nuk është nxjerrur një aktvendim i tillë e që paraqet një vështirësi shtesë në përcaktimin e dyshimit të bazuar. Nga kjo rrjedh se gjykata në këtë fazë ka mjaft vështirësi në definimin e dyshimit të bazuar, përkatësisht përcaktimin e kualitetit dhe kuantitetit të provave me qëllim të përcaktimit të ekzistimit apo jo të dyshimit të bazuar që është bazë për lëshimin e urdhërave për masa të veçanta hetimore. Konsiderojmë se ligjvënësi e ka lehtësuar punën e gjyqtarëve me rastin e vërtetimit të dyshimit të bazuar duke dhënë një përkufizim i cili është cituar dhe kjo pa dyshim se paraqet një premisë në të cilën duhet të mbështeten gjyqtarët me rastin e vendosjes përkitazi me dyshimin e bazuar. Pra është përcaktuar dyshimi i bazuar si: " N*johuri për informacionin që do të bindte një vëzhgues objektiv që një vepër penale ka ndodhur, po ndodh ose ka mundësi të konsiderueshme që do të ndodhë dhe se personi në fjalë ka më shumë gjasa që të ketë kryer veprën penale se sa që të mos e ketë kryer atë dhe i cili dyshim i bazuar duhet të mbështetet në prova të artikulueshme."*[26]

Është e rëndësishme të theksohet fakti se ekzistimi apo mos ekzistimi i dyshimit të bazuar si kusht themelor për urdhrin për masat e veçanta hetimore çmohet nga ana e gjyqtarit të procedurës paraprake dhe i cili vlerësim duhet të bazohet në fakte dhe të dhëna që gjenden në shkresat e lëndës dhe në asnjë mënyrë nuk duhet të jetë i bazuar në supozime. Gjithashtu në këtë aspekt është e rëndësishme të theksohet fakti se në këtë rast dyshimi i bazuar nuk duhet vlerësuar në mënyrë abstrakte apo duke bërë citim të dispozitave ligjore, por duhet që për secilin rast të vlerësohen në mënyrë konkrete dhe përmes çmuarjes së lirë të provave që janë në dispozicion deri në momentin kur vendoset lidhur me kërkesën e prokurorisë. Pra përcaktimi i dyshimit të bazuar paraqet pragun fillestar, përkatësisht hapin e parë drejt lëshimit

[26] Neni 19 paragrafi 1.9 i KPP-së.

të urdhrit dhe fakti i mos përmbushjes të këtij kriteri në mënyrë automatike përjashton mundësinë e lëshimit të urdhrit.

Deri sa përcaktimi i dyshimit të bazuar është kusht i domosdoshëm (conditio sine qua non), kushtet tjera janë më fleksibile dhe atë së pari nuk është e nevojshme të dihet emri dhe as adresa e personit apo personave që i nënshtrohen urdhrit dhe të dhënat e personave që i nënshtrohen urdhri të tillë. E rëndësishme është përcaktimi i i saktë i masës dhe bazës ligjore dhe posaçërisht gjetjet aktuale dhe gjasat reale të përcaktuara me nenin 19 nën paragrafi 1.11 i KPP-së. Gjithashtu të rëndësishme dhe të domosdoshme janë edhe të dhënat e kohës përkitazi me fillimin dhe përfundimin e masës dhe personin e autorizuar për zbatimin e saj, posaçërisht e rëndësishme është koha e vlefshmërisë së urdhrit të lëshuar dhe se disa urdhra përveç datës së caktuar duhet të lëshohen edhe me orë të caktuar, kjo veçmas vlen te masat e përgjimit, me ç'rast duhet të shënohet me saktësi edhe ora e fillimit të zbatimit të masës dhe gjithashtu edhe përfundimi i saj. Nga praktika gjyqësore në mënyrë të gabuar shpesh herë janë lëshuar urdhra vetëm me datë të caktuar duke mos paraqitur kohën e saktë të fillimit të zbatimit të masës dhe kjo pastaj mund të shkakton probleme lidhur me kohën e saktë të zbatimit të masës.

Dispozitat në vijim të këtij neni kanë përcaktuar detyrimet e zbatuesve të urdhrit i cili duhet të përpiloj raport në formë të shkruar për zbatimin e saj brenda afatit prej pesëmbëdhjetë (15) ditëve nga dita e lëshimit të urdhrit. Për më tepër, është përshkruar në detaje se çka përmban raporti i shkruar dhe i cili raport i dorëzohet prokurorit të shtetit dhe pastaj gjyqtarit të procedurës paraprake. Megjithëse kjo dispozitë ka përcaktuar si detyrim dorëzimin e raportit e që bazuar në këtë raport edhe mund të ndërmerren masa adekuate për ndalimin e masës në rastet kur nuk ka ndonjë të dhënë relevante për rastin e kjo me qëllim që këto masa të zgjasin në kohë sa të shkurtër. Për më tepër, nëse urdhri përfshinë hyrjen në lokale private, veprimet e zyrtarëve të autorizuar policor në zbatim të parimit të proporcionalitetit duhet të kufizohet vetëm në aktivizimin apo çaktivizimin e pajisjes teknike e që kjo nënkupton se nuk lejohet hyrjet dhe daljet të cilat janë të panevojshme dhe të pajustifikueshme.

Në rastet kur urdhërohet regjistrimi i bisedave telefonike ose përgjimin e komunikimeve nëpërmjet rrjetit kompjuterik duhet të përfshijë të gjitha elementet për identifikimin e secilit telefon ose secilës pikë të qasjes në rrjetin kompjuterik që duhet të përgjohet, kurse urdhri për përgjimin e

telekomunikimeve dhe përdorimi i lexuesit – IMSI – identifikimi ndërkombëtar i shfrytëzuesit mobil mund të përfshijë vetëm një përshkrim të përgjithshëm të telefonave që mund të përgjohen, kur gjyqtari i procedurës paraprake të gjykatës themelore kompetente çmon se ekziston dyshim i bazuar që i dyshuari shfrytëzon telefona të ndryshëm me qëllim të shmangies nga vëzhgimi i zyrtarit të autorizuar të policisë dhe një telefon apo telefonat e paraqitur në urdhër shfrytëzohen ose do të shfrytëzohen nga i dyshuari. Pra në këtë rast duhet të plotësohen këto kushte në mënyrë kumulative.

Me rastin e zbatimit të urdhrit për përgjimin e telekomunikimeve dhe përdorimi i lexuesit – IMSI – identifikimi ndërkombëtar i shfrytëzuesit mobil është lëshuar nga gjyqtari i procedurës paraprake, zyrtarët e autorizuar të policisë, pas zbatimit të urdhrit për një telefon të caktuar, menjëherë informojnë me shkrim gjyqtarin e procedurës paraprake mbi faktet e rëndësishme, duke përfshirë edhe numrin e telefonit dhe urdhri nuk mund të shfrytëzohet për të përgjuar telekomunikimet e personit i cili nuk është i dyshuar. Kjo në fakt paraqet një kufizim që urdhri të mos zbatohet ndaj personave të cilët nuk janë të dyshuar.

Tutje përmes dispozitave ligjore[27] janë përshkruar kushtet e posaçme të zbatimit të masave të veçanta dhe atë urdhri për kontroll të dërgesave postare ose dërgim të kontrolluar të dërgesave postare i cili urdhër duhet të përfshijë adresën në dërgesat postare që duhet të kontrollohen ose dërgohen dhe të cilat adresa duhet të përputhet me atë të personit ose të personave të përfshirë në urdhër. Duke pasur parasysh se disa urdhra të veçantë nuk kanë mundësi të zbatohen nga ana e personave të autorizuar policor, siç janë (masat për përgjimin e telekomunikimeve dhe përdorimi i lexuesit – IMSI – identifikimi ndërkombëtar i shfrytëzuesit mobil, përgjimin e komunikimeve nëpërmjet rrjetit kompjuterik, regjistrimin e thirrjeve telefonike, kontrollin e dërgesave postare, dërgimin e kontrolluar të dërgesave postare ose zbulimin e të dhënave financiare), atëherë është e nevojshme që krahas urdhrit të përpilohet edhe një udhëzim i veçantë me shkrim për personat të cilët janë të nevojshëm për zbatimin e urdhrit. Udhëzimi lëshohet nga ana prokurorit të shtetit apo gjyqtarit të procedurës penale dhe i dërgohet drejtorit ose zyrtarit përgjegjës

[27] Neni 90 paragrafi 9,10 dhe 11 i KPP-së.

të sistemit të telekomunikimeve, rrjetit kompjuterik, shërbimit postar, bankës ose institucioneve të tjera financiare dhe duhet të përfshijë vetëm informacionin që kërkohet për ndihmë në zbatimin e urdhrit. Lëshimi i këtij udhëzimi ka për qëllim marrjen e ndihmës profesionale për zbatimin e urdhrit dhe normalisht se përmban të dhëna më të kufizuara se sa urdhri, kjo duke marrë parasysh se urdhri në mënyrë të detajuar përmban të dhëna të cilat janë të natyrës konfidenciale dhe se këta persona nuk kanë qasje në urdhër, por vetëm në udhëzim përmes të cilit realizohen dy qëllimet e cekura më lartë. Kjo gjithsesi është e nevojshme edhe tek urdhri për regjistrimin e simuluar të personave juridik ose përdorimi i personave ekzistues juridik për mbledhjen e të dhënave përfshinë krijimin e subjekteve afariste të cilat mund të krijohen me qëllim të zbatimit të shërbimeve të simuluara të biznesit dhe mund të kryhet duke aplikuar veprimin e fshehjes së identitetit të një personi, pasurie dhe personave juridik, meqë edhe kjo masë nuk do të mund të zbatohej pa ndihmën dhe bashkëpunimin e policisë me organe të tjera të administratës shtetërore, me personat juridik, autoritete publike, persona të tjerë juridikë dhe shoqata të personave.

Një ndër masat e veçanta hetimore që mjaft shpesh gjen zbatim është edhe hetimi i fshehtë e cila masë zakonshëm realizohet përmes hetuesit të fshehtë apo bashkëpunëtorit të policisë. Kjo mënyrë e veprimit realizohet vetëm përjashtimisht dhe atë në rastet kur provat e tilla nuk mund të mblidhen me mjete tjera, apo kur mbledhja e provave të tilla do të ishte e vështirë. Pra bëhet fjalë për rastet kur përmes hetimit të zakonshëm nuk mund të mblidhen provat apo mbledhja e tyre do të ishte e vështirë. Përndryshe angazhimi i bashkëpunëtorit të policisë bëhet sipas urdhrit të përcaktuar dhe para fillimit të veprimeve të veçanta bashkëpunëtori i policisë do të nënshkruajnë një deklaratë ku theksohet se bie dakord për të kryer veprime të veçanta hetimore si bashkëpunëtor, dhe në të cilën do të qartësohen të gjitha të drejtat dhe detyrimet. Pastaj në urdhër specifikohen të gjitha të dhënat lidhur me veprimin e tij dhe të dhënat për persona dhe grupin ndaj të cilëve po zbatohet, përshkrimi i veprave penale të mundshme, mënyra, vëllimi, vendi dhe kohëzgjatja e urdhrit dhe i cili mund të përdorë mjetet teknike për fotografim, videoregjistrim ose për incizim optik, elektronik apo të zërit. Angazhimi i hetuesit të fshehtë varësisht prej rastit mund të zgjat sa është nevoja që të mblidhen provat, por jo më shumë se një (1) vit e i cili afat mund të zgjatet

edhe gjashtë (6) muaj, por gjithsesi edhe mund të ndërpritet kur pushojnë arsyet për zbatimin e urdhrit.

Gjatë ekzekutimit të urdhrit, hetuesi i fshehtë mund të përdorë masat mbrojtëse apo anonimitetin për të mbuluar karakteristikat e një zyrtari të policisë e nëse kërkohet nga rrethanat e posaçme të rastit edhe personi tjetër, që mund të jetë edhe shtetasi i huaj. Kurse për mbrojtjen e identitetit të hetuesit të fshehtë, organet kompetente mund të ndryshojnë të dhënat në bazat e të dhënave të regjistrave dhe të lëshojnë dokumente personale me të dhënat e ndryshuara, mirëpo është e ndaluar dhe e sanksionuar që hetuesi i fshehtë të nxisë kryerjen e veprës penale, pra nevojitet gjithmonë një kujdes i jashtëzakonshëm i zyrtarit të involvuar që të mos nxisë kryerjen e veprës penale, meqë kjo do të mund të shpallte këto prova si të papranueshme.

Përndryshe të gjitha të dhënat e siguruara nga ana e hetuesit të fshehtë pas përfundimit të angazhimit i dërgohen gjyqtarit të procedurës paraprake. Hetuesi i fshehtë vepron brenda strukturës që e heton dhe varësisht prej kushteve ka të drejtë të merr pjesë në biseda me persona të cilët mund të jenë dëshmitarë apo të dyshuar të mundshëm të veprave penale. Gjatë këtyre bisedave, ai mund të parashtrojë pyetje lidhur me veprën penale. Kur është e mundur, këto biseda incizohen. Nëse këto biseda nuk mund të incizohen, hetuesi i fshehtë përmbledh saktë bisedat dhe shpjegon se përse bisedat nuk janë shënuar sa më parë që ka qenë e mundur në raport policor. E rëndësishme është të theksohet fakti se hetuesi i fshehtë mund të dëgjohet si dëshmitar në procedurën penale edhe lidhur me përmbajtjen e bisedave me të dyshuarit ndaj të cilëve janë urdhëruar masat, vetëm nën shifër ose pseudonim përmes video-konferencës, duke zbatuar dispozitat ligjore për masat mbrojtëse apo anonimitet. Marrja në pyetje do të kryhet në atë mënyrë që mbrojtësit dhe palëve të mos u zbulohet identiteti i hetuesit të fshehtë. Hetuesi i fshehtë ftohet përmes eprorit i cili drejtpërdrejtë para marrjes në pyetje, me deklaratën e tij para gjykatës pohon identitetin e hetuesit të fshehtë. Të dhënat e identitetit të hetuesit të fshehtë i cili merret në pyetje si dëshmitarë paraqesin të dhëna konfidenciale.

2.8 Zbatimi i urdhrit për masat e veçanta hetimore

Pas lëshimit të urdhrit për masat e veçanta hetimore fillohet me zbatimin e tij, me ç 'rast fillimisht është përcaktuar se zyrtari i autorizuar i policisë fillon zbatimin e urdhrit për zbatimin e ndonjë mase nga ky Kapitull jo më vonë se pesëmbëdhjetë (15) ditë nga dita e lëshimit.[28] Kjo në fakt paraqet një afat mjaft të gjatë, por në praktikë vërehet fakti se zbatimi i masave në shumicën e tyre bëhet menjëherë, mirëpo në rastet kur duhet të planifikohet zbatimi i urdhrit ekziston mundësia e fillimit të tij pas 15 ditëve e me këtë rast duhet pasur kujdes që të aplikohet parimi që të minimizohen përgjimet që janë të panevojshme. Gjithsesi duhet pasur parasysh faktin se ndodhë që në ndërkohë ndonjë prej kushteve për urdhërimin e masave pushon të vlejë, atëherë duhet të pezullojë zbatimin e urdhrit dhe të njoftojë me shkrim gjyqtarin, përkatësisht prokurorin e shtetit dhe të cilët menjëherë duhet të ndërprejnë urdhrin, kjo duke pasur parasysh një ndër parimet fundamentale të cenimit të të drejtave kushtetuese të personave që u nënshtrohen këtyre masave, përkatësisht parimit të kufizimit në kohë.

Autoriteti i cili zbaton urdhrin duhet të shënon kohën dhe datën e fillimit dhe të përfundimit të secilit veprim të ndërmarrë për zbatimin e urdhrit dhe emrat e zyrtarëve të autorizuar të policisë të cilët kanë ndërmarrë cilindo veprim dhe funksion. Kurse për ndërmarrjen e veprimeve specifike, përkatësisht zbatimin e urdhrit (për përgjimin e telekomunikimeve dhe përdorimin e lexuesit – IMSI – identifikimi ndërkombëtar i shfrytëzuesit mobil, përgjimin e komunikimeve nëpërmjet rrjetit kompjuterik, kontrollin e dërgesave postare, dërgimin e kontrolluar të dërgesave postare dhe regjistrimin e thirrjeve telefonike), personat përgjegjës për punën me telekomunikimet, rrjetat kompjuterike ose shërbimet postare duhet të lehtësojnë zbatimin e urdhrit nën mbikëqyrjen e drejtorit ose të zyrtarit përgjegjës për sistemin e telekomunikimeve, rrjetin kompjuterik ose shërbimin postar. Kjo vlen edhe për zbatimin e urdhrit për zbulimin e të dhënave financiare, punonjësit e institucionit financiar duhet të lehtësojnë zbatimin e urdhrit të tillë nën mbikëqyrjen e drejtorit ose të zyrtarit përgjegjës të institucionit financiar.

Për shkak të natyrave të ndryshme të masave të veçanta hetimore dhe kompleksitetit në zbatimin e tyre, specifikisht është rregulluar zbatimi i masës

[28] Neni 91 paragrafi 1 i KPP-së.

së veçantë hetimore, përkatësisht zbatimi i shitjes dhe blerjes së simuluar të artikujve, shërbimeve apo sendeve[29] e cila mund të realizohet duke bërë shitje dhe blerje të simuluar të artikujve, shërbimeve apo sendeve apo dhënien dhe marrjen e simuluar të ryshfetit. E që kjo masë përdoret mjaft shpesh edhe te veprat penale të blerjes së armëve, lëndëve narkotike, dhënien apo marrjen e simuluar të ryshfetit, mirëpo zbatimi i kësaj mase duhet të bëhet me kujdes të shtuar pasi që nuk mund të nxisë personin tjetër të kryejë vepër penale të cilën personi nuk do ta kryente sikur të mos ishte intervenimi i personit i cili zbaton urdhrin dhe gjithashtu personi që zbaton urdhrin nuk kryen vepër penale. Këto dy kushte janë mjaft të rëndësishme, meqë shpesh herë duhet pasur kujdes në kufirin deri ku mund të zbatohet kjo masë, por njëkohësisht të mos kemi një joshje apo nxitje të kryerësit të veprës penale, pasi që shkelja e këtyre detyrimeve shpie deri te dështimi i rastit përkatësisht pamundësia e fillimit të ndjekjes penale. Si përjashtim është përcaktuar fakti se masat nuk mund të zbatohen në rastet kur bëhen komunikimet mes të dyshuarit dhe mbrojtësit të tij pasi që këto konsiderohen si shkelje e komunikimit mes tyre, mirëpo ky restrikcion nuk zbatohet në rastet kur ekziston dyshim i bazuar se i dyshuari dhe mbrojtësi i tij janë angazhuar së bashku në veprimtari kriminale që përbën bazën e urdhrit.

2.9 Afatet, zgjatja dhe ripërtëritja e urdhrit për masat e veçanta hetimore

Masat e veçanta hetimore për kah karakteri i tyre kanë kufizime strikte kohore dhe mos marrja parasysh e këtij aspekti mund të sjell deri te fakti që provat e mbledhura të shpallen si të papranueshme, andaj duhet pasur kujdes të madh në afatet e përcaktuara për zbatimin e këtyre masave e të cilat afate janë përcaktuar në mënyrë taksative si afatet fillestare[30] e gjithashtu në mënyrë të qartë është përcaktuar edhe zgjatja e afateve,[31] e po ashtu edhe ripërtëritja e urdhrave të veçanta hetimore[32] dhe që është përkufizuar se afati fillestar për lëshimin e urdhrit si nga ana e prokurori i shtetit apo gjyqtari i procedurës paraprake është për një afat prej nëntëdhjetë (90) ditësh nga dita e lëshimit të urdhrit. Po ashtu është dhënë mundësia e zgjatjes së këtij afati edhe për një

[29] Neni 90 paragrafi 7, 8, 9 dhe 10 i KPP-së.
[30] Neni 92 paragrafi 1 i KPP-së.
[31] Neni 92 paragrafi 2 i KPP-së.
[32] Neni 92 paragrafi 7 i KPP-së.

periudhë prej nëntëdhjetë (90) ditësh brenda periudhës kohore prej treqindegjashtëdhjetepesë (365) ditësh, mirëpo për këtë zgjatje të afatit fillimisht duhet të vlejnë parakushtet sikurse te lëshimi i masës dhe gjithashtu paraqitet nevoja e grumbullimit të mëtejshëm të provave. Zgjatja e afatit sipas dispozitës në fjalë ka karakter subsidiar gjithsesi duhet bërë përpjekje që masat e veçanta hetimore të mund të realizohen brenda periudhës fillestare të afatit, mirëpo duke aplikuar parimin e kufizimit kohor dhe faktit se përmes këtyre masave kufizohen liritë themelore të njeriut të garantuara me kushtetutë, atëherë pa dyshim se zgjatja e afatit duhet të jetë një përjashtim dhe i cili kufizohet që kjo masë të zbatohet brenda afatit prej treqindegjashtëdhjetepesë (365) ditësh. Dispozita ligjore heshtë për faktin se a duhet të ketë kontinuitet që pas urdhrit të parë menjëherë të vazhdohet me vazhdimin e tij apo kjo mund të bëhet pas një periudhe të caktuar kohore, përkatësisht pas kalimit të afatit fillestar të masës së lëshuar. Po ashtu nuk është e qartë se a mund të lëshohet masa e tillë pas kalimit të afatit prej treqindegjashtëdhjetepesë (365) ditësh, pra a mund të fillohet me aplikimin e masave prej fillimit duke aplikuar afatet e përcaktuara ligjore. Mirëpo, duke pasur parasysh faktin se kemi të bëjmë me masa të cilat janë të karakterit kufizues kohore, atëherë nga interpretimi i këtyre dispozitave ligjore mund të konkludojmë se nuk mund të vazhdohet me masa të këtilla jashtë afateve të përcaktuara ligjore. Për më tepër, zgjatja e urdhrit për masat e veçanta hetimore nga gjyqtari i procedurës paraprake mund të bëhet vetëm me propozim të arsyetuar të prokurorit të shtetit ku ceken arsyet se përse është i nevojshëm grumbullimi i mëtejshëm i provave e që në fakt nga leximi i kësaj dispozite del se gjyqtari i procedurës paraprake ka mundësi të mos aprovimit të zgjatjes së afatit.

Duke analizuar edhe dispozitat përkatëse të Kodit të Procedurës Penale të Malit të Zi del se urdhri fillimisht lëshohet për periudhën kohore prej katër (4) muajve, kurse maksimumi i zgjatjes së masës është deri në tetëmbëdhjetë (18) muaj, mirëpo e cila masë mund në ndërkohë të pezullohet dhe prapë të vazhdohet me aplikimin e saj, mirëpo në periudhën e masës llogaritet edhe periudha e pezullimit. Kurse në mënyrë taksative është potencuar fakti se masa kundër personit të njëjtë dhe veprës së njëjtë penale pas kalimit të afatit prej tetëmbëdhjetë (18) muaj nuk mund të vazhdohet me këto masa. Gjithashtu edhe dispozita e Kodit të Procedurës Penale të Kroacisë fillimisht përcaktojnë afatin prej tre (3) muaj me mundësi vazhdimi edhe dy herë nga gjashtë (6) muaj, pra për një periudhë kohore prej pesëmbëdhjetë (15) muaj. Edhe këto

dispozita nuk përcaktojnë decidivisht mundësinë e aplikimit tutje të këtyre masave, mirëpo duke pasur parasysh karakterin e këtyre masave, atëherë del se këto masa mund të aplikohen vetëm një herë dhe brenda periudhës së caktuar kohore.

E rëndësishme është të potencohet fakti se vazhdimi i masës së veçantë hetimore duhet të bëhet me kujdes të shtuar për faktin se deri sa me rastin e lëshimit të urdhrit fillestar mund të jetë një kohë kur nuk mund të priten informacione të plota gjithsesi pas periudhës së parë dhe kalimit të afatit prej 90 (nëntëdhjetë) ditëve, pa dyshim se pritet që dyshimi i bazuar ose të rritet apo edhe të zbehet dhe për këto arsye arsyetimi i kërkesë nga ana e prokurorit të shtetit dhe arsyetimi i urdhrit për vazhdimin e masës nga ana e gjyqtarit të procedurës paraprake duhet të jetë më i arsyetuar dhe jo vetëm në mënyrë sipërfaqësore apo duke cituar dispozitat ligjore të i përshkruaj kushtet dhe rrethanat dhe të vazhdoj masën e veçantë hetimore.

Afati kohor i përcaktuar vlen vetëm për disa masa, kurse urdhri për shitje dhe blerje të simuluar të artikujve, shërbimeve apo sendeve ose urdhri për dhënie dhe marrje të simuluar të ryshfetit autorizohet vetëm për një blerje të sendit ose për një vepër të simuluar të korrupsionit. Gjyqtari i procedurës paraprake mund të lëshojë urdhër tjetër për personin e njëjtë kur parakushtet për urdhërimin e masës sipas këtij kapitulli, siç parashihet në nenin 88 të këtij Kodi, vazhdojnë të zbatohen dhe ka shpjegim të arsyeshëm për dështimin në sigurimin e ndonjë ose të gjitha të dhënave të kërkuara me urdhrin e mëparshëm.[33] Pra, vetëm përjashtimisht kjo masë mund të vazhdohet dhe atë vetëm edhe një herë.

Tutje me dispozitat ligjore është dhënë mundësia e ndryshimit të urdhrit kur çmohet se ndryshimi i tillë është i nevojshëm për të siguruar se parakushtet për urdhërimin e masës sipas këtij kapitulli. E gjithashtu është lënë mundësia e pushimit të urdhrit kur pushojnë të vlejnë kushtet e përcaktuara në nenin 88 të këtij Kodi. Pra nga kjo dispozitë ligjore del se mbikëqyrja e urdhrit duhet të bëhet në mënyrë permanente, meqë në ndërkohë mund të ndryshojnë dhe kjo për faktin se ofrohen mundësitë për aplikimin e hetimit të zakonshëm dhe për këtë fakt menjëherë mund të pushohen këto masa dhe të vazhdohet me hetim apo ekziston mundësia që të ndryshohet dyshimi i bazuar dhe i cili ndryshim

[33] Neni 92 paragrafi 3 i KPP-së.

del se nuk ka bazë të aplikohen masat e veçanta hetimore, pra vepra për të cilën tani hetohet nuk hynë në kuadër të nenit 89 të KPP-së, atëherë urdhri duhet të pushohet menjëherë. Prokurori i shtetit ose gjyqtari i procedurës paraprake në çdo kohë mund të pushojnë urdhrin kur çmojnë se parakushtet për urdhërimin e masës, siç është paraparë në nenin 88 të këtij Kodi, pushojnë të vlejnë.

Me dispozitën e nenit 92 paragrafi 7 të KPP-së është përcaktuar mundësia e ripërtrirjes së urdhrit nëse i njëjti nuk ka mund të zbatohet për shkaqe objektive. Mirëpo ripërtrirja e urdhrit nuk e zgjat afatin e zbatimit të urdhrit dhe është e domosdoshme argumentimi për shkaqet objektive që kanë pamundësuar zbatimin e urdhrit. Gjithsesi afatet e përcaktuara me dispozitat e këtij neni nuk zbatohen për masën e hetimit të fshehtë pasi që afatet për këtë masë janë të natyrës specifike dhe janë të poërcaktuara me dispozitën e nenit 90 paragrafi 14 të KPP-së.

2.10 Materialet e siguruara me masa të veçanta hetimore

Një rëndësi e posaçme te masat e veçanta hetimore i kushtohet edhe materialeve të siguruara përmes këtyre masave e cila është e rregulluar me dispozitën e nenit 93 i KPP-së, me ç'rast është përcaktuar si detyrim i zyrtarit të autorizuar policor që pas përfundimit të zbatimit të masës dërgimi i materialeve të mbledhura prokurorit të shtetit e që për shkaqe të sigurisë materiali duhet të përpilohet në dy kopje e që njëra kopje mbahet në Arkivin e Policisë, kurse kopja tjetër me raport të posaçëm i dorëzohet prokurorit të shtetit.

Gjithashtu materialet e mbledhura duhet ti deponohen gjykatës dhe atë gjitha materialet teknike audio dhe video së bashku me aktakuzën për ti mbështetur provat e mbledhura. Në të kundërtën, materialet e siguruara përmes këtij urdhri, të cilat nuk janë deponuar në gjykatë, konsiderohen prova të papranueshme. Ky material mbahet i mbyllur deri në urdhrin e mëtutjeshëm të gjykatës. Është e rëndësishme të theksohet fakti se materialet mund të mbyllen dhe të mbahen në fshehtësi nëse prokurori i shtetit konsideron që bërja publike e tyre do të pengonte hetimin e mëvonshëm ose do të paraqiste rrezik për të dëmtuarit, dëshmitarët, hetuesit ose personat tjerë.

2.11 Njoftimi për masat e veçanta hetimore

Duke marrë parasysh faktin se zbatimi i masave të veçanta hetimore zhvillohet me konfidencë të plotë, atëherë personi i cili i nënshtrohet masave të veçanta hetimore nuk njoftohet për rrjedhën apo rezultatin deri në përfundimin e masës. Pra kjo për shkak të faktit se njoftimi i tij do të mund të dëmtonte zbatimin e këtyre masave. Vlerësojmë se një dispozitë e tillë as që do të duhej të ishte fare e shkruar, meqë do të ishte në tërësi jashtë domenit të këtyre masave njoftimi i personit gjatë zbatimit të saj dhe këto masa nuk do të kishin asnjë kuptim. Për më tepër, asnjë nga kodet procedurale në rajon (Kodi i Procedurës së Malit të Zi, Kroacisë dhe as Bosnjes dhe Hercegovinës) nuk përmban dispozitë të tillë, mirëpo përmban dispozita ligjore që rregullojnë procesin e njoftimit dhe shkatërrimit të të dhënave pas përfundimit të masës së veçantë hetimore.

Mirëpo, kjo situatë ndryshon pas përfundimit të masës dhe pas kësaj faze prokurori i shtetit apo gjyqtari i procedurës paraprake varësisht se cili ka urdhëruar masën e tillë duhet të e njofton personin i cili i është nënshtruar masave të veçanta hetimore nëse dihet identiteti i tij.[34] Mirëpo me këtë rast personi edhe mund të mos njoftohet fare në rastet kur njoftimi paraqet rrezik serioz për jetën apo shëndetin e personave apo rrezikon ndonjë hetim në zhvillim e sipër. Me këtë rast është e nevojshëm balansimi mes të drejtës së njoftimit të personit dhe rrezikut që paraqet mos njoftimi i tij apo të rrezikoj hetimin e ndonjë rasti. Me rastin e njoftimit është përcaktuar se personi ka të drejtë që të kontrollojë materialin e mbledhur. Duke bërë interpretimin e kësaj dispozite ligjore del se njoftimi duhet bërë vetëm në dy situata dhe atë e para kur nuk vazhdohet ndjekja penale, pra janë zhvilluar hetimet, por nuk është ngritur aktakuza dhe në rastin kur materialet e mbledhura përmes masave të veçanta hetimore nuk janë të nevojshme për procedurë penale. Kurse duke analizuar kushtet tjera të përcaktuara del se edhe këto raste nuk është specifikuar se si veprohet në rastet kur konstatohet se përkitazi me zbatimin e masave të veçanta hetimore nuk duhet të njoftohet personi që i është nënshtruar kësaj mase. Për më tepër, nuk ka ndonjë praktikë që ndiqet në këto raste, mirëpo do të duhej që prokurori, përkatësisht gjyqtari i procedurës paraprake të përpilojnë shënim zyrtar ku do të konstatoheshin arsyet e mos

[34] Neni 94 paragrafi 2 i KPP-së.

njoftimit për shkak të kushteve të veçanta të përcaktuara me dispozitën e nenit 94 paragrafi 2 të KPP-së.

Gjithsesi materialet e grumbulluara duhet të asgjësohen duke përfshirë edhe kopjen e materialit të mbajtur në polici dhe përkitazi me këtë përpilohet procesverbal i veçantë.

Ligjvënësi në mënyrë specifike ka rregulluar rastet nëse materialet e siguruara përmes masave të veçanta hetimore nuk shërbejnë për procedurës penale duke specifikuar se materialet e siguruara përmes masave të veçanta hetimore të cilat nuk janë të nevojshme për qëllim të ndjekjes penale apo ndonjë shqyrtimi të mundshëm të masës nga gjykata, fshihen pa vonesë.[35] Fakti i fshirjes duhet të dokumentohet dhe në rastet kur fshirja e të dhënave është shtyrë për shkak të shqyrtimit të mundshëm të masës nga gjykata, të dhënat nuk përdoren për asnjë qëllim tjetër pa pëlqimin e personit në fjalë, dhe qasja në të dhëna kufizohet përshtatshmërisht.

Konsiderojmë se dispozitat e nenit 94 të KPP-së e titulluar *njoftimi për masat e veçanta hetimore* nuk përkon me brendësinë e dispozitës ligjore dhe çështjeve që rregullohen përmes kësaj dispozite dhe atë së pari titulli nuk është i qartë pasi që dispozita ka për synim njoftimin e personit vetëm në rastet kur me materialet e siguruara përmes masave të veçanta hetimore nuk janë të nevojshme me qëllim të ndjekjes penale apo shqyrtimi i masës nga gjykata. Pra duhet të jetë e qartë se materialet e grumbulluara gjatë zbatimit të kësaj mase ose janë të panevojshme për ndjekjen penale ose ka rezultuar me pushim të hetimeve dhe vetëm në këto raste aplikohen këto dispozita ligjore, përkatësisht duhet njoftohet personi, kurse përjashtimisht personi mund të mos njoftohet për shkaqet e përcaktuara, megjithatë nuk është qartësuar se si veprohet në këto rastet me materialet e mbledhura e që sipas interpretimit sistematik të tërësisë së dispozitës ligjore këto materiale duhet të asgjësohen, meqë nuk ka asnjë arsye të mbeten të pa asgjësuara. Gjithashtu edhe shprehja e përdorur "*kontrollimi i materialit"* nga ana e personit që i është nënshtruar masës së veçantë hetimore nuk është adekuate pasi që i njëjti sipas interpretimit ka të drejtë vetëm të shikojë materialin e mbledhur kjo dispozitë e që kontrolli nënkupton aspekt tjetër nga shikimi i materialit.

[35] Neni 94 paragrafi 4 i KPP-së.

2.12 Pranueshmëria e provave të siguruara me anë të urdhrit për masat e veçanta hetimore

Qëllimi i procedurës penale është që të bëhet sigurimi i provave të pranueshme dhe kjo si e tillë përfshinë një gamë mjaft të gjerë dhe që rregullon kornizën veprimin e organeve të procedurës penale. Posaçërisht është potencuar fakti se prova e marrë nëpërmjet masës nga ky kapitull është e papranueshme nëse urdhri për masën dhe zbatimin e saj është i kundërligjshëm dhe njëkohësisht është përcaktuar se provat e siguruara me anë të urdhrit për masat e veçanta hetimore për veprat e parapara në pajtim me dispozitat e këtij kapitulli, janë prova të pranueshme dhe mund të përdoren si prova në procedurë penale.

Shpesh herë në praktikë ndodhë me rastin e zbatimit të masave të veçanta hetimore të sigurohen prova që përfshijnë vepra penale tjera apo të dyshuar tjerë që nuk kanë qenë të përfshirë në urdhrin e lëshuar. Në rastet e tilla këto materiale transkriptohen dhe dorëzohet tek prokurorit i shtetit e të cilat materiale përjashtimisht mund të përdoret si provë në procedurë, vetëm nëse lidhet me një vepër penale për të cilën mund të lëshohet urdhri për masa të fshehta hetimore. Pra për të u përdorur në procedurës patjetër duhet të plotësohet kushti që ky urdhër të mund të lëshohet për veprat penale të përcaktuara.

Një fazë e rëndësishme e procedurës penale është faza e ngritjes së aktakuzës dhe në këtë fazë, gjyqtari i vetëm gjykues apo kryetari i trupit gjykues vlerëson kundërshtimet e të pandehurit lidhur me pranueshmërinë e provave të mbledhura. Kundër vendimit mbi kundërshtimin nga ky paragraf mund të paraqitet ankesë. Mirëpo pranueshmëria e provave nuk përfundon këtu pasi që pranueshmëria e materialeve mund të shqyrtohet në çdo kohë para se aktgjykimi të merr formën e prerë dhe atë sipas detyrës zyrtare në rastet kur ka indikacione për shkelje të të drejtave kushtetuese, përkatësisht materialet janë mbledhur në mënyrë të kundërligjshme.[36] Në rastet kur aktvendimi për paligjshmërinë e urdhrit ose të zbatimit të tij merr formën e prerë, gjyqtari i vetëm gjykues apo kryetari i trupit gjykues i cili drejton procedurën heq materialin e mbledhur nga procesverbali dhe materialet e tilla ia dërgon Panelit për Shqyrtimin e Vëzhgimit dhe Hetimit nëpërmjet kryetarit të gjykatës themelore për vendim mbi kompensim.

[36] Neni 95 paragrafi 5 i KPP-së-Kodi nr.08/L-032

2.13 Paneli për Shqyrtimin e Vëzhgimit dhe Hetimit

Në rast se personi konsideron se në mënyrë të kundërligjshme i është nënshtruar masës së veçantë hetimore, atëherë mund të paraqes ankesë kryetarit të gjykatës themelore dhe i cili duhet të themeloj një Panel për Shqyrtimin e Vëzhgimit dhe Hetimit dhe duhet të marrë vendim mbi ankesën e ushtruar, i cili vendim ka dy dimensione së pari përkitazi me masën ose urdhrin dhe të vendosë mbi kompensimin përkatës në rastet kur gjyqtari ka marrë aktvendim të formës së prerë se urdhri ose zbatimi i tij është i kundërligjshëm.[37] Më tutje dispozitat ligjore kanë përcaktuar përbërjen e panelit nga tre gjyqtarë të cilët emërohen nga kryetari i gjykatës themelore dhe që anëtarët nuk duhet të jenë profesionalisht të lidhur me personin që i nënshtrohet ankesës ose me materialet e mbledhura. Është përcaktuar që zyrtarët e autorizuar të policisë dhe prokurorët e shtetit të i sigurojnë dokumentet e nevojshme lidhur me punën e tyre. Përndryshe aktvendimi i gjyqtarit përkitazi me masën apo zbatimin e saj rezulton se është i kundërligjshëm është detyrues për panelin e që del se paneli nuk ka kompetencë të shqyrtimit të vendimit të gjyqtarit, por vetëm vendosë përkitazi me pushimin e urdhrit nëse ende është në fuqi, të urdhërojë asgjësimin e materialeve të mbledhura dhe kompensimin e personit ose personave që i janë nënshtruar urdhrit.

2.14 Ndihma nga Organet Tjera për Zbatimin e Masave

Me dispozitën e nenit 97 të KPP-së është përcaktuar se me rastin e zbatimit të masave, atëherë policia, sipas nevojës, mund të kërkojë ndihmën e organeve të tjera përgjegjëse për zbatimin e ligjit, sigurimin e rendit dhe të një ambienti të sigurt në Kosovë. Kurse me dispozitën e nenit 98 të KPP-së është theksuar fakti se dispozitat që rregullojnë dispozitat e këtij kapitulli vlejnë për zbatim të vëzhgimit dhe hetimit me rastin e ofrimit të shërbimeve doganore dhe shërbimeve të tjera të ngjashme.

[37] Neni 96 paragrafi 1 i KPP-së-Kodi nr.08/L-032

PËRFUNDIMET DHE REKOMANDIMET

Duke pasur parasysh faktin se jetojmë në një botë ku krimi i organizuar, korrupsioni, terrorizmi, pastrimi i parave paraqesin vepra penale të cilat janë mjaft të sofistikuara, atëherë pa asnjë dyshim mund të konkludojmë se luftimi i këtyre veprave penale por edhe i të tjerave është mjaft i vështirë i arritshëm pa aplikimin e masave të posaçme hetimore, kjo për shkak të hetimit dhe ndjekjes së suksesshme të këtyre veprave penale gjithsesi këto masa janë mjaft efikase dhe që ndihmojnë organet për zhvillimin e procedurave penale.

Aplikimi i masave të veçanta mundëson ndriçimin e veprave penale më të rënda por në të njëjtën kohë cenon të drejtat themelore dhe kushtetuese të njeriut dhe në dritën e kësaj gjendemi në kufirin mes të dy interesave shoqërore, luftimin e kriminalitetit dhe mbrojtjen e të drejtave të njeriut, andaj qëllimi i ligjvënësit dhe aplikimi i këtyre masave është të vë balansin mes këtyre dy interesave dhe në asnjë mënyrë në dëm të njërës prej këtyre interesave.

Bazuar në dispozitat e KPP-së është dhënë autoritet prokurorit të shtetit dhe gjyqtarit të procedurës paraprake se mund të autorizojnë masat e veçanta hetimore vetëm në rastet kur informacioni i kërkuar në lidhje me veprën penale nuk mund të sigurohet me veprimet tjera hetimore. Në këtë mënyrë, prokurori i shtetit dhe gjyqtari i procedurës paraprake, duhet që masat e veçanta hetimore t'i konsiderojnë vetëm si mjet të fundit ***("Ultima ratio")*** në drejtim të hetimit të veprave penale dhe sigurimit të informacionit të rëndësishëm.

Prokurori i shtetit dhe gjyqtari i procedurës paraprake duhet që të përmbushin detyrimet që drivojnë nga sipas nenit 94 të KPP-së. Në këtë mënyrë, të njëjtit pas përfundimit të masës, duhet që ta njoftojnë personin i cili i nënshtrohet masave të veçanta hetimore, nëse gjatë zbatimit të masës është mësuar identiteti i tij dhe nëse njoftimi i tillë nuk paraqet rrezik serioz për jetën apo shëndetin e personave apo nuk rrezikon ndonjë hetim në zhvillim e sipër. Kurse, me rastin e njoftimit, personi në fjalë ka të drejtë që të kontrollojë materialin e mbledhur, ndërsa prokurori i shtetit ose gjyqtari i procedurës paraprake duhet që të marrin vendim për asgjësimin e materialeve të mbledhura, përfshirë kopjen e materialit të mbajtur në polici dhe mban procesverbal të procesit të asgjësimit. Po ashtu, materialet e siguruara përmes

masave të veçanta hetimore të cilat nuk janë të nevojshme për qëllim të ndjekjes penale apo ndonjë shqyrtimi të mundshëm të masës nga gjykata, fshihen pa vonesë, kurse fakti i fshirjes duhet të dokumentohet. Në rastet kur fshirja e të dhënave është shtyrë për shkak të shqyrtimit të mundshëm të masës nga gjykata, të dhënat nuk përdoren për asnjë qëllim tjetër pa pëlqimin e personit në fjalë, dhe qasja në të dhëna kufizohet përshtatshmërisht.

Siç me të drejt ka konstatuar edhe Gjykata Kushtetuese, në rastin nr.KI113/21, "përgjimi retroaktiv, duke përfshirë nxjerrjen dhe leximin i mesazheve (SMS-ve) në mënyrë retroaktive, është i ndaluar" dhe nuk janë "masa të parapara me ligj", ashtu si kërkohet me parimet e të drejtës për privatësi të garantuar me nenin 36 të Kushtetutës dhe nenin 8 të KEDNj-së. Në këtë kontekst, prokurori i shtetit dhe gjyqtari i procedurës paraprake duhet që të kenë në konsideratë një standard të tillë, në kuptim zbatimit të masave të veçanta hetimore për periudhën nga data e lëshimit e tutje ***("Ex nunc")***, e në asnjë mënyrë, në zbatimin e ndonjërës prej këtyre masave në mënyrë retroaktive ***("Ex tunc")***. Natyrisht, se përjashtim nga një standard i tillë, për shkak të rrezikut të vonesës, bën situata e parashikuar në nenin 90, paragrafi 2 të KPP-së, kuptohet nën supozimin e përmbushjes së të gjitha kushteve përkatëse ligjore që parashihen po me këtë dispozitë ligjore.

Duhet theksuar faktin se gjatë hartimit të këtij punimi janë bërë krahasime mes kodeve procedurale të rajonit përkitazi me masat e veçanta hetimore dhe me këtë rast konsiderojmë se dispozitat e KPP-së janë mjaft mirë të kompletuara dhe të sistemuara përkitazi me masat e veçanta hetimore dhe të cilat kanë rregulluar të gjitha aspektet e rëndësishme të masave të veçanta hetimore. Duke përcaktuar qartë personat që mund të u nënshtrohen këtyre masave, veprat penale për të cilat aplikohen këto masa, afatet fillestare dhe vazhdimi i tyre.

Në mënyrë të hollësishme është rregulluar mënyra e zbatimit të masave të veçanta hetimore dhe rastet kur këto prova mund të shpallen si prova të papranueshme dhe po ashtu është trajtuar specifikisht aspekti i njoftimit të personit ndaj të cilit është zbatuar masa e veçantë hetimore dhe e drejta e tij për shkatërrimin dhe kompenzimin përkitazi me dëmin e pësuar si rezultat i aplikimit të masës së veçantë hetimore.

Në fund, përmes rasteve të paraqitura nga praktika gjyqësore është fokusuar rëndësia e aplikimit të masave të veçanta hetimore dhe po ashtu efikasiteti i këtyre masave përmes të cilave janë arritur të sigurohen prova të rëndësishme gjatë procedurës penale dhe të cilat prova nuk do të mund të siguroheshin përmes hetimeve të zakonshme.

KAPITULLI III

KRIMET KIBERNETIKE DHE SIGURIA KIBERNETIKE

Afrim Shala, Gjyqtar në Gjykatën Supreme të Kosovës

Afrim Shala, Gjyqtar në Gjykatën Supreme të Kosovës

1. KRIMET KIBERNETIKE DHE SIGURIA KIBERNETIKE

1.1 Vështrime të përgjithshme

Në vitet e fundit, shoqëritë në të gjithë botën kanë bërë përparime të mëdha drejt kalimit në një shoqëri të informacionit, ndërsa teknologjia e informacionit dhe komunikimit, tani përshkon pothuajse çdo aspekt të jetës së njerëzve. Fakti që shoqëria po mbështetet dhe varet gjithnjë e më shumë nga teknologjia e informacionit dhe komunikimit, normalisht e bën atë të ekspozuar ndaj kërcënimeve të tilla si krimet kibernetike,[38] përkatësisht krimet e kryera kundër të dhënave dhe sistemeve kompjuterike ose nëpërmjet tyre. Përveç një numri të madh veprave penale kundër teknologjisë së informacionit dhe komunikimit ose nëpërmjet saj, një numër gjithnjë e më i lartë i çështjeve penale që dërgohen në gjykata përfshijnë edhe provat elektronike që janë memorizuar në një sistem kompjuterik ose në pajisje të tjera teknologjike.[39] Në këtë drejtim, rezulton se krimet kibernetike janë të ndërlidhura në masë të madhe me provat elektronike, dhe sigurisht se është domosdoshmëri e kohës që gjyqtarët dhe prokurorët të jenë të përgatitur për të trajtuar rastet e tilla, përkatësisht çështjet penale që ndërlidhen me këto dy (2) aspekte, në njërën anë me krimet kibernetike, kurse në anën tjetër, me provat elektronike.[40]

---

[38] Fjala *"kibernetikë"* rrjedh nga gjuha e lashtë greke *"kibernete"* që do të thotë *"drejtuesi i anijës"*. Kjo për faktin se në drejtimin e një anijeje, pozicioni i timonit rregullohet në përgjigje të vazhdueshme të efektit që vërehet se ka, duke iu përgjigjur shqetësimeve nga erërat dhe baticat e ndryshme.

[39] *Trajnim për krimin kibernetik për gjyqtarë dhe prokurorë: një koncept*, Projekti për Krimin Kibernetik www.coe.int/cybercrime dhe Rrjeti i Lisbonës www.coe.int/lisbon-network, Këshilli i Evropës, Departamenti i Shoqërisë së Informacionit dhe Aksionit kundër Krimit Drejtoria e Përgjithshme e të Drejtave të Njeriut dhe Çështjeve Ligjore, Strasburg, 2009, fq. 7.

[40] Këshilli Konsultativ i Gjyqtarëve Evropianë, është shprehur se "është thelbësore që gjyqtarët, pasi të kenë mbaruar ciklin e plotë të studimeve, të marrin një trajnim të detajuar, të larmishëm që ata të jenë të aftë t'i kryejnë detyrat e tyre në mënyrë të kënaqshme", kurse, "Një trajnim i tillë është gjithashtu një garanci për pavarësinë dhe paanshmërinë e tyre" (para 4), dhe se trajnimi duhet "të ketë parasysh nevojën për t'u mirinformuar dhe për të njohur gjerësisht çështje të ndryshme që pasqyrojnë kompleksitetin e jetës në shoqëri" (para 27). Aq e madhe është rëndësia e teknologjisë së informacionit dhe komunikimit në shoqëritë e sotme saqë gjyqtarët dhe prokurorët duhet të kenë të paktën disa njohuri bazë të këtyre teknologjive

Në literaturën penale ka mendime të ndryshme lidhur me atë se kur saktësisht janë paraqitur krimet kibernetike, megjithëse është e qartë se këto krime janë të ndërlidhura me paraqitjen e kompjuterëve dhe rrjeteve kompjuterike, por që me kalimin e viteve këto krime janë zhvilluar dhe sofistikuar. Tani në botën bashkëkohore, krimet kibernetike konsiderohen kërcënimet më të mëdha për sigurinë kombëtare dhe ekonomike të shteteve, madje edhe të shteteve më të zhvilluara ekonomikisht në botë.

Krimet kibernetike konsiderohen krime me karakter ndërkombëtar, pasi ato i tejkalojnë kufijtë në mes shteteve, ngase kriminelët, viktimat dhe infrastruktura teknike shtrihen në juridiksione të shumta, duke sjellë shumë sfida në hetimet dhe ndjekjen penale të kryesve dhe grupeve të ndryshme të organizuara, të cilët realizojnë përfitime të mëdha. Për këto arsye, bashkëpunimi në mes të shteteve është thelbësor në luftimin dhe parandalimin e krimeve kibernetike. Tani përmes kompjuterëve dhe pajisjeve tjera teknologjike është bërë e mundur që të kryhen një sërë veprash penale, nga vende të ndryshme të botës, ku kryesit e tyre mund të gjenden në një shtet, viktimat në shtetet tjera. Në këtë mënyrë, në botën bashkëkohore janë të pranishme veprimtari të ndryshme kriminale me karakter kibernetik, duke përfshirë, përveç tjerash: mashtrimet e ndryshme financiare dhe bankare; vjedhja e të dhënave financiare ose të pagesës së kartave; vjedhja dhe shitja e të dhënave të korporatave; vjedhja e identitetit, përkatësisht përdorimi i të dhënave të personale të personit tjetër për përfitime financiare; sulmet e ndryshme ndaj sistemeve kompjuterike (hakimi, viruese të ndryshme, sulme në sisteme; bllokime të sistemeve dhe pamundësia e qasjes në të dhëna, etj.); piratimi dhe shkelja e të drejtave të autorit, përkatësisht shkarkimi dhe shpërndarja e paligjshme e materialeve të mbrojtura; përdorimi i rrjeteve për veprimtari kriminale; shantazhet dhe ngacmimet online, etj.

dhe të problemeve që lidhen me to. Ndërsa në shumë vende, organet e zbatimit të ligjit kanë arritur t'i fuqizojnë kapacitetet e tyre për të hetuar krimet kibernetike dhe për të siguruar provat elektronike, kjo duket se ka ndodhur në një shkallë më të ulët për gjyqtarët dhe prokurorët, të cilët megjithatë luajnë një rol kyç në proceset ligjore penale. Përvoja sugjeron që në pjesën më të madhe të çështjeve, gjyqtarët dhe prokurorët hasin vështirësi në përballje me realitetet e reja të botës kibernetike. Opinioni nr. 4 - për trajnimin e duhur fillestar dhe të vazhduar për gjyqtarët në nivel kombëtar dhe në nivel evropian, (CCJE (2003) Op. nr. 4).

Është e rëndësishme që të theksohet se krimet kibernetike kanë të bëjnë me veprimtarinë kriminale të zhvilluar në rrjet, gjithashtu duke përdorur kompjuterin si cak ose si vegël. Gjithashtu, krimi kibernetik përveç veprave penale të veçanta që hyjnë në fushën e krimit kibernetik mund të përfshijë dhe mashtrimin, falsifikimet e ndryshme, shantazhet e ndryshme, krimin financiar, terrorizmin, krimin e organizuar, spiunazhin kibernetik, terrorizmin kompjuterik, kërcënimet apo kanosjet e ndryshme, lajmërimet e rrejshme, etj.[41]

Krimet kibernetike në përgjithësi duhet kuptuar si akte kriminale, ku kompjuterët, pajisjet tjera teknologjike dhe rrjetet janë shënjestër kryesore, përdoren si mjete për të kryer vepër penale ose janë vendndodhja e krimit.

Përveç këtyre, krimi kibernetik konsiderohet veprimtari kriminale që ose synon ose përdor një kompjuter, një rrjet kompjuterik ose një pajisje në rrjet, ndërsa në shumicën e rasteve kryhen me qëllime të përfitimeve materiale. Megjithatë, herë pas here krimi kibernetik synon të dëmtojë kompjuterët apo rrjetet për arsye të tjera, siç mund të jenë politike, personale, konkurrencës, etj.

Edhe pse nuk ka përkufizim të pranuar në mënyrë universale, prapë se prapë mund të bëhet dallim midis dy llojeve kryesore të krimit kibernetik:

1) **Krimi i mundësuar nga kibernetika,** duke iu referuar formave "tradicionale" të krimit tani të transferuara në sferën kibernetike, siç janë: aktet kriminale të fokusuara në financa, aktet që pengojnë sigurinë e fëmijëve dhe të rinjve, dhe madje edhe terrorizmi;

2) **Krimi i avancuar kibernetik** (i njohur edhe si **"krimi i teknologjisë së lartë"**), duke iu referuar sulmeve të sofistikuara ndaj pajisjeve kompjuterike dhe softuerit.[42]

[41] *Udhëzuesi i Përgjithshëm për Matjen e Dënimit II*, Gjykata Supreme e Kosovës, Kapitulli XXIV/A Krimet kibernetike, fq.221. Udhëzuesi mund të gjendet në këtë link: 337_Udhezuesi per matjen e denimit_Nentor 2024.pdf

[42] *Introduction to Cybersecurity Governance* - A Tool for Members of Parliament, Geneva Centre for Security Sector Governance, fq.7.

Ndërkohë që numri i krimeve kibernetike po rritet, shumë shtete po shqyrtojnë mundësinë e krijimit të gjykatave të specializuara për t'i trajtuar rastet e natyrës së tillë në mënyrë sa më efikase. Kështu, në Indi janë krijuar gjykata të veçanta për krime kibernetike (si p.sh."Cyber Appellate Tribunal"), kurse në shtete tjera, janë krijuar departamente apo divizione të veçanta në kuadër të gjykatave të rregullta për të trajtuar këto raste, si: Shtetet e Bashkuara të Amerikës, Britania e Madhe, etj.

Në legjislacionin tonë penal, duke përshirë këtu Kodin Penal të Republikës së Kosovës[43] dhe Ligjin për Plotësimin dhe Ndryshimin e Kodit Penal të Republikës së Kosovës[44] janë përcaktuar disa vepra penale të natyrës së tillë, mirëpo nuk është përcaktuar definicioni krimeve kibernetike.

Për dallim nga këto akte juridike, me Ligjin për Parandalimin dhe Luftimin e Krimit Kibernetik,[45] i cili tani më nuk është në fuqi, **"Krimi kibernetik"** ishte përkufizuar si "një aktivitet kriminal i zhvilluar në rrjet që ka si objekt apo si mënyrë të kryerjes së krimit, keqpërdorimin e sistemeve kompjuterike dhe të të dhënave kompjuterike".

Përndryshe, me dispozitat ligjore të Ligjit për Plotësimin dhe Ndryshimin e Kodit Penal të Republikës së Kosovës, në një Kapitull të veçantë (KAPITULLI XXIV/A), i cili emërtohet "KRIMET KIBERNETIKE", janë parashikuar disa vepra penale të natyrës së tillë, të cilat do të paraqiten dhe trajtohen në vijim të këtij punimi.

Duhet theksuar se veprat penale nga kapitulli i "Krimeve kibernetike" kryhen përmes sistemeve kompjuterike. Sipas dispozitës ligjore të nenit 3, paragrafi

[43] Kodi Nr.06/L-074 Penal i Republikës së Kosovës, datë 23.11.2018 (në tekstin e mëtejmë: KPRK). KPRK mund të gjendet në këtë link: **https://gzk.rks-gov.net/ActDetail.aspx?ActID=18413**

[44] Ligji Nr.08/L-188 për Plotësimin dhe Ndryshimin e Kodit Penal të Republikës së Kosovës, datë 26.10.2023. Ky Ligj mund të gjendet në këtë link: ActDetail.aspx

[45] Ligji Nr.03L-166 për Parandalimin dhe Luftimin e Krimit Kibernetik, datë 10.06.2020, është shfuqizuar me Ligjin Nr.08/L-188 për Plotësimin dhe Ndryshimin e Kodit Penal të Republikës së Kosovës, datë 26.10.2023 dhe Ligjin Nr.08/L-173 për Sigurinë Kibernetike, datë 02.02.2023.

1.4. të Ligjit për Siguri Kibernetike,[46] **"sistem kompjuterik"** nënkupton një pajisje apo grup pajisjesh të ndërlidhura, një ose më shumë prej të cilave, në bazë të një programi, kryejnë përpunim automatik të të dhënave. Përkufizim të njëjtë të sistemit kompjuterik përmban edhe Konventa e Këshillit të Evropës mbi Krimin Kibernetik, e njohur gjithashtu edhe si "Konventa e Budapestit" ("Convention on Cybercrime") që u hap për nënshkrim më 23.11.2001 në Budapest të Hungarisë (ETS.nr.185), ndërsa ka hyrë në fuqi më 01.07.2004.[47] Në nenin 1 të Konventës është përcaktuar se "Sistem kompjuterik" do të thotë çdolloj pajisje apo grup i ndërlidhur ose pajisje të lidhura, një ose më shumë prej të cilave, vazhduese të një programi kryejnë procesime automatike të të dhënave.

Është e rëndësishme të mos ngatërrohet krimin kibernetik me sigurinë kibernetike. Të dy këto kërcënime të lidhura me kibernetikën dallojnë për nga motivi, dashja, mjetet e përdorura, shënjestra, shtrirja, pasojat, si dhe aktorët e përfshirë në parandalim dhe zbutje. Në praktikë, krimi kibernetik është i shumëllojshëm nga spam-i dhe email-et phishing, mashtrimet në internet, si dhe përfaqësimi i rremë, deri te përmbajtja e ndaluar fyese dhe e kundërligjshme, vjedhja e identitetit, materiali online i abuzimit seksual të fëmijëve, etj. Motivi kryesor prapa akteve kriminale kibernetike, si në rastin e krimit 'tradicional', përgjithësisht konsiderohet se është fitimi financiar dhe kriminelët kibernetikë janë, në thelb, hakerë me dashje qëllimkeqe,[48] kështu që në vijim, do të paraqitet edhe infrastruktura ligjore e sigurisë kibernetike në Republikën e Kosovës dhe mekanizmat kombëtarë që kanë përgjegjësinë që të kujdesen në lidhje me sigurinë kibernetike.

Siç u theksua edhe më parë, krimi kibernetik në shumtën e rasteve ka karakter ndërkombëtar, andaj edhe si tillë, për shkak të rrezikshmërisë së lart dhe nevojës për bashkëpunim në mes të shteteve, siç do të shohim në vijim të këtij punimi, janë aprovuar dokumente dhe instrumente të shumta juridike ndërkombëtare, si dhe janë krijuar një sërë organizatash dhe mekanizma ndërkombëtarë me qëllim të parandalimit dhe luftimit të krimeve kibernetike.

[46] Ligji Nr.08/L-173 për Sigurinë Kibernetike, datë 02.02.2023.

[47] Linku i Konventës: https://rm.coe.int/16800cce5b

[48] *Introduction to Cybersecurity Governance* - A Tool for Members of Parliament, Geneva Centre for Security Sector Governance, fq.7-8.

Kryes të krimeve kibernetike mund të jenë çdo person, si personat fizik, ashtu edhe personat juridik, kështu që krimet kirbernetike janë të ashtuquajtura **"delicta communia"**[49] - vepra penale të cilat mund t'i kryejë çdo person.

Këto vepra penale mund të kryhen vetëm me dashje, pasi që me dispozitat ligjore të Ligjit për Plotësimin dhe Ndryshimin e Kodit Penal të Republikës së Kosovës, nuk është parashikuar përgjegjësi penale, nëse këto vepra penale janë kryer nga pakujdesia. Gjithashtu, për ekzistimin e disa veprave penale është e domosdoshme që të njëjtat të jenë kryer për motive apo me qëllime të caktuara.

Për disa vepra penale të këtij Kapitulli, është parashikuar në mënyrë shprehimore edhe ndëshkimi i tentativës për të kryer veprën penale.

Gjithashtu, në Kapitullin "Krimeve Kibernetike" gjenden edhe dispozita të ashtuquajtura "sqaruese" apo "shpjeguese", pasi që me to sqarohet apo shpjegohet domethënia e shprehjeve të caktuara që janë përdorur në kuadër të figurës konkrete të veprës penale.

Përveç dënimeve me burgim dhe me gjobë, të cilat janë parashikuar në disa raste edhe në mënyrë alternative, është parashikuar edhe konfiskimi i detyrueshëm i pajisjeve dhe programeve elektronike. Kështu, sipas dispozitës ligjore të nenit 277/L të KPRK-së, pajisjet dhe programet elektronike që përdoren për kryerjen e veprave penale të këtij Kapitulli, konfiskohen sipas Kodit të Procedurës Penale.

Po ashtu, duhet theksuar se në kuptimin e përgjithshëm, jo vetëm në Kapitullin e "Krimeve Kibernetike" gjendet vepra penale të cilat mund të kryhen përmes sistemeve kompjuterike, por kemi edhe disa vepra tjera penale të ashtuquajtura "kriminalitet klasik" që mund të kryhet përmes sistemeve të tilla. Kështu, vepra penale të natyrës së tillë që mund të kryhen përmes sistemeve kompjuterike, konsiderohen p.sh. "Kanosja", nga neni 181 i KPRK-së; "Ngacmimi", nga neni 182 i KPRK-së; "Cenimi i fshehtësisë së korrespondencës dhe i bazave të të dhënave kompjuterike", nga neni 199 i

[49] SHALA, AFRIM, *Hyrje në të drejtën penale,* f. 54 Prishtinë 2024.

KPRK-së; "Shkelja e urdhrave për masat e fshehura ose teknike të vëzhgimit ose hetimit", nga neni 203 i KPRK-së; "Prodhimi, furnizimi, shitja, posedimi ose dhënia në shfrytëzim e mjeteve për falsifikim", nga neni 298 i KPRK-së; "Vjedhja e shërbimeve", nga neni 314 i KPRK-së dhe shumë vepra penale tjera. Sidoqoftë, në vijim, do të trajtohen vetëm veprat penale që parashihen në Kapitullin e "Krimeve kibernetike", si një kapitull i ri që është parashikuar në pjesën e posaçme të KPRK-së.

2. KRIMET KIBERNETIKE

2.1 Shpërndarja kompjuterike e materialeve pro gjenocidit ose krimeve kundër njerëzimit (Neni 277/A)

Kjo vepër penale dhe dy (2) veprat penale në vijim janë parashikuar si vepra penale, duke u bazuar në "Protokollin shtesë të Konventës së Budapestit mbi inkriminimin e akteve me natyrë raciste dhe ksenofobike të kryera nëpërmjet sistemeve kompjuterike" (ETS.nr.189)[50] që është nënshkruar në Strasburg të Francës, më 28.01.2003, ndërsa ka hyrë në fuqi më 01.03.2006.

Sipas dispozitës ligjore të nenit 277/A të KPRK-së, këtë vepër penale e kryen çdokush që ofron në publik ose shpërndan qëllimshëm në publik, nëpërmjet sistemeve kompjuterike, materiale që mohojnë, minimizojnë në mënyrë të ndjeshme, arsyetojnë ose justifikojnë veprën penale të gjenocidit ose krimit kundër njerëzimit.

Veprimet kryerëse të kësaj vepre penale janë të përcaktuara në mënyrë alternative dhe konsistojnë:

- **ofrimin në publik të materialeve që mohojnë, minimizojnë në mënyrë të ndjeshme, arsyetojnë ose justifikojnë veprën penale të gjenocidit ose krimit kundër njerëzimit ose**
- **shpërndarja në publik e materialeve të lartcekura.**

Këto veprime kryerëse duhet që kryhen përmes sistemeve kompjuterike.

Për ekzistimin e kësaj vepre penale duhet që materialet të cilat ofrohen ose shpërndahen në publik të mohojnë, minimizojnë në mënyrë të ndjeshme,

[50] Linku i Protokollit: https://rm.coe.int/168008160f

arsyetojnë ose justifikojnë veprën penale të gjenocidit[51] ose krimit kundër njerëzimit.[52]

Këtë vepër penale mund ta kryejë çdo person i cili përmes sistemit kompjuterik i ofron ose shpërndan në publik materialet e lartcekura.

Kjo vepër penale mund të kryhet vetëm me dashje, e cila në vete përfshinë edhe qëllimin e ofrimit ose shpërndarjes së këtyre materialeve, me anë të të cilave mohohet, minimizohet në mënyrë të ndjeshme, arsyetohet ose justifikohet vepra penale e gjenocidit ose krimit kundër njerëzimit.

Për këtë vepër penale është parashikuar dënim me burgim nga tre (3) deri në gjashtë (6) vjet.

Gjithashtu, duke u bazuar në dispozitën ligjore të nenit 277/L të KPRK-së, duhet të konfiskohen pajisjet dhe programet elektronike që janë përdorur për kryerjen e kësaj vepre penale, ndërsa konfiskimi do të kryhet sipas dispozitave ligjore të KPP-së.

2.2 Kanosja me motive racizmi dhe ksenofobie nëpërmjet sistemit kompjuterik (Neni 277/B)

Në kuptimin e së drejtës penale, kanosjen duhet konsideruar si deklaratë apo ndonjë veprim tjetër me të cilën një person i drejtohet tjetrit, ia bënë me dije, se do t'ia shkaktojë një të keqe.
Nga ky përkufizim i përgjithshëm i kanosjes rezulton se me këtë vepër penale mbrohet ndjenja e sigurisë personale dhe e drejta e njeriut që të jetojë në paqe

[51] Gjenocidi është parashikuar si vepër penale në nenin 142 të KPRK-së. Në këtë dispozitë ligjore është parashikuar se "Kushdo që me qëllim të asgjësimit të tërësishëm apo të pjesërishëm të ndonjë grupi kombëtar, etnik, racor apo fetar kryen një ose më shumë nga veprimet e mëposhtme, do të dënohet me burgim së paku pesëmbëdhjetë (15) vjet ose me burgim të përjetshëm: 1.1. vrasjen e anëtarëve të grupit; 1.2. shkaktimin e lëndimeve të rënda trupore apo mendore të anëtarëve të grupit; 1.3. vënien e qëllimshme të grupit në kushte të tilla të jetës të cilat shpijnë në shfarosje të plotë apo të pjesërishme fizike; 1.4. vënien e masave të cilat kanë për qëllim që të pengojnë lindjet brenda grupit; 1.5. transferimin me dhunë të fëmijëve të grupit në një grup tjetër.

[52] Krimet kundër njerëzimit janë të parashikuara në nenin 143 të KPRK-së.

dhe të jetë i qetë, që të mos e shqetësojë tjetri, përkatësisht që të mos e rrezikojnë të tjerët.[53]

Vepra penale "Kanosja me motive racizmi dhe ksenofobie nëpërmjet sistemit kompjuterik" sipas nenit 277/B të KPRK-së, është vepër penale e veçantë, në raport me veprën penale "Kanosja", sipas nenit 181 të KPRK-së.

Është e vepër penale e veçantë, për së paku tre (3) arsye:

- **aspekti subjektiv i kryesit** - motivet e racizmit dhe ksenofobisë, për shkak të përkatësisë etnike, kombësisë, racës apo fesë;
- **mënyra e kryerjes** - përmes sistemeve kompjuterike dhe
- **veprave penale për të cilat është kanosur se do t'i kryejë kryesi** - vrasje ose "plagosje e rëndë".

Kështu, në dispozitën ligjore të nenit 277/B të KPRK-së është parashikuar se këtë vepër penale e kryen kushdo që kanos seriozisht për vrasje ose plagosje të rëndë, që i bëhet një apo më shumë personave, nëpërmjet sistemeve kompjuterike, për shkak të përkatësisë etnike, kombësisë, racës apo fesë.

Veprimi i kryerjes së kësaj vepre penale konsiston në kanosjen serioze për vrasje ose plagosje të rëndë që i bëhet një apo më shumë personave, përmes sistemeve kompjuterike.

Për ekzistimin e kësaj vepre penale, duhet që kanosja të jetë serioze. Kanosja është serioze në rastet kur sipas rrethanave të rastit, realisht është e mundur dhe e përshtatshme që të realizohet, si dhe nëse personi ndaj të cilit është e drejtuar kanosja, formon bindjen se vërtetë do të shkaktohet e keqja e kanosur. Nëse kanosja është apo jo serioze, kjo çështje zgjidhet në çdo rast konkret, duke marrë parasysh rrethanat e rastit, karakterin e kanosjes, mënyrën e kryerjes, etj.

Veprimi kryerës i kësaj vepre penale duhet që të ndërmerret përmes sistemeve kompjuterike.

[53] SHALA, AFRIM, Pjesa e posaçme e së drejtës penale me raste nga praktika gjyqësore, Gjilan, 2010, f. 118.

Element tjetër i domosdoshëm i kësaj vepre penale është fakti se i referohet vetëm disa veprave penale të caktuara, për dallim nga vepra penale "Kanosja", sipas nenit 181 të KPRK-së, e cila ka karakter të përgjithshëm.

Kështu, kjo vepër penale konsiderohet se kryhet vetëm në rastet kur kryesi kanos seriozisht se do të kryejë ndonjë "vrasje ose plagosje të rëndë", pra jo të çdo vepre penale apo të ndonjë të keqe tjetër. "Vrasje", në kuptim të këtij inkriminimi duhet kuptuar vrasjet nga nenet 172 dhe 173 të KPRK-së, kurse "plagosje e rëndë", duhet kuptuar veprën penale "Lëndimi i rëndë trupor", nga neni 186 të KPRK-së.

Këtë vepër penale mund ta kryejë çdo person i cili përmes sistemit kompjuterik kanos seriozisht për vrasje ose plagosje të rëndë, një apo më shumë personave, për shkak të përkatësisë etnike, kombësisë, racës apo fesë, kurse subjekt pasiv i kësaj vepre penale janë personat që i përkasin grupeve të caktuara etnike, kombëtare, racore apo fetare.

Kjo vepër penale mund të kryhet vetëm me dashje, e cila në vete përfshinë edhe qëllimin dhe motivin e kryesit që të kanos seriozisht për vrasje ose plagosje të rëndë personin apo personat, për shkak të përkatësisë së tyre etnike, kombësisë, racës apo fesë ("motive racizmi dhe ksenofobie").

Për këtë vepër penale është parashikuar dënim me burgim nga një (1) deri në tre (3) vjet.

Gjithashtu, duke u bazuar në dispozitën ligjore të nenit 277/L të KPRK-së, përveç dënimit të shqiptuar, duhet të konfiskohen edhe pajisjet dhe programet elektronike që janë përdorur për kryerjen e kësaj vepre penale, ndërsa konfiskimi do të kryhet sipas dispozitave ligjore të KPP-së.

2.3 Shpërndarja e materialeve raciste ose ksenofobie nëpërmjet sistemit kompjuterik (Neni 277/ C)

Sipas dispozitës ligjore të nenit 277/C të KPRK-së, këtë vepër penale e kryen kushdo që ofron në publik ose shpërndan qëllimshëm në publik, nëpërmjet sistemeve kompjuterike, materiale me përmbajtje raciste ose ksenofobie.

Veprimet kryerëse të kësaj vepre penale janë të përcaktuara në mënyrë alternative dhe konsistojnë:

- **ofrimin në publik të materialeve me përmbajtje raciste ose ksenofobie ose**
- **shpërndarja në publik e materialeve të lartcekura.**

Këto veprime kryerëse duhet që kryhen përmes sistemeve kompjuterike.

Për ekzistimin e kësaj vepre penale duhet që materialet të cilat ofrohen ose shpërndahen në publik të kenë përmbajtje raciste ose ksenofobie. Sipas dispozitave të Protokollit shtesë të Konventës së Budapestit mbi inkriminimin e akteve me natyrë raciste dhe ksenofobike të kryera nëpërmjet sistemeve kompjuterike, **"material racist dhe ksenofobik"** konsiderohet çdo material i shkruar, apo çdo imazh ose përfaqësim tjetër i mendimeve ose teorive, që favorizon, përhap ose nxit urrejtje, diskriminim ose dhunë kundër çdo individi ose grupi individësh, bazuar mbi racën, ngjyrën, prejardhjen, origjinën kombëtare ose etnike, si edhe fenë, nëse përdoret si pretekst për çdonjërin nga këta faktorë.[54]

Këtë vepër penale mund ta kryejë çdo person i cili përmes sistemit kompjuterik i ofron ose shpërndan në publik materialet e lartcekura.

Kjo vepër penale mund të kryhet vetëm me dashje, e cila në vete përfshinë edhe qëllimin e ofrimit ose shpërndarjes së këtyre materialeve, të cilat kanë përmbajtje raciste ose ksenofobike.

Për këtë vepër penale është parashikuar dënim me gjobë ose me burgim nga gjashtë (6) muaj deri në dy (2) vjet.

2.4 Hyrja e paautorizuar kompjuterike (Neni 277/D)

Fillimisht, duhet sqaruar se me dispozitën ligjore të nenit 8 të LPNKPRK-së është shfuqizuar dispozita ligjore e nenit 327 të KPRK-së në të cilën ishte parashikuar vepra penale "Hyrja në sistemet kompjuterike".

[54] Neni 2, paragrafi 1 i Protokollit.

Tani kjo vepër penale është parashikuar në nenin 277/D të KPRK-së, dhe ka pësuar ndryshime të theksuara në raport me veprën penale që ishte parashikuar në nenin 327 të KPRK-së.

Dispozita ligjore e nenit 277D të KPRK-së, në të cilën është parashikuar vepra penale "Hyrja e paautorizuar kompjuterike", përveç që ka përcaktuar tre (3) forma të kryerjes së veprës penale (forma themelore; forma e veçantë dhe forma e rëndë), përmban edhe një dispozitë sqaruese, në lidhje me domethënien e shprehjes "veprime të paautorizuar".

Formën themelore të veprës penale "Hyrja e paautorizuar kompjuterike", sipas paragrafit 1 të nenit 277/D të KPRK-së, e kryen kushdo që në mënyrë të paautorizuar hyn në një pjesë apo në tërësi të një sistemi kompjuterik dhe të informacionit, duke shkelur masat e sigurisë, me qëllim përfitimin e të dhënave kompjuterike ose qëllimet e tjera të paligjshme ose në ndërlidhje me një sistem kompjuterik që është i lidhur me një sistem tjetër kompjuterik.

Veprimet e kryerjes së kësaj forme të veprës penale konsistojnë në hyrjen në një pjesë apo në tërësi të një sistemi kompjuterik dhe të informacionit, duke shkelur masat e sigurisë, ose në ndërlidhje me një sistem kompjuterik që është i lidhur me një sistem tjetër kompjuterik.

E rëndësishme për ekzistimin e kësaj forme të veprës penale është që veprimet kryerëse të ndërmerren, duke shkelur masat e sigurisë dhe në mënyrë të paautorizuar.

Kryes i kësaj forme të veprës penale mund të jetë çdo person i cili i ndërmerr veprimet e lartcekura, duke shkelur masat e sigurisë dhe në mënyrë të paautorizuar.

Kjo formë e kësaj vepre penale mund të kryhet vetëm me dashje dhe me qëllim të përfitimit të të dhënave kompjuterike ose me qëllimet tjera të paligjshme.

Për këtë formë themelore të kësaj vepre penale është parashikuar dënim me gjobë ose me burgim nga një (1) deri në tre (3) vjet.

Forma e veçantë e kësaj vepre penale është parashikuar në paragrafin 2 të nenit të lartcekur. Sipas kësaj dispozite ligjore, kjo formë e kësaj vepre penale kryhet në rastet kur ndonjë person pa autorizim dhe me qëllim që të përfitojë në mënyrë të kundërligjshme dobi pasurore, për vete apo personin tjetër apo që t'i shkaktojë dëm personit tjetër, ndryshon, publikon, shlyen, asgjëson apo shkatërron të dhënat apo programet kompjuterike ose në ndonjë mënyrë tjetër hyn në sistemin kompjuterik të tjetrit.

Veprimet e kryerjes së kësaj forme të veprës penale janë të përcaktuara në mënyrë alternative dhe konsistojnë në:

- **ndryshimin,**
- **publikimin,**
- **shlyerjen,**
- **asgjësimin apo**
- **shkatërrimin e të dhënave apo programeve kompjuterike ose**
- **në ndonjë mënyrë tjetër hyrjen në sistemin kompjuterik të tjetrit.**

Për ekzistimin e kësaj forme të veprës penale është e domosdoshme që veprimet kryerëse të ndërmerren pa autorizim dhe me qëllim që të përfitojë në mënyrë të kundërligjshme dobi pasurore, për vete apo personin tjetër apo që t'i shkaktojë dëm personit tjetër.

Kryes i kësaj forme të veprës penale mund të jetë çdo person i cili e ndërmerr ndonjërin prej veprimeve kryerëse të lartcekura në mënyrë të paautorizuar.

Kjo formë e kësaj vepre penale mund të kryhet vetëm me dashje dhe me qëllim që kryesi të përfitojë në mënyrë të kundërligjshme dobi pasurore, për vete apo personin tjetër apo që t'i shkaktojë dëm personit tjetër.

Për këtë formë të kësaj vepre penale është parashikuar dënim me gjobë ose me burgim nga një (1) deri në tre (3) vjet.

Forma e rëndë e kësaj vepre penale është parashikuar në paragrafin 3 të nenit të lartcekur. Sipas kësaj dispozite ligjore, kjo formë të rëndë të kësaj vepre penale konsiderohet se është kryer në rastet kur kjo vepër kryhet në sistemet e kompjuterike dhe të informacionit ushtarak, të sigurisë kombëtare, të rendit

publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik me rëndësi publike.

Konsiderohet formë e rëndë e kësaj vepre penale, pasi që sistemet e kompjuterike dhe të informacionit ushtarak, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik me rëndësi publike janë me interes të veçantë për çdo shtet dhe shoqëri.

Përndryshe, kryerës i kësaj forme të veprës penale mund të jetë çdo person dhe e njëjta mund të kryhet vetëm me dashje.

Për këtë formë të kësaj vepre penale është parashikuar dënim me burgim jo më pak se tre (3) vjet.

Ndërsa, sipas paragrafit 4 të nenit të lartcekur, për qëllim të këtij neni **"veprime të paautorizuara"** konsiderohen:

- veprimet e personit që nuk është i autorizuar sipas ligjit ose kontratës;
- veprimet e pësonit që tejkalojnë kufijtë e autorizimit;
- veprime për të cilat nuk ka leje nga personi kompetent dhe i kualifikuar, sipas ligjit, për të shfrytëzuar, administruar ose kontrolluar sistemin kompjuterik apo të kryej hulumtime shkencore në një sistem kompjuterik.

2.5 Përgjimi i paligjshëm i të dhënave kompjuterike (Neni 277/E)

Përmes kësaj vepre penale mbrohen transmetimet jopublike të të dhënave kompjuterike.

Kjo vepër penale përmban dy (2) forma të saj dhe atë: formën themelore të parashikuar në paragrafin 1, si dhe formën e rëndë të parashikuar në paragrafin 2.

Formën themelore të kësaj vepre penale e kryen kushdo që pa autorizim, përdorë pajisje teknike ose program kompjuterik, për të përgjuar transmetimet jopublike të të dhënave kompjuterike, nga ose brenda një sistemi kompjuterik dhe të informacionit, përfshirë emetimet elektromagnetike nga një sistem kompjuterik që bartë të dhëna kompjuterike.

Veprimi i kryerjes së kësaj vepre penale konsiston në përgjimin e transmetimeve jopublike të të dhënave kompjuterike.

Kjo formë e kësaj vepre penale kryhet duke përdorur pajisje të caktuara teknike apo programeve kompjuterike, nga ose brenda një sistemi kompjuterik dhe të informacionit, përfshirë emetimet elektromagnetike nga një sistem kompjuterik që bartë të dhëna kompjuterike.

Përgjim në kontekstin e kësaj vepre penale duhet kuptuar përgjimin e komunikimeve zanore, komunikimeve tekstuale ose komunikimeve tjera përmes përdorimit të pajisjeve apo programeve të lartcekura.

Kjo formë e kësaj vepre penale konsiderohet se është kryer vetëm nëse veprimi kryerës është kryer në mënyrë të paautorizuar, përkatësisht në kundërshtim me ligjin. Kjo për faktin, nëse përgjimi i tillë është kryer në harmoni me dispozitat ligjore të Ligjit për Përgjimin e Komunikimeve Elektronike[55] dhe të Kodit të Procedurës Penale[56], atëherë kjo nuk përbën vepër penale.
Kryes i kësaj forme të veprës penale mund të jetë çdo person i cili ndërmerr veprimin e lartcekur në mënyrë të paautorizuar dhe mund të kryhet vetëm me dashje.

[55] Ligji Nr. 05/L-030 për Përgjimin e Komunikimeve Elektronike, datë 28.05.2015. Me Ligjin për Përgjimin e Komunikimeve Elektronike rregullohen procedurat dhe kushtet mbi përgjimin e komunikimeve elektronike që realizohen për nevoja të procedurës penale nga institucionet shtetërore të themeluara me ligj, dhe procedurat dhe kushtet e përgjimit për nevojat e sigurisë së Republikës së Kosovës dhe qytetarëve të saj të themeluara me ligj. Gjithashtu, me këtë Ligj përcaktohen edhe rregullat, detyrimet dhe procedurat për Operatorët e Rrjeteve dhe Ofruesit e Shërbimeve në lidhje me përpunimin e të dhënave të caktuara nga ana e tyre, si dhe përcaktohen detyrimet dhe autorizimet e institucioneve shtetërore të themeluara me ligj për të garantuar respektimin e të drejtave dhe lirive të njeriut në procesin e përgjimit të ligjshëm, si dhe kontrollin në zbatimin e procedurave të përgjimit. Sipas nenit 5 të këtij Ligji, ekzistojnë dy (2) lloje të përgjimeve: 1) Përgjimi për nevoja të procedurës penale dhe 2) Përgjimi për nevojat e sigurisë së Republikës së Kosovës dhe qytetarëve të saj.

[56] Kodi nr.08/L-032 i Procedurës Penale, datë 14.07.2022. Në dispozitën ligjore të neni 85, paragrafi 4 të KPP-së është parashikuar si masë e veçantë hetimore "përgjimi i telekomunikimeve dhe përdorimi i lexuesit – IMSI – identifikimi ndërkombëtar i shfrytëzuesit mobil" do të thotë përgjim i komunikimeve zanore, komunikimeve tekstuale ose komunikimeve tjera përmes rrjeteve të telefonive fikse apo mobile. Kjo përfshinë çfarëdo mjeti apo sistemi tjetër të ngjashëm teknologjik që bartë të dhëna që kryesisht kanë për qëllim të jenë private.

Për këtë formë të kësaj vepre penale është parashikuar dënim me burgim nga një (1) deri në pesë (5) vjet.

Forma e rëndë e kësaj vepre penale, siç u theksuar më lart, është parashikuar në paragrafin 2 të nenit të lartcekur. Sipas kësaj dispozite ligjore, kjo formë të rëndë të kësaj vepre penale konsiderohet se është kryer në rastet kur kjo vepër kryhet brenda sistemeve kompjuterike dhe të informacionit ushtarak, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile apo në çdo sistem tjetër kompjuterik, me rëndësi publike.

Konsiderohet formë e rëndë e kësaj vepre penale, pasi që sistemet e kompjuterike dhe të informacionit ushtarak, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, apo në çdo sistem tjetër kompjuterik me rëndësi publike janë me interes të veçantë për çdo shtet dhe shoqëri.

Përndryshe, kryerës i kësaj forme të veprës penale mund të jetë çdo person dhe e njëjta mund të kryhet vetëm me dashje.

Për këtë formë të kësaj vepre penale është parashikuar dënim me burgim jo më pak se pesë (5) vjet.

2.6 Pengimi i funksionimit të sistemeve kompjuterike dhe të informacionit (Neni 277/F)

Kjo vepër penale përmban dy (2) forma dhe atë: formën themelore të parashikuar në parashikuar në paragrafin 1 dhe formën e rëndë të parashikuar në paragrafin 2.

Formën themelore të kësaj vepre penale e kryen kushdo që krijon pengesa serioze dhe të paautorizuara për të cenuar funksionimin e një sistemi kompjuterik dhe të informacionit, nëpërmjet futjes, dëmtimit, shtrembërimit, ndryshimit dhe fshirjes së të dhënave ose i bënë të palexueshme.

Veprimi i kryerjes së kësaj vepre penale konsiston në krijimin e pengesave serioze me anë të të cilave cenohet funksioni i një sistemi kompjuterik dhe të informacionit.

Veprimi kryerës realizohet nëpërmjet futjes, dëmtimit, shtrembërimit, ndryshimit dhe fshirjes së të dhënave ose i bënë të palexueshme.

Duhet theksuar se për të ekzistuar kjo formë e kësaj vepre penale duhet që pengesat të jenë të karakterit "serioz", ndërsa një gjë e tillë përcaktohet varësisht nga rrethanat specifike të secilit rast veç e veç dhe se të gjitha këto pengesa serioze duhet të bëhen në mënyrë të paautorizuar.

Për këtë formë të kësaj vepre penale është parashikuar dënim me burgim nga një (1) deri në pesë (5) vjet.

Forma e rëndë e kësaj vepre penale kryhet kur kjo vepër kryhet në sistemet kompjuterike dhe të informacionit ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike.

Për formën e rëndë të kësaj vepre penale është parashikuar dënim me burgim jo më pak se pesë (5) vjet.

Kryes i kësaj vepre penale mund të jetë çdo person dhe kjo vepër penale, në të dyja format e saj mund të kryhet vetëm me dashje.

2.7 Keqpërdorimi i pajisjeve dhe programeve kompjuterike (Neni 277/G)

Kjo vepër penale siç rezulton edhe nga vetë emërtimi i saj ka të bëjë me keqpërdorimin e pajisjeve dhe të programeve të caktuara me qëllim të kryerjes së veprave penale përkatëse.

Kështu, sipas dispozitës ligjore të nenit 277/G të KPRK-së, këtë vepër penale e kryen kushdo që prodhon, mban, shet, ofron për përdorim, shpërndan apo në çfarëdo forme tjetër, vë në dispozicion pajisje, programe apo kode kompjuterike keqbërëse, një fjalëkalim kompjuterik, një kod hyrjeje apo një të dhënë të tillë të ngjashme, të cilat janë krijuar ose përshtatur për hyrjen në një sistem kompjuterik ose në një pjesë të tij, me qëllim kryerjen e veprave penale, të parashikuara në nenin 277/D, 277/E dhe 277/F të këtij Ligji.

Veprimet e kryerjes së kësaj vepre penale janë të përcaktuara në mënyrë alternative dhe konsistojnë në:

- **prodhimin,**
- **mbajtjen,**
- **shitjen,**
- **ofrimin për përdorim,**
- **shpërndarjen apo në çfarëdo forme tjetër, vënien në dispozicion të pajisjeve, programeve apo kodeve kompjuterike keqbërëse, një fjalëkalimi kompjuterik, një kod hyrjeje apo një të dhënë të tillë të ngjashme.**

Për të ekzistuar kjo vepër penale duhet që këto pajisje, programe, kode kompjuterike keqbërëse, fjalëkalimi kompjuterik, kodi i hyrjes apo një e dhënë e tillë e ngjashme, të jenë krijuar apo përshtatur me qëllim kryerjen e veprave penale, të parashikuara në nenin 277/D, 277/E dhe 277/F të këtij Ligji.

Për këtë vepër penale është parashikuar dënim me burgim nga një (1) deri në pesë (5) vjet.

Kryes i kësaj vepre penale mund të jetë çdo person dhe e njëjta kryhet vetëm me dashje.

2.8 Vjedhja e identitetit dhe kredencialeve (Neni 277/H)

Kjo vepër penale përmban dy (2) forma dhe atë: formën themelore të parashikuar në parashikuar në paragrafin 1 dhe formën e rëndë të parashikuar në paragrafin 2.

Formën themelore të kësaj vepre penale e kryen kushdo që gjatë dhe në lidhje me ndonjë vepër tjetër penale, me dashje transferon, posedon ose shfrytëzon, pa autorizim ligjor, të dhënat e identifikimit të personit tjetër, të dhënat e qasjes, të dhënat bankare, ose të dhënat e identifikimit të telekomunikimit, nëpërmjet sistemit kompjuterik.

Veprimet kryerëse të kësaj forme të veprës penale janë të përcaktuara në mënyrë alternative dhe konsistojnë në:

- **transferimin,**

- **posedimin ose**
- **shfrytëzimin e dhënave të identifikimit të personit tjetër, të dhënave të qasjes, të dhënave bankare, ose të dhënave të identifikimit të telekomunikimit.**

Veprimet kryerëse të kësaj forme të veprës penale duhet të kryhen përmes sistemit kompjuterik dhe të ndërmerren gjatë dhe në lidhje me ndonjë vepër tjetër penale. Pra, me fjalë të tjera, veprimet e kryerjes së kësaj vepre penale të cekura më lart duhet që të kenë lidhje me ndonjë vepër tjetër penale, ndërsa me dispozitën ligjore në fjalë nuk janë përcaktuar konkretisht se cilat janë këto vepra penale, e që nga kjo rrjedh përfundimi se mund të bëhet fjalë për çdo vepër tjetër penale.

Gjithashtu, është e rëndësishme të theksohet se veprimet kryerëse duhet të ndërmerren në formë të paautorizuar.

Për këtë formë të kësaj vepre penale është parashikuar dënimi me burgim nga një (1) deri në tri (3) vjet.

Tentativa për të kryer formën themelore të kësaj vepre penale është e dënueshme.[57]

Formën e rëndë të kësaj vepre penale e kryen kushdo që përpunon, mban, shet, ofron për përdorim, shpërndan apo në çfarëdo forme tjetër vë në dispozicion të dhënat sipas paragrafit 1 të këtij neni.

Siç shihet, veprimet kryerëse të kësaj forme të veprës penale janë të përcaktuara në mënyrë alternative dhe konsistojnë në:

- **përpunimin,**
- **mbajtjen,**
- **shitjen,**
- **ofrimin për përdorim,**
- **shpërndarjen apo**
- **në çfarëdo forme tjetër vënien në dispozicion të dhënat sipas paragrafit 1 të këtij neni.**

[57] Neni 277/H, paragrafi 4 i KPRK-së.

Për formën e rëndë të kësaj vepre penale është parashikuar dënim me burgim prej (6) muaj deri në pesë (5) vjet.

Kryes i kësaj vepre penale mund të jetë çdo person dhe e njëjta kryhet vetëm me dashje.

Paragrafi 3 i nenit të lartcekur është dispozitë ligjore e karakterit shpjegues, pasi që përcakton domethënien e shprehjes "të dhëna të identifikimit". Kështu, sipas kësaj dispozite ligjore, për qëllim të këtij neni, shprehja **"të dhëna të identifikimit",** nënkupton cilindo emër ose numër që mund të përdoret, i vetëm apo në lidhje me ndonjë informacion tjetër, për të identifikuar një individ të caktuar, përfshirë emrin, datën e lindjes, lejen e vozitjes apo numrin e identifikimit, numrin e pasaportës, numrin e identifikimit të punëdhënësit ose tatimpaguesit, numrin e sigurimit shëndetësorë ose çdo emër dhe numër unik identifikues i caktuar nga ndonjë institucion apo i krijuar nga vetë personi me qëllim identifikim dhe përcaktimi të autenticitet të një individi, të cilët janë krijuar dhe ruajtur në formë elektronike.

2.9 Materialet me përmbajtje të shfrytëzimit dhe keqpërdorimit seksual të fëmijëve (Neni 277/I)

Kjo vepër penale ka të bëjë me keqpërdorimin e fëmijëve për të prodhuar materiale me përmbajtje seksuale dhe në posedimin dhe shfrytëzimin e këtyre materiale, kurse në vete përmban tre (3) forma të kryerjes.

Forma e parë është e parashikuar në paragrafin 1 të nenit të lartcekur, të cilën e kryen kushdo që përdor apo përfshin fëmijët për të prodhuar materiale me përmbajtje të shfrytëzimit dhe keqpërdorimit seksual të fëmijëve, qoftë me apo pa kontakt fizik.

Veprimet kryerëse të kësaj forme të veprës penale janë të përcaktuara në mënyrë alternative dhe konsistojnë në:

- **përdorimin apo**
- **përfshirjen e fëmijëve për të prodhuar materiale me përmbajtje të shfrytëzimit dhe keqpërdorimit seksual të fëmijëve.**

Veprimet e lartcekura kryerëse mund të kryhen me apo pa kontakt fizik të fëmijëve.[58]

Për këtë formë të kësaj vepre penale është parashikuar dënimi me burgim prej pesë (5) deri në pesëmbëdhjetë (15) vjet.

Forma e rëndë e kësaj vepre penale është parashikuar në paragrafin 2 të nenit të lartcekur, të cilën e kryen kushdo që shet, shpërndan, promovon, shfaq, transmeton, ofron ose e vë në dispozicion materialet me përmbajtje të shfrytëzimit dhe keqpërdorimit seksual të fëmijëve nëpërmjet një sistemi kompjuterik.

Veprimet kryerëse të formës së rëndë të kësaj vepre penale janë të përcaktuara në mënyrë alternative dhe konsistojnë në:

- **shitjen,**
- **shpërndarjen,**
- **promovimin,**
- **shfaqjen,**
- **transmetimin,**
- **ofrimin ose**
- **vënien në dispozicion materialet me përmbajtje të shfrytëzimit dhe keqpërdorimit seksual të fëmijëve nëpërmjet një sistemi kompjuterik.**

Për këtë formë të kësaj vepre penale është parashikuar dënim me burgim prej tre (3) deri në dhjetë (10) vjet.

Forma e lehtë e kësaj vepre penale është e parashikuar në paragrafin 3 të nenit të lartcekur dhe e kryen kushdo që siguron për vetveten apo personin tjetër ose posedon materiale me përmbajtje të shfrytëzimit dhe keqpërdorimit seksual të fëmijëve.

Veprimet e kryerjes së kësaj forme të veprës penale janë të përcaktuara në mënyrë alternative dhe konsistojnë në:

[58] Fëmijë konsiderohet personi i cili nuk e ka mbushur moshën tetëmbëdhjetë (18) vjet, referuar nenit 3, paragrafi 1, nën-paragrafi 1.1. të Kodit të Drejtësisë për të Mitur; nenit 113, paragrafi 22 të KPRK-së dhe nenit 1 të Konventës për të Drejtat e Fëmijës.

- **sigurimin për vetveten apo personin tjetër ose**
- **posedimin materialeve me përmbajtje të shfrytëzimit dhe keqpërdorimit seksual të fëmijëve.**

Për këtë formë të kësaj vepre penale është parashikuar dënimi me burgim prej një (1) deri në pesë (5) vjet.

Në paragrafin 4 të nenit të lartcekur është parashikuar se tentativa për të kryer vepër penale nga ky nen është e dënueshme, megjithëse një gjë e tillë është e panevojshme, duke qenë se për të gjitha format e kësaj vepre penale është parashikuar dënimi me burgim mbi tre (3) vjet, kështu që duke u bazuar në nenin 28, paragrafi 2 të KPRK-së, tentativa është e dënueshme, bazuar në dënimin e parashikuar për këto vepra penale. Kështu, në dispozitën ligjore të nenit 28, paragrafi 2 të KPRK-së është parashikuar se tentativa për të kryer vepër penale për të cilën mund të shqiptohet dënimi me tre ose më shumë vjet burgim dënohet. Tentativa për të kryer ndonjë vepër penale tjetër, dënohet vetëm nëse shprehimisht parashihet me ligj.

Paragrafi 5 i nenit të lartcekur është dispozitë ligjore e karakterit shpjegues, pasi që përcakton domethënien e shprehjes "materiale me përmbajtje të shfrytëzimit dhe keqpërdorimit seksual të fëmijëve". Kështu, sipas kësaj dispozite ligjore, për qëllime të këtij neni, termi **"materiale me përmbajtje të shfrytëzimit dhe keqpërdorimit seksual të fëmijëve"**, nënkupton ekspozimin aktual përmes videove dhe fotografive, përfshirë me anë të mjeteve të teknologjisë së informimit dhe së komunikimit, të:

- një fëmije të përfshirë në sjellje seksualisht eksplicite, qoftë të vërtetë apo të simuluar; ose
- organeve gjenitale të një fëmije për qëllime kryesisht seksuale.

Kryes i kësaj vepre penale mund të jetë çdo person, kurse viktima të kësaj vepre penale mund të jenë vetëm fëmijët.

Kjo vepër penale mund të kryhet vetëm me dashje dhe me **"qëllime seksuale"**. Sipas dispozitës ligjore të nenit 225, paragrafi 10 të KPRK-së, **"qëllime seksuale"** duhet nënkuptuar çdo veprim i bërë për qëllimet e kënaqësisë seksuale të një personi.

2.10 Falsifikimi kompjuterik (Neni 277/J)

Kjo vepër penale siç rrjedh edhe nga vetë emërtimi i saj i referohet falsifikimeve të ndryshme kompjuterike dhe përmban dy (2) forma të kryerjes, formën themelore të parashikuar në paragrafin 1 dhe formën e rëndë të parashikuar në paragrafin 2.

Formën themelore të kësaj vepre penale e kryen kushdo që fut, ndryshon, fshin apo fsheh të dhënat kompjuterike, pa të drejtë, për krijimin e të dhënave të rreme, me qëllim paraqitjen dhe përdorimin e tyre si autentike, pavarësisht nëse të dhënat e krijuara janë drejtpërdrejt të lexueshme apo të kuptueshme.

Veprimet e kryerjes së kësaj forme të veprës penale janë të përcaktuara në mënyrë alternative dhe konsistojnë në futjen, ndryshimin, fshirjen apo fshehjen të dhënave kompjuterike, pa të drejtë, për krijimin e të dhënave të rreme, me qëllim paraqitjen dhe përdorimin e tyre si autentike, pavarësisht nëse të dhënat e krijuara janë drejtpërdrejt të lexueshme apo të kuptueshme.

Për këtë formë të kësaj vepre penale është parashikuar dënimi me burgim nga gjashtë (6) muaj deri në tri (3) vjet.

Forma e rëndë e kësaj vepre penale kryhet në rastet kur kjo vepër kryhet nga personi që ka për detyrë ruajtjen dhe administrimin e të dhënave kompjuterike ose në bashkëpunim, për të cilën është parashikuar dënim me burgim jo më pak se tri (3) vjet.

Kryes i kësaj vepre penale mund të jetë çdo person dhe e njëjta kryhet vetëm me dashje.

Kurse, për tentativë të kryerjes së veprës penale nga paragrafi 1 i këtij neni, kryesi dënohet me burgim prej tre (3) muaj deri një (1) vit.[59]

[59] Neni 277/J, paragrafi 3 i KPRK-së.

2.11 Mashtrimi Kompjuterik (Neni 277/K)

Formën themelore të kësaj vepre penale sipas paragrafit 1 të nenit të lartcekur e kryen kushdo që fut, ndryshon, fshin apo fsheh të dhënat kompjuterike apo ndërhyn në funksionimin e një sistemi kompjuterik, me qëllim për t'i siguruar vetes apo palës tjetër, me mashtrim, një përfitim ekonomik të padrejtë apo për t'i shkaktuar një pale tjetër pakësimin e pasurisë.

Veprimet e kryerjes së kësaj vepre penale janë të përcaktuara në mënyrë alternative dhe konsistojnë në: futjen, ndryshimin, fshirjen apo fshehjen e dhënave kompjuterike apo ndërhyn në funksionimin e një sistemi kompjuterik.

Për këtë formë të kësaj vepre penale është parashikuar dënimi me burgim nga një (1) deri në pesë (5) vjet.

Forma e rëndë e kësaj vepre penale kryhet në rastet kur kjo vepër kryhet nga kryesi si anëtar i grupit,[60] për të cilën është parashikuar dënim me burgim jo më pak se pesë (5) vjet.

Kryes i kësaj vepre penale mund të jetë çdo person dhe e njëjta kryhet vetëm me dashje, si dhe me qëllim për t'i siguruar vetes apo palës tjetër, me mashtrim, një përfitim ekonomik të padrejtë apo për t'i shkaktuar një pale tjetër pakësimin e pasurisë.

Kurse, për tentativë të kryerjes së veprës penale nga paragrafi 1 i këtij neni, kryesi dënohet me burgim prej tre (3) muaj deri një (1) vit.[61]

3. LIGJI PËR SIGURINË KIBERNETIKE

3.1 Vështrime të përgjithshme

Kuvendi i Republikës së Kosovës më 02.02.2023 ka miratuar Ligjin Nr.08/L-173 për Sigurinë Kibernetike (në vijim: LSK), i cili është shpallur me dekretin

[60] Sipas dispozitës ligjore të nenit 113, paragrafi 12 të KPRK-së, grup njerëzish konsiderohet tre (3) ose më shumë persona.
[61] Neni 277/K, paragrafi 3 i KPRK-së.

Nr. DL-18/2023, datë 20.02.2023 nga Presidentja e Republikës së Kosovës znj.Vjosa Osmani-Sadriu, ndërsa në Gazetën Zyrtare të Republikës së Kosovës është publikuar më 27.02.2023. Ky ligj ka hyrë në fuqi pesëmbëdhjetë (15) ditë pas publikimit në Gazetën Zyrtare të Republikës së Kosovës.[62]

Ky ligj konsiderohet njëri prej ligjeve më të rëndësishme në fushën e sigurisë kibernetike dhe vjen si rezultat i nevojës së Republikës së Kosovës për të harmonizuar të drejtën e brendshme me "asquis-in" e BE-në, duke qenë se vendi jonë më 27.10.2015, në Strasburg e ka nënshkruar Marrëveshjen e Stabilizim Asociimit me BE-në,[63] mbi bazën e së cilës, përveç tjerash, ka marrë për sipër që të përafron dhe harmonizon legjislacionin vendor me legjislacionin e BE-së. Në këtë mënyrë, bazuar në dispozitat e MSA-së, është detyrë e Republikës së Kosovës që të bëjë transpozimin e "acquis" të BE-së në sistemin juridik të brendshëm.

Bazuar në këto detyrime që burojnë nga MSA, me këtë ligj synohet që të transpozohet pjesërisht Direktiva (BE) 2013/40 e Parlamentit Evropian dhe Këshillit të datës 12 gusht 2013 për Sulmet kundër Sistemeve të Informacionit,[64] që zëvendëson Vendimin Kornizë të Këshillit 2005/222/JHA, si dhe Direktivën (BE) 2016/1148 të Parlamentit Evropian dhe Këshillit të datës 6 korrik 2016 për Masat e Sigurisë së Sistemeve të Rrjetit dhe Informacionit.[65]

Me këtë Ligj janë përcaktuar parimet e sigurisë kibernetike, institucionet që zhvillojnë, zbatojnë dhe promovojnë politikën e sigurisë kibernetike, përgjegjësitë e autoriteteve në fushën e sigurisë kibernetike, detyrat e subjekteve të sigurisë kibernetike, bashkëpunimin ndërinstitucional, parandalimin e sulmeve kibernetike në Republikën e Kosovës, si dhe është themeluar Agjencia për Siguri Kibernetike (në vijim: ASK).[66]

[62] Neni 28 i LSK-së.
[63] Linku i MSA-së: https://integrimievropian.rks-gov.net/msa/
[64] Linku i Direktivës: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng
[65] Neni 1, paragrafi 2 i LSK-së.
[66] Neni 1, paragrafi 1 i LSK-së.

Është e rëndësishme që të theksohet se ky ligj zbatohet nga ASK-ja dhe mekanizmat tjerë institucionalë të Republikës së Kosovës për propozimin, zbatimin e masave kibernetike, si dhe garantimin e sigurisë kibernetike.[67]

3.2 Përkufizimet e shprehjeve të përdorura në LSK

Sikurse çdo ligj tjetër i rëndësishëm, edhe me dispozitat ligjore të LSK-së janë përcaktuar përkufizimet e disa shprehjeve, termave dhe shkurtesave që janë përdorur, të cilat si të tilla do të paraqiten në vijim, ashtu siç janë të paraqitura në këto dispozita ligjore, pasi që vlerësojmë se janë të rëndësishme për gjyqtarët dhe prokurorët, por jo vetëm, që t'i kuptojnë sa më drejtë dhe mirë këto që shprehje që i përkasin fushës së sigurisë kibernetike, një fushë kjo jo shumë e zhvilluar në Republikën e Kosovës.

Në këtë drejtim, në nenin 3 të LSK-së, është parashikuar se shprehjet, termet dhe shkurtesat e përdorura në këtë ligj kanë këto kuptime:

1. Kibernetika - nënkupton aktivitete që ndërlidhen me përfshirjen e kompjuterëve ose rrjeteve kompjuterike, siç është interneti;

2. Hapësirë kibernetike - nënkupton mjedisi kompleks që rezulton nga ndërveprimi i njerëzve, softuerëve dhe shërbimeve në internet me anë të pajisjeve teknologjike dhe rrjeteve të lidhura me të, i cili nuk ekziston në ndonjë formë fizike;

3. Siguria kibernetike - nënkupton aktivitetet e nevojshme për të mbrojtur sistemet e rrjetit dhe informacionit, përdoruesit e këtyre sistemeve dhe personave të tjerë të prekur nga incidenti kibernetik;

4. Sistem kompjuterik - nënkupton një pajisje apo grup pajisjesh të ndërlidhura, një ose më shumë prej të cilave, në bazë të një programi, kryejnë përpunim automatik të të dhënave;

5. Incident kibernetik - nënkupton çdo ngjarje që ka efekt negativ real në sigurinë e sistemeve të rrjetit dhe informacionit;

[67] Neni 2 i LSK-së.

6. Trajtimi i incidentit kibernetik - nënkupton të gjitha procedurat që mbështesin zbulimin, analizën dhe mbajtjen nën kontroll të incidentit kibernetik dhe reagimin ndaj tij;

7. Sistem informacioni - nënkupton një pajisje ose grup pajisjesh të ndërlidhura, ku një ose më shumë prej tyre në bazë të një programi, përpunojnë në mënyrë automatike të dhëna kompjuterike, po ashtu të dhëna kompjuterike të ruajtura, përpunuara, të marra ose transmetuara nga ajo pajisje ose grup i pajisjeve për qëllime të operimit, përdorimit, mbrojtjes dhe mirëmbajtjes së tyre;

8. Të dhëna kompjuterike - nënkupton një paraqitje të fakteve, informatave ose koncepteve në një formë të përshtatshme për përpunim në një sistem informacioni, përfshirë një program të përshtatshëm i cili mundëson që një sistem informacioni të kryejë një funksion. Të dhënat kompjuterike përfshijnë, por nuk kufizohen në dokumente të shkruara, fotografi, audio dhe video materiale, programet softuerike dhe materialet tjera që ruhen në formë digjitale;

9. Rrjeti i komunikimeve elektronike - nënkupton sistemin e transmetimit dhe nëse ekzistojnë, pajisjet e komutimit ose rutinimit dhe resurset tjera, duke përfshirë elementet e rrjetit që nuk janë aktive, të cilat lejojnë përcjelljen e sinjaleve nëpërmjet përcjellësve, radios, mjeteve optike ose mjeteve të tjera elektromagnetike, duke përfshirë rrjetet satelitore, rrjetet fikse (me komutim të qarqeve ose me komutim të paketave, përfshirë internetin), rrjetet mobile tokësore, sistemet e kabllove elektrike në raste kur ato përdoren për transmetimin e sinjaleve, rrjetet e përdorura për transmetimet radiotelevizive dhe të televizionit kabllor, pavarësisht nga tipi i informacionit të bartur;

10. Sistemi i rrjetit dhe informacionit - nënkupton:

10.1. një rrjet komunikimi elektronik, siç definohet në nën-paragrafin 1.9 të këtij neni;

10.2. çdo sistem informacioni, siç definohet në nën-paragrafin 1.7 të këtij neni;

10.3. të dhënat digjitale të ruajtura, përpunuara, pranuara ose transmetuara nga elementet e mbuluara në nën-paragrafin 10.1. dhe 10.2. të këtij neni për qëllimet e operimit, përdorimit, mbrojtjes dhe mirëmbajtjes së tyre;

11. Siguria e sistemeve të rrjetit dhe informacionit - nënkupton aftësinë e sistemeve të rrjetit dhe informacionit për të rezistuar, në një nivel të caktuar besueshmërie, çdo veprimi që komprometon disponueshmërinë, origjinalitetin, integritetin ose konfidencialitetin e të dhënave të ruajtura ose të transmetuara ose të përpunuara ose shërbimet përkatëse të ofruara nga, apo të qasshme nëpërmjet këtyre sistemeve të rrjetit dhe informacionit;

12. Operatori i shërbimeve esenciale - nënkupton një subjekt publik ose privat i cili posedon infrastrukturë kritike kombëtare sipas Ligjit përkatës për Infrastrukturën Kritike;

13. Ofruesi i shërbimit digjital - nënkupton personin juridik me seli kryesore ose me një degë, të regjistruar në Republikën e Kosovës, i cili ofron shërbime digjitale;

14. Shërbimet digjitale - nënkuptojnë një grup shërbimesh të bazuara në teknologji të informacionit dhe komunikimeve ku përfshin: shërbimet e tregut online, kërkimit në internet dhe shërbimet e cloud-computing;

15. Treg online - një shërbim digjital që i mundëson konsumatorëve dhe tregtarëve, të shesin në internet ose të lidhin kontrata të shërbimit në ueb faqen e tregut online ose në ueb faqen e një tregtari që përdor shërbime kompjuterike të ofruara nga tregu online, ku; **"konsumator" -** çdo person fizik që vepron për qëllime që janë jashtë tregtisë, biznesit, zanatit ose profesionit të tij; **"tregtar"-** çdo person fizik ose çdo person juridik, pavarësisht nëse është në pronësi private apo publike, i cili vepron, duke përfshirë çdo person që vepron në dobi të tij apo në emër të tij, për qëllime që lidhen me tregtinë, biznesin, zanatin ose profesionin e tij.

16. Motor kërkimi në internet - nënkupton një shërbim digjital që i mundëson përdoruesve të kryejnë kërkime, në parim, në të gjitha ueb-faqet, ose në të gjitha uebfaqet në një gjuhë të caktuar, në bazë të një kërkese për

çfarëdo teme në formën e një fjale, fraze ose të dhëne tjetër, dhe kthen linqe në të cilat mund të gjenden informatat lidhur me përmbajtjen e kërkuar;

17. Shërbimi i cloud computing - nënkupton një shërbim digjital që mundëson qasje në një pako të shkallëzuar dhe elastike të burimeve/resurseve kompjuterike të shpërndara. Burimet kompjuterike përfshijnë burime të tilla si rrjetet, serverët ose infrastruktura tjetër, hapësira ruajtëse, aplikacionet dhe shërbimet;

18. I shkallëzuar - i referohet burimeve kompjuterike që shpërndahen në mënyrë fleksibile nga ofruesi i shërbimit cloud, pavarësisht nga vendndodhja gjeografike e burimeve, në mënyrë që të trajtojë luhatjet e kërkesës;

19. Elastike - përdoret për të përshkruar ato burime kompjuterike që sigurohen dhe lëshohen sipas kërkesës në mënyrë që të rriten dhe zvogëlohen me shpejtësi burimet e disponueshme në dispozicion;

20. Regjistri - nënkupton regjistrin e incidenteve kibernetike;

21. ASK - nënkupton Agjencinë për Siguri Kibernetike;

22. CERT kombëtar - nënkupton Ekipi i Republikës së Kosovës për reagim ndaj emergjencave kompjuterike në nivel kombëtar;

23. CSIRT-at sektorial kombëtar - nënkupton ekipet për reagim ndaj incidenteve të sigurisë kompjuterike ose të sigurisë kibernetike që prekin një sektor specifik në nivel kombëtar. CSIRT-at sektorial kombëtar mund të themelohen në sektorë përkatës të infrastrukturës kritike;

24. CSIRT-at e OShE - nënkupton ekipet për reagim ndaj incidenteve të sigurisë kompjuterike ose të sigurisë kibernetike që prekin një operator të shërbimeve esenciale dhe.

25. CSIRT-at e OShD - nënkupton ekipet për reagim ndaj incidenteve të sigurisë kompjuterike ose të sigurisë kibernetike që prekin një ofrues të shërbimeve digjitale.

3.3 Parimet e garantimit të sigurisë kibernetike

Në dispozitat ligjore të LSK-së janë parashikuar disa parime mbi bazën e të cilave garantohet siguria kibernetike në Republikën e Kosovës. Kështu, sipas dispozitës ligjore të nenit 4 të LSK-së parimet mbi bazën e të cilave garantohet siguria kibernetike janë: parimi i personalitetit, parimi i mbrojtjes integrale, parimi i minimizimit të efektit negativ dhe parimi i bashkëpunimit.

Sipas kësaj dispozite ligjore:

1. Parimi i personalitetit - që nënkupton se garantimi i sigurisë së një sistemi do të organizohet nga ofruesi i shërbimit;

2. Parimi i mbrojtjes integrale - që nënkupton se ofruesi i shërbimit do të konstatojë rreziqet e mundshme që paraqiten në sistem të rrjetit dhe informacionit dhe do të zbatojë masat e duhura organizative dhe teknike për mbrojtjen e sistemit të rrjetit dhe informacionit;

3. Parimi i minimizimit të efektit negativ - që nënkupton se në rastin e incidentit kibernetik, ofruesi i shërbimeve duhet të zbatojë kujdesin e duhur dhe masat për të shmangur përshkallëzimin e efektit të incidentit kibernetik dhe përhapjen e saj të mundshme në një sistem tjetër, dhe njofton autoritetin mbikëqyrës të paraparë sipas këtij ligji për incidentin kibernetik dhe

4. Parimi i bashkëpunimit - që nënkupton se në garantimin e sigurisë kibernetike dhe zgjidhjen e incidentit kibernetik, palët do të bashkëpunojnë dhe nëse është e nevojshme, të marrin parasysh lidhjen e ndërsjellë dhe varësinë e sistemeve dhe shërbimeve.
Duhet theksuar se këto janë katër (4) parimet bazë të garantimit të sigurisë kibernetike, mirëpo si të tilla nuk janë të vetme, pasi që me dispozitat ligjore të LSK-së janë parashikuar dhe rregulluar edhe një sërë parimesh dhe çështjes tjera që ndërlidhen me sigurinë kibernetike.

3.4 Masat e sigurisë për garantimin e sigurisë kibernetike

Me dispozitat ligjore të LSK-së janë parashikuar disa masa të sigurisë të cilat duhet që t'i ndërmarrin operatorët e shërbimeve esenciale. Në këtë mënyrë,

përgjegjësi e operatorit të shërbimeve esenciale është që në mënyrë të përhershme të zbatojë masa të sigurisë organizative, fizike dhe të teknologjisë së informacionit për parandalimin e incidentit kibernetik; zgjidhjen e incidentit kibernetik, si dhe parandalimin dhe zbutjen e ndikimit në vazhdimësinë e shërbimit ose sigurinë e sistemit për shkak të incidentit kibernetik ose për parandalimin dhe zbutjen e një ndikimi të mundshëm mbi vazhdimësinë e një shërbimi tjetër të varur ose sigurisë së një sistemi.[68]

Në situata të tilla, operatori i shërbimeve esenciale duhet të informojë ASK-në menjëherë, por jo më vonë se njëzetë e katër (24) orë pasi që të jetë vënë në dijeni të incidentit kibernetik, i cili ka një ndikim të konsiderueshëm në sigurinë e sistemit ose vazhdimësinë e shërbimit, ndikimi i konsiderueshëm i të cilit për sigurinë e sistemit apo vazhdimësinë e shërbimit nuk është i qartë, por mund të supozohet në mënyrë të arsyeshme.[69]

Gjithashtu, brenda një periudhe të arsyeshme kohore, operatori i shërbimeve esenciale është i detyruar të njoftojë personat potencialisht të prekur nga incidenti kibernetik me një ndikim të konsiderueshëm, ose publikun, kur personat e prekur nuk mund të njoftohen individualisht.[70] Përveç që duhet ta njoftojë ASK-së për incidentin kibernetik, për zgjidhjen e një incidenti kibernetik me ndikim të konsiderueshëm, operatori i shërbimit esencial duhet t'i dërgojë ASK-së raport i cili përfshin informacione për shkaqet e incidentit kibernetik, kohën e kaluar në zgjidhjen e tij, masat e zbatuara dhe ndikimin e incidentit kibernetik.

Masat e sigurisë janë parashikuar edhe për sistemin e ofruesit të shërbimeve digjitale, nga të cilët kërkohet të konstatojë rreziqet që cenojnë sigurinë e sistemit të tyre, t'i analizojnë ato dhe të marrin masa adekuate organizative dhe teknike për menaxhimin e rrezikut,[71] të cilët gjithashtu janë të detyruar që ta njoftojnë ASK-në për një incident kibernetik që ka një ndikim të konsiderueshëm në shërbimin digjital të ofruar, menjëherë pasi që të jetë në dijeni të incidentit kibernetik dhe të ndërmarrin të gjitha masat përkatëse ligjore në drejtim të ofrimit të sigurisë së shërbimeve digjitale.

[68] Neni 5, paragrafi 1 i LSK-së.
[69] Neni 6, paragrafi 1 i LSK-së.
[70] Neni 6, paragrafi 4 i LSK-së.
[71] Neni 7, paragrafi 1 i LSK-së.

Përndryshe, garantimi i sigurisë kibernetike dhe parandalimi dhe zgjidhja e një incidenti kibernetik në masën e parashikuar nga ky ligj, duhet që të koordinohet nga ASK-ja. Me qëllim të garantimit të sigurisë kibernetike, ASK në koordinim me Ministrinë e Mbrojtjes, Autoritetin Rregullativ të Komunikimeve Elektronike dhe Postare dhe institucionet tjera të sigurisë, analizon rreziqet që cenojnë sigurinë e sistemeve dhe ndikimin e tyre në shtet, shoqëri dhe sigurinë e sistemeve.[72]

Përveç këtyre, me dispozitat ligjore të LSK-së janë parashikuar edhe një sërë masash në drejtim të garantimit të sigurisë kibernetike, është paraparë që të krijohet një regjistër i incidenteve kibernetike, që administrohet nga ASK-ja dhe është rregulluar çështja e mbikëqyrjes dhe monitorimit.

3.5 Mekanizmat shtetërorë të sigurisë kibernetike

Me dispozitat ligjore të LSK-së është parashikuar edhe krijimi i disa mekanizmave shtetërorë që kanë përgjegjësi të caktuara në drejtim të garantimit të sigurisë kibernetike, siç janë: Agjencia për Siguri Kibernetike;[73] Këshilli Shtetëror për Siguri Kibernetike dhe Qendra Shtetërore Trajnuese për Sigurinë Kibernetike.

[72] Neni 9, paragrafët 1-2 të LSK-së.

[73] Deri në vitin e kaluar, në kuadër të Ministrisë së Punëve të Brendshme ka ekzistuar Departamenti për Siguri Kibernetike dhe Administrim të Sistemeve, që ka pasur për detyrë dhe përgjegjësi të: Përgatit dhe mbikëqyrë zbatimin e politikave për siguri kibernetike në nivel nacional; Koordinon aktivitetet e sigurisë kibernetike duke përfshirë aktivitetet në rast të incidenteve kibernetike në institucionet publike dhe private; Përgatit raporte periodike për gjendjen e sigurisë kibernetike në Republikën e Kosovës, të cilat i përcjell tek Sekretari i Përgjithshëm i MPB-së dhe Koordinatori Nacional për Siguri Kibernetike; Përgatit politikat për administrim të sistemeve, bazave të të dhënave dhe aplikacioneve softuerike dhe kujdeset për zbatimin e tyre, njëkohësisht i koordinon ato me institucionet e tjera qeveritare; Zhvillon projekte të teknologjisë së informacionit që ndërlidhen me sigurinë dhe administrimin e sistemeve për të gjitha departamentet, zyrat dhe agjencitë e MPB-së; Administron me infrastrukturën e teknologjisë së informacionit për sistemet e komunikimeve, për departamentet, zyrat dhe agjencitë e MPB-së duke përfshirë edhe njësitë lokale; Administron me regjistrat elektronik të departamenteve, zyrave dhe agjencive të MPB-së dhe të përfaqëson Republikën e Kosovës në forumet e sigurisë kibernetike. https://mpb.rks-gov.net/f/23/Departamenti-per-Siguri-Kibernetike-dhe-Administrim-te-Sistemeve

3.5.1. Agjencia për Siguri Kibernetike

ASK është institucion përgjegjës për propozim dhe zbatimin e masave për siguri kibernetike në Republikën e Kosovës dhe ka për detyrë të monitoroj, inspektoj dhe koordinoj aktivitetet e institucioneve përgjegjëse për siguri kibernetike në Republikën e Kosovës, si dhe të ndërmerr masa në rast të moszbatimit, në pajtim me këtë ligj, duke përfshirë këtu reagimin ndaj kërcënimeve dhe incidenteve në hapësirën kibernetike të Republikës së Kosovës.

Po ashtu, ASK në bashkëpunim me Qendrën Shtetërore Trajnuese për Siguri Kibernetike ka për detyrë realizimin e testimeve dhe ushtrimeve të përbashkëta me operatorët e shërbimeve esenciale dhe ofruesit e shërbimeve digjitale, me qëllim evidentimin e cenueshmërisë.

Përtej këtyre, ASK duhet që të bashkëpunon me autoritetet e shteteve të huaja dhe organizatat ndërkombëtare në lidhje me aspektet që janë nën përgjegjësinë e ASK-së dhe është pika e vetme e kontaktit.[74]

3.5.2. Këshilli Shtetëror për Siguri Kibernetike

Këshilli Shtetëror për Siguri Kibernetike (në vijim: KSHSK) është organ këshillimor i pavarur i Qeverisë së Republikës së Kosovës dhe komunitetit të biznesit, i përbërë nga përfaqësues të nivelit të lartë nga institucionet qeveritare, institucionet e zbatimit të ligjit, organizatat publike, ato private dhe komunitetit shkencor. KSHSK duhet ndërmerr masa në nivel strategjik[75] për të rritur nivelin e sigurisë kibernetike në Republikën e Kosovës.

Gjithashtu, KSHSK ka qëllim të vendos një mbulueshmëri sa më të gjerë të aspekteve të ndryshme të fushës së sigurisë kibernetike, si dhe është përgjegjës për forcimin e koordinimit dhe bashkëpunimit midis institucioneve të

[74] Neni 16 i LSK-së.
[75] Qeveria e Republikës së Kosovës më 11.09.2018, kishte marrë vendimin nr.19/64, me të cilin e kishte aprovuar Koncept Dokumentin për Parandalimin dhe Luftimin e Krimit Kribernetik. https://kryeministri.rks-gov.net/vvp-content/uploads/2022/05/Koncept-Dokumenti-per-Parandalimin-dhe-Luftimin-e-Krimit-Kibernetik-MPBShqip-1.pdf

ndryshme publike me kompetencat në çështjet e sigurisë kibernetike, si dhe ndërmjet sektorit publik dhe atij privat. Gjithashtu, ky këshill do e lehtësoj procesin e vendimmarrjes nëpërmjet analizës, studimit dhe propozimit të nismave në nivel kombëtar dhe ndërkombëtar.[76]

3.5.3. Qendra Shtetërore Trajnuese për Sigurinë Kibernetike

Në kuadër të Ministrisë së Mbrojtjes dhe Forcës së Sigurisë së Kosovës është paraparë që themelohet Qendra Shtetërore Trajnuese për Sigurinë Kibernetike, e cila ofron trajnime për të gjitha institucionet e Republikës së Kosovës në fushën e sigurisë kibernetike.

Qendra Shtetërore Trajnuese për Siguri Kibernetike në Ministrinë e Mbrojtjes/Forca e Sigurisë së Kosovës, në bashkëpunim me ASK-në, përcakton procedurën dhe formatin e programeve të specializuara për trajnime dhe certifikime të personelit të angazhuar në fushën e sigurisë kibernetike në përputhje me kompetencat që ushtrojnë, kurse detyrat dhe përgjegjësitë e Qendrës Shtetërore Trajnuese për Sigurinë Kibernetike përcaktohen më akt nënligjor nga Qeveria e Kosovës.[77]

4. KONVENTA E KËSHILLIT TË EVROPËS MBI KRIMIN KIBERNETIK

4.1 Vështrime të përgjithshme

Konventa e Këshillit të Evropës mbi Krimin Kibernetik, e njohur gjithashtu edhe si **"Konventa e Budapestit"** ***("Convention on Cybercrime")*** është traktati i parë ndërkombëtar që kërkon të trajtojë krimin kibernetik, duke harmonizuar ligjet kombëtare, përmirësuar teknikat e hetimit dhe duke rritur bashkëpunimin midis shteteve.

Me këtë Konventë, trajtohen krimet e kryera nëpërmjet internetit dhe rrjeteve të tjera kompjuterike, që kanë të bëjnë veçanërisht me shkeljet e të drejtave të autorit, mashtrimin lidhur me kompjuterin, pornografinë e fëmijëve dhe

[76] Neni 20 i LSK-së.
[77] Neni 21 i LSK-së.

shkeljet e sigurisë së rrjetit. Gjithashtu, kjo Konventë përmban një sërë kompetencash dhe procedurash, si kërkimi i rrjeteve kompjuterike dhe përgjimi.

Objektivi kryesor i Konventës mbi Krimin Kibernetik, i përcaktuar në preambulë, është të ndjekë një politikë të përbashkët kriminale që synon mbrojtjen e shoqërisë nga krimi kibernetik, veçanërisht duke miratuar legjislacionin e duhur dhe duke nxitur bashkëpunimin ndërkombëtar në mes të shteteve.[78]

Drafti i Konventës është hartuar nga Këshilli i Evropës në Strasburg të Francës, me pjesëmarrjen aktive të shteteve vëzhguese të Këshillit të Evropës, Kanadasë, Japonisë, Filipineve, Afrikës së Jugut dhe Shteteve të Bashkuara të Amerikës.

Konventa mbi Krimin Kibernetik dhe Raporti Shpjegues[79] u miratuan nga Komiteti i Ministrave të Këshillit të Evropës në sesionin e 109-të më 08.11.2001. Kjo Konventë u hap për nënshkrim më 23.11.2001 në Budapest të Hungarisë (ETS.nr.185), ndërsa ka hyrë në fuqi më 01.07.2004.

Konventa mbi Krimin Kibernetik, si instrument i rëndësishëm ndërkombëtar, është plotësuar nga dy (2) protokolle shtesë dhe atë:

1) PROTOKOLLI I PARË është "Protokolli shtesë mbi inkriminimin e akteve me natyrë raciste dhe ksenofobike të kryera nëpërmjet sistemeve kompjuterike" (ETS.nr.189)[80] që është nënshkruar në Strasburg të Francës, më 28.01.2003, ndërsa ka hyrë në fuqi më 01.03.2006. Përmes këtij Protokolli Shtesë të Konventës u kërkohet shteteve që të kriminalizojnë (inkriminojnë) shpërndarjen e materialeve raciste dhe ksenofobike përmes sistemeve kompjuterike, si dhe kërcënimet dhe fyerjet e motivuara nga racizmi ose ksenofobia.

2) PROTOKOLLI I DYTË është "Protokolli i Konventës mbi Krimin Kibernetik për bashkëpunimin e zgjeruar dhe zbulimin e provave elektronike"

[78] Linku i Konventës: https://rm.coe.int/1680081561
[79] Linku i Raportit Shpjegues: https://rm.coe.int/16800cce5b
[80] Linku i Protokollit: https://rm.coe.int/168008160f

(ETS nr.224),[81] që është nënshkruar në Strasburg të Francës, më 12.05.2022, por që deri më tani ende nuk ka hyrë fuqi.

Ky Protokoll ofron një bazë ligjore për zbulimin e informacioneve të rëndësishme dhe bashkëpunimin e drejtpërdrejtë me ofruesit e shërbimeve për informacionin, ofron mjete efektive për të marrë informacionin dhe të dhënat tjera, bashkëpunim të menjëhershëm në raste urgjente, mjete të ndihmës së ndërsjellë, si dhe masa mbrojtëse për mbrojtjen e të dhënave personale.

Konventa mbi Krimin Kibernetikë konsiderohet më shumë se një dokument ligjor, për faktin se është një kornizë që lejon hetuesit policor, prokurorët dhe gjyqtarët nga shtetet e ndryshme që të ndajnë përvojat e tyre dhe të krijojnë marrëdhënie që lehtësojnë bashkëpunimin në raste specifike, duke përfshirë situatat emergjente, përtej dispozitave specifike të parashikuara në këtë Konventë.

Përndryshe, çdo shtet mund të përdorë Konventën mbi Krimin Kibernetik si një udhëzues, listë kontrolli ose ligj model dhe për më tepër, bërja palë e këtij traktati sjell shumë avantazhe shtesë.[82] Konventa ofron një kuadër ligjor për bashkëpunimin ndërkombëtar, jo vetëm në lidhje me krimin kibernetik **("vepra kundër dhe me anë të kompjuterëve")**, por edhe në lidhje me çdo krim që përfshin prova elektronike.

Shtetet palë në Konventën mbi Krimin Kibernetikë mund të nënshkruajnë dhe ratifikojnë Protokollin e Dytë Shtesë të Konventës, i cili ofron mjete shtesë dhe të përshpejtuara për bashkëpunim të zgjeruar dhe zbulimin e provave elektronike, të tilla si "bashkëpunimi i drejtpërdrejtë me ofruesit e shërbimeve përtej kufijve" ose "bashkëpunimi në situata emergjente".

Po ashtu, është tejet e rëndësishme që të theksohet se shtetet palë të Konventës mbi Krimin Kibernetikë janë anëtarë edhe të Komitetit të Konventës për Krimet Kibernetike (T-CY)[83] dhe ndajnë informacione dhe përvojën e tyre në

[81] Linku i Protokollit: https://rm.coe.int/1680a49dab
[82] Linku i Konventës: Full list - Treaty Office
[83] Komiteti i Konventës për Krimet Kibernetike (T-CY) përfaqëson shtetet palë në Konventën e Budapestit për krimin kibernetik. Bazuar në nenin 46 të Konventës, konsultimi i Komitetit

këto drejtime, mandej vlerësojnë zbatimin e Konventës, si dhe e interpretojnë Konventën përmes Udhëzuesve përkatës.

Përveç këtyre, shtetet palë në Konventë angazhohen me njëra-tjetrën në një bashkëpunim të besueshëm dhe efikas. Indikacionet janë se edhe subjektet e sektorit privat kanë më shumë gjasa të bashkëpunojnë me autoritetet e drejtësisë penale të shteteve palë në Konventë, duke pasur parasysh se shtetet duhet të kenë një kuadër ligjor të brendshëm për krimin kibernetik dhe provat elektronike, duke përfshirë masat përkatëse mbrojtëse.[84]

4.2 Përkufizimet sipas Konventës

Në nenin 1 të Konventës është përcaktuar domethënia e disa shprehjeve që ndërlidhen me krimin kibernetik. Kështu, në këtë dispozitë është përcaktuar se për qëllimet e kësaj Konvente:

a) "Sistem kompjuterik" do të thotë çdolloj pajisje apo grup i ndërlidhur ose pajisje të lidhura, një ose më shumë prej të cilave, vazhduese të një programi kryejnë procesime automatike të të dhënave.
b) "Të dhëna kompjuterike" do të thotë çfarëdolloj përfaqësimi të fakteve, informacioni apo konceptesh në një formë të përshtatshme për procesim në një sistem kompjuterik, që përfshijnë një program të përshtatshëm për punën e një sistemi kompjuterik për të kryer një funksion;
c) "Dhënës shërbimesh" do të thotë:
(i) çfarëdo entiteti publik apo privat, që i siguron shërbimin e tij përdoruesve, me mundësinë për të komunikuar nëpërmjet një sistemi kompjuterik; dhe
(ii) çfarëdo entiteti tjetër, që proceson apo memorizon të dhëna kompjuterike në të mirë të një shërbimi të këtillë komunikimi apo të përdoruesve për këtë shërbim.
d) "Të dhëna trafiku" do të thotë çdolloj të dhënash kompjuterike, të lidhura me komunikimin nëpërmjet një sistemi kompjuterik të prodhuara nga një sistem kompjuterik që përfaqëson një pjesë në zinxhirin e komunikimit, duke treguar origjinën e komunikimit, destinacionin, rrugën,

synon të lehtësojë përdorimin dhe zbatimin efektiv të Konventës, shkëmbimin e informacionit dhe shqyrtimin e çdo amendamenti të ardhshëm.
[84] Linku: https://rm.coe.int/cyber-buda-benefits-2024-july-2789-5929-5498-v-1/1680b0d659

kohën, datën, përmasat, kohëzgjatjen apo tipin e shërbimit të poshtëshënuar.

4.3 Përmbajtja e Konventës

Siç do të elaborojmë edhe në vijim të këtij punimi, Konventa në vete përmban dispozita që i referohen tre (3) aspekteve të rëndësishme për prokurorët dhe gjyqtarët që trajtojnë raste të natyrës së krimeve kibernetike:

I) Dispozita penale materiale;
II) Dispozita penale procedurale dhe
III) Dispozita që i referohen bashkëpunimit ndërkombëtar.[85]

4.4 Dispozitat penale materiale

Në kuadër të dispozitave penale materiale janë parashikuar masat të cilat shtetet duhet që t'i ndërmarrin në kuptimin e inkriminimit të veprimeve të caktuara në legjislacionet penale vendore. Në këtë pjesë të Konventës, veprat penale janë ndarë në katër (4) grupe, në kuadër të të cilave janë sistemuar disa vepra penale.

KATEGORIZIMI I VEPRAVE PENALE SIPAS KONVENTËS MBI KRIMIN KIBERNETIK	
1.	**Veprat penale kundër konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave dhe sistemeve kompjuterike**
2.	**Krimet e lidhura me kompjuterët**
3.	**Veprat penale të lidhura me përmbajtjen**
4.	**Veprat penale të lidhura me dhunimin e të drejtës së autorit dhe të drejtave të tjera të lidhura më to**

[85] Gjithashtu, Konventa përmban edhe "Dispozitat përfundimtare" (Nenet 36-48) me të cilat janë rregulluar disa çështje të karakterit administrativ, që kanë të bëjnë me nënshkrimin, hyrjen në fuqi, anëtarësimin, zbatimin territorial, efektet e Konventës, etj.

Gjithashtu, në kuadër të kësaj pjese, janë parashikuar edhe dispozita me anë të të cilave shtetet palë të Konventës janë të detyruara që në legjislacionet e tyre të parashikojnë përgjegjësi penale edhe: për personat që tentojnë të kryerjen njërës nga veprat penale të parashikuara me Konventë; për personat që ndihmojnë kryesit e këtyre veprave penale,[86] si dhe për personat juridikë dhe personat përgjegjës të personave juridikë.[87]

Përveç këtyre, shtetet duhet që të adaptojnë në legjislacionin e tyre, edhe masa të tjera, që mund të jenë të nevojshme që të sigurohet që veprat penale sipas kësaj Konvente, të jenë të dënueshme me sanksione efektive proporcionale, të cilat përfshijnë edhe dënimin me burgim. Po ashtu, çdo shtet duhet të sigurohet që personat juridikë t'i nënshtrohen sanksioneve apo masave penale dhe jo penale, efektive, proporcionale, duke përfshirë sanksionet monetare.[88]

4.4.1. Veprat penale kundër konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave dhe sistemeve kompjuterike

Vepra penale të natyrës së tillë konsiderohen:

a) Hyrjet e paligjshme (Neni 2)

Sipas kësaj dispozite të Konventës, çdo shtet palë duhet të adapton legjislacion të tillë dhe masa të tjera që mund të jenë të nevojshme për të përcaktuar si vepra penale sipas ligjit të brendshëm, kur kryhet me qëllim hyrja në një pjesë apo në tërësi të një sistemi kompjuterik pa të drejtë. Një shtet palë mund të kërkojë që vepra të jetë kryer nga shkelje e masave të sigurimit, me qëllimin e përftimit të të dhënave kompjuterike ose qëllimet e tjera të pandershme ose në marrëdhënie me një sistem kompjuterik që është i lidhur me një sistem tjetër kompjuterik.

b) Interceptimi i paligjshëm (Neni 3)

Në këtë dispozitë të Konventës është parashikuar se çdo shtet palë do të adaptojë legjislacion të tillë dhe masa të tjera, që mund të jenë të nevojshme

[86] Neni 11 i Konventës.
[87] Neni 12 i Konventës.
[88] Neni 13 i Konventës.

të përcaktojnë si vepra penale sipas ligjit të brendshëm, kur kryhet me qëllim interceptimi pa të drejtë, kryer me mjete teknike, të transmetimeve jopublike të të dhënave kompjuterike, nga ose brenda një sistemi kompjuterik, duke përfshirë emitime elektromagnetike nga një sistem kompjuterik që mbart të këtilla të dhëna kompjuterike. Një shtet palë mund të kërkojë që vepra të jetë shkaktuar me qëllim të pandershëm ose në marrëdhënie me një sistem kompjuterik që është i lidhur me një sistem tjetër kompjuterik.

c) Interferenca e të dhënave (Neni 4)

Sipas nenit 4 të Konventës, çdo shtet palë duhet të adaptojë një legjislacion të tillë dhe masa të tjera, që mund të jenë të nevojshme të përcaktojnë si vepra penale sipas ligjit të brendshëm, kur kryhet me qëllim dëmtimi, fshirja, shtrembërimi, ndryshimi, apo shuarja e të dhënave kompjuterike pa të drejtë. Një shtet palë mund të rezervojë të drejtën të kërkojë që veprimi i përshkruar në paragrafin 1 të shkaktojë dëmtime serioze.

d) Interferenca e sistemeve (Neni 5)

Në dispozitën e nenit 5 të Konventës është parashikuar se çdo shtet palë do të adaptojë legjislacionin të tillë dhe masat të tjera që mund të jenë të nevojshme të përcaktojnë si vepra penale sipas ligjit të brendshëm, kur kryhet me qëllim, pengesat serioze pa të drejtë të funksionimit të një sistemi kompjuterik nëpërmjet futjes së të dhënave, transmetimit, dëmtimit, fshirjes, shtrembërimit, ndryshimit apo shuarjes të të dhënave kompjuterike.

e) Keqpërdorimi i pajisjeve (Neni 6)

Sipas kësaj dispozite të Konventës, çdo shtet palë do të adaptojë legjislacionin të tillë edhe masa të tjera, që mund të jenë të nevojshme që të përcaktojnë si vepra penale sipas ligjit të brendshëm, kur kryhet me qëllim dhe pa të drejtë:
a) prodhimin, shitjen, prokurimin për përdorim, importim, shpërndarje ose, përndryshe vënie në disponim të:
(i) një pajisjeje, që përmban në program kompjuterik, i projektuar apo i adaptuar kryesisht për qëllimin e kryerjes së njërës prej veprave penale të parashikuara, në përputhje me nenin 2 deri në 5;

(ii) një fjalëkalim kompjuterik, kod hyrjeje apo të dhëna të ngjashme, nëpërmjet të cilave mundësohet hyrja në tërësinë apo në ndonjë pjesë të një sistemi kompjuterik, me qëllimin që ai të përdoret për arsyen e kryerjes së një prej krimeve të përcaktuar në nenet 2 deri në 5; dhe
b) zotërimin e një pajisjeje të referuar në paragrafët (a) (1) ose (2) të mësipërm, me qëllimin që ai të përdoret për arsyen e kryerjes së një prej veprave penale të përcaktuar në nenet 2 deri në 5, një shtet palë mund të kërkojë me ligj që një numër i këtyre mjeteve të zotërohet përpara se të lindë përgjegjësia penale. Ky nen nuk duhet të interpretohet si ngarkesë e përgjegjësisë penale kur prodhimi, shitja, prokurimi për përdorim, importimi, shpërndarja apo, përndryshe, vënia në disponim ose zotërimi që referohet në paragrafin 1 të këtij neni nuk bëhet për qëllimet e kryerjes së një vepre penale, të përcaktuar në përputhje me nenet 2-5 të kësaj Konvente, sikurse dhe për testimin e autorizuar apo mbrojtjen e një sistemi kompjuterik. Çdo shtet palë mund të rezervojë të drejtën të mos aplikojë paragrafin 1 të kësaj Konvente, me kusht që rezervimi të mos përfshijë shitjen, shpërndarjen ose, përndryshe, vënien në disponim të çështjeve të referuara në paragrafin 1 (a) (ii).

4.4.2. Krimet e lidhura me kompjuterët

Vepra penale të natyrës së tillë konsiderohen:

a) Falsifikimet e lidhura me kompjuterët (Neni 7)
Në nenin 7 të Konventës është përcaktuar se çdo shtet palë do të adaptojë legjislacion të tillë dhe masa të tjera që mund të jenë të nevojshme të përcaktojnë si vepra penale sipas ligjit të brendshëm, kur kryhet me qëllim dhe pa të drejtë, futja e të dhënave, ndryshimi, fshirja, apo heqja e të dhënave kompjuterike që rezultojnë në të dhëna joautentike, me qëllim që ato të konsiderohen apo të veprohet mbi to për qëllime ligjore sikurse ato të ishin autentike, pavarësisht nëse të dhënat janë të lexueshme apo të kuptueshme direkt. Një shtet palë mund të kërkojë synimin për të mashtruar ose një synim të ngjashëm të pandershëm përpara lindjes së përgjegjësisë penale.

b) Mashtrimet e lidhura me kompjuterët (Neni 8)
Sipas kësaj dispozite të Konventës, çdo shtet palë do të adaptojë legjislacion të tillë dhe masa të tjera, që mund të jenë të nevojshme të përcaktojnë si vepra

penale sipas ligjit të brendshëm, kur kryhet me qëllim dhe pa të drejtë, shkaktimin e humbjes së pasurisë të një tjetri nëpërmjet:
a) futjes së ndonjë të dhëne, ndryshimin, fshirjen apo heqjen e të dhënave kompjuterike;
b) ndonjë interferencë me funksionimin e një sistemi kompjuterik, me synimin e pa ndershëm e mashtrues për prokurimin pa të drejtë të një përfitimi ekonomik për vete apo për një tjetër.

4.4.3. Veprat penale të lidhura me përmbajtjen

Vepër penale e natyrës së tillë konsiderohet "Veprat penale të lidhura me pornografinë e fëmijëve" e parashikuar në nenin 9 të Konventës. Në këtë dispozitë të Konventës është parashikuar se çdo shtet palë do të adaptojë legjislacion të tillë dhe masa të tjera, që mund të jenë të nevojshme të përcaktojnë si vepra penale sipas ligjit të brendshëm, kur kryhet me qëllim dhe pa të drejtë, në drejtimet e mëposhtme:
a) prodhimin e pornografisë me fëmijë, me qëllimin e shpërndarjes së tij nëpërmjet një sistemi kompjuterik;
b) ofrimi apo vënia në disponim e pornografisë për fëmijë nëpërmjet një sistemi kompjuterik;
c) shpërndarja apo transmetimi i pornografisë për fëmijë nëpërmjet një sistemi kompjuterik;
d) prokurimi i pornografisë për fëmijë nëpërmjet një sistemi kompjuterik për vete apo për një tjetër
e) zotërimi i pornografisë për fëmijë nëpërmjet një sistemi kompjuterik apo në një mjet të memorizimit të të dhënave kompjuterike.

Për qëllimin e kësaj vepre penale, shprehja **"pornografi me fëmijë"** do të përfshijë material pornografik që dallon nga ana pamore:

a) një minoren, i cili angazhohet në drejtime të qarta seksuale;
b) një person, i cili duket që është minoren, i angazhuar në drejtime të qarta seksuale;
c) imazhe realiste që prezantojnë një minoren të angazhuar në drejtime të qarta seksuale.

Kurse, termi **“minoren”** do të përfshijë të gjithë personat nën moshën 18 vjeç, mirëpo një Palë mundet, megjithatë, të kërkojë një limit moshe më të vogël, e cila nuk duhet të jetë më pak se 16 vjeç.

4.4.4 Veprat penale të lidhura me dhunimin e të drejtës së autorit dhe të drejtave të tjera të lidhura më to

Vepër penale e natyrës së tillë konsiderohet “Veprat penale të lidhura me dhunimin e të drejtës së autorit dhe të të drejtave të tjera të lidhura me të" e parashikuar në nenin 10 të Konventës. Në këtë dispozitë të Konventës është parashikuar se çdo shtet palë do të adaptojë legjislacion të tillë dhe masa të tjera, që mund të jenë të nevojshme të përcaktojnë si vepra penale sipas ligjit të brendshëm, dhunimin e të drejtës së autorit, sikurse është përcaktuar në ligjet e atij shteti në pajtim me detyrimet që ajo ka marrë sipas Aktit të Parisit të 24 korrikut 1971 të Konventës së Bernës për Mbrojtjen e Veprave Letrare dhe Artistike, Marrëveshjen në Aspektet e Lidhura me Tregtimin e të Drejtave të Pasurisë Intelektuale dhe të Traktatit ẂIPO të të drejtave të autorit, me përjashtim të të drejtave morale të kështilluara nga kjo Konventë, ku akte të tilla janë kryer me dëshirë në shkallë komerciale dhe nëpërmjet një sistemi kompjuterik. Çdo shtet palë do të adaptojë legjislacion të tillë dhe masa të tjera, që mund të jenë të nevojshme të përcaktojnë si vepra penale sipas ligjit të brendshëm dhunimin e të drejtave përkatëse, sikurse janë përcaktuar sipas ligjit të asaj Pale, në pajtim me detyrimet që kanë ndërmarrë nën Konventën Ndërkombëtare për Mbrojtjen e Ekzekutuesve, Prodhuesve të Fonogrameve dhe Organizatave të Transmetimit, bërë në Romë (Konventa e Romës), Marrëveshjes në Aspektet e Lidhura me Tregtimin e të drejtave të Pasurive të Intelektualëve dhe të Ekzekutimeve ẂIPO dhe Traktateve të Fonogrameve, me përjashtim të ndonjë të drejte morale të kështilluar nga konventa të tilla, ku akte të tilla janë kryer me dëshirë në shkallë komerciale dhe nëpërmjet sistemeve kompjuterike.

4.5 Dispozitat penale procedurale

Në kuadër të dispozitave penale procedurale janë parashikuar masat të cilat shtetet duhet që t’i ndërmarrin në kuptimin e harmonizimit të legjislacionit gjatë fazës së hetimeve dhe gjykimit të rasteve të krimeve kibernetike, por jo vetëm.

Në këtë kontekst, me dispozitat e kësaj pjese të Konventës, janë rregulluar këto çështje të rëndësishme:

1) Ruajtja e përshpejtuar e të dhënave kompjuterike të memorizuara;[89]
2) Ruajtja e përshpejtuar dhe hapja e pjesshme e të dhënave të trafikut;[90]
3) Porosia e prodhimit;[91]
4) Kërkimi dhe ngrirja e të dhënave kompjuterike të memorizuara;[92]
5) Mbledhja e të dhënave kompjuterike në kohën reale;[93]
6) Interceptimi i të dhënave të përmbajtjes[94] dhe
7) Kompetenca.[95]

4.6 Dispozitat që i referohen bashkëpunimit ndërkombëtar

Pjesa apo Kapitulli i III-të i Konventës përmban rregulla apo parime mbi bazën e të cilave shtetet palë duhet që të bashkëpunojnë në rastet që ndërlidhen me krimet kibernetike.

Në këtë drejtim, në nenin 23 të Konventës është parashikuar se shtetet palë bashkëpunojnë me njëra-tjetrën në pajtim me dispozitat e këtij Kapitulli, duke zbatuar instrumentet përkatëse ndërkombëtare mbi bashkëpunimin ndërkombëtar për çështjet penale, të masave për të cilat është rënë dakord mbi bazën e legjislacionit uniform ose reciprok dhe ligjeve vendase, në masën më të gjerë të mundur për qëllimin e hetimeve ose të gjykimeve në çështjet penale të lidhura me sistemet kompjuterike dhe të të dhënave ose për mbledhjen e provave elektronike të një vepre penale.

Bashkëpunimi i shteteve palë të Konventës duhet të mbështetet në këto aspekte:

[89] Neni 16 i Konventës.
[90] Neni 17 i Konventës.
[91] Neni 18 i Konventës.
[92] Neni 18 i Konventës.
[93] Neni 20 i Konventës.
[94] Neni 21 i Konventës.
[95] Neni 22 i Konventës.

1) Zbatimi i ekstradimit në mes të shteteve palë të Konventës për vepra penale të caktuara, duke e pasur në konsideratë edhe Konventën Evropiane mbi Ekstradimin[96] (ETS Nr.24);[97]
2) Ofrimi i ndihmës së ndërsjellë deri në masën më të gjerë të mundur për qëllimet e hetimeve ose gjykimeve të veprave penale që kanë të bëjnë me sistemet dhe të dhënat kompjuterike ose për mbledhjen e provave elektronike;[98]
3) Shkëmbimi i informacioneve spontane, brenda kufijve të ligjit të brendshëm dhe pa kërkesë paraprake, i cili është marrë në kuadrin e hetimeve, kur konsiderohet se dhënia e një informacioni të tillë mund ta ndihmojë shtetin tjetër në fillimin ose kryerjen e hetimeve ose gjykimeve në lidhje me veprat penale të përcaktuara në këtë Konventë;[99]
4) Realizimin e procedurave që kanë të bëjnë me kërkesat për ndihmë të ndërsjellë juridike, në mungesë të marrëveshjeve ndërkombëtare të zbatueshme;[100]
5) Ruajtja e menjëhershme e të dhënave të ruajtura në kompjuter, në rastet kur një shtet palë kërkon në shteti tjetër ruajtjen e përshpejtuar të të dhënave të regjistruara nëpërmjet një sistemi kompjuterik, i cili ndodhet brenda territorit të shtetit tjetër dhe në lidhje me të cilën shteti kërkues ka ndërmend të bëjë një kërkesë për ndihmë të ndërsjellë për të kërkuar hyrje të ngjashme, ngrirje, sigurim të ngjashëm ose hapje të të dhënave.[101]
6) Njoftimi i përshpejtuar i të dhënave të ruajtura mbi komunikimin;[102]
7) Ndihma e ndërsjellët në lidhje me hyrjen në të dhënat kompjuterike të regjistruara;[103]
8) Hyrja ndërkufitare në të dhënat e regjistruara në kompjuter me leje ose kur janë të hapura për publikun;[104]

[96] Linku i Konventës: https://rm.coe.int/1680064587
[97] Neni 24 i Konventës.
[98] Neni 25 i Konventës.
[99] Neni 26 i Konventës.
[100] Neni 27 i Konventës.
[101] Neni 29 i Konventës.
[102] Neni 30 i Konventës.
[103] Neni 31 i Konventës.
[104] Neni 32 i Konventës.

9) Ndihma e ndërsjellë në lidhje me marrjen brenda kohës reale të të dhënave;[105]
10) Ndihma e ndërsjellë në lidhje me interceptimin e të dhënave të përmbajtjes;[106] etj.

4.7 Protokolli shtesë mbi inkriminimin e akteve me natyrë raciste dhe ksenofobike të kryera nëpërmjet sistemeve kompjuterike

4.7.1 Shqyrtime të përgjithshme

Siç është theksuar edhe më parë, Protokolli shtesë mbi inkriminimin e akteve me natyrë raciste dhe ksenofobike të kryera nëpërmjet sistemeve kompjuterike (ETS.nr.189)[107] është nënshkruar në Strasburg të Francës, më 28.01.2003, ndërsa ka hyrë në fuqi më 01.03.2006.

Përmes këtij Protokolli u kërkohet shteteve palë të Konventës që të kriminalizojnë (inkriminojnë) shpërndarjen e materialeve raciste dhe ksenofobike përmes sistemeve kompjuterike, si dhe kërcënimet dhe fyerjet e motivuara nga racizmi ose ksenofobia.

Ky Protokoll përfshin një zgjerim të fushës së veprimit të Konventës mbi krimin kibernetikë, duke përfshirë dispozitat e saj thelbësore, procedurale dhe të bashkëpunimit ndërkombëtar, në mënyrë që të mbulojë edhe veprat e propagandës raciste ose ksenofobike.

Kështu, përveç harmonizimit të elementeve të së drejtës materiale të një sjelljeje të tillë, Protokolli synon të përmirësojë aftësinë e shteteve palë për të përdorur mjetet dhe rrugët e bashkëpunimit ndërkombëtar të përcaktuara në Konventë.

Sipas dispozitave të Protokollit, **"material racist dhe ksenofobik"** konsiderohet çdo material i shkruar, apo çdo imazh ose përfaqësim tjetër i mendimeve ose teorive, që favorizon, përhap ose nxit urrejtje, diskriminim ose dhunë kundër çdo individi ose grupi individësh, bazuar mbi racën, ngjyrën,

[105] Neni 33 i Konventës.
[106] Neni 34 i Konventës.
[107] Linku i Protokollit: https://rm.coe.int/168008160f

prejardhjen, origjinën kombëtare ose etnike, si edhe fenë, nëse përdoret si pretekst për çdonjërin nga këta faktorë.[108]

4.8 Veprat penale sipas Protokollit

Në këtë Protokoll janë parashikuar katër (4) vepra penale, të cilat si të tilla duhet që çdo shtet palë t'i parashoh edhe në legjislacionin e brendshëm.

	VEPRAT PENALE SIPAS PROTOKOLLIT
1.	**Shpërndarja e materialeve raciste dhe ksenofobike në një sistem kompjuterik**
2.	**Kërcënimi me motive racizmi dhe ksenofobie**
3.	**Fyerja me motive racizmi dhe ksenofobie**
4.	**Mohimi, minimizimi i konsiderueshëm, aprovimi ose justifikimi i gjenocidit ose krimeve kundër njerëzimit**

4.8.1 Shpërndarja e materialeve raciste dhe ksenofobike në një sistem kompjuterik[109]

Kjo vepër penale kryhet në rastet kur ndonjë person shpërndan ose në mënyra të ndryshme bënë publike nëpërmjet një sistemi kompjuterik të materialeve raciste dhe ksenofobike.

Veprimet e kryerjes së kësaj vepre penale janë të përcaktuara në mënyrë alternative dhe konsistojnë në:

- **shpërndarjen e materialeve raciste dhe ksenofobike ose**
- **bërjen publike në mënyra të ndryshme të materialeve raciste dhe ksenofobike.**

[108] Neni 2, paragrafi 1 i Protokollit.
[109] Neni 3 i Protokollit.

Veprimet kryerëse duhet që të kryhen përmes sistemit kompjuterik, ndërsa sistem kompjuterik do të thotë çdolloj pajisje apo grup i ndërlidhur ose pajisje të lidhura, një ose më shumë prej të cilave, vazhduese të një programi kryejnë procesime automatike të të dhënave.[110]

Kjo vepër penale mund të kryhet vetëm me dashje dhe me qëllim të shpërndarjes apo bërjes publike në ndonjë mënyrë tjetër të materialeve të lartcekura përmes sistemit kompjuterik.

Gjithashtu, në dispozitën e nenit 3, paragrafi 1 të Protokollit është parashikuar se për të ekzistuar kjo vepër penale si e tillë, duhet që veprimet kryerëse të ndërmerren "pa të drejtë" apo pa autorizim, përkatësisht në mënyrë të pa autorizuar.

Kryes i kësaj vepre penale mund të jetë çdo person, i cili përmes sistemit kompjuterik i ndërmerr veprimet e lartcekura.[111]

4.8.2 Kërcënimi me motive racizmi dhe ksenofobie

Vepra penale kërcënimi me motive racizmi dhe ksenofobie[112] përfshinë kërcënimin, nëpërmjet një sistemi kompjuterik, me kryerjen e një vepre të rëndë penale sipas parashikimit në ligjin e brendshëm, ndaj personave për arsyen se i përkasin një grupi, të dalluar nga raca, ngjyra, prejardhja, origjina kombëtare ose etnike, si dhe feja, kur përdoret si pretekst për njërin nga këta faktorë, ose të një grupi personash që dallohet nga njëra prej këtyre karakteristikave.

[110] Neni 1 i Konventës.
[111] Përndryshe, në paragrafin 2 të nenit të lartcekur është parashikuar se një shtet palë mund të rezervojë të drejtën për të mos ngarkuar me përgjegjësi penale një sjellje sipas paragrafit 1 të këtij neni, kur materiali në fjalë favorizon, përhap ose nxit diskriminimin që nuk lidhet me urrejtje ose dhunë, me kusht që të jenë të mundshme mjete të tjera të efektshme. Në ndryshim nga paragrafi 2, një palë mund të rezervojë të drejtën për të mos zbatuar paragrafin 1 në ato raste diskriminimi për të cilat në sajë të principeve të përcaktuara në sistemin ligjor kombëtar, nuk mund të parashikojë mjete të efektshme sipas përcaktimit të paragrafit 2.
[112] Neni 4 i Protokollit.

Pra, siç shihet kjo vepër penale, kryhet në rastet kur ndonjë person kërcënon apo kanos se do të kryejë ndonjë vepër të rëndë penale ndaj dy (2) kategorive të personave:

- **ndaj personave për arsyen se i përkasin një grupi, të dalluar nga raca, ngjyra, prejardhja, origjina kombëtare ose etnike, si dhe feja, kur përdoret si pretekst për njërin nga këta faktorë, ose**
- **të një grupi personash që dallohet nga njëra prej këtyre karakteristikave.**

Në dispozitën e nenit 4 të Protokollit, në të cilën është parashikuar kjo vepër penale, nuk është përcaktuar se çka konsiderohet "Vepër e rëndë penale", mirëpo një gjë e tillë, i është lënë në kompetencë shteteve palë që të përcaktojnë një gjë të tillë.[113]

Përmes kësaj vepre penale synohet që të mbrohen grupet e veçanta në një shoqëri, të cilët i përkasin një grupi, të dalluar nga raca, ngjyra, prejardhja, origjina kombëtare ose etnike, si dhe feja, kur përdoret si pretekst për njërin nga këta faktorë, ose të një grupi personash që dallohet nga njëra prej këtyre karakteristikave.

Kjo vepër penale konsiderohet e kryer me vetë faktin e ndërmarrjes së kërcënimit (kanosjes) për kryerjen e ndonjë vepre të rëndë penale ndaj kategorive të lartcekura të personave, përmes sistemit kompjuterik.

Për të ekzistuar kjo vepër penale si e tillë, duhet që veprimet kryerëse të ndërmerren "pa të drejtë" apo pa autorizim, përkatësisht në mënyrë të pa autorizuar.

Kjo vepër penale mund të kryhet vetëm me dashje dhe motive të racizmit dhe ksenofobisë ndaj grupeve të lartcekura.

[113] Në nenin 277/B të Ligjit Nr.08/L-188 për Plotësimin dhe Ndryshimin e Kodit Penal të Republikës së Kosovës, datë 26.10.2023 është parashikuar një vepër e tillë penale, që është emërtuar "Kanosja me motive racizmi dhe ksenofobie nëpërmjet sistemit kompjuterik". Sipas kësaj dispozite ligjore, këtë vepër penale e kryen "Kushdo që kanos seriozisht për vrasje ose plagosje të rëndë, një apo më shumë persona, nëpërmjet sistemeve kompjuterike, për shkak të përkatësisë etnike, kombësisë, racës apo fesë", për të cilën është parashikuar dënim burgim nga një (1) deri në tre (3) vjet". Pra, siç shihet legjislacioni jonë shprehjen "Vepër e rëndë penale" e ka specifikuar si "Vrasje ose plagosje e rëndë".

Gjithashtu, edhe kjo vepër penale mund të kryhet vetëm përmes sistemit kompjuterik dhe kryes i saj mund të jetë çdo person.

4.8.3 Fyerja me motive racizmi dhe ksenofobie

Vepra penale fyerja me motive racizmi dhe ksenofobie[114] përfshinë fyerjen, nëpërmjet një sistemi kompjuterik, publikisht të personave për arsyen se i përkasin një grupi, të dalluar nga raca, ngjyra, prejardhja, origjina kombëtare ose etnike, si dhe feja, kur përdoret si pretekst për njërin nga këta faktorë, ose të një grupi personash që dallohet nga njëra prej këtyre karakteristikave.[115]

Pra, siç shihet kjo vepër penale, kryhet në rastet kur ndonjë person i fyen përmes një sistemi kompjuterik, publikisht personat me arsyen si i përkasin dy (2) kategorive:

- **personave për arsyen se i përkasin një grupi, të dalluar nga raca, ngjyra, prejardhja, origjina kombëtare ose etnike, si dhe feja, kur përdoret si pretekst për njërin nga këta faktorë, ose**
- **të një grupi personash që dallohet nga njëra prej këtyre karakteristikave.**

Kjo vepër penale konsiderohet e kryer me vetë faktin e fyerjes së ndonjë personi me arsyen se i përkasin kategorive të lartcekura të personave, përmes sistemit kompjuterik.

Për të ekzistuar kjo vepër penale si e tillë, duhet që veprimet kryerëse të ndërmerren "pa të drejtë" apo pa autorizim, përkatësisht në mënyrë të pa autorizuar.

Kjo vepër penale mund të kryhet vetëm me dashje dhe motive të racizmit dhe ksenofobisë ndaj grupeve të lartcekura.

[114] Neni 5 i Protokollit.

[115] Përndryshe, në paragrafin 2 të nenit 5 të Protokollit është parashikuar se "Çdo shtet palë mund: i) të kërkojë që vepra penale e përmendur në paragrafin 1 të këtij neni të ketë efektin që personi ose grupi i personave të përmendur në paragrafin 1 t'i jenë ekspozuar urrejtjes, përçmimit ose vënies në lojë, ose ii) të rezervojë të drejtën për të mos zbatuar, plotësisht ose pjesërisht, paragrafin 1".

Gjithashtu, edhe kjo vepër penale mund të kryhet vetëm përmes sistemit kompjuterik dhe kryes i saj mund të jetë çdo person.

4.8.4 Mohimi, minimizimi i konsiderueshëm, aprovimi ose justifikimi i gjenocidit ose krimeve kundër njerëzimit

Veprën penale mohimi, minimizimi i konsiderueshëm, aprovimi ose justifikimi i gjenocidit ose krimeve kundër njerëzimit[116] përfshinë shpërndarjen ose ofrimin në publik nëpërmjet një sistemi kompjuterik të materialit që mohon, minimizon në mënyrë të konsiderueshme, aprovon ose justifikon akte që përbëjnë gjenocid ose krime kundër njerëzimit, sipas të drejtave ndërkombëtare dhe të njohura si të tilla me vendime të formës të prerë dhe të detyrueshme të Gjykatës Ndërkombëtare Ushtarake, të krijuara nga Marrëveshja e Londrës e 8 prillit 1945 ose të ndonjë gjykate tjetër ndërkombëtare, të krijuar me instrumentet përkatëse ndërkombëtare, juridiksioni i të cilave është njohur nga ky shtet palë.[117]

Veprimet e kryerjes së kësaj vepre penale janë të përcaktuara në mënyrë alternative dhe konsistojnë në:

- **shpërndarjen e materialit që mohon, minimizon në mënyrë të konsiderueshme, aprovon ose justifikon akte që përbëjnë gjenocid ose krime kundër njerëzimit, sipas të drejtave ndërkombëtare dhe të njohura si të tilla me vendime të formës të prerë dhe të detyrueshme të Gjykatës Ndërkombëtare Ushtarake, të krijuara nga Marrëveshja e Londrës e 8 prillit 1945 ose të ndonjë gjykate tjetër ndërkombëtare, të krijuar me instrumentet përkatëse ndërkombëtare, juridiksioni i të cilave është njohur nga ky shtet palë ose**
- **ofrimin në publik të këtyre materialeve.**

Veprimet kryerëse duhet që të kryhen përmes sistemit kompjuterik.

[116] Neni 6 i Protokollit.

[117] Përndryshe, në paragrafin 2 të nenit 6 të Protokollit është parashikuar se "Çdo shtet palë mund: i) të kërkojë që mohimi ose minimizimi i konsiderueshëm i përmendur në paragrafin 1 të këtij neni të jetë kryer për të nxitur urrejtjen, diskriminimin ose dhunën kundër një individi ose grupi individësh, bazuar mbi racën, ngjyrën prejardhjen, origjinën kombëtare ose etnike si dhe fenë, nëse përdoret si pretekst për një nga këta faktorë ose ii) të rezervojë të drejtën për të mos zbatuar, plotësisht ose pjesërisht, paragrafin 1".

Pasojë e kësaj vepre penale është mohimi, minimizimi i konsiderueshëm, aprovimi ose justifikimi i gjenocidit ose krimeve kundër njerëzimit.

Kjo vepër penale mund të kryhet vetëm me dashje dhe me qëllim të shpërndarjes apo ofrimit në publik të këtyre materialeve të lartcekura përmes sistemit kompjuterik.

Gjithashtu, në dispozitën e nenit 6, paragrafi 1 të Protokollit është parashikuar se për të ekzistuar kjo vepër penale si e tillë, duhet që veprimet kryerëse të ndërmerren "pa të drejtë" apo pa autorizim, përkatësisht në mënyrë të pa autorizuar.

Kryes i kësaj vepre penale mund të jetë çdo person, i cili përmes sistemit kompjuterik i ndërmerr veprimet e lartcekura.[118]

4.8.5 Inkriminimi i veprimeve tjera

Përveç katër (4) veprave penale të lartcekur, nga nenin 7 të Protokollit është parashikuar se çdo shtet palë duhet të ndërmerr masa legjislative, si dhe masa të tjera, të nevojshme për të përcaktuar si vepër penale sipas ligjit të brendshëm sjelljen e mëposhtme, kur kryhet me qëllim dhe pa të drejtë: dhënien e ndihmesës ("ndihma") ose shtytjen në kryerjen e njërës prej veprave penale të parashikuara në këtë protokoll, me synimin që një vepër e tillë të kryhet.

Të gjitha çështjet tjera që kanë të bëjnë me veprat penale të lartcekura, duke përfshirë këtu edhe dënimet e parashikuara për këto vepra penale, duhet që shtetet t'i rregullojnë me legjislacionet e tyre të brendshme.

[118] Përndryshe, në paragrafin 2 të nenit të lartcekur është parashikuar se një shtet palë mund të rezervojë të drejtën për të mos ngarkuar me përgjegjësi penale një sjellje sipas paragrafit 1 të këtij neni, kur materiali në fjalë favorizon, përhap ose nxit diskriminimin që nuk lidhet me urrejtje ose dhunë, me kusht që të jenë të mundshme mjete të tjera të efektshme. Në ndryshim nga paragrafi 2, një palë mund të rezervojë të drejtën për të mos zbatuar paragrafin 1 në ato raste diskriminimi për të cilat në sajë të principeve të përcaktuara në sistemin ligjor kombëtar, nuk mund të parashikojë mjete të efektshme sipas përcaktimit të paragrafit 2.

5. E DREJTA E PRIVATËSISË

5.1. Vështrime të përgjithshme

E drejta e privatësisë është një nga të drejtat themelore të njeriut. Edhe pse nocioni privatësisë në shikim të parë është i njohur për të gjithë, prapëseprapë nuk ekziston një përkufizim i përgjithshëm për privatësinë.[119]

Disa autorë janë të mendimit se nocioni "privatësisë është shumë i papërcaktuar, për shkak se ka shumë gjëra në jetën tonë të përditshme, të cilat nuk mund t'i ruajmë për vete dhe shumë gjëra të tjera që duam t'i ruajmë në privatësi".[120] Përndryshe, privatësia nënkupton qasje të kufizuar të tjerëve ndaj personit dhe ajo mbron individualitetin, pavarësinë, dinjitetin dhe integritetin e personit.

Përmes rregullimit juridik të konceptit për privatësi, shteti në fakt duhet të sigurojë respektimin e kësaj të drejte nga të gjithë personat tjerë, institucionet dhe nga vetë shteti.

GjEDNj-ja edhe pse është e mendimit se "jeta private është një koncept i gjerë për të cilin nuk mund të jepet përkufizim gjithëpërfshirës", përmes praktikës së saj gjyqësore, ka dhënë disa udhëzime dhe sqarime të caktuara në kuptim të rëndësisë dhe shtrirjes që ka privatësia, të cilat do të trajtohen në pika të përgjithshme në vijim të këtij punimi.

E rëndësishme të theksohet se qëndrimet lidhur me privatësinë mund të dallojnë dhe t'i nënshtrohen ndryshimeve, varësisht nga vendi, personi dhe periudha kohore. Kështu, privatësia mund të përjetohet ndryshe në shoqëri apo vende të caktuara dhe nga persona të ndryshëm, e gjithashtu, qëndrimet e tilla lidhur me privatësinë mund të evoluojnë "me kalimin e kohës". Me fjalë të tjera, nocioni i privatësisë është i natyrës "relative", që do të thotë se "nuk ka karakter absolut", për faktin se mund të dallon, varësisht nga vendi, personi dhe koha. Një veprim i caktuar në një shoqëri apo vend të caktuar mund të kualifikohet "privatësi", kurse në një shoqëri apo vend tjetër, nuk mund të

[119] MALIQI, AGIM; SHALA, AFRIM: *Masat e veçanta hetimore*, Prishtinë, 2025, fq. 31.
[120] *Doracak për zbatimin e masave për ndjekje të komunikimeve,* Shkup, Dhjetor, 2019, fq. 23.

trajtohet si i tillë. Apo, një veprim të caktuar, një person mund ta kualifikon si "privatësi", kurse personi tjetër nuk e konsideron të tillë. Dhe aspekti i tretë, se një veprim i caktuar, në një kohë të caktuar, mund të kualifikohet si "privatësi", kurse me kalimin e kohës, nuk konsiderohet i tillë, apo anasjelltas.[121]

5.2. Aspekte kushtetuese

E drejta e privatësisë konsiderohet një nga të drejtat më të rëndësishme të njeriut dhe për shkak të kësaj rëndësie, garantohet dhe mbrohet, jo vetëm me aktet juridike të brendshme të shteteve, por edhe me një sërë aktesh juridike ndërkombëtare.

Kjo e drejtë është ngritur edhe në rang të të drejtave kushtetuese, pasi që me Kushtetutën e Kosovës[122] është parashikuar dhe garantuar si e tillë. Kështu, në nenit 36 të Kushtetutës **("E Drejta e Privatësisë")** është parashikuar se "Çdokush gëzon të drejtën që t'i respektohet jeta private dhe familjare, pacenueshmëria e banesës dhe fshehtësia e korrespondencës, telefonisë dhe e komunikimeve të tjera".[123]

Përveç që është parashikuar si e drejtë themelore, gjithashtu në dispozitën e nenit 36 të Kushtetutës, janë parashikuar edhe rastet dhe situatat kur kjo e drejtë mund të kufizohet nga ana e autoriteteve publike/shtetërore. Kështu, në dispozitën e lartcekur kushtetuese është parashikuar se "Kontrollet e cilësdo banesë ose cilitdo objekt privat, që mendohet se janë të domosdoshme për hetimin e krimit, mund të bëhen vetëm deri në shkallën e domosdoshme dhe vetëm pas miratimit nga ana e gjykatës, pas shpjegimit të arsyeve pse një kontroll i tillë është i domosdoshëm. Shmangia nga kjo rregull lejohet, nëse është e domosdoshme për arrestim të ligjshëm, për mbledhjen e provave që ka rrezik të humbasin ose për mënjanimin e rrezikut të drejtpërdrejtë dhe serioz për njerëzit dhe për pasuri, në mënyrën e përcaktuar me ligj. Gjykata duhet që të miratoj veprimet e tilla në mënyrë retroaktive".[124]

[121] MALIQI, AGIM; SHALA, AFRIM: *Masat e veçanta hetimore*, fq. 32.
[122] Kushtetutën e Kosovës dhe amandamentet kushtetuese mund t'i gjeni në këtë link: **https://gzk.rks-gov.net/ActDetail.aspx?ActID=3702**
[123] Neni 36.1. i Kushtetutës së Kosovës.
[124] Neni 36.2. i Kushtetutës së Kosovës.

Gjithashtu, në këtë dispozitë kushtetuese, është parashikuar dhe garantuar "Fshehtësia e korrespondencës, telefonisë dhe komunikimit tjetër", ndërsa "kjo e drejtë mund të kufizohet vetëm përkohësisht, në bazë të vendimit gjyqësor, nëse është e domosdoshme për ecurinë e procedurës penale ose për mbrojtjen e vendit, në mënyrën e parashikuar me ligj."[125]

Përveç këtyre, në kuadër të dispozitës së nenit 36 të Kushtetutës, është parashikuar dhe garantuar edhe e drejta e mbrojtës së të dhënave personale, si pjesë përbërëse të drejtës në privatësi. Kështu, në dispozitën e nenit 36.4. të Kushtetutës është parashikuar se "Secili person gëzon të drejtën e mbrojtjes së të dhënave personale. Mbledhja, ruajtja, qasja, korrigjimi dhe shfrytëzimi i tyre rregullohet me ligj".

Siç u theksua më lart, me dispozitat e lartcekura kushtetuese, përveç që janë parashikuar dhe garantuar shumë aspekte të së drejtës në privatësi **("Pacenueshmëria e jetës private dhe familjare, banesës, korrespodencës, telefonisë dhe komunikimeve tjera")**, janë parashikuar edhe rastet kur autoritetet publike/shtetërore mund të kufizojnë këto të drejta, pas miratimit të veprimeve të tilla nga gjykata, nëse të njëjtat janë të domosdoshme, e që në fakt përbëjnë thelbin e disa prej masave të veçanta hetimore.

Përndryshe, në Kushtetutën e Kosovës është përvetësuar një koncept më i gjerë i të drejtës në privatësi, pasi që pjesë përbërëse e të drejtës në privatësi janë konsideruar edhe "të dhënat personale", si dhe "komunikimet tjera në përgjithësi".

Duke qenë një e drejtë e ngritur në rang të të drejtave kushtetuese, e drejta e privatësisë gëzon edhe mbrojtje institucionale dhe shtetërore. Në këtë drejtim, përveç mbrojtjes së rregullt gjyqësore dhe ligjore, vlen të theksohet se kjo e drejtë, në një mënyrë apo tjetër, mbrohet edhe përmes shumë mekanizmave institucional, ku në këtë drejtim, është e rëndësishme që të përmenden:

[125] Neni 36.3. i Kushtetutës së Kosovës.

Gjykata Kushtetuese e Kosovës,[126] Agjencia për Informim dhe Privatësi,[127] Institucioni i Avokatit të Popullit, etj.[128]

[126] Gjykata Kushtetuese (https://gjk-ks.org/) është autoriteti përfundimtar për interpretimin e Kushtetutës dhe të përputhshmërisë së ligjeve me Kushtetutën. Ajo siguron funksionalitetin e institucioneve të vendit në pajtim me Kushtetutën dhe garanton mbrojtjen e të drejtave dhe të lirive individuale të garantuara me Kushtetutë, në këtë rast edhe të së drejtës në privatësi, si e drejtë kushtetuese. Përderisa gjykatat e niveleve të tjera merren me shqyrtimin e fakteve, me verifikimin e ligjshmërisë së krijimit dhe të marrjes së provave, Gjykata Kushtetuese merret vetëm me kontrollin kushtetues të procesit të rregullt gjyqësor. Gjykata Kushtetuese shqyrton dhe merrë vendim për një çështje specifike vetëm pas parashtrimit të kërkesës nga palët e autorizuara me Kushtetutë. Sipas nenit 113, paragrafi 1 të Kushtetutës, Gjykata Kushtetuese vendos vetëm për rastet e ngritura para Gjykatës në mënyrë ligjore nga pala e autorizuar. Përndryshe, edhe individët janë të autorizuar të ngrenë shkeljet nga autoritetet publike të të drejtave dhe lirive të tyre individuale, të garantuara me Kushtetutë, mirëpo vetëm pasi të kenë shteruar të gjitha mjetet juridike të përcaktuara me ligj.

[127] Agjencia për Informim dhe Privatësi (https://aip.rks-gov.net/) është agjenci e pavarur e cila është përgjegjëse për mbikëqyrjen dhe zbatimin e Ligjit Nr.06/L-082 për Mbrojtjen e të Dhënave Personale dhe Ligjit NR.06/L-081 për Qasjen në Dokumente Publike në Republikën e Kosovës. Qëllimi kryesor i Agjencisë për Informim dhe Privatësi është mbrojtja e të drejtave dhe lirive themelore të personave fizik lidhur me përpunimin e të dhënave personale dhe garantimin e qasjes në dokumente publike, me qëllim të transparencës dhe llogaridhënies të institucioneve publike. Bazuar në legjislacionin e zbatueshëm, Agjencia ka të drejt të ndërmarrë masa dhe shqiptoj gjoba të cilat parashihen me ligjet e lartcekura. Mbrojtja e të Dhënave Personale në Kosovë garantohet me mbrojtje kushtetuese e ligjore, bazuar në Ligjin Nr. 06/L-082 për Mbrojtjen e të Dhënave Personale, rregullohet e drejta e privatësisë, respektimi i jetës private dhe familjare, pacenueshmëria e banesës, konfidencialiteti i korrespondencës, telefonisë, komunikimeve dhe mbrojtja e të dhënave personale. Si institucion përgjegjës për mbikëqyrjen dhe zbatimin e këtij ligji, Agjencia ka ndërmarrë një sërë iniciativash të cilat janë në funksion të avancimit të mbrojtjes të të dhënave personale, si pjesë përbërëse e të drejtës në privatësi, duke trajtuar një numër të konsiderueshëm të ankesave, duke shqiptuar gjoba për shkelje që kanë të bëjnë me mbrojtjen e të dhënave personale. Këshill dhënia e organeve publike dhe private, marrja e vendimeve për ankesat e paraqitura, inspektimet dhe kontrollet, informimi i publikut, promovimi dhe përkrahja e të drejtave themelore për mbrojtjen e të dhënave personale janë pjesë e fushë veprimtarisë kryesore të Agjencisë për Informim dhe Privatësi.

[128] Institucioni i Avokatit të Popullit (https://oik-rks.org/) paraqet mekanizmin ligjor për mbrojtjen, mbikëqyrjen dhe promovimin e të drejtave dhe lirive themelore të personave fizik dhe juridik. Në këtë drejtim, Institucioni i Avokatit të Popullit zhvillon hetime, jep rekomandime, publikon raporte, si dhe avokon për të drejtat dhe liritë e njeriut. Institucioni i Avokatit të Popullit ka mundësi të hapë hetime "Ex Officio" (pa ankesë individuale) për dyshimet e shkeljeve të të drejtave të njeriut. Po ashtu, ka për mision t'i vëzhgojë politikat dhe ligjet e miratuara nga autoritetet vendore, për të siguruar që ato të jenë në pajtim me standardet e të drejtave të njeriut dhe me kërkesat e qeverisjes së mirë. Institucioni i Avokatit të Popullit mund të paraqitet në cilësinë e mikut të gjykatës ***("Amicus Curiae")*** në proceset gjyqësore që kanë të bëjnë me të drejtat e njeriut, çështjet e barazisë dhe mbrojtjes nga diskriminimit. Institucioni i Avokatit të Popullit mund të iniciojë çështje në Gjykatën Kushtetuese në pajtim me Kushtetutën dhe Ligjin për Gjykatën Kushtetuese.

5.3. Aspekte ndërkombëtare

E drejta në privatësi, përveç tjerash, është trajtuar dhe rregulluar edhe me disa dokumente dhe instrumente juridike ndërkombëtare. Janë një sërë dokumentesh juridike ndërkombëtare të cilat e parashohin këtë të drejtë, si në nivel të Organizatës së Kombeve të Bashkuara, ashtu edhe në kuadër të organizatave të ndryshme kontinentale dhe rajonale.

Në radhë të parë, duhet përmendur se e drejta në privatësi është e parashikuar dhe garantuar edhe me nenin 12 të Deklaratës së Përgjithshme të të Drejtave të Njeriut,[129] në të cilën theksohet se "Asnjeri nuk duhet t'i nënshtrohet ndërhyrjes arbitrare në jetën, familjen, banesën ose korrespondencën vetjake, si dhe sulmeve kundër nderit dhe prestigjit personal. Gjithkush ka të drejtën të mbrohet nga ligji kundër ndërhyrjeve ose sulmeve të tilla".

Kurse, në nenin 16 të Konventës për të Drejtat e Fëmijës,[130] është parashikuar se "Asnjë fëmijë nuk duhet t'u nënshtrohet ndërhyrjeve arbitrare ose to paligjshme në jetën e tij private, në familje, në shtëpi ose në letërkëmbimin e tij, as cenimeve të kundërligjshme të nderit dhe reputacionit të tij. Fëmija ka të drejtën e mbrojtjes me ligj kundër ndërhyrjeve ose cenimeve të tilla".

Gjithashtu, edhe në nenin 17 të Paktit Ndërkombëtar për të Drejtat Civile dhe Politike[131] është parashikuar se "Askush nuk duhet të jetë objekt i ndërhyrjeve arbitrare ose të paligjshme në jetën e tij private, në familje, në shtëpi ose letërkëmbim, e as duhet t'i shkelet nderi dhe reputacioni i tij në mënyrë të

[129] Asambleja e Përgjithshme e Kombeve të Bashkuara më 10.12.1948, nxori dhe shpalli Deklaratën e Përgjithshme mbi të Drejtat e Njeriut. Pas këtij akti historik, Asambleja ftoi të gjitha shtetet anëtare që ta shpallin tekstin e Deklaratës dhe të përpiqen që të përhapet, paraqitet, lexohet dhe të shpjegohet, sidomos në shkolla dhe institucione të tjera edukuese, në të gjitha vendet dhe shtetet pa marrë parasysh statusin e tyre politik. Linku i Deklaratës: https://gzk.rks-gov.net/ActsByCategoryInstDetail.aspx?Index=3&InstID=1&CatID=127

[130] Konventa për të Drejtat e Fëmijës është miratuar dhe hapur për nënshkrim, për ratifikim dhe për aderim nga Asambleja e Përgjithshme me Rezolutën nr.44/25, datë 20.11.1989, ndërsa ka hyrë në fuqi më 02.09.1990. Linku i Konventës: https://gzk.rks-gov.net/ActsByCategoryInstDetail.aspx?Index=3&InstID=1&CatID=127

[131] Pakti Ndërkombëtar për të Drejtat Civile dhe Politike është miratuar dhe hapur për nënshkrim, për ratifikim dhe për aderim nga Asambleja e Përgjithshme me Rezolutën nr.2200 A (XXI), datë 16.12.1966, ndërsa ka hyrë në fuqi më 23.03.1976. Linku i Paktit Ndërkombëtar për të Drejtat Civile dhe Politike: https://gzk.rks-gov.net/ActsByCategoryInstDetail.aspx?Index=3&InstID=1&CatID=127

paligjshme. Secili ka të drejtë të ketë mbrojtje ligjore kundër ndërhyrjeve dhe shkeljeve të tilla".

Kurse, kjo e drejtë do të elaborohet në vijim, sipas KEDNj-së, duke qenë se ky dokument i rëndësishëm i Këshillit të Evropës është objekt i interpretimit të vazhdueshëm të GjEDNj-së dhe sipas nenit 22 të Kushtetutës së Kosovës ("Zbatimi i drejtpërdrejtë i Marrëveshjeve dhe Instrumenteve Ndërkombëtare"), zbatohet drejtpërdrejtë në Kosovë dhe ka prioritet, në rast konflikti, ndaj dispozitave e ligjeve dhe akteve të tjera të institucioneve publike.

KEDNj-ja, këtë të drejtë, e ka parashikuar në nenin 8, i cili përmban dy (2) paragrafë.

Neni 8 i KEDNj-së **("E drejta për respektimin e jetës private dhe familjare")** përcakton se "Çdokush ka të drejtën e respektimit të jetës së tij private dhe familjare, banesës dhe korrespondencës së tij. Autoriteti publik nuk mund të ndërhyjë në ushtrimin e kësaj të drejte, përveçse në shkallën e parashikuar nga ligji dhe kur është e nevojshme në një shoqëri demokratike, në interes të sigurisë publike, për mbrojtjen e rendit publik, shëndetit ose moralit ose për mbrojtjen e të drejtave dhe lirive të të tjerëve".

Nga kjo rezulton në mënyrë të qartë se neni 8 i KEDNj-së në ndahet në dy (2) pjesë:

1) Pjesa e parë përcakton të drejtat e privatësisë që i garantohen një personi nga shteti dhe atë: të drejtën për respektimin e jetës private, familjare, banesës dhe korrespondencës, kurse

2) Pjesa e dytë përcakton faktin se këto të drejta nuk janë absolute, pasi që legjitimon mundësinë që autoritetet publike/shtetërore të ndërhyjnë në të këto drejta, në rrethana të caktuara dhe atë: vetëm nëse ndërhyrjet janë në përputhje me ligjin dhe janë të nevojshme në një shoqëri demokratike, në ndjekje të një ose më shumë synimeve legjitime të paraqitura në këtë dispozitë, duke përfshirë këtu: interesin e sigurisë publike, mbrojtjen e rendit publik, shëndetit ose moralit ose mbrojtjen e të drejtave dhe lirive të të tjerëve.

Përndryshe, bazuar në paragrafin 1 të nenit 8 të KEDNj-së, e drejta në privatësi, në kuadrin e saj, përfshinë mbrojtjen e disa aspekteve të rëndësishme të njeriut, të cilat janë paraqitur në këtë tabelë.

	E DREJTA NË PRIVATËSI SIPAS KEDNJ-SË
I)	**Jeta private**
II)	**Jeta familjare**
III)	**Vendbanimi**
IV)	**Korrespodenca**

Ndërsa, në paragrafin 2 të nenit 8 të KEDNj-së, janë parashikuar garancitë për mosndërhyrje të autoriteteve publike/shtetërore në të drejtën për privatësi, por edhe kushtet dhe llojet e interesave të përgjithshme, për shkak të të cilave kjo e drejtë mund të kufizohet. Kështu, sipas kësaj dispozite, "Autoriteti publik nuk mund të ndërhyjë në ushtrimin e kësaj të drejte, përveçse në shkallën e parashikuar nga ligji dhe kur është e nevojshme në një shoqëri demokratike, në interes të sigurisë publike, për mbrojtjen e rendit publik, shëndetit ose moralit ose për mbrojtjen e të drejtave dhe lirive të të tjerëve". Bazuar në këtë dispozitë, shkalla e ndërhyrjes së autoriteteve publike/shtetërore në ushtrimin e kësaj të drejte duhet të përcaktohet në mënyrë të qartë me ligj.

Tjetër, aspekt i rëndësishëm në këtë drejtim, është që një gjë e tillë të **"vlerësohet"** si **"e nevojshme në një shoqëri demokratike"**.

Në vlerësimin e nevojës për një ndërhyrje të tillë, në shtetet e ndryshme zbatohet doktrina e ashtuquajtur **"margjinë e vlerësimit"**, e cila bazën e saj e ka në praktikën gjyqësore të GjEDNj-së. Kjo "margjinë e vlerësimit" përmban koncepte që janë analoge me parimin e subsidiaritetit dhe qëllimi i kësaj doktrine është t'i balancojë të drejtat individuale me interesat publike, si dhe të ndihmojë në zgjidhjen e çfarëdo lloj konflikti potencial.

Mirëpo, një doktrinë e tillë nuk mundëson fuqi të pakufizuar në vlerësimin e shteteve, ndërsa nga praktika gjyqësore e GJEDNj-së mund të konstatohet se gjykatat nacionale të drejtën diskrete më së shumti e përdorin për kushtin për domosdoshmëri, kur në rrethana konkrete ato vlerësojnë se zmbrapsja nga e drejta për privatësi është legjitime. Gjykata ka të drejtën diskrete ta vlerësojë domosdoshmërinë duke marrë parasysh specifikat e rastit konkret, si dhe në kontekst të ambientit të sigurisë në vend, por edhe domosdoshmërisë nga aspekti i vlerave morale, normave zakonore, politike dhe rrethanave të tjera.[132]

Përndryshe, duke u bazuar në nenin 8 të KEDNJ-së, mund të konstatojmë se e drejta në privatësi nuk është absolute dhe mund të kufizohet në llogari të disa interesave të tjera më madhore të shoqërisë ose të të drejtave tjera të individëve.

Në këtë mënyrë, autoritetet publike/shtetërore mund të kufizojnë të drejtën në privatësi, me synimin që kjo shërben:

I) Për interes të sigurisë publike;
II) Për mbrojtjen e rendit publik, shëndetit ose moralit ose
III) Për mbrojtjen e të drejtave dhe lirive të të tjerëve.

Janë këto tre (3) synime, të cilat mund të shërbejnë si bazë e ndërhyrjes së autoriteteve publike/shtetërore në të drejtën në privatësi. Përndryshe, "e drejta diskrete e shtetit" për të ndërhyrë në privatësinë e personit varet nga konteksti i rrethanave, si dhe nga tradita, politikat dhe praktikat e ndryshme në shtete të ndryshme.

5.4. Praktika gjyqësore e GjEDNj-së

Fillimisht duhet theksuar se procedura pranë GjEDNj-së në rastet që ndërlidhen me nenin 8 të KEDNj-së ("E drejta për respektimin e jetës private dhe familjare") kalon nëpër dy (2) faza:

1) FAZA E PARË përfshinë trajtimin e rastit në kuptimin nëse e drejta për të cilën është iniciuar rasti është e përfshirë me nenin 8, paragrafi 1 të

[132] Doracak për zbatimin e masave për ndjekje të komunikimeve, fq. 30.

KEDNj-së, përkatësisht nëse kjo e drejtë e pretenduar garantohet sipas këtij neni. Nëse e drejta e pretenduar nga një individ nuk është e mbuluar me nenin 8, paragrafi 1 të KEDNj-së, atëherë rasti përfundon në këtë fazë, kurse në situatat kur e drejta e pretenduar nga ndonjë individ mbulohet nga kjo dispozitë e KEDNj-së, atëherë, procedura do të vazhdon me fazën e dytë të vlerësimit.[133]

2) FAZA E DYTË përfshinë trajtimin e rastit në kuptimin e përgjigjes në këto pyetje:

1. A ka ndodhur një ndërhyrje në të drejtën e nenit 8 të KEDNj-së?
2. Nëse po,
2.1. A është ajo në përputhje me ligjin?
2.2. A ndjek një synim legjitim, të përcaktuar në nenin 8, paragrafi 2 të KEDNj-së?
2.3. A është e nevojshme në një shoqëri demokratike?

Në këtë mënyrë, zbatimi i masave të veçanta hetimore në një mënyrë përbënë ndërhyrje në të drejtën e garantuar me nenin 8, paragrafi 1 të KEDNj-së, por jo domosdoshmërisht në çdo rast. Kjo për faktin se "E drejta për respektimin e jetës private dhe familjare" nga neni 8, paragrafi 1 të KEDNj-së nuk është e drejtë absolute dhe se autoritetet publike/shtetërore e kanë mundësinë e ndërhyrjes në ushtrimin e kësaj të drejte, nën rrethanat dhe kushtet e përcaktuara në paragrafin 2 të të njëjtit nen, siç është theksuar edhe më parë.

Kështu, referuar nenit 8, paragrafi 2 të KEDNj-së, autoritetet publike/shtetërore mund të ndërhyjnë në ushtrimin e kësaj të drejte, nëse:

1) Nëse ndërhyrjet e tilla janë në pajtim me ligjin;
2) Këto ndërhyrje janë të nevojshme në ndjekje të një ose më shumë synimeve legjitime të paraqitura në këtë dispozitë, duke përfshirë këtu:
   - interesin e sigurisë publike,
   - mbrojtjen e rendit publik, shëndetit ose moralit ose
   - mbrojtjen e të drejtave dhe lirive të të tjerëve dhe

[133] KILKELLY, URSULA: *E drejta për respektimin e jetës private dhe familjare,* Një udhëzues për zbatimin e Nenit 8 të Konventës Evropiane për të Drejtat e Njeriut, Manualet e të drejtave të njeriut, Nr. 1, Strasbourg, 2003, fq.8-9.

3) Se këto ndërhyrje janë të nevojshme në një shoqëri demokratike.

Sigurisht, se kriteri i parë që GjEDNj-ja ka në konsideratë për të vlerësuar nëse zbatimi i masave të veçanta hetimore përbënë ndërhyrje në të drejtën e garantuar me nenin 8, paragrafi 1 të KEDNj-së është nëse këto "ndërhyrje" me zbatimin e këtyre masave janë **"në pajtim apo përputhje me ligjin"**.

Shprehjen "ligj", GjEDNJ-ja e konsideron çfarëdo lloj kornize ligjore të shtetit, me të cilat parashihen masat e veçanta hetimore. Në këtë aspekt, nëse shteti nuk posedon një kornizë të tillë ligjore, kjo do të thotë se bëhet fjalë për ndërhyrje në të drejtën e garantuar me nenin 8 të KEDNj-së, përkatësisht shkelje të kësaj të drejte.[134] Pra, GjEDNj-ja kërkon që masat e veçanta hetimore të gjejnë mbështetje në dispozita përkatëse ligjore, të cilat autorizojnë autoritetet publike/shtetërore që të ndërhyjnë në të drejtën e garantuar sipas nenit 8, paragrafi 1 të KEDNj-së dhe se këto dispozita ligjore duhet të jenë specifike dhe të qasshme.[135]

Në këtë kontekst, ligji apo dispozitat ligjore duhet të jenë mjaftueshëm të qartë në termat e tyre, për t'iu dhënë individëve mundësi që të njihen me rrethanat dhe kushtet nën të cilat autoritetet publike/shtetërore mund të përdorin masat e veçanta hetimore.[136]

GjEDNj-ja ka sqaruar se në lidhje me masat e veçanta hetimore, dispozitat ligjore duhet të përcaktojnë në mënyrë të qartë kategoritë e individëve që mund të shënjestrohen, llojin e veprave penale për të cilat mund të përdoren

[134] Në çështjen *"Khan kundër Mbretërisë së Bashkuar"*, GjEDNj-ja u shpreh se përdorimi i një mjeti të fshehtë për përgjim nga autoritetet e Mbretërisë së Bashkuar nuk ishte në pajtim me ligjin brenda kuptimit të Nenit 8, sepse nuk kishte një sistem statutor që të ligjëronte përdorimin e mjeteve të tilla, që drejtohej nga Udhëzuesit e Zyrës së Brendshme, udhëzimet e të cilës nuk ishin as të detyrueshme, as të aksesueshme drejtpërdrejt për publikun. Sipas KILKELLY, URSULA: Vepra e cituar, fq. 27.

[135] Rasti *"Silver dhe të tjerët kundër Mbretërisë së Bashkuar"*, nr.5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, aktgjykimi i datës 25.03.1983, paragrafët 111-119.

[136] Rasti *"Kopp kundër Zvicrrës"*, nr.13/1997/797/1000, aktgjykimi i datës 25.03.1998, paragrafët 62-72; Rasti *"Taylor-Sabori kundër Mbretërisë së Bashkuar"*, nr.47114/99, aktgjykimi i datës 22.10.2022, paragrafët 16-19.

këto masa, kohëzgjatja e tyre dhe mënyrën e shkatërrimit të të dhënave që janë siguruar përmes këtyre masave.[137]

Në rastin *"Kruslin kundër Francës"*[138], GjEDNj-ja ka konstatuar shkelje të drejtës për respektimin e jetës private dhe familjare", nga neni 8, paragrafi 1 i KEDNj-së, që kishte të bënte me përgjimet telefonike, për shkak të këtyre mangësive ligjore në procedurat franceze:

- nuk kishte përcaktim të kategorive të personave, telefonat e të cilëve mund të përgjoheshin;
- nuk kishte përcaktim të kategorive të veprave penale që do të justifikonin përgjimin e telefonit;
- nuk kishte asnjë kufizim në kohëzgjatjen e masave të veçanta hetimore të kësaj natyre;
- nuk ishin parashikuar procedura për raportimin në lidhje me bisedat e përgjuara;
- nuk ka pasur kontroll gjyqësor;
- nuk kishte asnjë dispozitë ligjore për shqyrtim nga ana e mbrojtjes dhe
- nuk kishte asnjë dispozitë ligjore për shkatërrimin e materialeve, në rastet kur personi shpallet i pafajshëm apo lirohet nga akuza.

Kurse, në rastin *"Klass dhe të tjerët kundër Gjermanisë"*, GjEDNj-ja konstatoi se masat e veçanta hetimore janë instrument i domosdoshëm i organeve për ndjekje penale në shoqëritë bashkëkohore demokratike, si mjet adekuat për parandalim të kriminalitetit, mirëpo nëse zbatimi i tyre nuk është i rregulluar me ligj, ekziston rrezik për rrënim ose madje shkatërrim të demokracisë.[139]

Një tjetër aspekt i rëndësishëm për GjEDNj-në është edhe i ashtuquajturi "kushti i parashikueshmërisë". Në këtë drejtim, ligji apo dispozitat përkatëse ligjore me anë të të cilave parashihet masat e veçanta hetimore duhet të jenë të qasshme për personat e interesuar, dhe të jenë të formuluar me saktësi të

[137] Rasti *"Huvig kundër Francës"*, nr.11105/84, aktgjykimi i datës 24.04.1990, paragrafët 18-20.
[138] Rasti *"Kruslin kundër Francës"*, nr. 11801/85, aktgjykimi i datës 24.07.1990, paragrafët 28-36.
[139] Rasti *"Klass dhe të tjerët kundër Gjermanisë",* nr.5029/71, aktgjykimi i datës 06.09.1978, paragrafët 39-60.

mjaftueshme për të mundësuar që personat e tillë të parashikojnë deri në njëfarë mase se sa kanë qenë të arsyeshme masat në bazë të rrethanave, pasojat e të cilave kanë shkaktuar një veprim të caktuar.[140]

Përndryshe, të gjitha këto që u theksuan më lart, ndërlidhen edhe me parimin e ligjshmërisë, që konsiderohet parimi bazë dhe themelor në lidhje masat e veçanta hetimore.

Në rastet kur një ndërhyrje rezulton se është në pajtim me ligjin, atëherë GjEDNj-ja do të vazhdojë, për të shqyrtuar nëse kjo ndërhyrje ndjek një synim legjitim sipas nenit 8, paragrafi 2 të KEDNj-së.

Në këtë drejtim, njëra prej çështjeve që trajtohet ka të bëjë me pyetjen se **"A është ndërhyrja e nevojshme në një shoqëri demokratike?"**, ndërsa kjo ndërlidhet edhe me parimin e proporcionalitetit, i cili parim përcakton se të drejtat e njeriut nuk janë absolute dhe se ushtrimi i të drejtave të një individi gjithmonë duhet të kontrollohet nga një interes më i gjerë i publikut. Përndryshe, vendimi nëse ndërhyrja është e nevojshme dhe në proporcion me qëllimin që ajo ndjek është shpesh një proces kompleks i cili përfshin marrjen në konsideratë të një sërë faktorësh. Ato përfshijnë interesin që duhet mbrojtur nga ndërhyrja, rëndësinë e ndërhyrjes dhe nevojës shoqërore imperative që shteti ka si synim të përmbushë.[141]

Në rastin *"Sunday Times kundër Mbretërisë së Bashkuar"*,[142] GjEDNj-ja theksoi se: "Me termin "e nevojshme në një shoqëri demokratike" nënkuptohet që ndërhyrja në jetën private të individit të jetë veprim që mbështetet në një nevojë urgjente shoqërore. Nuk mjafton që kjo ndërhyrje të jetë vetëm e duhur dhe e arsyeshme, por njëkohësisht shteti duhet të tregojë se ekziston marrëdhënie proporcionaliteti në mes qëllimit që duhet të arrihet dhe mjetet që përdoren për atë qëllim".

Kurse, me termin proporcionalitet nënkuptohen dy (2) momente:

[140] KILKELLY, URSULA: Vepra e cituar, fq. 27.
[141] KILKELLY, URSULA: Vepra e cituar, fq. 33.
[142] Rasti *"Sunday Times kundër Mbretërisë së Bashkuar"*, nr.6538/74, aktgjykimi i datës 26.04.1979, paragrafët 58-68.

I. ***Së pari,*** proprocionaliteti ndërmjet qëllimit të masave dhe mjeteve që përdoren për atë qëllim dhe
II. ***Së dyti,*** proporcionaliteti ndërmjet interesit të përgjithshëm të shoqërisë dhe mbrojtjes së të drejtave të individit.[143]

Gjatë përcaktimit të proporcionalitetit, shqyrtohen rrethanat se a është ndonjë ndërhyrje e caktuar në jetën private të qytetarëve tepër e bezdisshme ose imponon ngarkesë të tepërt për individë të caktuar, e po ashtu merret parasysh se cili është interesi i shoqërisë. Shteti duhet të vërtetojë se ndërhyrja në jetën private të individit nuk ka qenë më e madhe se që ka qenë e nevojshme. Në kontekst të kësaj, në rastet kur ndërhyrja në jetën private të individit është e karakterit imponues ose kur informatat që i mbledh shteti janë të një karakteri të ndjeshëm, veprimi duhet të argumentohet fuqishëm (Rasti *"Kopp kundër Zvicrrës"*, nr.13/1997/ 797/1000, aktgjykimi i datës 25.03.1998).

Po ashtu, faktorët që duhen marrë parasysh në përcaktimin nëse një ndërhyrje apo masë e veçantë hetimore është proporcionale me qëllimin e ndjekur, sipas GjEDNj-së përfshijnë:

- nëse janë paraqitur arsye relevante dhe të mjaftueshme në mbështetje të masës së veçantë hetimore;
- nëse ekzistonte një masë alternative më pak kufizuese;
- nëse është zbatuar një procedurë e rregullt me rastin e marrjes së vendimit për caktimin e masave të veçanta hetimore;
- nëse ekzistojnë masa mbrojtëse adekuate kundër arbitraritetit, etj.

[143] *Doracak për zbatimin e masave për ndjekje të komunikimeve,* fq. 36 - 37.

BIBLIOGRAFIA

I. Libra dhe botime tjera

ALEXANDER, LARRY; FERZAN KIMBERLY KESSLER: *Crime and Culpability, A Theory of Criminal Law*, Cambridge,2 2009.

BIANKU, LEDI; KUMBARO, ODETA: *Jurisprudenca e Gjykatës së Strasburgut*, Botimi i katërt, Strasburg, 2017.

BOHLANDER, MICHAEL: *Principles of German Criminal Law*, Oxford and Portland, Oregon, 2009.

DRESSLER, JOHN: *Criminal Law*, Third Edition, Santa Monica, 1996.

ELEZI, ISMET; KAÇUPI, SKËNDER; HAXHIA, MAKSIM: *Komentar i Kodit Penal të Republikës së Shqipërisë*, Pjesa e Përgjithshme, Tiranë, 2004.

ELLIOT, CATHERINE; QUIN, FRANCES: *Criminal Law*, Third Edition,"Pearson Education", Harlow, 2000.

FLETCHER, GEORGE: *Basic Concepts of Criminal Law*, Oxford University Press, New York- Oxford, 1998.

GASHI, REXHEP: *Krimi i organizuar*, Prishtinë, 2023.

HAJDARI, AZEM: *Procedura penale, Komentar*, Prishtinë, 2009.

HALL, E. DANIEL: . *Criminal Law and Procedure*, Fifth Edition, Delmar Cengage, NewYork, 2009

HALLEVY, GABRIEL: *A Modern Treatise on the Principle of Legality in Criminal Law*, Sprinder, London, 2010.

HALPIN, ANDREV: *Definition in the Criminal Law*, Hart Publishing, Oxford, 2004.

HERRING, JONATHAN: *Criminal law*, Third Edition, "Palgrave Maxmillan", Bristol, 2002.
E drejta penale, Teori, kazuse dhe materiale, Botim V/Volumi I, Tiranë, Tetor 2013
Criminal Law, The Basic, Routledge, Abingdon, 2010

HASANI, FEJZULLAH: *Vrasja në gjendje të tronditjes së fortë mendore*, Prishtinë, 2019.

ISMAILI, HILMI; SEJDIU, FATMIR: *Historia e përgjithshme e shtetit dhe e së drejtës*, Prishtinë, 2000.

KAMBOVSKI, VLLADO: *E drejta penale*, Pjesa e përgjithshme, Shkup, 2007.

KAPLAN, JOHN: *Criminal Law*, Third Edition, Boston, 1996.

KASSAB, HANNA; ROSEN, JONATHAN: *Illicit Markets, Organized Crime, and Global Security*, 2019.

KILKELLY, URSULA, *E drejta për respektimin e jetës private dhe familjare*, Një udhëzues për zbatimin e Nenit 8 të Konventës Evropiane për të Drejtat e Njeriut, Manualet e të drejtave të njeriut, Nr. 1, Strasbourg, 2003.

LATIFI, VESEL; DEMOLLI, HAKI: *Kriminalistika - zbulimi dhe të provuarit e krimit,* Prishtinë, 2019.

LUARASI, ALEKS: *Kodi penal me praktikë gjyqësore*, Tiranë, 2003.

MALIQI, AGIM; SHALA, AFRIM: *Përmbledhje me raste nga praktika gjyqësore lidhur me armët e zjarrit,* *Volume 1* | 2020-2024, E drejta penale dhe praktika gjyqësore në Kosovë, Prishtinë, 2024.
Veprat penale të armëve, Komentar, *Prishtinë, 2024.*
Masat e veçanta hetimore, Aspekte juridike dhe praktike, Prishtinë, 2024.

MOLAN, MIKE: *Cases and materials on criminal law*, Fourth Edition, London and New York, 2008.

JEAN, PRADEL; CORSTENS, GEERT; VERMEULEN, GERT: *E drejta penale evropiane*, Tiranë, 2009.

SAHITI, EJUP; MURATI, REXHEP: *E drejta e procedurës penale*, Prishtinë, 2016.

SALIHU, ISMET: *Kodi Penal i Republikës së Kosovës,* Prishtinë, 2016.
E drejta penale, Pjesa e përgjithshme, Prishtinë, 2015.
E drejta penale, Pjesa e posaçme, Prishtinë, 2014.

SALIHU, ISMET; ZHITIJA, HILMI; HASANI, FEJZULLAH: *Kodi Penal i Republikës së Kosovës, Komentar*, Botimi I, 2014, Prishtinë.

SAMAHA, JOEL: *Criminal Law*, Tenth Edition, wadsworth, Cengage Learning, 2011.

SHALA, AFRIM: *Kompetencat e gjyqtarit të procedurës paraprake sipas Kodit të Procedurës Penale të Kosovës,* Revista *"Justicia"*, Instituti Gjyqësor i Kosovës, Prishtinë, 2009.
Ankesa kundër aktgjykimit në procedurën penale të Republikës së Kosovës, Prishtinë, 2010.
Pjesa e posaçme e së drejtës penale me raste nga praktika gjyqësore, Gjilan, 2010.
Përmbledhje e ligjëratave nga "E drejta penale I", Gjilan, 2011.

Sistemet kryesore të caktimit të dënimit me gjobë në të drejtën penale bashkëkohore, Revista "E drejta", Nr.2-2011, Fakulteti Juridik i Universitetit të Prishtinës, Prishtinë, 2011, faqe 129-136.
Roli i shërbimit sprovues në shqiptimin dhe mbikëqyrjen e Ekzekutimit të dënimeve alternative, Gjilan, 2011.
Veprat penale kundër mjedisit, kafshëve, bimëve dhe objekteve Kulturore sipas Kodit Penal të Republikës së Kosovës, Revista "Avokatura", nr.14, Oda e Avokatëve të Kosovës, Prishtinë, 2012, faqe 15-31.
Organizimi i sistemit gjyqësor në Republikën e Kosovës sipas Ligjit për gjykatat, Revista shkencore "Norma", Gjilan, 2012.
Kodi i Drejtësisë për të Mitur, Moduli Trajnues, Instituti Gjyqësor i Kosovës, Prishtinë, 2012, (bashkautor).
Veprat penale kundër të drejtave të votimit, "Opinio Juris", Revistë shkencore juridike, Akademia e Drejtësisë, Viti I, nr.1, Prishtinë, 2015.
Doracaku për procedurë penale, Prishtinë, 2015, (bashkautor).
Disa aspekte praktike të seancës për vërtetimin e fakteve relevante lidhur me dënimin, Revista shkencore juridike "*Opinio Juris*", Akademia e Drejtësisë, Viti II, nr.2, Prishtinë, 2016.
Shqyrtimi fillestar, shqyrtimi i dytë dhe shqyrtimi gjyqësor, Akademia e Drejtësisë, Prishtinë, 2018.
Modulet e trajnimit bazik për bashkëpunëtorët profesional (Penale-materiale dhe procedurale), Prishtinë, Prishtinë, 2021, (bashkautor).
Shqyrtimi gjyqësor dhe gjykimi në mungesë, Akademia e Drejtësisë, Prishtinë, 2012.
Bashkëpunimi në kryerjen e veprës penale, Akademia e Drejtësisë, Prishtinë, 2023 (bashkautor).
Hyrje në të drejtën penale, Botimi i katërt, Prishtinë, 2023.
Përmbledhje nga praktika e Gjykatës Supreme të Kosovës në çështjet penale dhe civile, Prishtinë, 2023 (kontribuues).
Vendime të përzgjedhura të Gjykatës Supreme të Kosovës, Prishtinë, 2023, (kontribuues).
Mbrojtja e mjedisit përmes të drejtës penale, Tiranë, 2023.

SHALA, AFRIM;
ADEMI, BURIM;
KUQI, RAMIZ: *Drejtësia Mjedisore*, Prishtinë, 2024.

II. Publikime tjera

Udhëzues për politikën ndëshkimore, Botimi 1, Gjykata Supreme e Republikës së Kosovës, Prishtinë, 2018.
Udhëzues i Përgjithshëm për Matjen e Dënimit II, Gjykata Supreme e Republikës së Kosovës, Prishtinë, 2024.

Përmbledhje e ligjeve penale, Instituti i Kërkimeve Juridike dhe Shoqërore, Fakulteti Juridik, Prishtinë, 1979.
Trajnim për krimin kibernetik për gjyqtarë dhe prokurorë: një koncept, Projekti për Krimin Kibernetik dhe Rrjeti i Lisbonës, Këshilli i Evropës, Departamenti i Shoqërisë së Informacionit dhe Aksionit kundër Krimit Drejtoria e Përgjithshme e të Drejtave të Njeriut dhe Çështjeve Ligjore, Strasburg, 2009;
Introduction to Cybersecurity Governance - A Tool for Members of Parliament, Geneva Centre for Security Sector Governance;
Koncept Dokumenti për Parandalimin dhe Luftimin e Krimit Kribernetik;
Doracak për zbatimin e masave për ndjekje të komunikimeve, Shkup, Dhjetor, 2019.

III. Akte juridike (vendore dhe ndërkombëtare)

Kodi Penal i Republikës së Kosovës;
Ligji për Plotësimin dhe Ndryshimin e Kodit Penal të Republikës së Kosovës;
Kodi i Procedurës Penale;
Kushtetuta e Republikës së Kosovës;
Ligji Penal i Krahinës Socialiste Autonome të Kosovës;
Kodi Penal i Republikës së Shqipërisë;
Kushtetuta e Republikës së Shqipërisë;
Konventa Evropiane për Mbrojtjen e të Drejtave të Njeriut dhe Lirive Themelore;
Deklarata e Përgjithshme për të Drejtat e Njeriut;
Konventa e Këshillit të Evropës mbi Krimin Kibernetik;
Protokolli shtesë të Konventës së Budapestit mbi inkriminimin e akteve me natyrë raciste dhe ksenofobike të kryera nëpërmjet sistemeve kompjuterike;
Protokolli i Konventës mbi Krimin Kibernetik për bashkëpunimin e zgjeruar dhe zbulimin e provave elektronike;
Direktiva (BE) 2013/40 e Parlamentit Evropian dhe Këshillit, datë 12.08.2013 për Sulmet kundër Sistemeve të Informacionit, që zëvendëson Vendimin Kornizë të Këshillit 2005/222/JHA, si dhe Direktivën (BE) 2016/1148 të Parlamentit Evropian dhe Këshillit, datë 06.07.2016 për Masat e Sigurisë së Sistemeve të Rrjetit dhe Informacionit;
Marrëveshja e Stabilizim Asociimit me BE-në;
Konventa Evropiane mbi Ekstradimin;
Konventa për të Drejtat e Fëmijës;
Pakti Ndërkombëtar për të Drejtat Civile dhe Politike;
Ligji për Parandalimin dhe Luftimin e Krimit Kibernetik (i shfuqizuar);
Ligji për Sigurinë Kibernetike;
Ligji për Përgjimin e Komunikimeve Elektronike;
Ligji për Mbrojtjen e të Dhënave Personale;
Ligji për Qasjen në Dokumente Publike.

IV. Jurisprudenca e GjEDNj-së

"Khan kundër Mbretërisë së Bashkuar";

"Silver dhe të tjerët kundër Mbretërisë së Bashkuar";
"Kopp kundër Zvicrrës";
"Taylor-Sabori kundër Mbretërisë së Bashkuar";
"Huvig kundër Francës";
"Kruslin kundër Francës";
"Klass dhe *të tjerët kundër Gjermanisë";*
"Sunday Times kundër Mbretërisë së Bashkuar".

KAPITULLI IV

KUFIZIMET SIPAS AKTEVE JURIDIKE NDËRKOMBËTARE DHE KUSHTETUTES, NË RAPORT ME TË DREJTËN E PRIVATËSISË

Burim Ademi, Gjyqtar në Gjykatën Supreme të Kosovës

Burim Ademi, Gjyqtar në Gjykatën Supreme të Kosovës

1. KUFIZIMET SIPAS AKTEVE JURIDIKE NDËRKOMBËTARE DHE KUSHTETUTES, NË RAPORT ME TË DREJTËN E PRIVATËSISË.

1.1 Shqyrtime të përgjithshme

E drejta e privatësisë është një nga të drejtat që garantohet me akte ndërkombëtare me dispozitat kushtetuese dhe me dispozitat ligjore. Koncepti i mbrojtjes së privatësisë ka si qëllim ruajtjen e jetës private dhe familjare. Më konkretisht e drejta e privatësisë synon që ruajtja e jetës private dhe familjare të bëhet përmes disa aspekteve që mund të qojnë në cenimin e të drejtës private. Më konkretisht të drejtën e privatësisë në jetën private dhe familjare përbën mbrojtje efektive, kur gëzohen disa kufizime që krijohen, në pronë, në korrespodencë – letërkëmbim apo komunikime tjera. Në këtë kuptim ruajtja e të drejtës së privatësisë, përveç se mundëson që të ruhet jeta private dhe familja, kjo e drejtë mundëson efektivisht edhe ruajtje të dinjitetit njerëzor si një ndër vlerat në shoqëri.

1.2 E drejta e privatësisë sipas akteve ndërkombëtare

Një mori e akteve ndërkombëtare përkufizojnë të drejtën e privatësisë, që gjejnë zbatim edhe në kuadër të sistemit juridik të vendit tonë.

1.3 Deklarata Universale për të drejtat e njeriut

Deklarata Universale për të drejtat e njeriut, si një nga aktet ndërkombëtare që gjen zbatim të drejtpërdrejt në Kosovë, duke qenë se hynë në kategorinë e nenit 22 të Kushtetutes së vendit si akte që gjejnë zbatim të drejtpërdrejt në Kosovë, e normon të drejtën e privatësisë, në nenin 12, si:” ***Askush nuk duhet t'i nënshtrohet ndërhyrjes arbitrare në jetën e tij private, në familje, në banesë ose në letërkëmbim vetjak, as sulmit kundër nderit dhe dinjitetit të tij. Secili ka të drejtën të mbrohet me ligj kundër ndërhyrjeve ose sulmeve të tilla”[144].***

[144] Deklarata universale për të drejtat e njeriut, 10 dhjetor 1948, Neni 12.

1.4 Pakti ndërkombëtar për të drejtat civile dhe politike

Një akt tjetër i karakterit ndërkombëtar siç është pakti për të drejtat civile dhe politike, parasheh po ashtu të drejtën e privatësisë, e që edhe ky akt ndërkombëtar hynë në kategorinë e akteve që bëjnë pjesë në nenin 22 të Kushtetutës së vendit që si akte ndërkombëtare gjejnë zbatim të drejtpërdrejt në Kosovë, dhe i cili në nenin 17, e normon të drejtën e privatësisë si: "1**.** ***Askush nuk duhet të jetë objekt i ndërhyrjeve arbitrare ose të paligjshme në jetën e tij private, në familje, në shtëpi ose letërkëmbim, e as duhet t'i shkelet nderi dhe reputacioni i tij në mënyrë të paligjshme. 2. Secili ka të drejtë të ketë mbrojtje ligjore kundër ndërhyrjeve dhe shkeljeve të tilla"***[145]**.**
Një ndër aktet më themelore ndërkombëtare që ruan të drejtat dhe liritë e njeriut është Pakti për të drejtat civile dhe politike, megjithatë përkundër se nga pakti i tillë edhe komiteti i cili trajton mbikëqyrjen e paktit ka raporte dhe rekomandime për sa i përket zbatimit të të drejtave dhe lirive që garantohen me këtë akt ndërkombëtar, në Kosovë nuk ka raste praktike që i referohen në kuadër të zgjidhjeve gjyqësore që jepen dhe që janë konstatuar se kishte ndërhyrje në të drejtën e privatësisë.

1.4.1 Masat mbikëqyrëse (përgjuese) sipas paktit për të drejtat civile dhe politike

Sipas paktit për të drejta civile dhe politike dhe komitetit për mbikëqyrjen e të drejtave të njeriut , mbikëqyrja nuk është e ndaluar në parim. Megjithatë, komiteti ka qenë veçanërisht i vëmendshëm në Vërejtjet Përfundimtare aty ku ka pasur autorizim dhe mbikëqyrje të pamjaftueshme gjyqësore, dhe ku interpretimi gjyqësor i legjislacionit dhe vendimeve të gjykatës përkatëse janë mbajtur kryesisht sekrete, duke i penguar kështu ata që preken të njohin ligjin me saktësi të mjaftueshme, ose të kenë qasje në mjete efektive juridike. Komiteti ka kërkuar, që aktivitetet e mbikëqyrjes, si brenda ashtu edhe jashtë territorit të një shteti, të jenë në përputhje me Nenin 17, pavarësisht kombësisë ose vendndodhjes së individëve komunikimet e të cilëve janë nën mbikëqyrje.
Komiteti ishte kritik ndaj fuqive ndërhyrëse të mbikëqyrjes në bazë të objektivave të gjera dhe të papërcaktuara në mënyrë të pamjaftueshme. Ishte shprehur shqetësim për urdhër-arreste të paqëllimshme për komunikime të caktuara të përgjuara, dhe

[145] Pakti ndërkombëtar për të drejtata civile dhe politike, 23.mars.1976, Neni 17.

një standard më të ulët të mbrojtjes kundër ndërhyrjeve arbitrare sesa normalja kur komunikimet janë marrë nga agjencitë e huaja të sigurisë ose të dhënat janë ndarë me to, kur në vend të kësaj sistemet e fuqishme të mbikëqyrjes duhet të parashikojnë përfshirjen gjyqësore në autorizimin e masave të tilla në të gjitha rastet për të parandaluar abuzimin. Gjithashtu ka qenë i shqetësuar për fuqitë e gjera për të ruajtur të dhënat, si dhe kur mbajtja është e detyrueshme

Për sa i përket masave të mbikëqyrjes (përgjimeve), duke i kushtuar vëmendje kërkesave të ligjit vendas, Komiteti ka rekomanduar që çdo ndërhyrje në të drejtën e privatësisë, familjes, shtëpisë ose korrespondencës të autorizohet nga ligje që:

- *a) janë të arritshme publikisht;*
- *b) dispozita që sigurojnë se mbledhja, qasja dhe përdorimi i të dhënave të komunikimit të jenë të përshtatura për qëllime specifike legjitime;*
- *c) janë mjaftueshëm të sakta dhe specifikojnë në detaje rrethanat e sakta në të cilat mund të lejohet çdo ndërhyrje e tillë, procedurat për autorizim, kategoritë e personave që mund të vendosen nën mbikëqyrje, kufirin e kohëzgjatjes së mbikëqyrjes; procedurat për përdorimin dhe ruajtjen e të dhënave të mbledhura; dhe*
- *d) ofrojnë mbrojtje efektive kundër abuzimit*[146]*.*

1.5 Konventa evropiane për mbrojtjen e të drejtave dhe lirive themelore të njeriut

Konventa Evropiane për mbrojtjen e të drejtave të njeriut dhe lirive themelore, poashtu është një nga aktet ndërkombëtare që gjen zbatim të drejtpërdrejt në Kosovë, pasi që e njëjta sipas nenit 22 të Kushtetutës së vendit në mënyrë të njëanshme është bërë pjesë e sistemit juridik të vendit, e cila në nenin 8 të saj ka normuar të drejtën për privatësi. Më konkretishtë, "Neni 8, E drejta për respektimin e jetës private dhe familjes", paragrafi 1." ***Çdokush ka të drejtën e respektimit të jetës së tij private dhe familjare, banesës dhe korrespondencës së tij". Paragrafi 2. " Autoriteti publik nuk mund të ndërhyjë në ushtrimin e kësaj të drejte, përveçse në shkallën e parashikuar nga ligji dhe kur është e nevojshme në një shoqëri demokratike, në interes***

[146] A COMMENTARY ON THE international covenant on civil and political rights The UN Human Rights Committee's Monitoring of ICCPR Rights, PAULM.TAYLOR, page 476 – 477.

të sigurisë publike, për mbrojtjen e rendit publik, shëndetit ose moralit ose për mbrojtjen e të drejtave dhe lirive të të tjerëve"[147].

2. Garancionet kushtetuese për të drejtën e privatësisë

Kushtetuta e Kosovës në kuadër të Kapitullit II, "Të Drejtat dhe Liritë Themelore", e ka normuar të drejtën për privatësi, në nenin 36 të saj. E drejta e privatësisë sipas kushtetutës së Kosovës, në kuadër të paragrafit 1, parasheh se: " ***Çdokush gëzon të drejtën që t'i respektohet jeta private dhe familjare, pacenueshmëria e banesës dhe fshehtësia e korrespondencës, telefonisë dhe e komunikimeve të tjera"[148].***

Sipas kësaj dispozite vihet në fokus qëllimi i ruajtjes dhe gëzimit të jetës private dhe familjare, ndërsa për të arritur që të ruhet jeta private dhe familja, duhet të gëzojnë ruajtje përkatësisht mos cenimin e:

a) ***Banesës;***
b) ***Fshehtësinë e korrespodencës;***
c) ***Fshehtësinë e telefonisë;***
d) ***Fshehtësinë e komunikimeve tjera.***

Në kuadër të paragrafit 1 i nenit 36 në Kushtetutë, parasheh, " ***Çdokush***", kjo nënkuptim se gëzimin e kësaj të drejte kushtetuta e Kosovës nuk e lidh me ndonjë status të personit, p.sh. Me shtetësinë e shtetasve që e gëzojnë qytetarët, apo me kategorinë e refugjatëve, apo kategorinë e imigrantëve. Madje dispozita kushtetuese mënyrën e formulimit që e ka përdorur, "***Çdokush***", nënkupton se kjo e drejtë i takon edhe personave që mund të jenë kundërligjshëm me qëndrim në territorin e vendit, pasi që nuk përjashton asnjë kategori për shkak të një cilësie apo ndonjë statusi që e gëzon qytetari për ta gëzuar këtë të drejtë, rrjedhimisht çdo person që gjindet në çfardo rrethane në territorin e vendit i garantohet e drejta e privatësisë, qoft shtetas apo jo i Kosovës, qoft nga fakti se është apo nuk është me qëndrim të ligjshëm në territorin e Kosovës.

Ndërsa paragrafi 2 i nenit 36 në Kushtetutë, ka përcaktuar se: ***"Kontrollet e cilësdo banesë ose cilitdo objekti privat, që mendohet se janë të domosdoshme për hetimin e krimit, mund të bëhen vetëm deri në shkallën e domosdoshme dhe vetëm pas miratimit nga ana e gjykatës, pas shpjegimit të***

[147] Konveta Evropiane per Mbrojtjen e te Drejtave dhe Lirive Themelore te Njeriut, 4 nentor 1950, neni 8.
[148] Kushtetuta e Republikes se Kosoves, 15.Qershor.2008, Neni 36.

arsyeve pse një kontroll i tillë është i domosdoshëm. Shmangia nga kjo rregull lejohet, nëse është e domosdoshme për arrestim të ligjshëm, për mbledhjen e provave që ka rrezik të humbasin ose për mënjanimin e rrezikut të drejtpërdrejtë dhe serioz për njerëzit dhe për pasuri, në mënyrën e përcaktuar me ligj. Gjykata duhet që të miratoj veprimet e tilla në mënyrë retroaktive"[149].

Sipas kësaj dispozite, krijohet baza e ndërhyrjes në të drejtën e privatësisë, vetëm mbi kushtet e parapara dhe sipas një qëllimi legjitim që parasheh ligji. Dispozita parasheh dy mundësi të ndërhyrjes:

a) Me miratimin e Gjykatës para se të bëhet ndërhyrja;
b) Me miratimin e Gjykatës pas ndërhyrjes.

I. Miratimi i Gjykatës para ndërhyrjes dhe kushtet që duhet përmbushur

Në kuadër të kësaj dispozite në pjesën e parë mundësohet ndërhyrja në banesë apo objekt privat nëse plotësohen kushtet e:

a) Domosdoshmëria e hetimit të krimit;
b) Vetëm në shkallën e domosdoshme;
c) Vetëm pas shpjegimit të arsyeve për domosdoshmërinë e ndërhyrjes.

II. Miratimi i Gjykatës pas ndërhyrjes dhe kushtet që duhet plotësuar

Siq është theksuar më sipër dispozita kushtetuese në paragrafin 2 të nenit 36, ka paraparë dy mënyra të ndërhyrjes në banesë apo në objekt privat, mënyra kur lejohet ndërhyrja dhe ka efekt kushtetues vetëm nëse është miratuar nga gjykata, pasi të jetë bërë ndërhyrja parasheh disa situata se kur mund të ndërhyhet e që janë:

a) Për qëllim të arrestimit të ligjshëm;
b) Për qëllim të sigurimit të provave kur ka rrezik se do të humbasin;
c) Për qëllim të mënjanimit e rrezikut të drejtpërdrejt e serioz për njerëzit.

Të gjitha këto mënyra të ndërhyrjes mund të bëhen vetëm siç është paraparë me dispozitat ligjore, dhe ka efekt ndërhyrja vetëm nëse Gjykata miraton veprimet e tilla në mënyrë prapavepruese.

Ndërsa paragrafi 3 i nenit 36 në Kushtetutë, parasheh ruajtjen e privatësisë e cila mund të cenohet përmes ndërhyrjes, në telefon, korrespodencë apo mënyra tjera të komunikimit, e cila më konkretisht përcakton se: " ***Fshehtësia***

[149] Kushtetuta e Republikes se Kosoves, 15.Qershor.2008, Neni 36 paragrafi 2.

e korrespondencës, telefonit dhe komunikimit tjetër, është e drejtë e pacenueshme. Kjo e drejtë mund të kufizohet vetëm përkohësisht, në bazë të vendimit gjyqësor, nëse është e domosdoshme për ecurinë e procedurës penale ose për mbrojtjen e vendit, në mënyrën e parashikuar me ligj".

Përmes kësaj dispozite, qytetarëve u garantohet jeta private dhe familjare, edhe kur kanë komunikim telefonik, korrespodencë apo mënyrë tjetër të komunikimit.

Megjithatë kjo e drejtë mund të kufizohet vetëm në dy situata dhe atë vetëm përkohësisht:

a) Për ecurinë e procedurës penale; ose
b) Për mbrojtjen e vendit.

Situata e parë për zbatimin e procedurës penale, lehtësisht është e definuar duke qenë se dihet sipas kodit të procedurës penale kur fillon procedura penale dhe në situata kur procedura penale nuk ka filluar atëherë dispozitat ligjore përcaktojnë nevojën urgjente për ndërhyrje në telefoni, korrespodenc apo komunikim tjetër.

Ndërsa situata e dytë, që është mbrojtja e vendit, kjo pa dyshim duhet nënkuptuar me çështjet e sigurisë së vendit, që kryesisht konsiston në veprime që ndërmarrin institucionet e veqanta të sigurisë e që edhe atyre u lejohet sipas ligjit që të bëjnë ndërhyrjen e tillë, për qëllim të eliminimit të të gjitha formave të rrezikut që mund të ekzistoj në sigurinë dhe mbrojtjen e vendit.

Megjithatë te situata e dytë është karateristikë se, duhet të shtrohet problematika e të drejtës dhe e rrezikut për siguri, që rreziku për siguri shpesh herë nuk mundëson zbatim rigoroz të procedurave për qëllim të respektimit të të drejtave kushtetuese.

Duhet të kemi parasysh se e drejta për privatësi shpesh herë vihet në dyshim nga rreziqet që mund të shkaktohen me vepra të rënda penale, e që në njërën anë ato vepra penale krijojnë edhe cenim të sigurisë për vendin. Në këtë kuptim Gjyqtari Federal në Gjykatën e Apelit, në një argument në vitin 2001, thekson se:

" Si në situatën e parë ashtu edhe në situatën e dytë, duhet që të plotësohen dy kushte kumulative që janë:

a) Ndërhyrja bëhet vetëm nëse është e domosdoshme, dhe
b) Vetëm sipas kushteve të parapara me ligj.

Paragrafi 4 i nenit 36 të Kushtetutës, zgjeron gamën e objektit mbrojtës që për pasoj do të mund të cenonin të drejtën e privatësisë. Sipas këtij paragrafi parasheh që: " ***Secili person gëzon të drejtën e mbrojtjes së të dhënave***

personale. Mbledhja, ruajtja, qasja, korrigjimi dhe shfrytëzimi i tyre rregullohet me ligj"[150].

Sipas kësaj dispozite, të dhënat personale janë kategori e mbrojtur në kuadër të së drejtës së privates. Se çfarë konsiderohet e dhënë personale, përcaktohet sipas ligjit 06/L-082 për mbrojtjen e të dhënave personale, ku në nenin 3 paragrafi 1 nënparagrafi 1.1, parashihet se: " ***E dhënë personale – çdo informacion në lidhje me një person fizik të identifikuar ose të identifikueshëm ("subjekt i të dhënave"); një person fizik i identifikueshëm është ai, i cili, mund të identifikohet drejtpërdrejt ose jo drejtpërdrejt, veçanërisht duke iu referuar një identifikuesi në bazë të një emri, një numri identifikimi, të dhënave rreth vendndodhjes, një identifikues online, ose një apo më shumë faktorë specifikë për identitetin fizik, psikologjik, gjenetik, mendor, ekonomik, kulturor ose social të atij personi fizik***"[151].

Në radhë të parë duhet të kemi parasysh se kjo e drejtë nuk është e karakterit absolut, duke qenë se e njëjta e drejtë mund të kufizohet përkohësisht, andaj nuk hynë në kategorin e të drejtave me natyrë absolute. Ndërsa poashtu duhet të kemi parasysh se kjo e drejtë ka karakter të detyrimit pozitiv dhe negativ.
E drejta e privatësisë synohet që të mbrohet nga ndërhyrja e autoritetit shtetëror, rrjedhimisht kjo e drejtë ka karakter me detyrim pozitiv dhe negativ. Në njërën anë në mënyrë të kjart parasheh se nuk mund të ketë ndërhyrje në privatësi përveç se sipas kushteve që parashihen në nenin 36 që këtu parashihet detyrimi pozitiv i shtetit, që nënkupton se asnjë institucion publik nuk mund të ndërmerr veprime në kundërshtim me këtë dispozitë që do të cenonte të drejtën në privatësi, dhe në anën tjetër parasheh detyrim negativ për organet shtetrore, pasi që është e ditur se institucionet shtetrore por edhe subjekte private përpunojnë të dhënat, andaj i vendos detyrim negativ shtetit për ndërmarrjen e vazhdueshme që kjo e drejtë të garantohet.

[150] Kushtetuta e Republikes së Kosoves, 15 Qershor 2008, Neni 36 paragrafi 3.
[151] Ligjit nr. 06/L-082 për mbrojtjen e të dhënave personale, Nenin 3 Paragrafi 1 nënparagrafi 1.1

3. Shtrirja e të drejtës së privatësisë tek personat juridik

Dispozitat kushtetuese nuk përjashtojnë të drejtat edhe ndaj personave juridik për sa i përket të drejtave dhe lirive themelore të njeriut që normohen në kapitullin II të Kushtetutës.
Më konkretisht, dispozita nga neni 21 të Kushtetutës, " Parimet e Përgjithshme" në paragrafin 4 është paraparë se: " ***Të drejtat dhe liritë themelore të parashikuara në Kushtetutë, vlejnë edhe për personat juridikë, për aq sa janë të zbatueshme"***[152]**.**

Nisur nga kjo dispozitë kushtetuese, rrjedh se edhe personat juridik si subjekte të së drejtës gëzojnë kategorinë e të drejtave dhe lirive të njëriut, por përcaktohet për aq sa janë të zbatueshme ndaj kësaj katergorie të subjekteve të së drejtës.

Në këndvështrim me të drejtën për privatësi, duhet të kemi parasysh se dispozita nga neni 36 i Kushtetutës, përcakton, se: " Çdokush gëzon të drejtën që t'i respektohet jeta private dhe familjare, ***pacenueshmëria e banesës dhe fshehtësia e korrespondencës, telefonisë dhe e komunikimeve të tjera"***.
Rrjedhimisht e drejta e privatësisë në përputhje me nenin 21 paragrafi 4, mund të shtrihet edhe ndaj personave juridik në:

a).Pacenueshmëri të banesës - objekteve;
b).Fshehtësisë së korrespodencës;
c).Telefonisë, apo
ç).Komunikimeve tjera.

Marrë për bazë se dispozita nga neni 21 paragrafi 4, përcakton se këto të drejta shtrihen edhe ndaj personave juridik, atëherë duhet të kemi të kjart se kufizimet në raport me pacenueshmërinë e objekteve, fshehtësisë së korrespodencës, telefonisë apo komunikimeve të tjera duhet të zbatohen në procedurën sipas ligjit siç vlejnë dispozitat në raport me çdo person, çka do të thotë se cilado ndërhyrje duhet të jetë sipas dispozitave ligjore edhe kur janë në pyetje personat juridik.

[152] Kushtetuta e Republikës së Kosovës, 15 Qershor 2008, Neni 21 paragrafi 4.

4. Fshehtësia e korrespodencës si garanci kushtetuese

Dispozitat e ligjit 06/L-038 për shërbimet postare, përcaktojnë përkufizimin e dërgimit të korrespodencës, në nenin 3 paragrafi 1, nenparagrafi 1.4 parasheh se: "***Dërgesa te korrespodencës - komunikimi me shkrim mbi çdo lloj dërgese fizike që do të bartet dhe dërgohet në adresën e treguar nga dërguesi mbi vetë dërgesën ose në ambalazhin e tij.*** ***Librat, katalogët, gazetat dhe shkrimet periodike nuk do të konsiderohen si dërgesa të korrespondencës"***[153]***.***

Rëndësi të veçantë duhet të ketë dallimi ndërmjet korrespodencës ndërmjet të pandehurit dhe mbrojtësit të tij, si dhe korrespodencës ndërmjet të pandehurit dhe cilitdo person tjetër, duke qenë se kur ka mbikëqyrje të korrespodencës atëherë këto të dhëna do të mund të shërbenin si prova në procedurën penale për qëllim të vërtetimit të aspekteve faktike dhe fajësisë.
Në këtë kuptim, duhet pasur parasysh që ka dispozita të kodit të procedurës penale, që korrespodenca e të pandehurit që mund të ketë me mbrojtësin e tij gëzon mbrojtje dhe ato as nuk mund të merren si prova.

Kodi i procedurës penale të Kosovës, në nenin 65 ka përcaktuar të drejtat e mbrojtësit, ku në paragrafin 1, parashihet se: *"Mbrojtësi gëzon të drejta të njëjta që ia njeh ligji edhe të pandehurit, përveç atyre që shprehimisht i rezervohen të pandehurit personalisht"*[154]. Kjo dispozitë ka përcaktuar garancionet procedurale të mbrojtësit kur është i angazhuar në çështjen penale ndaj të pandehurit, ndërsa përjashton aspekte të drejtash procedurale që nuk mund të njihen përveç së të pandehurit.

Ndërsa lidhur me korrespodencën, paragrafi 2 i nenit 65 të Kodit të procedurës penale të Kosovës, përcakton se: ***" Mbrojtësi ka të drejtë të komunikojë lirisht me të pandehurin gojarisht ose me shkrim sipas kushteve që garantojnë fshehtësinë"***. Kodi i procedurës penale nuk paraqet ndonjë rregullim ligjor, " kushtet që rregullojnë fshehtësinë" siç kërkohet në nenin 65 paragrafi 2, megjithatë kjo duhet nënkuptuar si e drejtë më e zgjeruar që i takon të pandehurit, rrjedhimisht asnjë aspekt i korrespodencës që i referohet çfarëdo komunikimi ndërmjet të pandehurit dhe mbrojtjes nuk mund të jetë i cenuar, më konkretisht komunikimet e të pandehurit dhe të mbrojtësit të tij për aspektin e angazhimit

[153] Ligjit nr. 06/L-038 për Shërbimet Postare, Nenin 3 paragrafi 1, nenparagrafi 1.4.
[154] Kodi nr. 08/L-032, I Procedures Penale të Kosoves, Neni 65.

dhe ndihmës ligjore e profesionale që ia jep mbrojtësi të pandehurit në asnjë rrethanë nuk mund të cenohet, për derisa korrespodenca është në dhënien e mbrojtjes profesionale që i bëhet të pandehurit.

Rrjedhimisht përveç garancioneve që parashihen për komunikimin dhe korrespodencën ndërmjet mbrojtësit dhe të pandehurit në procedurën penale, një mbrojte edhe më të theksuar i jap këtij aspekti dispozita e nenit 121 paragrafi 1 nënparagrafi 1.2. Në këtë dispozitë parashihet se mbrojtësi është dëshmitar i privilegjuar dhe se ai nuk mund të merret në pyetje në cilësinë e dëshmitarit për atë çfarë i ka komunikuar i pandehuri lidhur me mbrojtjen e tij, përveç kur këtë privilegj ia heq vet i pandehuri mbrojtësit të tij.

Rrethanat që mund të përbëjnë përjashtim, në ndërhyrjen e korrespodencës dhe që mund të përbëjnë prova në procedurën penale, korrespodenca e mbajtur ndërmjet të pandehurit dhe mbrojtësit të tij, është e rregulluar, sipas nenit 111 paragrafi 1, e cila dispozitë përcakton se cilat janë sendet që nuk mund të sekuestrohen si prova, ku parashihet se: ***"komunikimet me shkrim ndërmjet të pandehurit dhe personave të cilët sipas këtij Kodi nuk mund të dëshmojnë sipas nenit 123 të këtij Kodi, ose janë të liruar nga detyrimi për të dëshmuar dhe kanë refuzuar të bëjnë një gjë të tillë në pajtim me nenin 124 të këtij Kodi"***[155]. Kjo dispozitë garanton në çfarëdo rrethane se komunikimet me shkrim nuk mund të sekuestrohen, gjë që nënkupton se përjashton në çfarëdo mënyre ndërhyrjen e autoriteteve shtetërore apo detyrimin që mbrojtësi t'i deponoj komunikimet me shkrim që i ka pasur me të mbrojturin e tij.

Në anën tjetër, dispozita nga neni 111 paragrafi 2, parasheh një përjashtim ku sendet e tilla, mund t'i nënshtrohen sekuestrimit nëse konstatohet se, mbrojtësi ka nxitur të pandehurin në vepër penale, nëse bëhet për qëllim të pengimit të drejtësisë, nëse kanë të bëjnë me pranimin e mallrave të vjedhura, apo me sendet që janë përfituar nga vepra penale. Megjithatë dispozita rregullon çështjen e sendeve që mund të jenë te mbrojtësi por nuk i referohet komunikimeve, andaj sendet në këtë kuptim nuk duhet interpretuar në mënyrë të ekzagjeruar ku do të mund të prekej korrespodenca e të pandehurit me mbrojtësin e tij, por duhet interpretuar në mënyrë të ngushtë vetëm me sendet që janë sende në natyrë dhe jo komunikimi shkresor si aspekt i korrespodencës

[155] Kodi nr. 08/L-032, I Procedures Penale te Kosoves, Neni 111.

që ka qëllim ndërtimin e mbrojtjes efektive dhe strategjinë që mundëson mbrojtje efektive.
Ndërsa privilegjet me korrespodencën nuk i ka as një person që zhvillohet procedura penale ndaj tij në raport me personat tjerë siç i ka me mbrojtësin e tij i pandehuri.

5. Praktika e GJEDNJ-së për privilegjet ndaj avokatit lidhur me sekretin profesional si kategori e të drejtës nga neni 8 i KEDNJ-së

Gjykata evropiane për të drejtat dhe liritë e njeriut ka pasur në trajtim çështjen e korrespodencës së Avokatit dhe klientëve, me fokus korrespodenca që ishte e zhvilluar në mënyrë elektronike, ku edhe ka konstatuar se marrja e provave elektronike nga një zyrë e avokatit përbën shkelje të nenit 8, nëse kanë të bëjnë me komunikimin e avokatit dhe klientit të tij, duke konstatuar se sekreti profesional përbën po ashtu çështje thelbësore në dhënien e mbrojtjes nga ana e avokatit ndaj klientit.

Më konkretisht në rastin, ***dy parashtruesve të kërkesës*** e trajtuar si: " WIESER AND BICOS BETEILIGUNGEN GmbH v. AUSTRIA - 74336/01[156], vendimi i datës: 16.tetor.2007", në këtë çështje kishte pasur një urdhër të Gjyqtarit.

Çështja: Pretendimi se marrja e provave elektronike në zyrën e avokatit përbën cenim të nenit 8 të Konventës, të drejtës për respektimin e jetës private dhe familjes.

Veprimet: Me datë. 10.tetor.2000 ishte zhvilluar një kontroll i kompanisë në të cilën Wiser ishte avokat i Kompanisë dhe kishte selinë në kompani. Kontrolli u zhvillua nga hetuesit për krime ekonomike dhe zyrtarëve për sigurimin e të dhënave. Kontrolli u bë në prezencë të Wiser dhe një Përfaqësuesi të shoqatës së avokatëve. Kontrolli u shtri në Dokumente dhe **të dhëna elektronike.** Çdo dokument që ishte kontrolluar, kur përfaqësuesi i shoqatës së avokatëve kontestoj sekuestrimin për arsye se përbënte dokument të mbrojtur nga sekreti profesional, ai dokument vulosej për tu vlerësuar nga një gjyqtar nëse ai dokument cenonte sekretin profesional.

[156] *WIESER AND BICOS BETEILIGUNGEN GmbH v. AUSTRIA* - 74336/01.

Paralelisht me kontrollin e dokumenteve, zbatohej kontrolli i të dhënave elektronike, ku ishin kontrolluar dhe kopjuar shumë të dhëna elektronike nga kompjuterët që kishin zbatuar hetuesit. Këto të dhëna elektronike nuk iu treguan as Wiser, as përfaqësuesit të shoqatës së avokatëve, dhe nuk ishte mbajtur procesverbal mbi të dhënat elektronike në mënyrë të detajuar, për të treguar se qfarë të dhënash ishin kontrolluar, cilat të dhëna ishin marr dhe qfarë evidence ishte mbajtur.

Praktika e mëparshme: Gjykata për ta trajtuar këtë rast i ishte referuar praktikës së mëparshme për kontrollin e zyrave të avokatëve dhe sekuestrimin e sendeve nga këto zyra në domenin e nenit 8 e ndërlidhur me sekretin profesional, duke iu referuar rasteve:

a) *Niemietz kundër Gjermanisë, 16 dhjetor 1992,*
b) *Tamosius kundër Mbretërisë së Bashkuar (vendim), nr. 62002/00, GJEDNJ 2002*
c) *Sallinen dhe të tjerë kundër Finlandës, nr. 50882/99, 27 shtator 2005, i cili konfirmon se kontrolli i ambienteve të biznesit të një avokati ndërhyri gjithashtu në të drejtën e tij për respektimin e "shtëpisë" së tij.*
d) *Société Colas Est dhe të tjerë kundër Francës, nr. 37971/97, qe ka konstatuar se, Kontrolli i ambienteve të biznesit të një kompanie u konstatua gjithashtu si ndërhyrje në të drejtën për respektimin e "shtëpisë".*

Gjetjet e gjykatës: Tri nga standardet që gjykata kishte shqyrtuar: Ekzistimi i bazës ligjore, Qëllimi legjitim dhe Domosdoshmëria në një shoqëri Demokratike.

a) Ekzistimi i bazës ligjore – kishte konstatuar se ka bazë ligjore në Kodin e Procedurës Penale edhe pse jo dispozita specifike për kontrollin e të dhënave elektronike, por megjithatë dispozitat e kodit krijonin bazë për ndërhyrje në shtëpi me qëllim kontrolli.
b) Qëllimi legjitim – kishte konstatuar se urdhri për kontroll ishte dhënë për shkak të një të dyshuari për tregti me barna, që përbënte një qëllim legjitim në parandalimin e kriminalitetit.
c) Domosdoshmëria në një shoqëri demokratike – Në rastin konkret, kontrolli i sistemeve kompjuterike ishte bazuar në një urdhër arrest të lëshuar nga gjyqtari hetues në kontekstin e ndihmës ligjore për autoritetet italiane, të cilat po zhvillonin procedura penale për tregti të paligjshme të barnave. Për lëshimin e urdhrit u mbështet në

> faktin se ishin gjetur fatura të drejtuara Novamed, 100% në pronësi të kompanisë ndaj të cilës ushtrohej kontrolli, u konstatua se urdhri i kontrollit kishte bazë për dyshim të arsyeshëm.

Gjykata gjithashtu konstaton se urdhri i kontrollit kufizoi dokumentet ose të dhënat që duheshin kërkuar në një mënyrë të arsyeshme, duke i përshkruar ato si çdo dokument biznesi që zbulonte kontakte me të dyshuarit në procedurat italiane. Kontrolli mbeti brenda këtyre kufijve, pasi oficerët kërkuan dokumente ose të dhëna që përmbanin ose fjalën "Novamed" ose "Bicos" ose emrat e ndonjërit prej të dyshuarve.

Ishte konstatuar se Kodi i Procedurës Penale ofron mbrojtje të mëtejshme procedurale në lidhje me sekuestrimin e dokumenteve dhe të dhënave elektronike. Ishte konstatuar se dispozitat e mëposhtme të Kodit përcaktonin këtë procedurë:
(a) banori i ambienteve që kontrollohen duhet të jetë i pranishëm;
(b) në fund të kontrollit duhet të hartohet një raport dhe sendet e sekuestruara duhet të renditen;
c) nëse pronari kundërshton sekuestrimin e dokumenteve ose bartësve të të dhënave, ato duhet të vulosen dhe të vihen para gjyqtarit për të marrë një vendim nëse do të përdoren apo jo për hetimin; dhe
(d) përveç kësaj, për sa i përket kontrollit të zyrës së një avokati, kërkohet prania e një përfaqësuesi të Shoqatës së Avokatëve.

U konstatua se një numër hetuesish kryen kontrollin e ambienteve të dy palëve. Ndërsa një grup vazhdoi me sekuestrimin e dokumenteve, grupi i dytë kontrolloi sistemin kompjuterik duke përdorur kritere të caktuara kërkimi dhe sekuestroi të dhëna duke kopjuar skedarë të shumtë në disqe.

U konstatua se dispozitat e theksuara më sipër u përmbushën plotësisht në lidhje me sekuestrimin e dokumenteve: sa herë që përfaqësuesi i Shoqatës së Avokatëve kundërshtonte sekuestrimin e një dokumenti të caktuar, ai vulosej. U konstatua se disa ditë më vonë, gjyqtari hetues vendosi në prani të palëve se cilat dosje i nënshtroheshin sekretit profesional dhe ia ktheu një numër të tyre palëve që i u nënshtruan kontrollit mbi këtë bazë.
U konstatua që në rastin aktual të njëjtat dispozita mbrojtje nuk u respektuan në lidhje me të dhënat elektronike.

Një numër faktorësh tregojnë se ushtrimi i të drejtave të palëve që iu nënshtruan kontrollit në këtë drejtim ishte i kufizuar.

1. Së pari, anëtari i Shoqatës së Avokatëve, megjithëse i pranishëm përkohësisht gjatë kontrollit të pajisjeve kompjuterike, ishte kryesisht i zënë me mbikëqyrjen e sekuestrimit të dokumenteve dhe për këtë arsye nuk mund ta ushtronte siç duhet funksionin e tij mbikëqyrës në lidhje me të dhënat elektronike.
2. Së dyti, raporti që përcaktonte se cilat kritere kërkimi ishin zbatuar dhe cilat dosje ishin kopjuar dhe sekuestruar nuk ishte hartuar në fund të kontrollit, por vetëm më vonë po atë ditë. Për më tepër, oficerët me sa duket u larguan pasi kishin përfunduar detyrën e tyre pa informuar aplikuesin e parë ose përfaqësuesin e Shoqatës së Avokatëve për rezultatet e kontrollit.

Vendosja: U vendos që ka pasur shkelje të nenit 8 të Konventës për Mbrojtjen e të drejtave dhe Lirive Themelore të Njeriut për parashtruesin e parë.

U vendos me shumicë që ka pasur shkelje të nenit 8 të Konventës për mbrojtjen e të drejtave dhe Lirive Themelore të Njeriut për parashtruesin e dytë.

U vendos për kompensimin e dëmit jo material dhe për shpenzimet e procedurës që duhet t'i përmbush shtetit ndaj parashtruesve.

Në Kosovë, përveç që kodi i procedurës penale të Kosovës krijon disa privilegje për avokatin si për sa i përket korrespodencës ashtu edhe për sa i përket mundësisë për t'u thirrur si dëshmitar, ligji nr. 04/L-193 për Avokatinë, në nenin 17 ka paraparë se*: " 1.Avokati është i detyruar që, në pajtim me Statutin dhe Kodin të ruaj sekretin profesional dhe të kujdeset që, në mënyrë të njëjtë të veprojnë edhe të gjithë të punësuarit në zyrën tij. 2. Detyrimi i ruajtjes së fshehtësisë profesionale nuk është i kufizuar në kohë"*[157]. Në këtë kuptim dispozitat ligjore në fuqi jo vetëm se garantojnë sekretin profesional ndërmjet avokatit dhe klientit të tij në cilëndo procedurë që angazhohet, por ato madje nuk janë të kufizuara në kohë, çka do të thotë se asnjë e dhënë ndërmjet një klienti dhe një avokati qoftë edhe pas periudhave të caktuara nuk

[157] Ligji nr. 04/L-193 pwr Avokatinë, Nenin 17.

mund të konsiderohet si trajtim jashtë nenit 8 të Konventës për Mbrojtjen e të drejtave dhe Lirive Themelore të Njeriut.

6. Fshehtësia e telefonisë

Fshehtësia e telefonisë si kategori e të drejtës së privatësisë, garanton ruajtjen e të gjitha të dhënave që mund të sigurohen përmes telefonit, qoftë të dhënat (databaza), qoftë komunikimet me shkrim apo me zë, qoftë ato që janë në zhvillim apo ato që janë zhvilluar në të kaluarën.

Më konkretisht fshehtësia e telefonisë krijon të drejtën e mbrojtjes së privatësisë, në dimensionet më të gjera të mundshme, qoftë kur kemi të bëjmë me ndërhyrjen gjatë zhvillimit të formave të komunikimit të telefonisë apo qoftë kur kemi të bëjmë me të dhënat që mund të sigurohen përmes ekzaminimeve në aparatin e komunikimit. Telefoni nuk duhet nënkuptuar vetëm aparatin e formave të komunikimit zanor, pasi që me zhvillimin teknologjik ka shumë forma të komunikimit që në thelb përbëjnë aspekt të telefonisë, rrjedhimisht telefonia duhet nënkuptuar çdo formë e komunikimit elektronik.

Ligji 04/L-149 për shërbimet e telekomunikimit në përkufizimet e tij në nenin 4, paragrafi 1 nënpargarfi 1.34, ka paraparë se: ***“ Shërbim telefonik i disponueshëm për publikun – shërbim i disponueshëm për publikun, për gjenerimin dhe marrjen e thirrjeve kombëtare dhe ndërkombëtare, dhe qasjen në shërbimet e emergjencës nëpërmjet një numri nga plani i numeracionit telefoni”***[158]**.**
Nga ana tjetër marr për bazë komunikimin që zbatohet sot përmes aparateve telefonike apo aparateve tjera që mundësojnë komunikimin kombëtar dhe ndërkombëtar, mundësojnë që edhe pa një numër të numeracionit telefonik të zhvillohen komunikimet e tilla, andaj në këtë kuptim duhet trajtuar në interpretim më të zgjeruar mbrojtjen e të drejtës së privatësisë kur kemi të bëjmë me fshehtësinë e telefonisë, që do të thotë çdo mundësi e komunikimit qoftë zanor apo me shkrim përmes mjeteve elektronike duhet të konsiderohet si aspekt i ruajtjes së fshehtësisë së telefonisë.
Përkundër se fshehtësia e telefonisë hynë në garancionet kushtetuese të së drejtës së privatësisë, ajo mund të kufizohet siç është theksuar me sipër kur

[158] Ligji 04/L-149 për shërbimet e telekomunikimit, Neni 4, Paragrafi 1 Nenparagrafi 1.34.

plotësohen kushtet e përcaktuara me dispozitat ligjore dhe për qëllimet, e në proporcion që është përcaktuar sipas dispozitës kushtetuese në nenin 36 paragrafi 2.

7. Fshehtësia e komunikimeve tjera

E drejta e privatësisë garanton çdo lloj të fshehtësisë së komunikimeve, qoftë ajo kur kemi të bëjmë me komunikim fizik të shkruar apo komunikim elektronik të shkruar, siç mund të jenë rrjetet sociale apo komunikim përmes emaileve, apo komunikim përmes video - lojërave që shpesh herë përdoret në rrjetet e komunikimit përmes internetit si formë më e fshehtë e komunikimit.

Në këtë kuptim dispozitat kushtetuese nuk kanë përcaktuar në mënyrë konkrete se cilat lloje tjera të komunikimeve janë të mbrojtura por, marr për bazë se cila është vlera e mbrojtur që ka të bëjë me familjen dhe jetën, atëherë natyra e komunikimeve të tjera duhet nënkuptuar çdo lloj i komunikimit që mund të jetë ndërmjet personit që synohet të ndërhyhet në të drejtën e tij të privatësisë.

8. Konkurueshmëria e të drejtës për privatësi dhe Siguria Kombëtare

Sfidat më të mëdha lidhur me ruajtjen e të drejtës së privatësisë vijnë në shprehje kur veprimet e ndërhyrjes nga autoritetet shtetërore bëhen në qëllim të zbatimit të sigurisë kombëtare.
Nga njëra anë autoritetet shtetërore kanë detyrim për garancionet që duhet krijuar për ruajtjen e të drejtës së privatësisë, mirëpo kanë detyrim edhe për ndërmarrjen e masave për qëllim të sigurisë kombëtare apo publike.

Në anën tjetër, duhet të kemi parasysh se, kur një e drejtë individuale siç është e drejta e privatësisë, shkon në drejtim të kundërt me një të drejtë grupore siç është e drejta më e përgjithshme për liri dhe siguri, cila duhet të jetë më e shprehur. Në parim e drejta individuale gjithnjë duhet të interpretohet dhe prevalon edhe të drejtën grupore, por tek rasti i çështjes së sigurisë kombëtare apo sigurisë publike, çështja ndërlikohet duke qenë se për shkak të ekzistimit të rrezikut gjithnjë mund të ketë cenim të së drejtës së privatësisë që personit. Nuk ka një standard specifik për të ndarë çështjen se deri ku mund ta minimizoj rreziku i sigurisë kombëtare të drejtën e privatësisë. Kjo ka të bëjë

varësisht se shtetet cilën zgjidhje e bëjnë me prioritet. Në shtetet Evropiane e drejta e privatësisë ruhet maksimalisht dhe synohet që në çdo rast të balancohet me detyrimin për ruajtjen e sigurisë kombëtare, duke ndërmarr edhe iniciativa të ndryshme për ndryshimin e legjislacionit, por duke mos minimizuar të drejtën e privatësisë në asnjë rrethanë.

E kundërta është në Shtete e Bashkuara të Amerikës, që përmes ligjit të njohur " Patriot" që lejon ndërhyrjen më të ashpër në te drejtën e privatësisë, për qëllim të masave parandaluese që lidhen me sigurinë publike.
Për këtë situatë, është i njohur deklarimi publik i Gjyqtarit Federal në Apel, Riqard Posner që deklaroj se, avokuesit e të drejtave të njeriut gabojnë kur i japin më shumë rëndësi të drejtave civile si të drejtës së privatësisë se sa sigurisë. Më konkretisht ai deklaroj se: " E konsideroj këtë një qasje thellësisht të gabuar ndaj çështjes së balancimit midis lirisë dhe sigurisë. Gabimi themelor është vendosja e përparësisë te liria. Është një gabim për sa i përket ligjit dhe një gabim për sa i përket historisë. Ne jemi një komb nën ligj, por së pari jemi një komb. Ligji është një krijim njerëzor jo një dhuratë hyjnore. Është një mjet për të promovuar mirëqenien shoqërore, dhe ndërsa kushtet thelbësore për atë mirëqenie ndryshojnë, edhe ai duhet të ndryshoj".

Rëndësia e balancimit të së drejtës për privatësi në rrethanat kur ekziston rreziku për sigurinë kombëtare apo publike është gjithnjë e më i shprehur. Situata praktike të jetës mund të jenë të ndryshme posaçërisht në rrethanat kur kemi të bëjmë me rrezik të drejtpërdrejt të cenimit të rendit kushtetues nga grupet e armatosura qoftë si grupe apo si terrorist.

Rrethanat e tilla kërkojnë përveç ndërhyrjes së shpejt dhe efikase për mënjanimin e rrezikut dhe sigurimin e provave por edhe për qëllim të zbatimit të procedurës penale, njëkohësisht mund të krijohen rrethana që duhet ndërhyrje aq e shpejt që nuk premton përmbushje të kushteve procedurale që e garantojnë ndërhyrjen në privatësi, qoftë në pronë apo në telefoni apo me mjete tjera të komunikimit elektronik, psh. mund të ketë situatë që informacioni është ekzistent për sulmin terrorist, dhe detyrimi për ndërhyrje është po ashtu i nevojshëm për qëllim të parandalimit të rrezikut konkret të sigurisë kombëtare dhe publike, rrjedhimisht me ndërhyrjen e tillë në pronë mund të jetë e domosdoshme që për shmangien përfundimtare të pasojave të sulmit duhet ndërhyrë menjëherë në mjetet elektronike pasi që mund të ketë

informacion vetëm në ato mjete se ku gjendet një bombë për shpërthim që është e vendosur, në këto rrethana nuk mund të garantoj askush përmbushje procedurale për shkak të nevojës për ndërhyrje urgjente në shmangien e rrezikut.

Në këtë kontekst Kodi i Procedurës Penale të Kosovës, mundëson ndërhyrje në rrethana të veçanta që konsiderohen si autorizime ligjore për organet e ndjekjes, e që rregullohen sipas dispozitave nga neni 108 të Kodit të procedurës penale ku rregullohet, mundësia e ndërhyrjes në kontroll pa urdhër të gjykatës, dhe sipas kësaj dispozite ligjore përcaktohet se kontrolli mund të bëhet si:

a) ndaj personit;
b) ndaj shtëpisë;
c) apo ndaj pronës tjetër.

Marrë për bazë se autorizohet ndërhyrja për kontroll edhe ndaj pronës tjetër atëherë çdo mjet elektronik që mundë të përbëjë pronë e që lejohet ndërhyrja sipas kësaj baze ligjore është e arsyeshme në rrethana që ekziston rreziku i sigurisë kombëtare apo publike.

Nga ana tjetër duke qenë se aspektet e sigurisë kombëtare i ka në kompetencë edhe Agjencioni për Siguri i Kosovës – AKI, edhe sipas ligjit nr. 03-L/062, në nenin 29, është paraparë, " urdhri për përgjim emergjent" që është po ashttu aspekt i ndërhyrjes në telekomunikime apo komunikime tjera elektronike, apo masa të tjera që mund të cenojnë privatësinë.

Më konkretisht sipas nenit 29, parashihet se: " ***Në një situatë emergjente, kur koha nuk lejon përgatitjen e një kërkese me shkrim nga ana e drejtorit të AKI-së apo zëvendësdrejtorit të AKI-së apo dhënien e një urdhri me shkrim nga ana e një gjyqtari të Gjykatës Supreme, kërkesa mund të bëhet dhe urdhri për përgjim të fshehtë mund të jepet gojarisht, për t'u konfirmuar më shkrim brenda dyzetetetë (48) orësh"***[159]**.** Ndërsa po sipas këtij ligji është e rregulluar baza ligjore për ndërhyrje që plotëson edhe standardet ndërkombëtare që i lejohet këtij institucioni për ndërhyrje në privatësi me qëllim të marrjes së informatave për ruajtjen e sigurisë kombëtare dhe publike

[159] Ligjit nr. 03-L/062, Agjencioni për Siguri në Kosovë, Neni 29

e njëkohësisht edhe për procedim të mëtejmë penale ndaj subjekteve që krijohen dyshime për vepra penale.

Megjithatë ligji nuk përkufizon ndonjë rrethanë se çfarë mund të konsiderohet " emergjent", por nga vet përmbajtja e dispozitës nënkuptohet në rrethana të tilla që koha nuk është e mjaftueshme për tu ndjekur procedura e formalizuar pikërisht për shkak të rrezikut që ekziston në raport me sigurinë kombëtare apo publike, prandaj aspektin e emergjencës duhet ta ketë gjithnjë parasysh nga rrethanat faktike që kanë ekzistuar për tu vlerësuar nëse ndërhyrja ka qenë, e ligjshme dhe nëse ka qenë legjitime.

Andaj në legjislacionin tonë është e mundur ndërhyrja në të drejtën e privatësisë pa u formalizuar veprimet procedurale në rrethana të ngutshme kur ka arsyeshmëri dhe përmbushen kushtet ligjore qoftë sipas kodit të procedurës penale apo sipas ligjit brenda kompetencave që ka AKI-ja.

9. Shtrirja e të drejtës së privatësisë

Një nga qështjet e problemeve të vazhdueshme në zbatimin e drejtë të kërkesave kushtetuese por edhe të atyre ligjore është se deri në çfarë shkalle shtrihet e drejta e privatësisë. Kjo ndodh për faktin se gama e mbrojtjes që krijon dispozita nga neni 36 i Kushtetutës është shumë e zgjeruar, pasi që në paragrafin 2, përdoret togfjalëshi, : " ***ose cilitdo objekti privat",*** si dhe paragrafi 1 përdor togfjaleshin: ***" telekomunikimet"***, ***" komunikimet tjera"***.
Në këtë kuptim, duhet të kemi parasysh se çka duhet kuptuar me objekt tjetër privat. A përbën kjo vetëm me objekt që konsiderohet si send i paluajtshëm apo duhet nënkuptuar çfardo sendi që është në pronësi private të një subjekti të së drejtës qoftë person fizik apo person juridik, e që sendet e tilla mund të jenë të shumta, që janë sende të luajtshme që kanë edhe karakterin e objektit privat.

Po ashtu sa i përket telekomunikimit, a nënkupton kjo se disa kategori të veçanta e gëzojnë këtë të drejtë, si psh, nëse telekomunikimi është në rrethana të marrëdhënies së punës, a gëzohet kjo e drejtë kur mjeti i tillë i telefonit është i destinuar që shërben vetëm për punë, apo telekomunikimet që mund të jenë në shërbim të telefonisë publike a hyjnë edhe këto situata në mbrojtjen sipas të drejtës së privatësisë, apo të ndaluarit dhe të burgosurit që kanë të drejtën e

telefonisë me personat që iu lejohet, a e gëzojnë këtë të drejtë të privatësisë apo është e mjaftueshme që të vihen në dijeni se që komunikimi është paraprakisht i incizuar.

Ndërsa në situatën e komunikimeve tjera që mund të jenë të natyrës së shumtë, siç mund të jenë komunikimet me emaile, me sms, komunikimet me shkrim, komunikimet në hapësira publike ndër personale që mund t'i nënshtrohen incizimeve të ndryshme.

Më konkretisht duhet të kemi parasysh se e drejta e privatësisë a nënkupton se shtrohet vetëm në nivel të hapësirave private apo duhet të shikohet se ndërhyrja a përbën cenim të së drejtës së privatësisë pavarësisht se subjekti gjendet në hapësira publike mirëpo objekti mbrojtës që i nënshtrohet ndërhyrjes është në pronësi private, psh. Kompjuteri që qaset në të dhënat e internetit në një hapsirë publike – e dhëna e tillë e qasjes në IP të tillë publike për kufizim, a duhet për këtë të dhënë të zbatohet procedurë apo duhet që thjesht të merret nga databaza e të dhënave që janë ruajtur për qasjen e një mjeti të tillë.

Në këtë kuptim duhet të kemi parasysh se dispozitat kushtetuese mbesin të heshtura, përkundër se normat kushtetuese kanë ndërtim të aspektit parimor të të drejtave, në rrethana të tilla nuk sqarojnë se deri në çfarë niveli mund të shtrohet e drejta e privatësisë duke qenë se në thelb edhe në hapësira publike mund të cenohet kjo e drejtë marr parasysh zhvillimin shoqëror dhe kulturor. Sidoqoftë në çdo rrethanë kur subjekti i së drejtës është jashtë ambienteve tërësisht private të tij, duhet të vlerësohet rrethana nëse ai subjekt në rrethana të tilla ku është gjendur, ka pasur pritshmëri për privatësi.

Në legjislacionin tonë nuk ka një përkufizim të pritshmërisë për privatësi megjithatë standardi i tillë është i mishëruar në disa nga shtetet e zhvilluara e që edhe praktika Gjyqësore e ka trajtuar si standard pritshmërinë për privatësi. Pritshmëria për privatësi duhet nënkuptuar nëse subjekti i së drejtës, të dhënat që i ka a i ka të qasshme për publikun apo jo. Më konkretisht lidhur me çështjen e ndërhyrjes në telekomunikime apo në komunikime tjera, në manualin e Departamentit të Shtetit, " ***kërkimi dhe sekuestrimi i kompjuterëve dhe marrja e provave elektronike, ka paraparë se: " për të vlerësuar nëse një individ ka një pritshmëri të arsyeshme për privatësi mbi***

informacionin e ruajtur në një kompjuter (mjet elektronik), ndihmon që të trajtohet kompjuteri – mjeti elektronik si një enë e mbyllur, si një qante dore apo një dosje dokumentesh. Amendamenti i katërt zakonisht ndalon zbatuesit e ligjit që të hyjnë dhe të shikojnë në informacionin e ruajtur në një kompjuter pa një urdhër, ashtu siç do të ishte e ndaluar të hapnim një dosje ose një arkiv me dokumenta dhe të ekzaminonim përmbajtjen e saj në të njëjtën situatë"[160].

Në këtë kuptim duhet parë edhe garancioni kushtetues dhe të trajtohet se shtrirja e të drejtës së privatësisë nuk është e lidhur me vendin ku gjendet subjekti i së drejtës por shtrihet me të drejtën e tij që e ka të arsyeshme për privatësi, pavarësisht se a mund të gjendet në hapësira publike apo private.

Andaj, mjetet elektronike, ose objektet tjera apo komunikimet tjera, duhet të trajtohen në kuptimin, që personi a ka pritshmëri për privatësi, dhe të dhënat që mund të gjinden në mjetet elektronike apo në ndonjë objekt tjetër që mund të ketë të dhëna apo komunikime tjera që mund të përmbajnë të dhëna, duhet trajtuar të mbrojtura, pavarësisht faktit se ku gjinden ato nga se dispozita kushtetuese kërkon që ndërhyrja në këto të dhëna duhet të bëhet vetëm për qëllime legjitime, dhe deri në shkallën e domosdoshme, si dhe për zbatim të procedurës penale apo për qëllim të sigurisë publike, dhe në përputhje me dispozitat e ligjit në fuqi, sipas një urdhri të gjykatës.

10. Standardet e Krijuara nga praktika Gjyqësore e Gjykatës Kushtetuese për privatësi me rastin e ndërhyrjes ne mjetet elektronike

Pranë Gjykatës Kushtetuese janë disa raste që janë trajtuar për sa i përket një procesi të rregullt gjyqësor që ndërlidhet me dispozitën kushtetuese, të Drejtën për Gjykim të Drejtë dhe të paanshëm sipas nenit 31 si dhe të drejtën për një proces të rregullt që ndërlidhet me nenin 6 të Konventës Evropiane për mbrojtjen e të drejtave dhe lirive themelore të njeriut, si dhe të drejtën për privatësi në ndërlidhje me të drejtën për jetën private nga neni 36.

[160] Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations - Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, faqe 28.

Më konkretisht Gjykata Kushtetuese në vendimin nr. KI 113/2021, ka konstatuar se ka pasur shkelje të nenit 36 të Kushtetutës së Republikës së Kosovës – të drejtës për privatësi në lidhje me nenin 8 të drejtës për respektimin e jetës private dhe familjare të Konventës Evropiane për mbrojtjen e të drejtave dhe lirive themelore të njeriut.

Në këtë rast, Gjykata Kushtetuese kishte në çështje vlerësimin e cenimit të së drejtës për privatësi, e cila vihej në dukje se ishte cenuar përmes ndërhyrjeve në të drejtën kushtetuese për telekomunikimin.
Më konkretisht vlerësoj çështjet e: Përgjimit të telekomunikimeve, dhe Ruajtjen e të dhënave si thirrjet telefonike dhe SMS.

Në themel çështja shtrohej tek marrja e SMS-ve në mënyrë retroaktive që ruajtjen e tyre e bënte Operatori i telefonisë, e që iu kishte mundësuar Gjykatave që përmes urdhrave të merreshin sms në mënyrë retroaktive. Përkundër se Gjykatat e rregullta si ajo shkallës së parë dhe Gjykata e Apelit kishin shqyrtuar pretendimet për shkelje ligjore të parashtruara për marrjen retroaktive të SMS-ve, që të dy këto gjykata kishin refuzuar pretendimet që këto prova (SMS) të shpalleshin si prova të papranueshme. Ndërsa Gjykata Supreme, kishte arsyetuar se, fakti i marrjes së SMS në mënyrë retroaktive qëndron por se nuk ishin provat e tilla vendimtare për të ardhur në konkludimin për fajësinë e të akuzuarës.

Gjykata Kushtetuese, i është referuar praktikës së GJEDNJ-së, për sa i përket disa aspekteve të rëndësishme që krijojnë garancionet maksimale të respektimit të drejtës së privatësisë, dhe poashtu kur mund të bëhet ndërhyrja në të drejtën e privatësisë.

Fillimisht Gjykata Kushtetuese, duke pasur për shqyrtim çështjen e marrjes retroaktive të SMS-ve që përbënte ndërhyrje në telefoni, kishte konstatuar se, GJEDNJ-ja, ka konkluduar se: “ Bisedat Telefonike – janë të mbuluara me Nocionin e Jetës Private dhe korrespodencës” dhe se monitorimi i tyre përbën ndërhyrje në të drejtën e garantuar sipas nenit 8 të Konventës Evropiane për mbrojtjen e të drejtave dhe lirive themelore të njeriut. Nga kjo duhet kuptuar se nuk mund të vihet në mëdyshje që bisedat telefonike qofshin ato zanore apo të shkruara hyjnë në kuadratin e qëllimit të ruajtjes së të drejtës për privatësi.

Gjykata Kushtetuese, ka vlerësuar po ashtu standardet e GJEDNJ-së, që kanë konstatuar në praktikën e saj se ndërhyrja e tillë është në pajtim me nenin 8 vetëm nëse:

a) Është në pajtim me ligjin;
b) Ndjek një qëllim të ligjshëm, dhe
c) Nëse është e nevojshme për një shoqëri demokratike.

Tutje Gjykata Kushtetuese i referohet praktikës së GJEDNJ-së, çështjes së shprehjes, " ***në pajtim me ligjin***", që nënkupton se kjo shprehje ka të bëjë se ndërhyrja e tillë duhet të jetë e paraparë me të drejtën e brendshme por jo vetëm si normë por edhe si kualitet brenda normës, çka nënkupton se duhet të jetë për qëllim të sundimit të ligjit dhe i qasshëm për personin ndaj të cilit zbatohet që konsiston në mundësinë e ***parashikimit*** të pasojave për personin ndaj të cilit zbatohet.
Parashikueshmëria sipas vlerësimit të Gjykatës Kushtetuese, nuk duhet nënkuptuar se personi duhet të jetë në dijeni të veprimit të tillë që është duke u zbatuar një masë si ndërhyrje në të drejtën e privatësisë që ai t'i përshtat sjelljet.

Parashikueshmeria nënkupton përcaktimin e qartë të situatave dhe rrethanave se kur mund të aplikohet masa e tillë që përbën ndërhyrje ndaj të drejtës së privatësisë. Rrjedhimisht përmes situatave të tilla dhe rrethanave që individët mund të gjinden ata mund të parashikojnë se edhe mund të aplikohet masa e ndërhyrjes.

Parashikushmëria duke u definuar qartë në dispozitat ligjore që përbëjnë situata dhe rrethanat e qarta se kur mund të aplikohet masa e ndërhyrjes, shmang edhe arbitraritetin e organeve që iu jepet diskrecioni për aplikimin apo urdhërimin e masave të tilla.

Gjykata Kushtetuese duke iu referuar praktikës së GJEDNJ-së, thekson se: ***"Marrë parasysh rrezikun që sistemi i vëzhgimit sekret për sigurinë nacionale, mund të minojë apo shkatërrojë demokracinë me pretekst të ruajtjes së saj, GJEDNJ duhet të jetë e bindur që ekziston garanci ndaj abuzimeve që janë adekuate dhe efektive. Ky vlerësim varet nga të gjitha rrethanat e rastit, si natyra, fushëveprimi dhe kohëzgjatja e masave të mundshme, bazën që kërkohet për të urdhëruar ato, autoritetin kompetent***

që lejon, që ekzekuton dhe që mbikëqyr një gjë të tillë, dhe mundësitë e korrektimit që parashihen nga e drejta e brendshme"[161].

Gjykata kushtetuese po ashtu i referohet praktikës së GJEDNJ-së se çfarë është domosdoshmëria e ndërhyrjes në shoqëritë demokratike. Që konstaton se, shtetet kanë një hapësirë të madhe të vlerësimit të domosdoshmërisë së ndërhyrjes në qëllim për ruajtjen e shoqërisë demokratike, megjithatë kjo hapësirë i nënshtrohet mbikëqyrjes nga GJEDNJ. Nga ana tjetër theksohet se vlerat e nevojshme në shoqëritë demokratike duhet të ruhen në mirëbesim, në mënyrë që kufijtë e nevojës së domosdoshme të ndërhyrjes të mos tejkalohen, që do të përbënte ndërhyrje në cenim të drejtës për privatësi gjegjësisht të drejtës për jetë private dhe familjare.

Mbi këto parime të vendosura nga praktika e GJEDNJ-së, Gjykata Kushtetuese në çështjen konkrete ka trajtuar," Nëse marrja e sms-ve në mënyrë retroaktive konsiderohet ndërhyrje në të drejtën e saj për jetë private dhe familjare dhe nëse kishte cenuar të drejtën për privatësi kjo ndërhyrje, të drejta këto që parashihen me nenin 8 të KEDNJ-së dhe 36 të Kushtetutës së Republikës së Kosovës.

Gjykata Kushtetuese në radhë të parë në trajtimin e rastit kishte konstatuar se, përgjimi i telekomunikimeve dhe marrja e SMS-ve bëjnë pjesë në kategorinë e masave ndërhyrëse në të drejtën për jetë private dhe të privatësisë.
Tutje kishte konstatuar tri aspekte sipas legjislacionit të brendshëm:

a) Kompetencën për lëshimin e urdhrave për përgjimin e telekomunikimit dhe marrjen e sms-ve, që e kishte Gjyqtari i Procedurës Paraprake;
b) Kohëzgjatjen e vlefshmërisë së urdhrit për përgjim të telekomunikimit dhe marrjes së SMS-ve, që ishte afati 60 ditor, dhe
c) Afatin për ruajtjen e të dhënave nga operatorët telefonik të rrjetave që parashihej se ishte afati 1 vjeçar si afat i ruajtjes së të dhënave.

Më konkretisht në elaborimet e analizuara të pretendimeve nga Gjykata kushtetuese ishte konstatuar se:
"***Andaj, duke pasur parasysh parimet e përgjithshme të përcaktuara nga GJEDNJ, dispozitat relevante të KPPK-së dhe Ligjit për Komunikimet***

[161] Gjykata Kushtetuese e Republikës se Kosovës, Vendimin nr. KI 113/2021.

Elektronike rezulton se përgjimi retroaktiv, duke përfshirë nxjerrjen dhe leximin i mesazheve (SMS-ve) në mënyrë retroaktive, është i e ndaluar. Rrjedhimisht, Gjykata vlerëson se nxjerrja e përmbajtjes së SMS-ve në mënyrë retroaktive, në rastin konkret nuk është një masë e "paraparë me ligj", ashtu si kërkohet me parimet e të drejtës për privatësi të garantuar me nenin 36 të Kushtetutës, dhe nenin 8 të KEDNJ-së. Kjo për më tepër duke pasur parasysh faktin që neni 92 i KPPK-së përcakton në mënyrë shprehimore që urdhri për përgjim nuk duhet ta kalojë periudhën prej gjashtëdhjetë (60) ditëve nga "data e lëshimit".

"Në këtë drejtim, Gjykata rithekson se për rrethanat e rastit konkret relevante është "pyetja e parë" e testit të nenit 55 të Kushtetutës, respektivisht se "a ka qenë kufizimi i një lirie apo të drejtë themelore të garantuar me Kushtetutë " i përcaktuar me ligj?". Pasi Gjykata sapo konstatoi se kufizimi i të drejtës për privatësi të garantuar me nenin 36 të Kushtetutës, dhe nenin 8 të KEDNJ-së, nuk ka qenë i paraparë me ligj, atëherë nuk është e nevojshme përgjigja në pyetjet nëse ky kufizim ka pasur qëllim legjitim, dhe nëse ka qenë i nevojshëm në një shoqëri demokratike (shih, mutatis mutandis, rastin e Gjykatës KO157/18, parashtrues Gjykata Supreme, Aktgjykim i 13 marsit 2019, paragrafi 114)".

"Nga si u tha më lart, Gjykata konsideron se leximi retroaktiv i mesazheve SMS përmes Urdhrit [PP: 51/2014] të Gjykatës Themelore në Prizren, të 10 marsit 2014, ka shkelur të drejtën e parashtrueses së kërkesës të garantuar me nenin 36 [E Drejta e Privatësisë] të Kushtetutës, dhe nenin 8 (E drejta për respektimin e jetës private dhe familjare) të KEDNJ-së"[162].

Rrjedhimisht nga ky aktgjykim, marr për bazë parimet e vendosura nga GJEDNJ duhet të konkludojmë se, për respektimin e të drejtës së privatësisë nga neni 36 dhe respektimin e të drejtës për jetë private dhe familjare nga neni 8 i KEDNJ-së, janë të mishëruara parimet:

a) Bazës ligjore per ndërhyrje (e drejta e brendshme e përcaktuar);

[162] Gjykata Kushtetuese e Republikes se Kosoves, Vendimin nr. KI 113/2021.

b) Kualiteti i bazës ligjore të përcaktuar për masat ndërhyrëse (kjo nënkupton se duhet të jetë e qartë baza ligjore se në çfarë rrethanash dhe cilat situata do të mundet një qytetar t'i nënshtrohet ndërhyrjes);
c) Domosdoshmëria e ndërhyrjes (që nënkupton se ndërhyrja duhet të konsiderohet vetëm në shkallën e domosdoshme dhe vetëm për aq sa ruan vlerat demokratike të shoqërisë)
d) Parashikueshmëria (kjo nënkupton se qasja e tillë e rrethanave dhe kushteve që qytetari mund t'i nënshtrohet ndërhyrjes duhet të jenë të ditura për një sistem të parashikueshëm);
e) Zbatimi i diskrecionit dhe shmangia arbitrare, (kjo nënkupton se urdhërimi i masave të ndërhyrjes duhet të jetë, i mbikëqyrur me kushte të veçanta ligjore e të qarta dhe shmangia nga arbitrariteti).

Si efekt nga ky vendim i Gjykatës Kushtetuese, shumë raste që kanë rezultuar në marrjen e provave të tilla në mënyrë retroaktive, që është konstatuar se nuk ishte paraparë me ligj mënyra e tillë e ndërhyrjes si masë në të drejtën e privatësisë edhe raste të tjera kanë dështuar në procedurat para gjykatave të rregullta gjyqësore, marr parasysh se të provuarit e fakteve mbështetej për faktet vendimtare në të dhënat e tilla që ishin siguruar si prova në mënyrë retroaktive, dhe se Gjykatat e rregullta nuk kishin lejuar tutje konkludim për fajsinë që faktet vendimtare të mbështeteshin në provat e tilla që tashme Gjykata Kushtetuese kishte vendosur standarde që veprimet e tilla në shmangie të këtyre standardeve përbënte ndërhyrje në të drejtën e privatësisë dhe në të drejtën për jetën private dhe familjare, që efektivisht përbënin shkelje të të drejtave kushtetuese për qytetarët.

11. Heqja dorë nga të drejtat e garantuara

Kushtetuta e Republikës së Kosovës, nuk përcakton në mënyrë shprehimore ndonjë mundësi të heqjes dorë nga të drejtat individi që i gëzon sipas kushtetutës, rrjedhimisht as sa i përket heqjes dorë nga e drejta e privatësisë.

Megjithatë në të drejtat e njeriut në kapitullin II të Kushtetutës, në ato të drejta që mund të kufizohen përkohësisht, siç njëra nga to është edhe e drejta e privatësisë në të cilën përmes masave mund të ndërhyhet në të, parashihet se ndërhyrja mund të bëhet vetëm sipas ligjit.

Në këtë kuptim dispozitat e Kodit të Procedurës penale, pikërisht me disa aspekte të ndërhyrjes që janë ngushtë të lidhura me të drejtën e privatësisë, njohin dhënien e pëlqimit nga personi që i nënshtrohet masës së ndërhyrjes.

Pëlqimi në këtë kuptim, është mundësi që në thelb përbën heqje dore nga të drejtat kushtetuese e vet subjektit që i nënshtrohet masës së ndërhyrjes që mund të cenoj privatësinë, dhe përmes dhënies së pëlqimit legjitimohet ndërhyrja e organeve shtetërore në të drejtën e privatësisë.

Megjithatë, dispozitat e kodit të procedurës penale, ndërtojnë thjeshte mundësinë e dhënies së pëlqimit, por nuk rregullojnë më në detaje se dhënia e pëlqimit gjegjësisht heqja dorë nga e drejta a mund të revokohet nga ana e subjektit që lejon ndërhyrjen në të drejtën e tij.

Sipas Kushtetutës se Republikës së Kosovës, e drejta e privatësisë në nenin 36 parasheh mundësinë e ndërhyrjes në këtë të drejtë sipas ligjit, pastaj e drejta e integritetit personal në nenin 26 që parasheh se kjo e drejtë nuk mund të cenohet në kundërshtim me vullnetin e tij përveç se sipas ligjit, përkatësisht shume të drejta që garantohen përcaktojnë se ato mund të kufizohen vetëm sipas ligjit, në anën tjetër neni 55 i Kushtetutës që ka paraparë Kufizimin e të Drejtave dhe Lirive të Njeriut, nuk parasheh ndonjë dispozitë konkrete se individi a mund të heq dorë për qëllim që t'i lejoj autoriteteve shtetërore kufizimin e të drejtës së tij për efekt të ndërmarrjes së veprimeve të caktuar, mirëpo aspekti i heqjes dorë të së drejtave në procedurën penale është i njohur për disa të drejta që mund të hiqet dorë duke dhënë pëlqimin për ndërhyrje.
Ndërsa nga ana tjetër, sipas Kodit të Procedurës penale, kontrolli pa urdhër gjyqësor sipas nenit 103 mund të bëhet duke dhënë pëlqimi subjekti që i nënshtrohet kontrollit, apo sipas nenit 142 ekzaminimi i lëndimeve trupore apo ekzaminimi fizik (ku mund të ketë ndërhyrje në integritetin trupor), në paragrafin 3 personi që i nënshtrohet ekzaminimit mund të jap pëlqim dhe ndërhyrja bëhet pa urdhër të gjykatës, apo analiza kompjuterike sipas nenit 145, parasheh se ndërhyrja në pajisje kompjuterike, pajisje të ruajtjes apo pajisje të ngjashme, mund të bëhet edhe me dhënien e pëlqimit nga ana e subjektit që i është marr pajisja, pra janë një mori veprimesh që organet shtetërore mund të zbatojnë ndërhyrje që mund të prekin të drejtat kushtetuese përmes dhënies së pëlqimit nga subjektet që i nënshtrohen kësaj ndërhyrje dhe dhënia e pëlqimit në fakt përbën heqje dore nga të drejtat e garantuara

kushtetuese dhe shmangie të zbatimit të procedurës formale që bëhet përmes vendimeve si aspekt të masave ndaj atyre subjekteve.

Përkundër se dispozitat parashohin dhënie të pëlqimit që në themel përbën heqje dore nga të drejtat kushtetuese individuale, duhet të kemi parasysh se nuk është e mjaftueshme thjesht deklarimi por se duhet aspekt i të provuarit se në të vërtet individi ka dhënë pëlqimin për heqjen dore nga e drejta që i takon dhe ka lejuar një ndërhyrje që në të kundërtën e gëzon sipas kushtetutës.

Përveç se duhet të jetë e vullnetshme, heqja dorë vlerësojmë se duhet të jetë:

a) Njoftimi i plotë për qëllimin e dhënies së pëlqimit,
b) Vetëdije të plotë për shkaqet e sakta që bëhet heqja dorë dhe jepet pëlqimi;
c) Vetëdije të plotë për pasojat e mundshme me rastin e heqjes dorë nga e drejta dhe dhënia e pëlqimit.

Nisur nga këto rrethana, mund të jetë tepër sfiduese që dhënia e pëlqimit të konsiderohet si heqje dorë nga të drejtat, dhe lejimin e organeve shtetërore që të ndërhyjnë në jetën private të personit që i nënshtrohet ndërhyrjes, andaj në çdo rast të dhënies së pëlqimit duhet të kemi parasysh sfidat si:

a) Dispozitat e Kodit të Procedurës Penale nuk përcaktojnë një procedurë konkrete dhe të qartë për dhënien e pëlqimit nga ana e personit që lejon ndërhyrjen në privatësi, (procedurë kjo që do të konsiderohej si e paraparë me ligj) si një ndër standardet që kërkohet.

b) Në çdo rast konkret duhet të dëshmohet se është dhënë njoftim i saktë dhe i qatë nga autoritetet shtetërore që kërkojnë ndërhyrjen, e palës i është bërë me dije saktësisht që duhet të jap pëlqimin vullnetarisht për t'i lejuar që të ndërhyjnë në të drejtën e tij,

c) Në secilin rast konkret duhet të kemi parasysh se cilat janë rrethanat që mund të na japin të vlerësojmë nëse ka qenë i vetëdijshëm, p.sh a ka gjendje normale psiqike, a është në gjendje të frikës dhe si pasoj e frikës ka dhënë pëlqimin, a është i alkoolizuar apo nën ndikimin e substancave psikotrope, këto rrethana na mundësojnë që të vlerësojmë nëse personi që ka dhënë pëlqimin dhe heq dorë nga të drejtat kushtetuese është i vetëdijshëm.

d) Vetëdija për pasojat e mundshme të heqjes dorë, duhet të jetë vlerësim sipas rastit pasi që subjekti që heq dorë nuk mund të i kuptoj pasojat që mund t'i shkaktoj heqja dorë nga ana tjetër dhënia e pëlqimit duhet të shtrohet deri në atë masë që e kupton personi që i nënshtrohet kësaj ndërhyrje nga autoritetet shtetërore e që përbën heqje dorë nga të drejtat kushtetuese pasi që kjo efektivisht mundëson rrugë të inkriminimit të vetës së tij kur gjinden prova për procedim penal, pra kuptimi i pasojave duhet të shtrihet deri në masën që heqja dorë mundëson në mënyrë të tërthortë vet inkriminimin pasi që lejon autoritetet shtetërore që me aktin e heqjes dorë të mbledhin prova kundër subjektit që i nënshtrohet ndërhyrjes në të drejtën e tij.

Praktika e zbatueshme në Kosovë, për sa i përket disa aspekteve të heqjes dorë, formalizon procedurën, p.sh ndërhyrja për qëllim të ekzaminimit apo ndërhyrjes mjekësore bëhet me dhënien e pëlqimit me shkrim si formë standarde e dhënies së nënshkrimit, ndërsa dhënia e pëlqimit për zbatimin e kontrollit bëhet me konstatimin në procesverbalin e kontrollit që mbahet nga policia, në të cilin nënshkruan personi që ka dhënë pëlqimin, ndërsa dhënia e pëlqimit për ekzaminim të telefonit bëhet me konstatimin e nënshkrimit të dhënësit të telefonit se pajtohet për ndërhyrje nga ekzaminimi.

Megjithëse asnjëra nga këto procedura të formalizuara deri në këtë pikë, nuk përmbajnë qartësi të duhura, dhe të sakta, si për masën dhe arsyeshmërinë e ndërhyrjes si informacion që duhet t'i jepet personit që jep pëlqimin, si për konstatimin nëse i njëjti është i vetëdijshëm për pasojat e dhënies së pëlqimit dhe heqjes dorë, si për masën dhe të kuptuarit e shkaqeve të sakta që heq dorë nga e drejta e tij dhe jap pëlqimin për ndërhyrje.

Angazhimi i organeve të ndjekjes, në të ardhmen duhet të jetë që të standardizohet procedura e dhënies së pëlqimit e cila heq dorë pala nga të drejtat e tij kushtetuese dhe lejon ndërhyrjen e autoriteteve, në mënyrë që të përmbaj procedura qartësi për të gjitha detyrimet e organeve shtetrore që ndërhyrjen e bëjnë përmes marrjes së pëlqimit.

12. Revokimi i pëlqimit - revokimi i heqjes dorë

Dispozitat ligjore lejojnë mundësin e heqjes dorë nga të drejtat që iu garantohen me Kushtetutë, përveç se duhet të kemi parasysh se subjekti duhet të jetë plotësisht i vetëdijshëm për rrethanat, pasojat dhe shkaqet e që kjo të bëhet në mënyrë vullnetare, po ashtu duhet pasur parasysh nëse dhënia e pëlqimit gjegjësisht heqja dorë a mundet në çfarëdo rrethane të revokohet apo duhet konsideruar se heqja dorë në asnjë rrethanë nuk mund të konsiderohet si e mundshme të revokohet në asnjë moment.

Kodi i procedurës penale në këtë drejtim edhe pse njeh dhënien e pëlqimit gjegjësisht heqjen dorë nga e drejta kushtetuese, sa i përket revokimit të dhënies së pëlqimit nuk jep ndonjë zgjidhje të mëtejshme nëse duhet njohur të drejtën e individit që ka dhënë pëlqimin që atë pëlqim ta revokoj që në efekt do të përbënte revokim të asaj që ka hequr dorë nga e drejta e garantuar kushtetuese.

Megjithatë marr për bazë dispozitën e nenit 53 të Kushtetuës, e cila parasheh se autoritetet duhet t'i interpretojnë të drejtat dhe liritë e njeriut në përputhje me praktikën e GJEDNJ-së, është GJEDNJ që ka zhvilluar në disa raste praktikën dhe standardet për sa i përket dhënies së pëlqimit që lejon autoritetet shtetërore që sipas atij pëlqimi të palës të ndërhyjnë, dhe po ashtu aspektin e revokimit të pëlqimit.
Gjykata Evropiane për të drejtat dhe liritë e njeriut, në praktikën e saj ka theksuar se, heqja dorë nga e drejta është e mundur, por ka konstatuar se ajo heqë dorë, mund të bëhet vetëm në raport me disa të drejta që garanton Konventa Evropiane për Mbrojtjen e të Drejtave dhe Lirive Themelore të Njeriut, pra disa të drejta të natyrës me karakter absolut nga të drejtat e tilla nuk mund të njihet instituti i heqjes dorë nga të drejtat.

Nga ana tjetër në praktikën e saj, Gjykata Evropiane për të drejtat dhe liritë e njeriut, ka konstatuar se, edhe revokimi i heqjes dorë nga të drejtat është i njohur dhe duhet të jetë i vlefshëm nën kushtet e caktuara.

Më konkretisht GJEDNJ ka ndërtuar disa standarde kur heqja dorë mund të revokohet, gjegjësisht kur dhënia e pëlqimit mund të revokohet e që efektivisht përbën revokim të heqjes dorë nga e drejta, dhe se standardet e tilla konsistojnë në rrethanën kur pëlqimi nuk ka qenë real e që kushtet e tilla janë:

a) Kur heqja dorë është bërë nën presion;

b) Kur personi që ka hequr dorë nuk ka kuptuar pasojat;
c) Kur tejkalohet pëlqimi apo ajo që është hequr dorë.

Karakteristikë është se, gjykata revokimin e heqjes dorë nga të drejtat nuk e ndërlidh me natyrën e procedurës që ndiqet, kur është hequr dorë nga të drejtat. P.sh. Nuk ka në praktikën e GJEDNJ-së, situata që një person nëse ka hequr dorë dhe veprimi kryhet aty për aty nga organet e ndjekjes, por në rrjedhë e sipër pas përfundimit të veprimit personi mohon dhënien e pëlqimit për cilindo nga shkaqet e theksuara si me sipër siç mund të jetë arsyeja se nuk i ka kuptuar pasoja. Në këtë këndvështrim Gjykata nuk lëshohet në faktin se a është arritur ndërhyrja e autoriteteve deri në qëllimin që është dhënë pëlqimi, por vlerëson kriteret mbrojtëse për subjektin, që i bënë të detyrueshme në çdo rrethanë gjykatat e vendeve që t'i vlerësojnë në çdo situatë nëse janë cenuar këto standarde atëherë ajo duhet konsideruar efektivisht si revokim i pëlqimit.

Nga ana tjetër Gjykata njeh edhe kufizime të revokimit të dhënies së pëlqimit, në praktikën e saj ajo po ashtu ka përcaktuar standarde se REVOKIMI nuk mund të bëhet nëse:

a) Heqja dorë është bërë në mënyrë të qartë;
b) Heqja dorë është bërë në mënyrë të dokumentuar dhe me ndihmën e mbrojtësit;
c) Se heqja dorë nuk mund të bëhet për arsye subjektive pa shkaqe reale.

Më konkretisht praktika e GJEDNJ-së, kur ka konstatuar se heqja dorë nuk është e vlefshme dhe që përbënte shkelje, janë rastet e trajtuara në praktikën e saj:

1. Deëeer kundër Belgjikës, ku Gjykata konstatoj se: ***Hejqa dorë e bërë nën detyrim nuk prodhon efekt dhe mund të revokohet nga individi.***
2. Pfeifer dhe Plankl kundër Austrisë, ku Gjykata konstatoj se: ***Revokimi është i vlefshëm nëse personi nuk ka kuptuar plotësisht natyrën e heqjes dorë, heqja dorë duhet të jetë unequivocal and attended by minimum safeguards – heqja dorë duhet të jetë pa ekuivokë (pa mëdyshje) dhe me garancione minimale.***
3. Hermi kundër Italisë, ku Gjykata ka konstatuar se: ***Revokimi i heqjes dorë nga prania në gjykim duhet të pranohet nëse kërkohet në kohë dhe me qartësi.***

4. Natsvlishvilli dhe Togonidze kundër Gjeorgjisë, ku Gjykata ka konstatuar se: ***Heqja dorë nga e drejta për gjykim(marrveshja për pranimin e fajsisë), mund të revokohet vetëm nëse ishte e pavullnetshme ose e pambështetur në garanci.***
5. Sejdoviq kundër Italisë, ku Gjykata ka konstatuar se: ***Në mungesë të provave për heqje dorë të qartë, kërkesa për revokim duhet të pranohet.***
6. Jones kundër Mbretërisë, ku Gjykata ka konstatuar se: Revokimi i heqjes dorë nga ankesa duhet të pranohet deri në përfundimin e procesit.
7. e.Salihoglu dhe të tjerët kundër Turqisë, ku Gjykata ka konstatuar se: ***Pranimi/pëlqimi i dhënë nën presion apo pa ndihmën e avokatit nuk përbën heqje dorë të vlefshme.***

Nisur nga standardet e GJEDNJ-së, dhe mbështetur në dispozitën e nenit 53 të Kushtetutës së Kosovës, për çdo heqje dorë nga të drejtat dhe dhënien e pëlqimit nga i pandehuri që mundëson kodi i procedurës Penale, e marr parasysh se nuk ka ndonjë dispozitë që rregullonte revokimin e dhënies së pëlqimit, mund të përfundohet se në çdo rast kur veprimi i organeve shtetërore është ndërmarr në raport me të pandehurin që pëlqimi mund të përbëj heqje dorë nga të drejtat kushtetuese (për të drejtat që lejohet heqja dorë), gjithnjë duhet të vlerësojmë këto kushte:

1. A është bërë në mënyrë vullnetare heqja dorë – e kundërta presioni apo mënyra që do të përbënte cenim të vullnetit nuk konsiderohet heqje dore dhe duhet njohur revokimi i tillë.
2. A është njoftuar për pasojat e mundshme të heqjes dorë – e kundërta nëse heqja dorë nuk ka qenë e dokumentuar mjaftueshëm për ta njoftuar qartë dhe saktë për pasojat heqja dorë nuk duhet të konsiderohet dhe duhet njohur e drejta e revokimit,
3. A është i vetëdijshëm për heqjen dorë – e kundërta nëse mundësia e tij e vetëdijes në çfarëdo rrethane vënë në mëdyshje gjendjen e tij për të kuptuar pasojat duhet konsideruar pavlefshmerinë e pëlqimit dhe revokimi duhet njohur.
4. Heqja dorë a është e lirë dhe a është në ndihmën e mbrojtësit të tij – e kundërta nëse heqja dorë nuk mund të vërtetohet si liri e plotë e vullnetit dhe në pamundësinë e njoftimit dhe konsultës me

mbrojtës nuk mund të konsiderohet heqje dorë e drejtë dhe revokimi duhet njohur,

5. A ka pëlqim të tërësishëm për veprim të caktuar nga organet shtetërore apo vetëm të pjesshëm – tejkalimi i pëlqimit nga organet shtetërore nuk mund të konsiderohet heqje dorë dhe duhet njohur e drejta e revokimit.

Çështja e tejkalimit në praktikën e GJEDNJ-së zë vend të rëndësishëm nga se lidhet me proporcionalitetin e veprimeve të organeve si ndërhyrje në të drejtën që proporcionaliteti është një nga standardet e përgjithshme që në çdo rrethanë e vlerëson GJEDNJ-ja nëse autoritetet kanë shkelur të drejtat e garantuara me Konventë.

Kjo posaçërisht është e ndërlidhur me dhënien e pëlqimit për një veprim kufizues nga i pandehuri që mund ta jap të organet e ndjekjes, në ndërhyrjen e mjeteve elektronike të tij. P.sh. Nëse autoritetet i kërkojnë pëlqimin për komunikimin e zhvilluar në rrjetet sociale të ditës së ndalimit të pandehurit me një person tjetër. Pëlqimi i dhënë në këtë situatë për këtë ndërhyrje, nuk i krijon bazë të proporcionalitetit autoriteteve që të marrin tërë komunikimin me atë person. Apo nuk i krijon bazë autoriteteve që të marrin të gjitha të dhënat në telefonin e tij përfshirë edhe të dhënat që i ruan ai në telefon që mund të jenë me të njëjtin person.

Veprimet e tilla do të konsideroheshin si jo proporcionale dhe dhënia e pëlqimit nuk do të konsiderohej si e vlefshme rrjedhimisht i pandehuri do të mund të kërkonte revokimin e pëlqimit të tij. Efektivisht nga Gjykatat e rregullta ndërmarrja e një veprimi të tillë do të përbënte shkelje të dispozitave të Kodit të procedurës penale për sa i përket pranueshmërisë së provave në procedurën penale, pasi që do të cenohej e drejta e garantuar me Kushtetutë siç është e drejta e privatësisë. Prandaj edhe në rastin e heqjes dorë nga të drejtat parimi i proporcionalitetit të ndërhyrjes nuk humb vlerën e saj sipas praktikës së GJEDNJ-së pasi që do të përbënte cenim dhe bazë për tu tërhequr nga heqja dorë e të drejtës së garantuar.

13. Vlefshmëria e heqjes dorë në raport me personat e tretë

Gjykata Evropiane për të drejtat dhe liritë e njeriut, në praktikën e saj nuk ka trajtuar ndonjë rast kur subjekti i së drejtës ka hequr dorë nga të drejtat e tij (ato të drejta që nuk janë të natyrës absolute), se kjo heqje dore a ka efekt edhe ndaj personave të tretë, gjegjësisht se kur hiqet dorë nga të drejtat nga një i dyshuar a cenohet privatësia e të drejtave të personave të tjerë nëse po ashtu në shtëpitë apo objektet tjera apo pajisjet elektronike ka të dhëna të personave të tretë që nuk janë fare subjekt i procedurës.

Konsiderojmë se, e drejta qoftë ato të garantuara me konventën evropiane për mbrojtjen e të drejtave dhe lirive themelore të njeriut apo me aktet tjera ndërkombëtare apo me kushtetutën e vendit, kur ndonjë individ ndaj të cilit është duke u zhvilluar procedura penale heq dorë nga të drejtat e tij dhe lejon autoritetet shtetërore për të ndërhyrë në të drejtën e tij, efekti i heqjes dore duhet të jetë vetëm në raport me subjektin që ka hequr dorë, pasi që të drejtat janë të lidhura ngushtë me subjektin që jap pëlqimin dhe jo për tu shtrirë me efekt tek personat e tretë.
Dhënia e pëlqimit nuk duhet të shtrihet në aspektin e mundësisë për cenimin e personit të tretë nëse sendi apo objekti i nënshtrohet ndërhyrjes në të cilin edhe personi i tretë ka privatësi.

Në anën tjetër, duhet të kihet parasysh edhe çështja e statusit të provave të tilla, nëse përmes ndërhyrjes ndaj personit të tretë krijohet ndonjë bazë për ndjekje penale.

Më konkretisht në një shembull, ku: “ i dyshuari jap pëlqimin për ndërhyrje të autoriteteve shtetërore në kontroll të shtëpisë apo të telefonit të tij, dhe personi i tretë që ka po ashtu të drejtë në atë send për privatësi, pra kur i dyshuari jep pëlqimin për ndërhyrje të kontrollit në shtëpi apo në objekte tjera duhet të kemi parasysh nëse në kuadër të asaj prone heqja dorë nga të drejtat që është bërë nga i dyshuari a cenon të drejtën e privatësisë ndaj personave që po ashtu kanë privatësi në atë shtëpi apo objekt, në rrethana të tilla duhet që autoritetet shtetërore ose të sigurojnë pëlqimin e subjekteve që lejojnë autoritetet shtetërore për ndërhyrje ose për rrugën më të sigurt të sigurojnë urdhrin gjyqësor për ndërhyrje.

Kjo mënyrë e autoriteteve shtetërore, përveç se do të legjitimonte veprimet njëkohësisht nuk do të rrezikohej cenimi i ligjshmërisë së provave nëse eventualisht gjendet ndonjë bazë për ndjekje penale edhe ndaj personave të tretë.

Prandaj gjithnjë kur mëdyshjet ekzistojnë se në sendin që i nënshtrohet ndërhyrjes – kufizimit të të drejtës është hequr dorë nga subjekti nëse në atë send ka të drejta edhe subjekti tjetër gjithnjë është e rekomandueshme që ndërhyrja – kufizimi i kësaj të drejte të bëhet me urdhrin që sigurohet nga autoritetet nëse personat e tretë për çfarëdo arsye nuk mund të sigurohen për heqjen dorë apo nuk heqin dorë që te ndërhyhet në objektin apo sendin që i nënshtrohet ndërhyrjes.

Rrjedhimisht heqja dorë nga të drejtat gjithnjë krijon një bazë më të zbehtë të autoriteteve për ndërhyrje, marr parasysh se ka kritere për heqjen dorë dhe po ashtu ka bazë edhe për revokim dhe marr parasysh se kjo nuk garanton veprim të ligjshëm e proporcional në raport me personat e tretë.

KAPITULLI V

PROVAT ELEKTRONIKE

Burim Ademi, Gjyqtar në Gjykatën Supreme të Kosovës

Burim Ademi, Gjyqtar në Gjykatën Supreme të Kosovës

1. PROVAT ELEKTORNIKE

1.1 Shqyrtime të përgjithshme

Është theksuar më sipër se çdo send personal – privat që mund të përmbaj të dhëna e që nuk janë të qasshme për publikun qofshin edhe ato elektronike, duhet të konsiderohen në kuadrin e mbrojtjes për privatësi që parashihet në nenin 36 të Kushtetutës së Republikës së Kosovës, gjegjësisht në nenin 8 të Konventës për mbrojtjen e të drejtave dhe lirive themelore të njeriut.

Mjetet elektronike, janë të shumta dhe të ndryshme që si të tilla mund të përmbajnë të dhëna të ndryshme, qoftë të dhëna të qasjes, të dhëna të ruajtura apo çfardo të dhëne tjetër.

Si të tilla, mjetet elektronike nuk duhet nënkuptuar vetëm telefonin, kompjuterin, llaptopet, por edhe aparatet fotografike, printerët, skanerët, ruteret, kamerat, diviaret, sd kartat, usb, apo çdo gjë që mund të përbëj aspekt elektronik, përmes së cilit ka të dhëna të ruajtura apo të qasshme që mund të vijë deri te një informacion qoftë edhe për vendndodhjen e një personi apo vendndodhjen e një pajisje që lidhet me identifikimin e vendndodhjes së një personi.

Më konkretisht, mjetet elektronike nuk duhet ndërlidhur me faktin se a përmbajnë të dhëna personale në kuptim të emrit identifikues për personin, por çdo e dhënë që mund të shërbej se përmes asaj të dhëne mundësohet që të identifikohet subjekti apo vendndodhja e subjektit të së drejtës.

1.2 Garancionet sipas kodit të procedurës penale

Kodi i procedurës penale të Kosovës, ka paraparë dy mundësi që sendet elektronike gjegjësisht të dhënat nga sendet elektronike të merren për qëllime të procedurës penale që zhvillohet;

1. Përmes sekuestrimit të sendeve, dhe
2. Përmes dorëzimit nga vet i pandehuri të sendeve elektronike.

Sa i përket bazës së parë, dispozitat e kodit të procedurës penale, mundësojnë që në disa forma të sigurohen nga organet e ndjekjes sendet e tilla elektronike që mund të shërbejnë qoftë si prova apo edhe si sende që kanë shërbyer në kryerjen e veprës penale duke mos përjashtuar që ato të jenë edhe dobi pasurore e veprës penale.

Kur sendet e tilla elektronike që janë në disponim të të pandehurit apo personit të tretë, merren si prova kodi i procedurës kërkon që të njëjtat sende me rastin e ekzaminimit, të sigurohet zbatimi i kërkesave ligjore në mënyrë që të mos cenohet e drejta e privatësisë.

Nga ana tjetër edhe marrja e sendeve drejtpërdrejt nga i pandehuri gjegjësisht dorëzimi i sendeve nga i pandehuri me vullnet, përbën mundësinë e dhënies së pëlqimit për ndërhyrje të ekzaminimit të sendeve elektronike.

Më konkretisht sipas dispozitës nga neni 145 në Kodin e Procedurës Penale është paraparë rregullimi i analizës kompjuterike, e që sipas kësaj dispozite përcaktohet se çdo ekzaminim duhet t'i nënshtrohet rregullave nga neni 133 deri në nenin 140 (ku rregullohet raporti i ekspertit).

Paragrafi 2 i nenit 145 parasheh se: "*Për pajisjet kompjuterike, elektronike të ruajtjes, apo të ngjashme, që janë marr në mënyrë të ligjshme nëpërmjet një urdhri të gjykatës ose me pëlqim. Prokurori i shtetit mund të autorizoj zyrtarin policor apo ekspertin për të shqyrtuar analizuar apo kërkuar informata që gjenden brenda pajisjes elektronike"*[163].

Kjo dispozitë përcakton disa autorizime por njëkohësisht kjo dispozitë parasheh edhe mundësinë ndërhyrjes në të drejtën e privatësisë.

Fillimisht dispozita parasheh se çdo pajisje mund t'i nënshtrohet marrjes së sendit – si pronë e një personi që i takon, dhe marrja mund të bëhet:

a) Me urdhër të gjykatës, apo
b) Me pëlqimin e subjektit (dorëzimin e sendit).

Ndërsa tutje dispozita parasheh mundësin që të ndërhyhet në analizimin, mbledhjen apo marrjen e të dhënave.

[163] Kodi nr.08/L-032 i Procedures Penale te Kosoves, neni 145.

Sipas po kësaj dispozite, parashihet se: " Prokurori i shtetit mund të autorizoj policinë apo ekspertin për mbledhjen e të dhënave, analizimin e të dhënave apo kërkimin e të dhënave.

Kjo dispozitë bie ndesh me kërkesat e paragrafit 3 të nenit 36, të Kushtetutës së Kosovës, për sa i përket ndërhyrjes në telefoni, korrespodencë apo formave tjera të komunikimit.

Është e qartë se dispozita Kushtetuese nga neni 36, lejon ndërhyrjen në format e tilla të së drejtës së privatësisë, vetëm mbi dy kushte:

1. Që të jetë urdhëruar nga Gjykata;
2. Që pasi të jetë zbatuar retroaktivisht ta konfirmoj Gjykata ndërhyrjen.

Nga ana tjetër dispozita e paragrafit 2 të nenit 145, thekson se, ***" Prokurori i shtetit"*** mund të autorizoj policinë apo ekspertin.

Në këtë kuptim dispozita nga neni 145 i Kodit të Procedurës Penale, që jap kompetencë për prokurorinë të autorizoj policinë apo ekspertin, në ekzaminimin e pajisjeve elektronike është qartazi në shmangie të kërkesës së paragrafit 3 të nenit 36, ku në pasuesin e dytë paragrafi 3 i nenit 36 thekson: " *Fshehtësia e korrespondencës, telefonisë dhe komunikimit tjetër, është e drejtë e pacenueshme.* ***Kjo e drejtë mund të kufizohet vetëm përkohësisht, në bazë të vendimit gjyqësor,*** *nëse është e domosdoshme për ecurinë e procedurës penale ose për mbrojtjen e vendit, në mënyrën e parashikuar me ligj"*[164].

Ndërsa praktika jonë gjyqësore ka të ngjarë që shumë shpesh, të jetë shfrytëzuar kompetenca e prokurorit të shtetit që në momentin kur është marr pajisja elektronike, prokurori ka autorizuar ekzaminimin e atij mjeti.

Duhet të kemi parasysh se, dispozita nga neni 145 paragrafi 2 e Kodit të procedurës Penale të Kosovës, rregullon dy aspekte të pajisjes:

a) Marrjen e pajisjes që mund të bëhet me urdhër apo me pëlqim, dhe
b) Ndërhyrjen në pajisje.

[164] Kushtetuta e Republikës së Kosovës 15 Qershor 2008, Neni 36 paragrafi 3.

Më konkretisht paragrafi 2 i nenit 145 parasheh: *" Për pajisjet kompjuterike, pajisjet elektronike të ruajtjes apo pajisje të ngjashme* ***që janë marrë*** *në mënyrë të ligjshme nëpërmjet një urdhri të gjykatës ose me pëlqim,* ***prokurori i shtetit mund të autorizojë zyrtarin e policisë apo ekspertin për të shqyrtuar, analizuar dhe kërkuar për informata ose të dhëna që gjenden brenda pajisjeve kompjuterike, pajisjeve elektronike për ruajtje ose pajisjeve të ngjashëm***".

1.3 Standardet e ekzaminimit elektronik

Dispozita e nenit 145 paragrafi 4[165], përcakton se qoftë kur ekzaminimi bëhet nga ana e zyrtarit të autorizuar të policisë apo kur bëhet nga ana e ekspertit, kriteret e tilla duhet të përmbushen për sa i përket ekspertit lidhur me të dhënat që duhet të përmbaj raporti i ekzaminimit.

Dispozita nga nenparagrafi 4.1 po ashtu përcakton disa kritere për sa i përket ekzaminimit që janë:

1. Përshkrimin e pajisjes që i nënshtrohet ekzaminimit;
2. Qfarë është ekzaminuar – a janë ekzaminuar të dhënat e ruajtura apo dosjet e veçanta,
3. Emrin identifikues, si etiketat apo numrat e tilla të të dhënave apo dosjeve që mundësojnë identifikimin e provave të tilla.

Kjo dispozitë duhet të kemi parasysh se bënë fjalë për shikimin e vendit të ngjarjes në një rrethanë të hetimit të një vepre penale klasike, ndërsa kjo dispozitë në themel përcakton mënyrën e shikimit të pajisjes që i nënshtrohet ekzaminimit.

Standardi i tillë i përcaktimit ligjor është shumë me rëndësi për t'i mundësuar si gjykatës ashtu edhe prokurorit, për të vlerësuar ligjshmërinë dhe besueshmërinë e provës së tillë elektronike që është nxjerrë nga pajisja elektronik.
Tutje dispozita nga nënparagrafi 4.2 parasheh tutje standardet e ekzaminimit të pajisjes elektronike që janë:

[165] Kodi nr.08/L-032 I Procedurës Penale të Kosovës, neni 145 paragrafi 2.

1. Përshkrimin se si janë marr pajisjet elektronike që i nënshtrohen ekzaminimit;
2. Përshkruan se ku janë marr pajisjet elektronike që i nënshtrohen ekzaminimit;
3. Përshkruar se a janë vetëm pajisje kompjuterike apo edhe pajisje të të dhënave dhe dosjeve të veçanta kompjuterike.

Në esencë kjo përbën evidentimin e mjetit që i është nënshtruar ekzaminimit mirëpo përbën edhe mënyrën se si organet shtetërore kanë siguruar mjetet e tilla të pajisjeve elektronike që ekzaminohen, gjithnjë është me rëndësi se këto veprime e ruajnë integritetin e provës që rezulton nga ekzaminimi.

Ndërsa nënparagrafi 4.3, parasheh tutje kërkesa ligjore si standarde që duhet zbatuar me rastin e ekzaminimit, e që janë:

1. Përshkrimin e radhës së mbikëqyrjes së pajisjeve kompjuterike, apo dosjeve të veçanta apo pajisjeve të ruajtjes që i nënshtrohen ekzaminimit.

Ky veprim si standard kërkohet nga se kjo përbën aspekt të procedurës standarde të sigurimit të provave duke ruajtur çfarëdo kontaminimi të të dhënave, nga se kur pajisjet elektronike janë të lidhura me rrjet të internetit, shpesh herë mund të ndërhyhet nga distanca dhe përshkrimi i saktë pastaj mund edhe të lejoj mundësin e integritetit të të dhënave që janë gjetur që përdoren programe të veçanta për ta krahasuar të dhënat e marra në raport me të dhënat e ndërhyrjes nga distanca.

Ndërsa nënparagrafi 4.4 i nenit 145, përcakton çështjen më thelbësore që ndërlidhet me kompetencën nga paragrafi 2 i këtij neni që i theksua më sipër, duke qenë se kjo dispozitë në nënparagrafin 4.4, parasheh se, “ Zyrtari i autorizuar policor, duhet të përshkruaj në mënyrë specifike dhe faktike që ka qenë i autorizuar të kërkoj.

Fillimisht kjo dispozitë ngërthen çështjen nëse prokurori i shtetit ka kompetencë sipas kushtetutës që të autorizoj ndërhyrjen në pajisjen kompjuterike duke qenë se një bazë të tillë e bënë sipas dispozitës kushtetuese, vetëm Gjykata me urdhër që e lëshon.

Megjithatë kur gjykata autorizon ekspertin apo zyrtarin e autorizuar policor që ka aftësi profesionale për ekzaminim të pajisjeve elektronike, duhet që urdhri të jetë konkret dhe specifik, pra nuk mund të jetë urdhër i përgjithësuar për ekzaminim të pajisjes.

Ndërsa me rastin e ekzaminimit në raport kërkohet që të përshkruhet se:

1. Për çfarë ka qenë i autorizuar specifikisht që të kërkohet në pajisje elektronike eksperti apo zyrtari policor;
2. Cili është informacioni specifik që kërkohej në pajisjen elektronike që ekzaminohej.

Kjo dispozitë ndërlidhet me aspekti e parashikueshmërisë, duke qenë se urdhri mund të jetë për ekzaminim kompjuterik vetëm të të dhënave të fshira, dhe jo edhe të fajlleve apo dosjeve të veçanta kompjuterike.

Nga ana tjetër urdhri i tillë specifik dhe përshkrimi specifik që kërkohej i materialeve e në pajisjen elektronike, përbën edhe kufizimin dhe proporcionalitetin që është standard i institucioneve shtetërore që kanë për detyrë ta zbatojnë kur ndërhyjnë në të drejtat kushtetuese duke qenë se kriteri është se ndërhyrja lejohet vetëm deri në shkallën e domosdoshme.

Nënparagrafi 4.5 përcakton një metodologji që duhet të jetë e pranueshme e zbatueshme për kërkimin në pajisjen kompjuterike e që ka rëndësi të veçantë, pasi që kërkohet si aspekti profesional, ashtu edhe integriteti i provave por edhe besueshmëria e provave që sigurohen përmes ekzaminimit të pajisjes kompjuterike.

Nënparagrafi 4.5 i nenit 145[166] parasheh si standarde që duhet zbatuar e që janë:

1. Hapat që ndërmerr në përputhje me praktikën aktuale në fushën e forenzikës;
2. Mënyrën e kërkimit të saktë dhe të besueshme që është bërë në pajisjen kompjuterike;
3. Hapat që ka ndërmarr për mbrojtjen e të dhënave që të mos humbasin;

[166] Kodi nr.08/L-032 i Procedures Penale te Kosoves, neni 145 paragrafi 4 nenparagrafi 4.5.

4. Hapat që janë ndërmarr për deshifrimin e dosjeve të ndryshme që gjinden në pajisje;
5. Hapat që janë ndërmarr për rikthimin e dosjeve të fshira;
6. Hapat që janë ndërmarr për marrjen e të dhënave nga dosja kompjuterike apo emailet.

Ndërsa nënparagrafi 4.6, parasheh se, të gjitha këto të dhëna përfshihen në raportin që përpilohet me rastin e ekzaminimit të pajisjes kompjuterike dhe rrjedhimisht, në raport eksperti apo zyrtari i autorizuar i policisë përshkruan rezultatet e nxjerra me rastin e ekzaminimit të pajisjes. Raportit duhet t'i bashkëngjitet kopja elektronike e dosjeve elektronike që janë të rëndësishme për kërkimet e kryera.

1.4 Praktika e GJEDNJ-së për marrjen e provave elektronike

Gjykata Evropiane për mbrojtjen e të drejtave dhe lirive të njeriut, ka krijuar praktikë për sa i përket çështjes së marrjes së provave elektronike në trajtimin e rasteve që e ka pasur në shqyrtim.

Rëndësi të theksuar këto raste kanë se nuk ka mëdyshje se marrja e të dhënave nga pajisjet elektronike gjithnjë nga GJEDNJ-ja trajtohet se përbën ndërhyrje në nenin 8 në të drejtën për respektimin e jetës private dhe familjes.

Në rastin Benedik kundër Sllovenisë, me nr. 62357/14[167], vendimi i datës 27.07.2018, ka Konstatuar shkeljen e nenit 8 të drejtës për respektimin e jetës private dhe familjes.

Çështja: Policia zvicerane përmes monitorimit " racorback" përcaktoi se disa nga përdoruesit zotëronin dhe shkëmbenin pornografi të fëmijëve në formën e fotografive ose videove. Skedarët që përmbanin përmbajtje të paligjshme shkëmbeheshin përmes të ashtuquajturit rrjet ndarjeje skedarësh "p2p" (peer-to-peer) në të cilin secili prej kompjuterëve të lidhur vepronte si klient dhe si server. Prandaj, çdo përdorues mund të hynte në të gjitha skedarët e vënë në dispozicion për ndarje nga përdorues të tjerë të rrjetit dhe t'i shkarkonte ato për përdorimin e tij ose të saj. *Ndër adresat dinamike të Protokollit të Internetit ("IP") të regjistruara*

[167] Benedik kundër Sllovenisë, me nr. 62357/14.

nga policia zvicerane ishte edhe një adresë e caktuar dinamike IP, e cila më vonë u lidhë me te dyshuarin. Bazuar në të dhënat e marra nga policia zvicerane, më 7 gusht 2006, policia sllovene, pa marrë një urdhër gjykate, i kërkoi kompanisë S., një ofrues slloven i shërbimit të internetit (në tekstin e mëtejmë "ISP"), të zbulonte të dhëna në lidhje me përdoruesin të cilit i ishte caktuar adresa IP e lartpërmendur në orën 13:28. më 20 shkurt 2006. Policia e bazoi kërkesën e saj në nenin 149b(3) të Ligjit të Procedurës Penale, i cili kërkonte që operatorët e rrjeteve të komunikimit elektronik t'i zbulonin policisë informacion mbi pronarët ose përdoruesit e mjeteve të caktuara të komunikimit elektronik, detajet e të cilëve nuk ishin të disponueshme në drejtorinë përkatëse. Në përgjigje, më 10 gusht 2006, ISP-ja i dha policisë emrin dhe adresën e IP, i cili ishte abonent i shërbimit të internetit në lidhje me adresën përkatëse. Prokuroria kërkoj një urdhër dhe Gjyqtari i Procedurës dha urdhër për kontroll dhe sekuestrim në shtëpinë e të dyshuarit, ku policia gjeti 4 kompjuter në të cilin në njërin u gjetën materiale pornografike me fëmijë.

Vendosja nga Gjykatat e Vendore: *Parashtruesi në Gjykatën Supreme paraqiti një ankesë për çështje ligjore, duke përsëritur se një adresë dinamike IP nuk mund të krahasohej me një numër telefoni që nuk ishte futur në një drejtori telefonike, pasi një adresë e re IP i caktohej një kompjuteri çdo herë që përdoruesi kyçej. Prandaj, të dhëna të tilla duhet të konsiderohen si të dhëna trafiku që përbëjnë rrethana dhe fakte të lidhura me komunikimin elektronik dhe që kërkojnë mbrojtje të privatësisë së komunikimit. Aplikanti argumentoi se policia zvicerane nuk duhej të kishte marrë adresën përkatëse dinamike IP pa një urdhër gjykate, dhe as policia sllovene nuk duhej të kishte marrë të dhënat mbi identitetin e pajtimtarit të lidhur me adresën IP pa një urdhër të tillë.* ***Gjykata Supreme e hodhi poshtë ankesën e aplikantit për çështje ligjore, duke arsyetuar se duke pasur parasysh aksesueshmërinë e përgjithshme të faqeve të internetit dhe faktin se policia zvicerane mund të kontrollonte shkëmbimet në rrjetin p2p thjesht duke monitoruar përdoruesit që ndanin përmbajtje të caktuara, domethënë pa ndonjë ndërhyrje të veçantë në trafikun e internetit, një komunikim i tillë nuk mund të konsiderohej privat dhe kështu të mbrohej nga Neni 37 i Kushtetutës.***

Vendosja e Gjykatës Kushtetuese të Sllovenisë: *Tutje qështja ishte parashtruar në Gjykatën Kushtetuese, ku* ***Gjykata Kushtetuese theksoi, se përveç përmbajtjes së komunikimeve, Neni 37 i Kushtetutës mbronte edhe të dhënat e trafikut, domethënë çdo të dhënë të përpunuar për transmetimin e komunikimeve në një rrjet komunikimesh elektronike. Ajo konsideroi se adresat IP përfshiheshin në të dhëna të tilla trafiku. Megjithatë, Gjykata Kushtetuese arriti në përfundimin se aplikanti, i cili***

nuk e kishte fshehur në asnjë mënyrë adresën IP përmes së cilës kishte hyrë në internet, e kishte ekspozuar veten në mënyrë të vetëdijshme ndaj publikut dhe nuk mund të priste ligjërisht privatësi. Si rezultat, të dhënat që kishin të bënin me identitetin e përdoruesit të adresës IP nuk mbroheshin si privatësi komunikimi sipas Nenit 37 të Kushtetutës, por vetëm si privatësi informacioni sipas Nenit 38 të Kushtetutës, dhe nuk kërkohej asnjë urdhër gjykate për t'i zbuluar ato në rastin e aplikantit.

Gjetjet e GJEDNJ-së kishte konstatuar se: *Gjykata është e mendimit se ligji mbi të cilin bazohej masa e kontestuar, domethënë marrja nga policia e informacionit të lidhur me adresën dinamike IP në fjalë, dhe mënyra se si u zbatua nga gjykatat vendase, nuk kishte qartësi dhe nuk ofronte mbrojtje të mjaftueshme kundër ndërhyrjes arbitrare në të drejtat e Nenit 8. Në këto rrethana, Gjykata kishte konstatuar se ndërhyrja në të drejtën e aplikantit për respektimin e jetës së tij private nuk ishte "në përputhje me ligjin" siç kërkohet nga Neni 8.2 i Konventës. Si pasojë, Gjykata nuk ka nevojë të shqyrtojë nëse masa e kontestuar kishte një qëllim legjitim dhe ishte proporcionale. Duke marrë në konsideratë të gjitha sa më sipër, Gjykata arrin në përfundimin se ka pasur shkelje të Nenit 8 të Konventës.*

Vendimi: *Komepnsimin e demit jo material, Kompensimin e demit për gjykim të pabazuar, Kompensimin e demit për shkak të qëndrimit nën masën e paraburgimit, Kompensimin e demit për shkak të stigmatizimit si pasoëj e dënimit që ishte shqiptar.*

Raste të tjera qe janë trajtuar nga GJEDNJ-ja për ndërhyrje dhe cenim të nenit 8 të Konventës, janë: 1. Kruslin v.France Case no. 11801/85, 24. Prill 1990, 2. Huvig v.France case no. 11105/84, 24.prill 1990, 3. Copland v. United Kingdom case no. 62617/00, 3 prill 2007, 4. Roman Zakharov v. Russia (grand chamber) case no. 47143/06, 4 dhjetor 2015, Klass and others v.Germany, case no. 5029/71, 6 shtator 1978.

1.5 Hapat në fushën e ekzaminimit kompjuterik

Shumë shtete kanë zhvilluar udhëzues të veçantë sa i përket hapave që duhet ndjekur një proces i hetimit të një çështje penale kur kemi të bëjmë me provat elektronike që ndërlidhen në pjesën e hetimit në atë çështje penale.

Janë të njohur disa hapa që mbizotërojnë në procesin e hetimit forenzik të pajisjeve kompjuterike që kanë si qëllim sigurimin e provave në ato pajisje që i nënshtrohen ekzaminimeve.

Procesi i ekzaminimit kompjuterik përfshinë disa hapa që në themel janë kërkesa edhe të dispozitës nga neni 145 paragrafi 4 i Kodit të procedurës penale të Kosovës, që më konkretisht përbëjnë në vetvete praktikat e tilla që janë aktuale në zbatim.

Mbledhja e të dhënave: Provat elektronike duhet të mblidhen. Kjo mund të ndodhë duke mbledhur të dhëna të paqëndrueshme gjatë një bastisjeje shtëpie, duke marrë diskun e të dyshuarit nga një kompjuter i sekuestruar ose në çdo proces tjetër gjatë një hetimi. Zbatimi i procedurave të sakta dhe të forta në hapin e marrjes së të dhënave është thelbësor pasi ekziston një hapësirë e madhe për të bërë gabime të pakthyeshme. Është e rëndësishme të ruhet i paprekur zinxhiri i kujdestarisë, të dokumentohen me kujdes të gjitha hapat dhe të verifikohen të gjitha imazhet dhe kopjet që janë marrë.

Përpunimi: Gjatë përpunimit, ekzaminuesit mund të trajtojnë pajisje ose të dhëna të caktuara dhe do të prodhojnë një kopje ose imazh të saktë të përmbajtjes së çdo memorieje elektronike, të sekuestruar. Duke punuar në dublikatën (kurrë origjinalen) ata mund të aplikojnë filtra inteligjentë, specifikë për rastin ose ata mund thjesht të përpunojnë imazhin (p.sh. duke rikuperuar skedarët e fshirë, duke montuar kontejnerë, duke thyer enkriptimin, duke analizuar të dhënat e aplikacionit si historiku i internetit, regjistrat e bisedave, etj.).

Analiza: Gjatë fazës së analizës, ekzaminuesi në fakt kërkon prova elektronike në imazhe. Ky hap mund të kërkoj shumë kohë dhe mund të kërkojë shumë njohuri profesionale apo ekspertizë për të interpretuar gjurmët nga një sërë sistemesh skedarësh, sistemesh operative apo aplikacione.

1.6 Parimet e përgjithshme për analizimin e provave elektronike

Analizimi i provave elektronike, ka rendësi thelbësore në procedurën penale, duke qenë se përmes analizimit mund të ruhet ligjshmëria e provës, por nuk duhet nënkuptuar ligjshmëria vetëm nga aspekti i cenimit të vërtetësisë së saj, por edhe nga aspekti i ruajtjes së të drejtave dhe lirive themelore që garantohen me aktet ndërkombëtare apo me Kushtetutë.

Parimet e përbashkëta ndihmojnë për të siguruar që provat elektronike të merren në një mënyrë që mbron integritetin e tyre dhe në një mënyrë që mund të verifikohet. *"Meqenëse kompjuterët janë bërë kaq pjesë integrale e jetës moderne, ato nuk përdoren më vetëm për aktivitete biznesi, por përmbajnë të gjitha llojet e informacionit personal që mund të zbulojnë detaje intime rreth përdoruesit. Si pasojë, ka të ngjarë që herët a vonë të zbulohen informacione private, konfidenciale ose ligjërisht të privilegjuara që mund të shkaktojnë sfida ligjore dhe çështje të të drejtave themelore. Çështje të tilla, nëse ngrihen, nuk do të jenë të lehta për t'u zgjidhur menjëherë, por as nuk është domosdoshmërisht e kujdesshme të hidhen të dhënat për shkak të një sfide të tillë. Sfida mund të jetë e gabuar. Një zgjidhje është të sekuestrohen të dhënat, por t'i vulosin ato me një server procesi ose përmbarues derisa të mund të përcaktohet statusi ligjor. Në të vërtetë, vendosja e të dhënave nën vulë mund të lejojë gjithashtu kohë për të marrë autorizim për të aksesuar të dhënat edhe nëse ato janë vërtet konfidenciale"*[168].

Nga ky përcaktim i udhëzimit të parimeve, është e qartë se provat që kanë karakter privat dhe që janë me mëdyshje nëse janë të ligjshme apo mund të ketë qasje në ato të dhëna elektronike, shenjësohen dhe mbahen të tilla derisa të vlerësohet ligjshmëria e tyre, në të kundërtën do të përbënte ndërhyrje në të drejtën e privatësisë.

1.7 Integriteti i të dhënave

Është theksuar se një ndër kërkesat ligjore nga neni 145 paragrafi 4.5 i Kodit të procedurës penale kërkon që ekzaminimi i të dhënave të bëhet në mënyrë të

[168] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 135.

besueshme për t'i ruajtur të sakta dhe të pandryshuara të dhënat që sigurohen përmes ekzaminimit.

Analizimi i një pajisjeje kompjuterike është i ngjashëm me një hetues që shqyrton një vendngjarje të krimit, në atë që provat duhet të mbahen të paprekura, sa më afër gjendjes origjinale dhe të lira nga kontaminimi. *"Në mënyrë të ngjashme, analistët e forenzikës kompjuterike duhet të jenë të kujdesshëm që të mos shqetësojnë ose modifikojnë asnjë nga të dhënat elektronike që shqyrtojnë në laboratorin e forenzikës. Edhe operacioni më i vogël i aplikuar në një pajisje, ajo mund të ndryshojë përmbajtjen e memories së saj. Vetëm renditja e përmbajtjes së një skedari ose hapja e një skedari do të modifikojë hyrjen "qasja e fundit" e skedarit. Parimit të integritetit të të dhënave kërkon që, një ekzaminues me përvojë duhet të jetë gjithmonë vigjilent ndaj mundësisë së teknikave anti-forenzike. Ai/ajo duhet të ekzaminojë të dhënat për t'u siguruar që ato duken autentike dhe nuk shfaqin ndonjë tipar që sugjeron se të dhënat mund të jenë modifikuar ose manipuluar para se të sekuestrohen nga forcat e rendit. Njohuritë mbi teknikat anti-forenzike duhet të jenë gjithmonë pjesë e kurrikulës së ekzaminuesit të forenzikës"*[169].

1.8 Gjurmët në pajisjet kompjuterike

Është e njohur se sikurse në veprat penale të rëndomta ku gjithnjë mbesin gjurmë me rastin e kryerjes, edhe në kuadër të pajisjeve kompjuterike mbesin gjurmë nga çdo subjekt që operon me atë pajisje. Është thelbësore aftësia profesionale për t'i gjetur dhe siguruar gjurmët e tilla që janë mbetur në pajisjet elektronike, zakonisht gjurmët e tilla janë me rëndësi kur operohet në kryerjen e veprave penale përmes pajisjeve kompjuterike, siç mund të jenë: Mashtrimi kompjuterik, Thyerja e sistemeve kompjuterike – hakimi i kompjuterëve apo sistemeve të sigurisë apo veprime të tjera.

Po ashtu sikurse në kryerjen e një vepre penale ordinere që disa nga gjurmët janë të mundshme për tu humbur ndërsa disa gjurmë është e pamundur për tu humbur, njësoj edhe tek gjurmët elektronike disa nga gjurmët kompjuterike janë të shmangshme ndërsa disa nga gjurmët tjera janë të pashmangshme

[169] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 134.

gjegjësisht disa nga gjurmët e tilla duhet që kryesi të ketë aftësi të larta dhe të bëjë përpjekje të mëdha për tu shmangur si gjurmë.

Për të pasur një ide më të mirë të llojeve të gjurmëve elektronike që një ekzaminues mund të zbulojë gjatë analizës forenzike, ka kuptim të dallojmë dy lloje gjurmësh elektronike:

"Gjurmë të shmangshme: Këto janë gjurmë që ruhen nga sistemi operativ dhe aplikacionet si parazgjedhje, por që një sistem mund të konfigurohet të mos i ruajë. Shembull i një shfletuesi interneti. Ky program do të ruajë historikun e shfletimit të një të dyshuari, si dhe detajet e shkarkimeve të tij, futjet e formularëve, cookie-t, etj., por mund të çaktivizohet ose fshihet nga i dyshuari. Një shembull tjetër mund të jetë menyja "Start" dhe programet Office të të dyshuarit që "mbajnë mend" se cilat skedarë i dyshuari ka hapur së fundmi. Ekzistojnë lloje të ndryshme gjurmësh "të shmangshme" që ruhen automatikisht në hard disk në këtë mënyrë (siç tregohet në tabelën më poshtë). Megjithatë, ato mund të parandalohen nga dikush që di çfarë po bën".

"Gjurmë të pashmangshme: Në të kundërt, gjurmët e pashmangshme janë, sigurisht, ato që nuk mund të çaktivizohen ose ato që kërkojnë përpjekje të konsiderueshme për t'u ndaluar përkohësisht. Probabiliteti i gjetjes së gjurmëve të tilla është përkatësisht i lartë edhe nëse një i dyshuar është përpjekur të fshehë gjurmët e tij ose të saj"[170].

1.9 Përgatitja e prezantimit të provave

Një ndër çështjet thelbësore në kuadër të procedurës penale është edhe aspekti i shqyrtimit gjyqësor, ku mishërohen shumë parime procedurale, kështu ndër parimet procedurale që ndërlidhet me çështjen e provave elektronike është edhe parimi i drejtpërdrejtshmërisë dhe parimi i kontradiktoritetit.

Aspektit të provave elektronike është shumë me rëndësi për tu kuptuar nga ana e gjyqtarit që ka në shqyrtim çështjen penale. Megjithëse Gjyqtari nuk është i thirrur që t'i kuptoj të gjitha aspektet e termave dhe operacioneve teknologjike

[170] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 138.

që ndërlidhen me pajisjet kompjuterike apo pajisjet tjera, ai duhet të jetë në gjendje që të kuptoj thelbin e çështjes së provës në raport me faktin.

Për ta bërë që ta kuptoj drejt secili gjyqtar çështjen e provave elektronike është e nevojshme që të bëhet përgatitja e provave elektronike për tu prezantuar në shqyrtimin gjyqësor. Do të ishte problematike nëse nuk përgatitet një prezantim i provave elektronike për tu kuptuar nga shembulli si në vijim: " Qasja e një mjeti elektronik – , në një IP adresë që është në shfrytëzim për publikun, ku mund të ndryshohet vendi se ku gjendet telefoni përmes VPN – së, dhe përmes Mac Adreses" nëse nuk përgatitet në mënyrë të kjartë prezantimi i thjeshtë në procedurën penale që një Gjyqtar ta kuptoj drejt se kemi të bëjmë me veprimet që ka operuar një i dyshuar me VPN dhe Mac Adresen, lehtësisht do të vijë në konkludimin se qasja e Mjetit elektronik në IP adresën nuk rezulton të jetë provuar si fakt. Shembulli i tillë na jep të kuptojmë problematikën dhe rëndësinë e përgatitjes dhe prezentimit të provave elektronike që është me rëndësi të bëhet para gjykatës.

Në anën tjetër përdorimi i provave elektronike është bërë gjithnjë e me i pranishëm në proceset gjyqësore, kjo për faktin se thuajse edhe veprat penale më ordinere që kryhen tani mjetet elektronike gjithnjë mund të japin të dhëna për tu provuar faktet e caktuar, andaj rrethanat e zhvillimit shoqëror kanë krijuar domosdoshmërinë e përdorimit më të madh të provave elektronike.

Posaçërisht provat elektronike në kohën e sotme janë në shprehje ne thuajse çdo çështje penale, nga se zhvillimi i teknologjisë informative ka krijuar mundësinë e tillë që gjithnjë ndërveprimi të mund të hetohet edhe përmes pajisjeve elektronike në të cilat mund të gjinden gjurmë të ndryshme, qoftë edhe për veprat penale më të rënda që kryhen e që provojnë faktet e tilla, p.sh: " kërkimi në internet për përgatitjen e bombave artizanale – në situata të tilla gjurmët që mbesin nga ana e një kryesi që synon kryerjen e një vepre penale të terrorizmit janë evidente kur bëhet përgatitja e tillë e bombave, apo pornografia e fëmijëve – gjurmët që mbesin nga kryesi qoftë kur merr pjesë në shpërndarjen e pornografisë së të miturve apo kur merr pjesë në mbledhjen e materialeve me qëllim shpërndarje janë evidente se mund të gjinden në pajisjet elektronike.

Një pajisje elektronike e përfshirë në krim duhet të sigurohet ashtu siç do të sigurohej me format e tjera të provave fizike të gjetura në vendin e ngjarjes, sepse të gjitha pajisjet e tilla mbeten prova fizike. Ashtu si me provat e gjurmëve të gishtërinjve dhe ADN-së, provat elektronike janë të brishta dhe humbasin ose ndryshohen lehtë nëse është e nevojshme, nuk ndiqen masa paraprake. Në ditët e para të trajtimit të provave elektronike, zyrtare e pa trajnuar të zbatimit të ligjit ndiznin kompjuterët për të kërkuar prova para se t'i dorëzonin ato për një ekzaminim forenzike ose fiknin pajisjet dhe humbnin të dhënat dhe provat e mundshme të humbura në RAM. Është e rëndësishme të regjistrohet vendi ku është gjetur dhe sekuestruar pajisja elektronike, sepse kjo mund të zbulojë shumë rreth qëllimit të të dyshuarit për vepër penale.

Është praktikë e mirë të regjistrohet kontrolli dhe sekuestrimi me video. Kjo do të tregojë pozicionin e pajisjeve elektronike, në mënyrë që të mos ketë më një debat, për shembull, nëse pajisja pa tel është gjetur e fshehur në papafingo dhe jo në një zonë me akses të hapur në dhomën e ndenjes.

1.10 Cilësia e provave elektronike

Provat elektronike sikurse çdo provë në procedurën penale duhet të kenë disa cilësi për tu konsideruar se në të vërtetë mund të përdoren dhe mund të kenë cilësinë e provës në të provuarit e fakteve të çështjes penale.

Nisur nga kjo bazë se çdo provë duhet të ketë të bëjë me çështjen dhe duhet të shërbej për të provuar faktet dhe se çdo provë duhet të jetë e ligjshme, edhe provat elektronike kanë tri cilësi thelbësore që janë:

a) Pranueshmëria e provave,
b) Vërtetësia e provave, dhe
c) Besueshmëria e provës.

1.11 Pranueshmëria e provave

Për të qenë një proces gjyqësor i ligjshëm duhet që mbështetja e fakteve që konstatohet se provohen të jetë në prova të pranueshme, provat e pranueshme nënkuptojnë provat e ligjshëm që duhet të konsiderohen se shërbejnë për tu provuar faktet. Provat elektronike janë të pranueshme nëse janë në përputhje

me Kodin e procedurës penale apo me ligjet e veçanta që përcaktojnë mënyrën e marrjes së provës e që po ashtu nëse nuk janë cenuar dispozitat kushtetuese.

"Provat elektronike janë të pranueshme nëse ato përputhen me një sërë ligjesh dhe rregullash që sigurojnë që ato janë të pranueshme për gjykatën. Gjatë marrjes së provave duhet të ndiqen procedurat e duhura"[171].

1.12 Vërtetësia e provave

Për tu konsideruar një provë se mund të shërbej në të provuarit e fakteve dhe që të mund të shërbej në procedurën penale ajo duhet të jetë e vërtetë.

Vërtetësia nënkupton se prova është në përmbajtjen e saj ashtu siç është siguruar, pa ndërhyrë në përmbajtjen apo formën e saj, pa cenuar tërësinë e saj që mund të ndërlidhet me faktet e çështjes që janë objekti i të provuarit në procedurën penale.

Nga ana tjetër mundësia e ndërhyrjes në provat elektronike është dukshëm më e madhe se sa në provat fizike që janë në rastet e veprave penale ordinere. Rrjedhimisht një ndër kushtet që kërkohet te provat elektronike për të konkluduar mbi të provuarit e fakteve është vërtetësia e saj.
"Provat elektronike nuk ndryshojnë nga provat fizike, siç është një dokument i regjistruar në një copë letër. Është e nevojshme të sigurohet që provat janë autentike. Dallimi midis provave elektronike dhe provave fizike është zakonisht lehtësia me të cilën provat elektronike mund të ndryshohen dhe modifikohen, qoftë me qëllim ose pa dashje"[172].

1.13 Besueshmëria e provave

Besueshmëria e provës ka të bëjë me çështjen e përmbajtjes së saj për të provuar faktet në një çështje penale. Në besueshmëri ndikon thelbësisht edhe pranueshmëria por në mënyrë të veçantë ndikon vërtetësia e provës, nga se në rrethana që nuk legjitimohet si e ligjshme prova ajo rezulton edhe e

[171] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 149.
[172] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 149.

pabesueshme, siç mund të ndodh në rrethanën kur nuk ka vërtetësi – që do të thotë ka ndërhyrje ajo për shkak të ndërhyrjes humb tërësisht besueshmërinë gjegjësisht kredibilitetin. Besueshmëria e provës po ashtu përmban edhe dy cilësi të veçanta që janë:

a) Të mundshmen, dhe
b) Të provueshmen.

Prova në parim duhet të vërtetoj se fakti i tillë që ka ngjarë e që synohet të provohet me provën që propozohet duhet që të jetë i mundshëm se ka ndodhur.

Ndërsa provueshmëria nënkupton se prova ka të bëjë me faktet, që mund të jenë faktet kryesore, të ndërmjetme apo faktet periferike por që kanë rëndësi në tërësinë e rrethanave të gjendjes faktike.
"Një aspekt i rëndësishëm i provave elektronike, është se si janë marrë ato dhe nëse metodologjia me të cilën janë përcaktuar ato prova është e përshtatshme për vërtetim dhe shqyrtim objektiv, shkencor. Për shembull, nëse prokuroria mund të paraqesë një faturë telefonike që tregon se i pandehuri është lidhur me ofruesin e tij të shërbimeve të internetit në një kohë të caktuar të ditës, atëherë kjo zakonisht do të pranohet. Në të kundërt, nëse prokuroria pretendon se "I pandehuri i fshiu të gjitha skedarët në hard diskun e tij, e riformatoi atë, pastaj e hodhi nga një dritare 10-katëshe, por ne kemi qenë në gjendje t'i rindërtojmë skedarët duke shkuar në një firmë rikuperimi të dhënash", atëherë mbrojtja mund të vërë në dyshim vlefshmërinë e kësaj metode të rikuperimit të provave. Është detyrë e prokurorisë të tregojë se metodat e përdorura për të rikuperuar provat ishin të vlefshme dhe të bindë gjykatën se provat duhet të pranohen. Është e nevojshme të gjendet ekuilibri i duhur. Nga njëra anë, nuk është e arsyeshme të pritet që venduesit e fakteve (qofshin anëtarë të një jurie apo një gjyqtar i vetëm) të kuptojnë hollësitë teknike. Nga ana tjetër, është e papërshtatshme të pritet që ata të pranojnë teknikat e rikuperimit të të dhënave si "magji". Në disa vende, përgjigja është rishikimi nga kolegët - nëse specialistë të tjerë në këtë fushë e kanë studiuar teknikën, e kanë testuar atë dhe kanë validuar rezultatet, atëherë gjykata do t'i pranojë provat. Vlen të theksohet se, provat elektronike trajtohen në gjykatë në të njëjtën mënyrë si çdo formë tjetër prove. Prokuroria do të duhet të

provojë se dokumenti është autentik dhe përmbajtja e tij është e pranueshme"[173].

1.14 Administrimi i provave elektronike

Dispozitat e Kodit të Procedurës Penale nuk bëjnë ndonjë dallim për sa i përket provave elektronike dhe provave tjera fizike për aspekte të veçanta të administrimit në shqyrtimin gjyqësor. Në rrethana të tilla provat elektronike duhet të administrohen në shqyrtim gjyqësor, sikurse që përcaktojnë dispozitat administrimin e provave materiale qoftë duke i administruar si të vetme varësisht nga cila palë propozohen apo duke i administruar në mbështetje të deklaratës së dëshmitarit gjegjësisht të ekspertit, pasi që nuk ka rregulla specifike për sa i përket çështjes së provave që duhet administruar në shqyrtimin gjyqësor vetëm për faktin se ato janë siguruara nga pajisjet elektronike apo se përbëjnë prova elektronike.

Thelbësore është se kur prezantohen provat elektronike, duhet argumentuar se ato nuk janë më shumë apo më pak se sa kur janë siguruar që nga momenti kur organet shtetërore kanë marr pajisjen nga të cilat janë marr provat elektronike, kjo për faktin e sistemet operative kompjuterike shpesh ndryshojnë të dhënat dhe këtu rezulton edhe sfida e të provuarit se provat elektronike janë po ato që janë siguruar në përmbajtjen e tyre siç kanë qenë në pajisjen e ekzaminuar.

Si teknikë e shmangies së mëdyshjeve për ndryshime apo përmbajtjen e provave elektronike siç është theksuar, në nenin 145 paragrafi 4 nënparagrafi 4.5 kërkon që një kopje elektronike e dosjeve duhet t'i bashkëngjitet raportit, në mënyrë që të siguroj konstatimet e tilla se prova elektronike nuk ka ndryshuar.
"S*a herë që është e mundshme, duhet të bëhet një kopje e të gjithë pajisjes së synuar. Kopjimi i pjesshëm ose selektiv i skedarëve mund të konsiderohet si një alternativë në rrethana të caktuara, për shembull kur sasia e të dhënave që duhen fotografuar e bën këtë të pamundur. Megjithatë, hetuesit duhet të jenë të kujdesshëm që të jenë në gjendje të tregojnë se të gjitha provat*

[173] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 150.

përkatëse janë siguruar. Në raste të rralla, mund të mos jetë e mundur të merret një imazh duke përdorur një pajisje të njohur imazhe. Në këto rrethana, mund të bëhet e nevojshme të merret qasje në pajisjen origjinale për të rikuperuar provat. Duke pasur parasysh këtë, është thelbësore që një specialist i provave elektronike i kualifikuar në mënyrë të përshtatshme, i cili është kompetent për të dhënë prova në gjykatë, të marrë provat. Në gjyq është thelbësore të tregohet objektiviteti, si dhe vazhdimësia dhe integriteti i provave. Është gjithashtu e nevojshme të tregohet se si janë rikuperuar provat, duke treguar çdo proces nëpërmjet të cilit janë marrë provat. Provat duhet të ruhen në një masë të tillë që një palë e tretë të jetë në gjendje të përsërisë të njëjtin proces dhe të arrijë në të njëjtin rezultat me atë që i është paraqitur një gjykate"[174].

1.15 Zbulimi i provave elektronike ndaj mbrojtjes

Një ndër parimet më themelore të dispozitave të procedurës penale që inkorporon Kodi përbën parimi kontradiktor. Rrjedhimisht përmes këtij parimi Kodi ka paraparë edhe detyrimet e palës akuzuese por edhe mbrojtëse për të shfaqur provat ndërmjet tyre gjegjësisht t'i bëjnë publike prokurori palës mbrojtëse dhe mbrojtësi palës së kundër – prokurorit.

Zbulimi i provave për palën mbrojtëse nga ana e prokurorit në rastet e veprave ordinere gjegjësisht kur ka prova " Dokumentare apo dëshmitar" nuk do të ishte shumë sfiduese në procedurën penale.
E kundërta është zbulimi i provave elektronike ndaj palës mbrojtëse, jo për faktin se duhet shmangur detyrimin pasi që prokurori ka detyrimin e tillë dhe duhet ta përmbush por mënyra e dorëzimit të këtyre provave, dhe rreziku nëse provat e tilla nuk janë të sakta, mëdyshje për tërësinë e tyre, apo të kompromituara në përmbajtjen e tyre.

Zbulimi i provave elektronike ka në themel dy sfida që duhet të kihen parasysh:

a) Rreziku i fshirjes së provave nga ana e hetuesve deri në ruajtjen finale të tyre;

[174] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 150-151.

b) Zbulimi i hershëm i provave para se të ruhen në tërësinë e tyre, cilado nga këto rrethana do të përbënte një dëm të theksuar për çështjen penale në dëm të prokurorit për ta provuar akuzën.

Mënyra më e mirë për zbulimin e provave në praktikë përbën, detyrimin e hetuesve që nga momenti fillestar e deri në përfundimin e ruajtjes së tyre të ruajnë një kopje elektrike në tërësinë e procesit të ruajtjes së tyre, dhe atë të ja dorëzojnë prokurorit për ta zbuluar përball mbrojtjes[175], vetëm në këtë mënyrë do të mund të bëhet auditim i tërësishëm i procesit, si për sa i përket përmbajtjes, cilësisë dhe integritetit të provës.

1.16 Përdorimi i provave elektronike në Gjykatë

Provat elektronike fillimisht duhet të jenë të sakta dhe të plota, të pranueshme dhe autentike, si dhe të siguruara në përputhje me dispozitat ligjore në fuqi, në mënyrë që të mund të përdoren në procesin gjyqësor, në të kundërtën Gjykata mund t'i kategorizoj si:

a) Prova të papranueshme – paligjshme,
b) Apo prova të parëndësishme në lidhje me faktet dhe ti përjashtoj nga çështja penale (neni 253 i KPP-së).

Gjatë shqyrtimit gjyqësor ka rëndësi thelbësore që prokurori të sqaroj se si është krijuar prova digjitale në tërësi për ta bërë të besueshme dhe t'i shërbej në vërtetimin e fakteve.
Para përdorimit të provave në shqyrtim sugjerohet që prokurori të bëjë një shqyrtim paraprak për të vlerësuar, se në raport me cilat fakte dhe cilat prova elektronike janë të fuqishme ku është dobësia e provave ndaj fakteve të caktuara dhe ku duhet siguruar edhe më tutje prova elektronike apo nëse provat tjera mund të vërtetojnë faktet e caktuara mjaftueshëm. Për ta bërë këtë ka shumë rëndësi të veçantë eksperti i forenzikës që ka përgatitur raportet lidhur me provat elektronike, asgjë nuk e ndalon prokurorin që përveç raporteve të kërkoj sqarime të sakta dhe në detaje lidhur me provat elektronike që ka siguruar një ekzaminim elektronik, i cili sqarim do t'i ndihmoj edhe

[175] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 151.

prokurorit në procesin penal për të sqaruar saktësisht lidhshmërinë e provave me faktet.

Prokurori mund po ashtu të kërkoj nga eksperti i forenzikës sqarime të nevojshme lidhur me qështjet që do të mund të ngrit mbrojtja për provat elektronike, gjithnjë duke pasur parasysh se prokurori ka detyrim që të trajtoj si provat në favor ashtu në disfavor të të dyshuarit, andaj kjo është e nevojshme shpesh herë që të ngrit çështjet për sqarim që potencialisht do të ishin shqetësime për mbrojtjen ndaj të dyshuarit. Nga ana tjetër duke qenë se eksperti i forenzikës mund të thirret për tu dëgjuar dhe sqaruar mënyrën e sigurimit të provave elektronike, është e rëndësishme që provat që janë siguruar e që paraqiten në raportin e ekzaminimit kompjuterik të jenë:

a) Të besueshme
b) Të paanshme
c) Të qarta

1.17 Detyrimet për kujdesin ndaj viktimës dhe dëshmitarëve

Veprat penale që mund të kryhen përmes mjeteve kompjuterike janë të shumta, nga ana tjetër këto vepra penale krijojnë edhe pasoja të rënda ndaj viktimës por edhe ndaj dëshmitarëve që mund të kenë pasoja nga vepra penale. Mund të ketë raste kur kemi të bëjmë me veprat penale të cenimit të integritetit seksual qoftë ndaj madhorëve apo ndaj të miturve. Mund të ketë raste kur kemi të bëjmë me veprën penale të shpërndarjes së materialit pornografik të fëmijëve që si vepra krijojnë një pasojë të thellë traumatike për fëmijët por edhe për një rreth më të gjerë.
Në këtë kuptim duhet të kemi parasysh se provat e tilla me rastin e sigurimit dhe me rastin e administrimit në shqyrtim gjyqësor mund të ri viktimizojnë viktimën e veprës penale pasi që përmes imazheve që shfaqen në procedura mund të rikujtojnë përjetimet që ka pësuar në veprën penale që është kryer e që është viktimë, qoftë madhori apo i mituri.

Rrjedhimisht duhet të kihet kujdes edhe në rastin e provave elektronike dhe të merret në konsideratë kujdesi i viktimës apo dëshmitarit kur kemi të bëjmë me provat elektronike që mund të krijojnë një gjendje të rënduar psikologjike si pasoj e imazheve që shfaqen si prova elektronike.

"Duhet t'i kushtohet vëmendje efektit të veprës penale mbi viktimën. Kjo është veçanërisht e rëndësishme në rastet që përfshijnë abuzimin e fëmijëve dhe potencialin për ndjekje penale lidhur me imazhet dixhitale të një abuzimi të tillë. Shumë dëshmitarë të krimeve mund të ndiejnë stres dhe frikë gjatë hetimit të një krimi dhe më pas kur marrin pjesë në gjykatë dhe japin prova. Stresi mund të ndikojë në sasinë dhe cilësinë e dëshmive të dëshmitarëve të të gjitha moshave. Disa dëshmitarë mund të kenë vështirësi të veçanta në pjesëmarrjen në gjykatë dhe dhënien e provave për shkak të moshës së tyre, rrethanave personale, frikës nga kërcënimi ose për shkak të nevojave të tyre të veçanta. Duhet të sigurohen masa shtesë për dëshmitarët e cenueshëm dhe të frikësuar, për t'i ndihmuar ata të japin dëshminë e tyre më të mirë në gjykatë dhe për të lehtësuar disi stresin që lidhet me dhënien e dëshmisë"[176].

1.18 Sektori për hetimin e krimit kibernetikë në Policinë e Kosovës

Në kuadër të strukturave organizative të policisë, një ndër departamentet më të rëndësishme të hetimit është Departamenti për parandalimin dhe luftimin e krimit të organizuar. Në kuadër të ketij departamenti ekziston sektori i veqantë i hetimit të krimit kibernetik, që ka si fokus marrjen dhe ruajtjen e provave elektronike apo luftimin dhe hetimin e veprave penale që kryhen me anë të kompjuterëve apo përmes rrjetit të internetit.

1.19 Agjencia për Forenzikë në Kosovë

Një ndër agjencitë më të rëndësishme për ekzaminimin dhe kryerjen e akt ekspertimit në procedurën penale në vendin tonë është Agjencia për Foreznikë në Kosovë.

Në kuadër të kësaj agjencie është i sistemuar Departamenti për Teknologji Informative – forenzik, ku funksionon Divizioni për ekzaminim Kompjuterik. Në kuadër të këtij divizioni, rezulton se ekzaminimet kryhen te të gjitha llojet e ekspertimeve të forenzikës digjitale si:

a. Kryerja e ekzaminimeve të komjuterëve,

[176] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 152.

b. Kryerja e ekzaminimeve të telefonisë mobile,
c. Kryerja e ekzaminimeve të SIM kartelave,
d. Kryerja e ekzaminimeve të gjitha llojeve USB-ve,
e. Kryerja e ekzaminimeve të gjitha llojeve memory kartelave,
f. Kryerja e ekzaminimeve të gjitha llojeve CD/DVD,
g. Krijimi i imazhit të mediumeve elektronike (kopjimi fizik i mediumit) etj.

Sipas Agjencisë për Forenzikë, këto ekzaminime kryhen duke përdorur metoda të ndryshme bazuar në procedurat standarde të operimit si në vijim:

a. Udhëzues, divizioni për ekzaminim të kompjuterëve,
b. Programet e aprovuara për ekzaminim forenzik,
c. Procedura për nxjerrjen e hard disqeve,
d. Procedura për krijimin e imixheve (kopjes forenzike) të mediumeve,
e. Ekzaminimi dhe analizimi kompjutereve,
f. Ekzaminimi i telefonave mobil dhe sim kartelave,
g. Përgatitja e mostrave për testet e brendshme të aftësive profesionale.

Duhet të kemi parasysh se asnjë ekzaminim kompjuterik nuk mund të bëhet pa programe dhe sofver të caktuar. Në këtë kuptim duhet që programet dhe softveret të jenë të akredituara apo të licencuara e të cilat shërbejnë për ekzaminime kompjuterike, vetëm në këtë mënyrë kur programet apo softveret janë me licencë apo të akredituar atëherë mund të themi se janë ndjekur standardet siç edhe kërkohet nga Neni 145 i Kodit të procedurës penale të Kosovës.

Përveç licencimit apo akreditimit, është e nevojshme që në stafin profesional të ketë edhe trajnime për sa i përket ekzaminimit të kompjuterëve, marr parasysh se trajnimet mundësojnë marrjen e njohurive për praktikat më të avancuara që përdoren për ekzaminim e që po ashtu është kërkesë e nenit 145, të Kodit të procedurës Penale që me rastin e ekzaminimit duhet që të përdoren praktika të njohura dhe të pranueshme në ekzaminim kompjuterik.

1.20 Roli i ekspertit

Është e kuptueshme që disa fusha janë të panjohura në çështjet specifike për temat e caktuara si për prokurorin ashtu edhe për gjyqtarin, andaj kjo determinon edhe angazhimin e ekspertëve posaçërisht në fushën e ekzaminimeve kompjuterike.

Dispozitat e Kodit të Procedurës Penale, përcaktojnë disa kritere për sa i përket se kush mund të jetë ekspert, gjegjësisht se cilat kushte duhet plotësuar që në nenin 136 paragrafi 1 nënparagrafi 1.1 dhe 1.3 përcaktojnë qështjet e kushteve që duhet ti përmbush eksperti e që janë:

a). Të dhënat personale dhe profesionale të ekspertit;

b). Përvoja që ka eksperti në fushën e tillë të ekspertimit;

c). Trajnimet e specializuara që janë ndjekur e që ndërlidhen me fushën e specializimit;

ç). Argumentimin se përse këto trajnime ndërlidhen me fushën e ekspertimit dhe metodat që ndjekjen për ekzaminim.

"Një gjyqtar duhet të jetë në gjendje të vlerësojë kualifikimet dhe nivelin e njohurive që një ekspert sjell në çështje. Rregullat se kush mund dhe kush nuk mund të jetë dëshmitar ekspert ndryshojnë nga vendi në vend. Një ekspert duhet të jetë i pavarur dhe i paanshëm. Ai ka një detyrim ndaj gjykatës dhe duhet t'i sjellë në vëmendje gjykatës çdo dobësi ose kufizim në provat që ofrohen"[177].

1.21 Provat elektronike në procedurat jo penale

Përveç se në fushën penale provat elektronike gjithnjë e më shumë shërbejnë për çështjet gjyqësore edhe në procedurat jo penale kryesisht në procedurat gjyqësore me natyrë kontestimore apo me natyrë komerciale.

Është e njohur tashmë se komunikimi elektronik është shumë më i shprehur si në nivel vendi ashtu edhe në nivel ndërkombëtar, tashmë përdorimi i letrës si mënyrë për të lidhur marrëveshje të ndryshme në vende të ndryshme mund të themi se është përgjysmuar, ndërsa komunikimi elektronik edhe për lidhje të marrëveshjeve apo edhe për çdo çështje me natyrë civile apo komerciale është shumë më i shprehur ndërmjet subjekteve të së drejtës.

Përmes emaileve apo fakteve janë marrëveshjet e shumta që lidhen ndërmjet personave juridik si biznese në qarkullueshmërinë e mallrave dhe shërbimeve, të gjitha këto aspekte të komunikimeve elektronike po ashtu mund të shërbejnë si prova në procedurat kontestimore pranë gjykatave kur gjykojnë çështje ndërmjet subjekteve fizike apo edhe ndërmjet subjekteve juridike.

[177] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 159.

Në sistemin tonë ligjor të procedurës kontestimore, marrja e provave të tilla kur është në disponim të ndonjë personi apo të ndonjë subjekti juridik, mund të urdhërohet vetëm përmes aktvendimit të gjykatës për nxjerrjen e provës, ndërsa provat e tilla kryesisht gjykata i nxjerr vetëm sipas propozimit të palëve.

Në disa sisteme juridike janë të lejuar hetuesit privat që mund të sigurojnë prova për ndonjërën nga palët ndërgjyqësore kontestimore, ndërsa te një sistem i tillë i hetuesve privat nuk është i lejuar edhe më tutje. Megjithatë duhet të kemi parasysh se hetuesit privat nuk kanë autorizimet e tilla për marrjen e provave elektronike sikurse kanë autoritetet shtetërore që veprojnë në rrethana të qëllimit për sigurinë kombëtare apo që veprojnë në marrjen e provave elektronike sipas urdhrit që lëshohet nga gjykata në procedurën penale.

Gjersa në procedurën penale çështjet tërësisht personale (siç mund të jetë aspekti shëndetësor i palëve) që prova e tillë ndërlidhet me ndonjë aspekt të gjendjes së fakteve ËSHTË e pritshme që të kundërshtohet fuqishëm në procedurën penale apo sekretet afariste nëse kemi të bëjmë me konteste ndërmjet subjekteve afariste – personave juridik, është e pritshme që do të kundërshtohet çdo zbulim i sekreteve të tilla në procedurat gjyqësore që ai të mos zbulohet, në procedurën penale çështjet kur janë edhe nga aspekti subjektiv nëse kanë të bëjnë me çështjen e vërtetimit të fakteve nuk është e pritshme që të kundërshtohen nga palët në proces, p.sh të dhënat elektronike që mund të nxjerrën nga një ekzaminim kompjuterik për një të dyshuar e që kanë të bëjnë me çështjet e problemeve mendore edhe pse janë tërësisht të sferës personale, nëse i shërbejnë aspektit të gjendjes së përgjegjësisë do të trajtohen si prova[178].

1.22 Instruksionet për konfiskimin e provave elektronike

Gjatë sekuestrimit të një pajisjeje elektronike duhet të merren në konsideratë këto situata që duhet vepruar kur pajisja është e ndezur apo është e fikur;
a).Pajisja e ndezur:

[178] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 159-160.

Nëse pajisja është e ndezur, mos e fikni sepse fikja e saj mund të aktivizojë një mekanizëm bllokimi:

Fotografoni ekranin (nëse është e aplikueshme) dhe regjistroni informacionin e shfaqur;

Hiqni të gjitha kabllot e furnizimit me energji (zakonisht është më mirë t'i hiqni ato nga pajisja e synuar dhe jo nga priza e murit);

Mos u përpiqni të hyni në memorien e brendshme ose në ndonjë media ruajtjeje.

b).Paisja e fikur:

Nëse është e fikur, mos e ndizni sepse kjo mund të modifikojë/shkatërrojë provat (si në sistemet kompjuterike);

Shkëputni çdo linjë telefonike nga muri në vend të pajisjes dhe më pas dokumentoni dhe shenjëzoni atë;

Regjistroni informacione të rëndësishme:

Merrni manualet dhe udhëzimet e tjera nëse janë të disponueshme;

Regjistroni të dhënat përkatëse (p.sh. numrin e telefonit).

Sa i përket, paketimit, transportit dhe ruajtjes ato duhet të sigurohen në mënyrë që të mos dëmtohen dhe të pamundësohet ndërhyrja në ato pajisje nga distanca.

Bateritë kanë një jetëgjatësi të kufizuar, të dhënat mund të humbasin nëse ato dështojnë. Prandaj, zyrtarët hetues duhet të informohet se një telefon i mundësuar nga bateritë ka nevojë për vëmendje të menjëhershme;

Pas sekuestrimit, ia dorëzoni pajisjen një eksperti sa më shpejt të jetë e mundur.

Pas sekuestrimit, pajisja duhet t'i dorëzohet një specialisti sa më shpejt të jetë e mundur. Në rastin e PDA-ve dhe telefonave celularë kjo duhet të bëhet menjëherë[179].

1.23 Procesi i qasjes fizike në sekuestrim të pajisjeve elektronike

Qasje fizike dhe kërkimi mund të jetë i vështirë për tu përcaktuar lehtësisht nëse një kompjuter është i ndezur apo jo. Duhet të veprohet me kujdes për të përcaktuar statusin e kompjuterit-pajisjes elektronike, duke bërë një fotografi.

[179] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 160.

Duhet të shikohet dhe dëgjohet për shenja që tregojnë se kompjuteri është i ndezur. Kjo bëhet përmes zhurmës së ventilatorëve që punojnë, të disqeve që rrotullohen ose duke kontrolluar nëse lëshohet dritë në pajisje. Mund të lëvizet miu, por të mos shtypet asnjë buton.

Duhet kontrolluar ekranin për çdo tregues të një ruajtësi ekrani ose ekrani hyrjeje. Duhet vërtetuar statusi i ekranit duke bërë një fotografi. Nëse kompjuteri rezulton të jetë i ndezur, por po shfaqet një ruajtës ekrani, gjërat e para që duhet të bëni janë: Vëzhgoni ekranin ndërsa lëvizni miun; Nëse një ruajtës ekrani zhduket dhe ju merrni qasje në sistem pa ju kërkuar një fjalëkalim, mund të vazhdoni me hapat e ardhshëm të Live Data Forenzics (nëse jeni plotësisht të trajnuar dhe kompetentë për ta bërë këtë).

Nëse ruajtësi i ekranit është i bllokuar me fjalëkalim, pyeteni të dyshuarin, kontrolloni nëse aludimi për fjalëkalimin është aktivizuar në ndërfaqen e ruajtësit të ekranit, kërkoni shënime ose të dhëna të tjera.
Nëse fjalëkalimi është marrë, atëherë çaktivizoni dhe vazhdoni me hapat e ardhshëm të Live Data Forensics. Nëse nuk e zbuloni fjalëkalimin, ekzistojnë teknika për të marrë RAM-in nëpërmjet ndërfaqeve FireWire dhe Thunderbolt ose me metodën 'cold boot'.

Këto teknika duhet të përdoren vetëm nga specialistët e Live Data Forensics.
Në secilin prej këtyre rasteve: Vërtetoni statusin e ekranit duke bërë një fotografi. Nëse kompjuteri është i ndezur, por nuk është i mbrojtur nga një ruajtës ekrani ose ekran vërtetimi ose keni arritur të merrni fjalëkalimin: Kontrolloni ekranin e shfaqjes për shenja që provat dixhitale po shkatërrohen. Fjalët që duhen kërkuar përfshijnë "fshij", "formatoj", "hiq", "kopjoj", "zhvendos", "prit" ose "fshij". Duhet kërkuar për shenja të përdorimit të enkriptimit (të përshkruara më vonë). Duhet kërkuar për shenja që kompjuteri po aksesohet nga një kompjuter ose pajisje e largët. Duhet kërkuar për shenja që po përdoren shërbime cloud. Duhet kërkuar për shenja të komunikimeve aktive ose të vazhdueshme me kompjuterë ose përdorues të tjerë, siç janë dritaret e mesazheve të menjëhershme ose dhomat e bisedave. Duhet kërkuar për shenja që kamerat ose kamerat web (kamerat web) janë aktive. Duhet vazhduar me lëvizjen e miut për të shmangur aktivizimin e një ruajtësi ekrani ose bllokimi. Duhet kërkuar për shenja të makinave virtuale që janë të ndezura

dhe ndoshta janë në modalitetin e ekranit të plotë. Në të gjitha këto raste duhet vërtetuar statusin e ekranit duke bërë një fotografi[180].

1.24 Marrja e te dhënave nga Interneti

Mbledhja e provave nga interneti përfshinë mbledhjen e provave online. Janë të njohura dy aspekte të marrjes së provave online.

a) Informacioni i disponueshëm publikisht në internet, si dhe
b) Hetimet e fshehta në internet.

Kjo e fundit është shumë më e ndërlikuar kryerja e hetimeve të tilla kërkon njohuri dhe aftësi shtesë sesa ato të kërkuara në pajisjet elektronike.
Provat më të rëndësishme elektronike që mund të merren përmes Internetit janë:

1. IP adress – Internet Protockoll – Protokolli i Internetit për adresën; (Autoriteti i Numrave të Caktuar në Internet "(IANA)" rregullon adresat IP dhe koordinon ndarjen e adresave IP përmes entiteteve rajonale të njohura si Regjistra Rajonale të Internetit (RIR):
   RIPE (Evropa dhe disa pjesë të Azisë)
   APNIC (Azia dhe Rajoni i Paqësorit)
   ARIN (Amerika e Veriut)
   LACNIC (Amerika Latine dhe Karaibet)
   AfriNIC (Afrika)[181]

Janë të njohura po ashtu IP Adresat statike dhe Dinamike. IP adresat dinamike janë pikërisht për shkak të masës së madhe të kompjuterëve dhe pajisjeve që përdorin internetin, dhe shërbyesit e internetit iu mundësohet që të kenë edhe IP adresa dinamike që mund të jetë qasja e pajisjeve. ISP-ja është kërkesa e qasjes së një pajisje për në IP adresë, kjo e bënë edhe lidhjen e identitetit te subjekti që është qasur në IP adresë.

DNS – System Name Domeain - Sistemi i Emra të Domeinëve, (Sistemi i Emrave të Domeinëve (DNS) është një sistem që vepron si një libër

[180] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 161.
[181] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 91-94.

telefonash i madh dinamik dhe mban gjurmët e adresës (ose adresave) IP që i është caktuar cilit "emër" dhe anasjelltas. Marrëdhënia nuk është gjithmonë një emër me një adresë IP (për shembull, një emër mund t'u caktohet disa adresave IP dhe anasjelltas)[182].

URI – Uniform Resource Identifier – Identifikuese i Burimeve Uniforme, (URI është etiketa e përdorur për të identifikuar vendndodhjen e një 'burimi' ose komponenti në një sistem kompjuterik. URI-të ofrojnë një mënyrë që një burim të aksesohet nga pajisje të tjera në të njëjtin rrjet. URI më i zakonshëm është një adresë faqeje interneti dhe lejon ndërveprimin në të gjithë World Wide Web-in). Është i njohur edhe URL – që mundëson qasje tjera por edhe në faqe të internetit[183].

Whois lookup - Mund të ndihmoj hetuesinë për hetimin dhe zbulimin e një pronari specifik të domeinit[184].

Revers Whoisi – ky shërbim mundëson listimin e të gjitha të dhënat DNS/IP (të njohura për faqen/mjetin), të regjistruara nën identitetin e dhënë. Ky shërbim i mundëson hetuesi të kërkojë me emër, email, numër telefoni ose adresë fizike[185].

Një ndër burimet më të qasshme publike për provat elektronike janë WebSite. Pastaj rrjetet sociale të internetit, si: Internet IDs, Chatet, Fotografitë e publikuara, Fajllat Per to Per, Dark Ëeb-et, të gjitha këto mund të jenë, por jo vetëm, edhe shumë të tjera si burime publike që mund të shërbejnë si aspekt të marrjes së provave elektronike në Internet.
Ndërsa lidhur me hetimin online që mund të zbatohet, duhet të kemi parasysh se metodat janë të shumta por njëkohësisht ato zhvillohen shumë shpejt për

[182] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 98.
[183] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 99.
[184] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 100.
[185] Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, faqe 101.

shkak të zhvillimit të teknologjisë, megjithatë gjithnjë në hetimin e fsheht online kur bëhet, hetuesit duhet të kenë parasysh që:

a) Të janë në gjendje të identifikojnë kufijtë ligjorë të veprimeve të tyre, sepse mund të përfshihen vet në aktivitete kriminale nëse nuk i njohin kufijtë e tillë.
b) Të kuptojnë plotësisht nevojën për vërtetësinë e provave;
c) Të kujdesen për mos cenimin e të Drejtave të Njeriut, dhe të palëve të tjera të prekura nga hetimi.

Pasi të jenë marrë provat nga një sistem kompjuterik, faza tjetër e hetimit është nxjerrja e elementëve të rëndësishëm nga të dhënat e sekuestruara. Këtu rol të rëndësishëm kanë, elementët që lidhen me vërtetimin e fakteve në hetim. "Rëndësi të theksuar përbën një studim i Korporatës Ndërkombëtare të të Dhënave (IDC), që ka parashikuar se deri në vitin 2020 do të gjenerohen dhe konsumohen gjithsej 44 zeta bajt (44 trilion gigabajt) të dhënash në të gjithë botën. Studimi i IDC-së u bazua në premisën se sasia e të dhënave në të gjithë botën dyfishohet në madhësi çdo dy vjet dhe se këto të dhëna përbëhen kryesisht nga të dhëna të aktiviteteve të përdoruesit të kompjuterit. Në një hetim, të dhëna të tilla mund të ofrojnë fakte të vlefshme mbi aktivitetin e përdoruesit nëse është përfshirë në kriminalitet".

Literatura:

1. *Kushtetuta e Republikes se Kosoves.*
2. *Komentari i Kushtetutes se Republikes se Kosoves.*
3. *Deklarata Universale per te drejtata e njeriut.*
4. *Konventa evropiane per mbrojtjen e te drejtave dhe lirive te njeriut.*
5. *Pakti ndërkombëtar per te drejtata civile dhe politike.*
6. *A Commentary on the Internationalcovenant on Civil and Political Rights - The UN Human Rights Committee's Monitoring of ICCPR Rights - PAULM.TAYLOR Senior Research Fellow at the University of Queensland's TC Beirne School ofLawand Visiting Fellow at the Australian National University's College of Law - ISBN 978 1 108 49885 2 Hardback.*
7. *The Right to Privacy Origins and Influence of a Nineteenth-Century Idea Megan Richardson – Cambridge University- University Press, ISBN 978-1-108-41969-7 Hardback ISBN 978-1-108-41168-4 Paperback.*
8. *Volume 56, Number 1, winter 2015, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, Marko Milanovic.*
9. *Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges - Version 2.0 Cybercrime Division Directorate General of Human Rights and Rule of LawStrasbourg, France 15 December 2014.*
10. *Software agents, surveillance, and the right to privacy: a legislative framework for agent enabled surveillance – Liden University Press - ISBN 978 90 8728 021 5.*
11. *Maria Angela Biasiotti • Jeanne Pia Mifsud Bonnici • Joe Cannataci • Fabrizio Turchi Editors - Handling and Exchanging Electronic Evidence Across Europe - Law, Governance and Technology Series ISBN 978-3-319-74871-9*
12. *Forensic Examination of Digital Evidence: A Guide for Laë Enforcement - U.S. Department of Justice Office of Justice Programs 810 Seventh Street N.W. Washington, DC 20531: John Ashcroft Attorney General - Deborah J. Daniels Assistant Attorney General - Sarah V. Hart Director, National Institute of Justice.*
13. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations - Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, July 2002.*
14. *Digital Evidence in the Courtroom - John D. Nilsson (Editor) 2010. ISBN: 978-1-60741-803-0*
15. *Preserving Electronic Evidence for Trial, A Team Approach to the Litigation Hold, Data Collection, and Evidence Preservation Ann D. Zeigler Ernesto F. Rojas, SBN: 978-0-12-809335-1.*
16. *Doracak për krimin kompjuterik – Janar 2014 Maqedoni.*
17. *LIGJ nr. 6/L-038, PËR SHËRBIMET POSTARE.*
18. *KODI NR. 08/L-032, I PROCEDURËS PENALE.*
19. *LIGJI Nr. 04/L-109, PËR KOMUNIKIMET ELEKTRONIKE.*
20. *Ligji Nr. 03/L-063, LIGJI PËR AGJENCINË E KOSOVËS PËR INTELIGJENCË.*
21. *Gjykata Kushtetutese e Republikës së Kosovës - e aktgjykimit KI 113/21*
22. *LIGJI Nr. 04/L-193, PËR AVOKATINË*

Raste te Gjykates Evropiane për të Drejtat dhe Liritë e Njeriut:

e.Salihoglu and others v. Turkey – 2019.
Pfeifer and Plankl v. Austria – 1992.
Roman Zakharov v. Russia 2015 Grand Chamber.
Benedik v. Slovenia - 2018.
Barbulescu v. Romania 2017 Grand Chamber.
K.U. v. Finland – 2008.
Copland v. United Kingdom - 2007.
Weiser and Bicos

KAPITULLI VI

TERMAT DHE KUPTIMI I TYRE QË PËRDOREN MË SHPESH NË KRIMIN KOMPJUTERIK

Vaton Durguti, Gjyqtar në Gjykatën e Apelit

Vaton Durguti, Gjyqtar në Gjykatën e Apelit

1. TERMAT DHE KUPTIMI I TYRE QË PËRDOREN MË SHPESH NË KRIMIN KOMPJUTERIK

Krimi kompjuterik është një formë e krimit që përfshin përdorimin e kompjuterëve, rrjeteve dhe sistemeve informatike për të kryer veprime të paligjshme, të cilat mund të dëmtojnë individë, organizata ose qeveri. Ky lloj krimi përfshin një gamë të gjerë aktivitetesh, duke filluar nga vjedhja e identitetit deri te sulmet kibernetike në infrastrukturat kritike.
Termat më të përdorur në krimin kompjuterik janë:

1. Hacking – Akti i ndërhyrjes së paautorizuar në një sistem kompjuterik ose rrjet për të marrë informacione, për të modifikuar të dhënat ose për të shkaktuar dëmtime. Hackers ndahen në disa kategori, të cilët në varësi të qëllimit të tyre edhe emërtohen, si :

- **White-hat hackers** (hakerët etikë) – Punojnë për të gjetur dhe ndrequr dobësitë e sistemeve (Mitnick & Simon, 2005).
- **Black-hat hackers** (hakerët e dëmshëm) – Ndërhyjnë në sisteme për përfitime personale ose për të shkaktuar dëme.
- **Gray-hat hackers** – Operojnë në mes të etikës dhe keqdashjes, shpesh duke ekspozuar dobësi pa lejen e pronarit të sistemit.

2. Phishing – Një teknikë mashtrimi që përfshin dërgimin e mesazheve të rreme (zakonisht email) që imitojnë burime të besueshme për të vjedhur informacion personal, si fjalëkalime dhe numra kartash krediti (Schneier, 2015.) Pra, kjo teknik e ndërhyrjes paraqitet në form të postës eletronike që ngjan sikur është nga ndonjë burim që njihet mire (si shembull, banka ose dhënës i shërbimeve të internetit) me të cilën kërkohet të vërtetohen të dhënat personale.

3. Malware – shkurtesë (malicious software) që përfshin një gamë të gjerë programesh të dëmshme që synojnë të dëmtojnë ose të marrin kontrollin e një sistemi kompjuterik. Llojet kryesore të Malware përfshijnë:

Viruse kompjuterike – Programet që kopjojnë veten dhe infektojnë skedarët e sistemit, të cilët 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, duke shkaktuar; vjedhje të hapësirës së hard-diskut ose procesorit, hyrje në informatat private, kompromet të të dhënave, paraqitje të porosive të ndryshme 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.

Trojans – Fshehën brenda softuerëve legjitimë dhe mundësojnë hyrjen e paautorizuar në sistem. "Trojani" është program i dëmshëm 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 programi i dëmshëm 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 kur 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.

Spyware – Monitoron aktivitetet e përdoruesit dhe transmeton të dhëna pa leje. Spyware është një program keqdashës që hyn në kompjuterin e një përdoruesi, mbledh të dhëna nga pajisja dhe përdoruesi dhe i dërgon ato te palët e treta pa pëlqimin e tyre. Një përkufizim i pranuar gjerësisht i spyware është një fije e malware-it e projektuar për të hyrë dhe dëmtuar një pajisje pa pëlqimin e përdoruesit.Spyware mbledh informacione personale dhe të ndjeshme që u dërgon reklamuesve, firmave të mbledhjes së të dhënave ose aktorëve keqdashës për fitim. Sulmuesit e përdorin atë për të gjurmuar, vjedhur dhe shitur të dhënat e përdoruesit, të tilla si përdorimi i internetit,

kartat e kreditit dhe të dhënat e llogarisë bankare, ose për të vjedhur kredencialet e përdoruesit për të falsifikuar identitetin e tyre.

Ransomware – Enkripton të dhënat e përdoruesit dhe kërkon pagesë për çlirimin e tyre. Ransomware është një program keqdashës që enkripton skedarë të rëndësishëm në ruajtjen lokale dhe të rrjetit dhe kërkon një shpërblim për të dekriptuar skedarët. Hakerët e zhvillojnë këtë program keqdashës për të fituar para përmes zhvatjes dixhitale. Ransomware është i enkriptuar, kështu që çelësi nuk mund të detyrohet dhe e vetmja mënyrë për të rikuperuar informacionin është nga një kopje rezervë. Mënyra se si funksionon ransomware e bën atë veçanërisht të dëmshëm. Llojet e tjera të programeve keqdashëse shkatërrojnë ose vjedhin të dhëna, por lënë të hapura opsione të tjera rikuperimi. Me ransomware, nëse nuk ka kopje rezervë, duhet të paguani shpërblimin për të rikuperuar të dhënat. Ndonjëherë bizneset paguajnë shpërblimin dhe sulmuesi nuk dërgon çelësin e dekriptimit.

Denial of Service (DoS) dhe Distributed Denial of Service (DDoS) – Sulme që mbingarkojnë një shërbim duke dërguar kërkesa të shumta njëkohësisht, duke e bërë atë të papërdorshëm për përdoruesit e ligjshëm. Mohimi i Shërbimit (DoS) dhe Mohimi i Shpërndarë i Shërbimit (DDoS) janë sulme kibernetike që e bëjnë një sistem ose shërbim të padisponueshëm për përdoruesit legjitimë duke e mbingarkuar atë me trafik. Dallimi kryesor është se një sulm DoS buron nga një burim i vetëm, duke e bërë më të lehtë zbulimin dhe zbutjen e tij, ndërsa një sulm DDoS përdor makina të shumta të kompromentuara, siç është një botnet, për të nisur sulmin, i cili është më i vështirë për t'u bllokuar. Qëllimi është të përmbytet objektivi me më shumë kërkesa sesa mund të trajtojë, duke shkaktuar rrëzimin ose ngadalësimin e tij, duke çuar në ndërprerje të konsiderueshme

Social Engineering – Inxhinieria sociale është termi që përdoret për një gamë të gjërë aktivitetesh dashakeqe të kyera përmes ndërveprimeve njerëzore. Ky aktivitet përdor manipiulimin psikologjik për të mashtruar përdoruesit që të bëjnë gabime sigurie ose të japin informacione të ndjeshme. Sulmet e inxhinierisë sociale ndodhin në një ose më shumë hapa. Përdoruesi fillimisht heton viktimën e synuar për të mbledhur informacione të nevojshme siç janë pikat e mundshme të hyrjes dhe protokollet e dobëta të sigurisë, të nevojeshme

për të vazhduar me sulmin. Pastaj, sulmuesi lëviz për të fituar besimin e viktimës dhe për të ofruar stimuj për veprime të mëvonshme që shkelin praktikat e sigurisë, siç është zbulimi i informacionit të ndjeshëm ose dhënia e aksesit në burimet krikike.

Manipulimi psikologjik i individëve për të nxjerrë informacione të ndjeshme përdoret përmes teknikave si:

- **Pretexting** – Krijimi i një skenari të rremë për të bindur një person të japë informacion.
- **Baiting** – Përdorimi i stimujve joshës për të bindur viktimën të shkarkojë malware.
- **Quid pro quo** – Premtimi i një shërbimi ose përfitimi në këmbim të informacionit të ndjeshëm .

4. Identity Theft (Vjedhja e Identitetit) – Procesi i vjedhjes së informacionit personal të një individi për të kryer mashtrime financiare ose aktivitete të tjera të paligjshme. Vjedhja e identitetit është kur dikush përdor informacionin tuaj personal pa lejen tuaj për të kryer mashtrim, siç është hapja e llogarive të reja, kryerja e blerjeve me kartat tuaja të kreditit ose marrja e kujdesit mjekësor. Kjo mund të dëmtojë kreditin tuaj, reputacionin personal dhe madje të ndikojë në cilësinë e kujdesit tuaj mjekësor. Informacioni i vjedhur shpesh përfshin emrin, adresën, numrin e Sigurimeve Shoqërore dhe numrat e llogarisë suaj të kreditit ose bankare.

5. Man-in-the-Middle Attack – Një metodë ku një sulmues futet midis komunikimit të dy palëve për të vjedhur ose modifikuar të dhënat që shkëmbehen. Një sulm njeri-në-mes (MitM) është një formë sulmi kibernetik në të cilin kriminelët që shfrytëzojnë protokollet e dobëta të bazuara në internet futen midis entiteteve në një kanal komunikimi për të vjedhur të dhëna. Asnjë nga palët që dërgojnë email, dërgojnë mesazhe ose bisedojnë në një video-thirrje nuk është në dijeni se një sulmues ka futur praninë e tyre në bisedë dhe se sulmuesi po vjedh të dhënat e tyre.Ndërsa shumica e sulmeve kibernetike janë të heshtura dhe kryhen pa dijeninë e viktimave, disa sulme MitM janë e kundërta. Ato mund të përfshijnë një bot që gjeneron mesazhe teksti të besueshme, imiton zërin e një personi në një thirrje ose falsifikon një sistem të tërë komunikimi për të mbledhur të dhëna që sulmuesi mendon se janë të rëndësishme nga pajisjet e pjesëmarrësve.

6. Zero-day Exploit – Një sulm që shfrytëzon një dobësi të paidentifikuar më parë në softuer, për të cilën nuk është krijuar ende një përditësim i sigurisë. Një shfrytëzim zero-ditor është një vektor sulmi kibernetik që shfrytëzon një të metë sigurie të panjohur ose të paadresuar në softuerin, harduerin ose firmware-in e kompjuterit. "Zero day" i referohet faktit që shitësi i softuerit ose pajisjes ka zero ditë për të rregulluar të metën sepse aktorët keqdashës mund ta përdorin atë tashmë për të hyrë në sisteme të cenueshme.Cenueshmëria e panjohur ose e paadresuar quhet një cenueshmëri zero-ditore ose kërcënim zero-ditor. Një sulm zero-ditor është kur një aktor keqdashës përdor një shfrytëzim zero-ditor për të mbjellë programe keqdashëse, për të vjedhur të dhëna ose për të shkaktuar dëme te përdoruesit, organizatat ose sistemet. Një koncept i ngjashëm por i veçantë, programe keqdashëse zero-ditore, është një virus ose program keqdashës për të cilin nënshkrimi është i panjohur ose ende i padisponueshëm, dhe për këtë arsye i pazbulueshëm nga shumë zgjidhje softuerësh antivirus ose teknologji të tjera të zbulimit të kërcënimeve të bazuara në nënshkrime.

2. Mbrojtja kundër krimeve kompjuterike

Për të mbrojtur sistemet dhe të dhënat nga krimet kompjuterike, organizatat dhe individët sugjerohet të ndërmarrin masa të ndryshme sigurie, si:

- Përdorimi i fjalëkalimeve të forta dhe autentifikimit me dy faktorë (2FA).
- Instalimi dhe përditësimi i rregullt i softuerëve të sigurisë, si antivirusët dhe firewall-et.
- Trajnimi i përdoruesve për të identifikuar dhe shmangur mashtrimet kibernetike.
- Përdorimi i enkriptimit për të mbrojtur të dhënat e ndjeshme.
- Monitorimi i trafikut të rrjetit për të zbuluar dhe parandaluar sulmet e mundshme.

Përfundim

Krimi kompjuterik përbën një sfidë të vazhdueshme dhe komplekse për sigurinë kibernetike në nivel individual, institucional dhe shoqëror. Dinamika

e zhvillimit teknologjik kërkon që masat mbrojtëse të përshtaten në mënyrë të vazhdueshme me format e reja të kërcënimeve, të cilat po bëhen gjithnjë e më të sofistikuara. Në këtë kontekst, roli i edukimit digjital, trajnimeve profesionale dhe ndërgjegjësimit publik është thelbësor për ndërtimin e një kulture të qëndrueshme të sigurisë kibernetike.
Institucionet publike dhe private duhet të adoptojnë qasje gjithëpërfshirëse që kombinojnë politikat e forta të menaxhimit të informacionit me investime në teknologji mbrojtëse dhe analiza të vazhdueshme të rreziqeve. Po ashtu, bashkëpunimi ndërinstitucional dhe shkëmbimi i informacionit mbi incidentet kibernetike mundëson reagim më të shpejtë dhe më efikas ndaj kërcënimeve.
Në përfundim, mbrojtja nga krimi kompjuterik nuk duhet të shihet vetëm si detyrë teknike, por si përgjegjësi e përbashkët që kërkon angazhim të vazhdueshëm, planifikim strategjik dhe përmirësim të kapaciteteve në të gjitha nivelet e shoqërisë digjitale. Vetëm në këtë mënyrë mund të sigurohet një mjedis kibernetik i qëndrueshëm, i besueshëm dhe i mbrojtur.

3. IP - Protokoli i Internetit

Protokoli i Internetit (IP) është një nga protokollet themelore të paketës së protokolleve TCP/IP, i cili përdoret për të adresuar dhe transmetuar të dhëna përmes rrjeteve kompjuterike, duke përfshirë internetin. IP lejon dërgimin e paketave të të dhënave nga një pajisje në tjetrën, pavarësisht nga infrastruktura fizike që përdoret për lidhjen e tyre (Kurose & Ross, 2017).

3.1 Versionet e IP

Protokolli i Internetit ka dy versione kryesore:

1. IPv4 (Internet Protocol version 4) IP përcakton rregullat dhe kufizimet për komunikimin në internet ose në një rrjet lokal. Falë IP-së, ne mund të kemi rrugëzim të ndërlidhur të rrjetit me përçim të paketave sepse ai përcakton formatin, komunikimet, përdorimin e adresave IPv4 dhe rrugëtojnë të dhënat.

- Përdor adresa 32-bitëshe (p.sh., 192.168.1.1), duke lejuar rreth 4.3 miliardë adresa unike.
- Shpërndarja e adresave IPv4 ka krijuar nevojën për mekanizma si Network Address Translation (NAT) për të zgjeruar përdorimin e tyre.

- Është ende versioni më i përdorur në rrjetet kompjuterike (Forouzan, 2012).

2. IPv6 (Internet Protocol version 6) IPv6 është Protokolli i Internetit i përmirësuar, i projektuar për të përmbushur kërkesën në rritje për adresa IP që IPv4 nuk mund t'i trajtojë për shkak të hapësirës së kufizuar të adresave.

- Përdor adresa 128-bitëshe (p.sh., 2001:0db8:85a3::8a2e:0370:7334), duke mundësuar një numër pothuajse të pakufizuar adresash.
- Eliminon nevojën për NAT dhe siguron një menaxhim më të mirë të trafikut të rrjetit.
- Ka mbështetje më të mirë për sigurinë dhe performancën në krahasim me IPv4 (Stallings, 2013).

3.2 Funksionimi i IP

IP funksionon në Shtresën e Rrjetit (Layer 3) të modelit OSI dhe është përgjegjës për:

- Adresimin unik të pajisjeve në rrjet.
- Ndërtimin dhe dërgimin e paketave të të dhënave.
- Rutimin e paketave nëpërmjet rrjetit bazuar në adresat IP të dërguesit dhe marrësit.

3.3 Struktura e Paketës IP

Një paketë IP përbëhet nga:

- **Koka (Header)** – Përmban informacione si adresa burimore dhe e destinacionit, Time-to-Live (TTL), dhe protokollin e përdorur (p.sh., TCP ose UDP).
- **Përmbajtja (Payload)** – Të dhënat thelbëore të cilat transmetohen, pa përfshirë informacionin e rrjetit**(Header-in).**

3.4 Adresimi dhe Subnetimi

- **Adresimi IP** – Çdo pajisje në rrjet ka një adresë unike që i caktohet nga një administrator rrjeti ose nga një shërbim automatik si DHCP.

- **Subnetimi** – Lejon ndarjen e një rrjeti të madh në nën-rrjete më të vogla për menaxhim dhe siguri më të mirë (Tanenbaum & Wetherall, 2011).

Përfundim

Protokolli i Internetit luan një rol themelor në funksionimin e rrjeteve moderne, pasi mundëson komunikimin dhe shkëmbimin e të dhënave midis pajisjeve në mbarë botën. Me zhvillimin e teknologjisë dhe rritjen e nevojës për më shumë adresa, pritet që IPv6 të marrë gradualisht vendin e IPv4, duke ofruar më shumë hapësirë adresimi, siguri më të mirë dhe menaxhim më efikas të trafikut në rrjet.

4. Lidhja e Internetit

Lidhja e internetit është procesi përmes të cilit pajisjet kompjuterike dhe sistemet e rrjeteve lidhen me internetin për të shkëmbyer të dhëna dhe për të komunikuar globalisht. Në varësi të teknologjisë së përdorur, lidhjet e internetit mund të ndryshojnë në shpejtësi, stabilitet dhe aksesibilitet. Të gjitha këto lidhje bazohen në Protokollin e Internetit(IP), i cili siguron drejtim të saktë drejt destinacionit.

4.1 Llojet e Lidhjeve të Internetit

Lidhja me Tel (Wired Connection)

- **DSL (Digital Subscriber Line)** – Teknologji që përdor linjat telefonike ekzistuese për të ofruar internet me shpejtësi të lartë.
- **Kabel Broadband** – Ofron lidhje interneti përmes kabllove koaksiale, zakonisht përdoret nga ofruesit e shërbimeve televizive.
- **Fibra Optike** – Ofron shpejtësi shumë të larta dhe stabilitet të madh në transmetimin e të dhënave (Stallings, 2013).
- **Ethernet** – Lidhje me tela që përdoret kryesisht në rrjetet lokale (LAN) për një performancë të qëndrueshme, duke shfrytëzuar kabllot UTP/STP **(Twisted Pair)**.

Lidhja pa Tela (Wireless Connection)

- **Wi-Fi** – Teknologji për lidhje pa tela në rrjete lokale, e përdorur gjerësisht në shtëpi dhe biznese.
- **LTE/5G** – Teknologjitë celulare që mundësojnë lidhje të internetit për pajisjet mobile.
- **Satelitor** – Përdoret kryesisht në zona të largëta ku opsionet e tjera nuk janë të disponueshme, por mund të ketë vonesa të larta për shkak të distancës së transmetimit.

4.2 Pajisjet Kryesore për Lidhjen e Internetit

- **Modemi** – Pajisja që lidh përdoruesin me ISP (Internet Service Provider) përmes DSL, kabllos ose fibrës optike.
- **Routeri** – Përdoret për të shpërndarë lidhjen e internetit në pajisje të shumta në rrjet.
- **Access Point (AP)** – Pajisje që zgjeron mbulimin e sinjalit Wi-Fi në një rrjet.

4.3 Protokollet dhe Standardet për Lidhjen e Internetit

- **DHCP (Dynamic Host Configuration Protocol)** – Automatizon caktimin e adresave IP për pajisjet në rrjet.
- **PPPoE (Point-to-Point Protocol over Ethernet)** – Përdoret për të vendosur sesione të internetit mbi rrjetet Ethernet.
- **IPv4 dhe IPv6** – Përdoren për adresimin e pajisjeve në internet

- **TCP (Transmission Control Protocol)** – Punon së bashku me IP-në (TCP/IP) për të siguruar dorëzimin e besueshëm të paketa-të dhënave midis pajisjeve.

4.4 Faktorët që Ndikojnë në Cilësinë e Lidhjes së Internetit

- **Gjerësia e Bandës (Bandwidth)** – Sa më e lartë të jetë, aq më shumë të dhëna mund të transmetohen në një kohë të caktuar.
- **Latencia (Latency)** – Koha që i nevojitet një pakete të dhënash për të arritur destinacionin, matet në milisekonda (ms).
- **Ping dhe Jitter** – Matin stabilitetin dhe shpejtësinë e përgjigjes në komunikimin e rrjetit.

- **Interferenca Elektromagnetike** – Mund të ndikojë në performancën e rrjeteve pa tela.

Përfundim

Lidhja e internetit është një pjesë thelbësore e jetës moderne, pasi mundëson komunikimin, qasjen në informacion dhe përdorimin e shërbimeve të ndryshme dixhitale. Me përparimin e teknologjisë, interneti po bëhet gjithnjë e më i shpejtë, më i qëndrueshëm dhe më i sigurt. Këto zhvillime janë thelbësore për përparimin e inteligjencës artificiale, teknologjisë IoT (Internet of Things) dhe për ndërtimin e së ardhmes së realitetit virtual.

5. Llojet e Komunikimit Ndërmjet Shfrytëzuesve

Komunikimi ndërmjet shfrytëzuesve është një aspekt thelbësor i rrjeteve kompjuterike dhe internetit, duke mundësuar shkëmbimin e informacionit nëpërmjet teknologjive të ndryshme. Ky komunikim mund të jetë sinkron ose asinkron, i bazuar në tekst, audio ose video, dhe mund të realizohet përmes platformave të ndryshme.

5.1 Klasifikimi i Komunikimit Ndërmjet Shfrytëzuesve

Komunikimi Sinkron (Synchronous Communication)

Ky lloj komunikimi ndodh në kohë reale, ku të dyja palët janë të pranishme njëkohësisht.

- **Bisedat me tekst (Instant Messaging - IM)** – Platforma si WhatsApp, Telegram dhe Microsoft Teams mundësojnë biseda të drejtpërdrejta.
- **Thirrjet me zë (Voice Communication)** – Përdorimi i VoIP (Voice over IP) përmes aplikacioneve si Zoom, Skype dhe Google Meet.
- **Videokonferencat** – Mundësuar nga shërbime si Zoom, WebEx dhe Microsoft Teams, përdoren për takime virtuale.
- **Lojërat Online në Kohë Reale (Real-Time Online Gaming)** – Megjithëse nuk është komunikim në kuptimin tradicional të bisedës, komunikimi i të dhënave(si lëvizje dhe veprimet e lojtarëve) ndërmjet serverit dhe shfrytëzuesve duhet të jetë sinkron (në kohë reale) për të funksionuar loja.

Komunikimi Asinkron (Asynchronous Communication)

Ky lloj komunikimi nuk kërkon që palët të jenë aktive në të njëjtën kohë.

- **E-mail (Posta Elektronike)** – Një nga format më të zakonshme të komunikimit asinkron, përmes protokolleve si SMTP, IMAP dhe POP3.
- **Forumet dhe Bisedat në Grupa** – Platforma si Reddit, Discord dhe Slack përdoren për diskutime të vazhdueshme.
- **Mesazhet me tekst (SMS dhe MMS)** – Përdorimi i rrjeteve celulare për komunikim me vonesë të tolerueshme.
- **Blogjet/Komentet në Rrjete Sociale** (Shembull) – Kur dikush poston një status, foto ose artikull dhe të tjerët komentojnë më vonë, ky është një shembull i shkëlqyer i komunikimit asinkron, pasi nuk kërkon ndërveprim të menjëhershëm.

Komunikimi i Bazuar në Dokumente

- **Bashkëpunimi në dokumente online** – Shërbime si Google Docs dhe Microsoft OneDrive lejojnë përdoruesit të punojnë së bashku në dokumente në kohë reale.
- **Shkëmbimi i skedarëve (File Sharing)** – Përdorimi i cloud computing për ruajtje dhe ndarje të skedarëve përmes platformave si Dropbox dhe Google Drive.
- **Bashkëpunimi në dokumente online** – Shërbime si Google Docs dhe Microsoft OneDrive lejojnë përdoruesit të punojnë së bashku në dokumente në kohë reale. Kjo është thelbësore për prodhueshmërinë në distancë.
- **Ruajtja dhe Shkëmbimi i Skedarëve (File Sharing)** – Përdorimi i cloud computing për ruajtje dhe ndarje të skedarëve përmes platformave si Dropbox dhe Google Drive.

Komunikimi në Rrjetet Sociale

- **Platforma si Facebook, Instagram dhe Twitter** – Lejojnë ndarjen e përmbajtjes multimediale dhe mesazheve të drejtpërdrejta.
- **Blogjet dhe Mikroblogjet** – Përdoruesit mund të ndajnë përmbajtje të detajuar përmes platformave si WordPress dhe Medium.

- **Platformat me Përmbajtje Video dhe Transmetim Live** – Shërbime si YouTube dhe TikTok lejojnë komunikim asinkron përmes komenteve dhe sinkron përmes transmetimit direkt (live streaming) dhe bisedave të lidhura me to.

Komunikimi Peer-to-Peer (P2P)

- **Aplikacionet P2P** – Përdoren për ndarjen direkte të të dhënave midis përdoruesve, si BitTorrent dhe eMule.
- **VoIP P2P** – Platforma si Skype fillimisht përdornin një arkitekturë të decentralizuar për thirrjet zanore.
- **Arkitekturat e Decentralizuara (Blockchain)** – Teknologjitë si Bitcoin dhe Ethereum përdorin një rrjet P2P për të konfirmuar dhe regjistruar transaksionet. Kjo e bën rrjetin të decentralizuar, duke mos u bazuar te asnjë autoritet qendror.

Siguria në Komunikimin Ndërmjet Shfrytëzuesve

- **Kriptimi nga fundi në fund (End-to-End Encryption - E2EE)** – Siguron që vetëm marrësi dhe dërguesi mund të lexojnë mesazhin (e.g., Signal, WhatsApp).
- **Autentifikimi me shumë faktorë (MFA)** – Rrit sigurinë e llogarive të komunikimit.
- **Mbrojtja ndaj sulmeve phishing dhe malware** – Edukimi i përdoruesve për të shmangur mashtrimet dhe skemat e rrezikshme (Stallings, 2013).
- **Privatësia dhe Politikat e Ruajtjes së të Dhënave** – Shfrytëzuesit duhet të kuptojnë se si platformat i ruajnë, i përdorin dhe i ndajnë të dhënat e tyre (p.sh., në përputhje me rregulloret si GDPR), pasi disa platforma mund të ruajnë të dhënat e tyre.

Përfundim

Komunikimi ndërmjet përdoruesve ka evoluar ndjeshëm falë përparimeve teknologjike. Zgjedhja e metodës së duhur të komunikimit varet nga nevojat specifike të përdoruesve dhe nga niveli i sigurisë që kërkohet, duke garantuar një shkëmbim të informacionit efikas dhe të sigurt në epokën dixhitale.

6. Llojet e Mashtrimeve në Internet

Mashtrimet në internet janë një kërcënim i madh për përdoruesit individualë dhe organizatat, duke rezultuar në humbje financiare dhe shkelje të privatësisë. Me avancimin e teknologjisë, mashtruesit zhvillojnë metoda gjithnjë e më të sofistikuara për të manipuluar dhe mashtruar viktimat e tyre (Stallings, 2013). Këto mashtrime mund të klasifikohen gjerësisht në sulme inxhinierike sociale, sulme teknike dhe mashtrime financiare.

6.1 Phishing (Mashtrimi me Email dhe Website të Rreme)

- **Përshkrimi:** Mashtruesit dërgojnë email-e të rreme që duken si mesazhe nga institucione të ligjshme (banka, kompani të teknologjisë, etj.).
- **Qëllimi:** Për të vjedhur të dhëna personale si kredencialet e hyrjes dhe informacionin financiar.
- **Shembuj:** Email-et që kërkojnë verifikimin e llogarisë ose ndryshimin e fjalëkalimit përmes një faqeje të falsifikuar.

6.2 Vishing dhe Smishing

- **Vishing (Voice Phishing):** Përdorimi i telefonatave për të mashtruar viktimat dhe për t'i bërë ato të japin informacion të ndjeshëm. **Shembull:** Mashtruesi paraqitet si një agjent i bankës ose i shërbimit të taksave, duke thënë se llogaria e viktimës është kompromet uar dhe kërkon menjëherë konfirmimin e kredencialeve përmes zërit.
- **Smishing (SMS Phishing):** Mashtrimet që bëhen përmes mesazheve me tekst, zakonisht duke përfshirë një link të rrezikshëm që kërkon informacion personal. **Shembull:** Një mesazh SMS mashtrues njofton viktimën se duhet të klikojë një link për të ndjekur një dërgesë (pako) ose për të shlyer një gjobë të papritur.

6.3 Ransomware dhe Malware

- **Ransomware:** Një lloj programi i dëmshëm që enkripton skedarët e viktimës dhe kërkon një pagesë për t'i rikthyer ato.
- **Spyware dhe Keyloggers:** Softuerë që regjistrojnë aktivitetet e përdoruesit për të vjedhur të dhëna të ndjeshme si fjalëkalimet dhe informacionet bankare.

- **Viruse dhe Kërmij (Viruses & Worms):** Programe që riprodhohen duke u bashkëngjitur në skedarë të tjerë (Viruse) ose që shpërndahen në mënyrë të pavarur në rrjet (Kërmij) me qëllimin për të dëmtuar sistemin.

- **Trojanët (Trojan Horses):** Softuer që maskohet si një program i dobishëm ose i ligjshëm (p.sh., një lojë ose një mjet), por në fakt përmban kod të dëmshëm që lejon mashtruesin të hyjë në sistemin tuaj.

6.4 Mashtrimet me Kartat e Kreditit dhe Identitetin

- **Përdorimi i faqeve të falsifikuara për të mbledhur të dhënat e kartave të kreditit.**
- **Mashtrimet me identitetin:** Përdorimi i të dhënave të vjedhura për të kryer transaksione financiare ose për të hapur llogari të reja.

- **Skimming i Kartave (Card Skimming):** Përdorimi i pajisjeve të fshehura në bankomatë (ATM) ose terminalet e pagesave (POS) për të vjedhur informacionin e shiritit magnetik të kartës kur ajo përdoret fizikisht.

- **Mashtrimet e Llogarive të Reja:** Përdorimi i identitetit të vjedhur për të hapur llogari të reja krediti ose huaje, duke dëmtuar seriozisht historinë financiare të viktimës, gjë që është një pasojë kryesore e vjedhjes së identitetit.

6.5 Pyramidat dhe Skemat Ponzi

- Mashtrime financiare që premtojnë fitime të mëdha për investime të vogla, por funksionojnë duke përdorur fondet e investitorëve të rinj për

të paguar investitorët e mëparshëm. Shembull**:** Mashtrime me kriptovaluta dhe skema të marketingut me shumë nivele të rreme.

6.6 Mashtrimet në Rrjetet Sociale

- **Mashtruesit krijojnë profile të rreme për të mashtruar viktimat ose për të shpërndarë përmbajtje të dëmshme.** Shembull**:** Mashtrimet me dhurata të rreme, mesazhet nga "miq" që kërkojnë ndihmë financiare.
- **Mashtrimet e Investimeve ose Blerjeve të Rreme:** Mashtruesit përdorin reklama të sponsorizuara ose faqe fallso për të promovuar produkte që nuk ekzistojnë (p.sh., rroba me çmime të ulëta) ose skema të shpejta fitimi me kriptovaluta, duke i vjedhur paratë viktimës pa dhënë asnjë shërbim/produkt.

6.7 Mashtrimet me Marketplace dhe Ecommerce

- **Produkte të rreme ose shërbime që nuk ekzistojnë.**

- **Mashtrimi i Blerësit (Produktet dhe Shërbimet e Rreme):** Ky lloj mashtrimi konsiston në ofrimin e produkteve ose shërbimeve që janë të rreme ose që në realitet nuk ekzistojnë. Një formë e zakonshme e tij janë faqet e rreme të tregtisë elektronike (e-commerce), të cilat paraqiten me pamje bindëse dhe premtojnë oferta joshëse e çmime tepër të ulëta. Në shumicën e rasteve, këto faqe nuk dorëzojnë fare produktet e porositura ose dërgojnë mallra me cilësi shumë të dobët, që nuk përputhen me ato të reklamuarat.

- **Mashtrimet me Pagesa dhe Rikthim të Parave:** Mashtruesit kërkojnë që blerësi të paguajë përmes metodave të pasigurta (p.sh., transferta bankare direkte ose karta dhuratash) që nuk ofrojnë mbrojtje për blerësin.

- **Mashtrimi i Shitësit:** Kur një blerës mashtrues paguan me një kartë të vjedhur, ose pretendon se nuk e ka marrë produktin për të detyruar rikthimin e parave (chargeback), duke rezultuar në humbje për shitësin legjitim. **Shembull:** Faqe interneti që premtojnë oferta të pabesueshme, por nuk dorëzojnë produktet.

6.8 Deepfake dhe Manipulimi i Informacionit

- **Përdorimi i inteligjencës artificiale për të krijuar video ose audio të falsifikuara për të mashtruar ose përhapur dezinformata.**

- **Rreziku dhe Qëllimi:** Përveç lajmeve të rreme, deepfake-t gjithnjë e më shumë po përdoren për të kryer **mashtrime financiare** (p.sh., duke imituar zërin e një drejtuesi ekzekutiv për të urdhëruar transferta parash) ose për zhvatje personale. Shembull: Video të manipuluara të figurave publike për të përhapur lajme të rreme.

6.9 Masat e Mbrojtjes nga Mashtrimet në Internet

- **Verifikimi i burimeve dhe faqeve të internetit.**
- **Përdorimi i autentifikimit me shumë faktorë (MFA).**
- **Kuptimi dhe edukimi mbi mashtrimet e mundshme.**
- **Përdorimi i programeve të sigurisë si antivirus dhe firewall.**
- **Menaxhimi i Fjalëkalimeve dhe Azhurnimet (Updates)**

Përfundim

Mashtrimet në internet përbëjnë një kërcënim serioz që kërkon vigjilencë të vazhdueshme dhe masa mbrojtëse efektive. Edukimi i përdoruesve dhe përdorimi i teknologjive të sigurisë janë thelbësore për të reduktuar rreziqet e mashtrimeve kibernetike. Me zhvillimin e shpejtë të kërcënimeve, lufta kundër mashtrimeve kërkon një qasje kolektive, ku përgjegjësia ndahet mes individëve, organizatave dhe ofruesve të teknologjisë.

7. Memoria dhe Memorizimi i të Dhënave

Memoria dhe memorizimi i të dhënave janë koncepte kyçe në shkencën kompjuterike dhe teknologjinë e informacionit. Memoria përfshin të gjitha pajisjet dhe sistemet që përdoren për të ruajtur informacionin në mënyrë të përkohshme ose të përhershme, ndërsa memorizimi i të dhënave i referohet proceseve dhe metodave për të ruajtur, organizuar dhe rikthyer të dhënat kur është e nevojshme. Këto sisteme mund të ndahen në Memorie Primare

(volatile) dhe Memorie Sekondare (non-volatile), secila me rolin e saj specifik në funksionimin e kompjuterit.

7.1 Llojet e memories kompjuterike

Memoria kompjuterike ndahet në disa kategori kryesore bazuar në qëndrueshmërinë dhe funksionin e saj:

Memoria Primare (RAM dhe ROM)

- **Random Access Memory (RAM)** – Një lloj memorie që përdoret për të mbajtur të dhënat dhe programet që ekzekutohen në momentin e tanishëm. Është e shpejtë, por e paqëndrueshme, që do të thotë se të dhënat humbasin kur sistemi fiket (Stallings, 2015).
- **Read-Only Memory (ROM)** – Një memorie e qëndrueshme që ruan të dhëna të pandryshueshme, si firmware dhe BIOS.
- **Cache Memory (Memoria Cache):** Një lloj memorieje shumë e shpejtë, por me kapacitet të vogël, që ndodhet në ose afër CPU-së. Ajo ruaj të dhënat dhe instruksionet më të shpeshta të përdorura nga CPU, duke zvogëluar nevojën për të pritur Memoren Kryesore (RAM) dhe duke rritur performancën e sistemit.

Memoria Sekondare (Hard Disk, SSD, USB, etj.)

- **HDD (Hard Disk Drive)** – Përdor disqe magnetike për të ruajtur të dhënat në mënyrë të përhershme.
- **SSD (Solid State Drive)** – Një alternativë më e shpejtë ndaj HDD-së, që përdor memorien flash për ruajtje të dhënash (Patterson & Hennessy, 2017).
- **USB Flash Drive dhe Karta e Memories** – Pajisje të lëvizshme për ruajtjen dhe transferimin e të dhënave.
- **Ruajtja në Rrjet (Cloud Storage dhe NAS)** – Sisteme që lejojnë qasjen në të dhëna përmes rrjetit. Kjo përfshin shërbime publike (si Google Drive dhe AWS) ose pajisje personale/organizative (si NAS - Network Attached Storage) për ruajtje qendrore dhe të sigurt.Përmendet edhe te “Memorie e Lartë”

Memoria e Lartë (Cloud Storage, Data Centers)

- **Cloud Storage** – Ofron hapësirë të ruajtjes në serverë të largët, duke mundësuar akses nga kudo përmes internetit (Armbrust et al., 2010).
- **Data Centers** – Infrastruktura që përfshin serverë dhe pajisje të ruajtjes për të mbajtur sasi të mëdha të dhënash.

- **Ruajtja e Rezervimit dhe Ripërtëritja nga Fatkeqësitë (Disaster Recovery):** Përdorimi i shumë qendrave të dhënave (Data Centers) dhe teknologjive të kopjimit (backup) për të siguruar se të dhënat mbeten të qasshme edhe në rast të dështimit të harduerit, fatkeqësive natyrore ose sulmeve kibernetike.

7.2 Metodat e Memorizimit të të Dhënave

Memorizimi i të dhënave mund të ndahet në teknika të ndryshme, bazuar në formatin dhe organizimin e të dhënave:

1. **Memorizimi Hierarkik** – Një strukturë organizimi ku të dhënat ruhen në nivele të ndryshme bazuar në frekuencën e përdorimit dhe shpejtësinë e aksesit.
2. **Baza e të Dhënave Relacionale** – Përdor modele tabelare për të ruajtur dhe menaxhuar të dhënat (Codd, 1970).
3. **Sistemet e Skedarëve** – Organizimi i të dhënave në formë skedarësh dhe dosjeve.
4. **Memorizimi në Cache** – Ruajtja e përkohshme e të dhënave për të përmirësuar performancën e sistemeve kompjuterike (Tanenbaum & Bos, 2015).
5. **Bazat e të Dhënave Jo-Relacionale (NoSQL)** – Një metodë fleksibile e ruajtjes që nuk ndjek modelin tradicional tabelar. Këto baza të dhënash (p.sh., MongoDB ose Cassandra) përdoren për të menaxhuar sasi të mëdha të dhënash të pa-strukturuara ose gjysmë-strukturuara (si postimet në rrjetet sociale ose të dhënat e Big Data).

Përfundim

Memoria dhe memorizimi i të dhënave janë thelbësore për funksionimin e sistemeve kompjuterike. Me avancimin e teknologjisë, teknikat e ruajtjes dhe menaxhimit të dhënave po bëhen gjithnjë e më efikase dhe të sigurta, duke lehtësuar qasjen dhe përdorimin e informacionit. Ky zhvillim është thelbësor

për të mbështetur kërkesat e aplikacioneve moderne, si inteligjenca artificiale dhe Big Data, të cilat varen nga ruajtja dhe përpunimi i shpejtë i sasive të mëdha të dhënave.

8. Rrjeti Kompjuterik

Rrjeti kompjuterik është një grup kompjuterësh dhe pajisjesh të tjera të lidhura me njëri-tjetrin për të shkëmbyer të dhëna dhe resurse. Këto rrjete mund të variojn nga rrjetet lokale të vogla (LAN) deri te rrjetet globale si interneti. Rrjetet kompjuterike përbëjnë bazën e komunikimit modern, duke ndihmuar në transferimin e informacionit në mënyrë efikase dhe të sigurt. Funksionimi i tyre bazohet në protokolle të standardizuara dhe arkitektura të ndryshme si Klient-Server dhe Peer-to-Peer, të cilat përcaktojnë mënyrën se si pajisjet ndërveprojnë.

8.1 Llojet e Rrjeteve Kompjuterike

1. Rrjeti Lokal (LAN - Local Area Network)

LAN është një rrjet që mbulon një zonë të vogël gjeografike, si një ndërtesë apo një zyrë. LAN-et përdorin teknologji të ndryshme si Ethernet dhe Wi-Fi për lidhjen e pajisjeve.

- **Përcaktimi dhe Teknologjitë** – LAN është një rrjet që mbulon një zonë të vogël gjeografike, si një ndërtesë apo një zyrë. LAN-et përdorin teknologji të ndryshme si Ethernet dhe Wi-Fi për lidhjen e pajisjeve.
- **Qëllimi dhe Arkitektura** – Qëllimi kryesor i LAN-it është ndarja e burimeve (si printerët, skedarët dhe serverët lokalë). Arkitektura e tyre zakonisht është e thjeshtë, duke përdorur *switches* për të lidhur pajisjet me një ruter qendror (ose *gateway*).

2. Rrjeti Metropolitan (MAN - Metropolitan Area Network)

Ky lloj rrjeti mbulon një qytet ose një rajon më të gjerë se LAN, duke përdorur lidhje me shpejtësi të lartë për të transmetuar të dhëna midis organizatave ose institucioneve të ndryshme. MAN-et shpesh përdorin fibra optike dhe teknologji të tilla si Ethernet ose WiMAX, duke shërbyer si një urë lidhëse mes rrjeteve më të vogla lokale (LAN).

3. Rrjeti i Gjerë (WAN - Wide Area Network)

WAN përfshin rrjete që lidhin vende të largëta gjeografikisht, si interneti. Lidhjet në WAN shpesh realizohen përmes fibrave optike, satelitëve ose rrjeteve të tjera me shpejtësi të lartë (Forouzan, 2012).

- **Përcaktimi dhe Teknologjitë e Transmetimit** – WAN përfshin rrjete që lidhin vende të largëta gjeografikisht, si interneti. Lidhjet në WAN shpesh realizohen përmes fibrave optike, satelitëve ose rrjeteve të tjera me shpejtësi të lartë.
- **Roli dhe Funksionimi** – Roli kryesor i WAN-it është të mundësojë shkëmbimin e të dhënave dhe komunikimin global, duke lidhur LAN-et dhe MAN-et e ndryshme me njëra-tjetrën. Funksionimi i WAN-it varet nga protokollet e ruterimit (routing protocols) dhe pajisjet e veçanta si ruterët (routers) dhe modulat (modems) për të menaxhuar trafikun në distanca të gjata.

4. Rrjeti Pa Tela (Wireless Network)

Rrjetet pa tela përdorin sinjale elektromagnetike për të lidhur pajisjet pa përdorur kabuj fizikë. Teknologjitë më të zakonshme për rrjete pa tela përfshijnë Wi-Fi, Bluetooth dhe LTE.

Përcaktimi dhe Teknologjitë – Rrjetet pa tela përdorin sinjale elektromagnetike për të lidhur pajisjet pa përdorur kabuj fizikë. Teknologjitë më të zakonshme për rrjetet pa tela përfshijnë Wi-Fi, Bluetooth dhe LTE.

- **Siguria dhe Sfidat** – Siguria është një shqetësim kryesor, pasi sinjalet pa tela mund të përgjohen më lehtë. Për këtë arsye, përdorimi i protokolleve të kriptimit si WPA2/WPA3 është thelbësor. Rrjetet pa tela janë gjithashtu subjekt i ndërhyrjes

elektromagnetike (Interferenca Elektromagnetike), e cila mund të ndikojë në cilësinë e lidhjes.

8.2 Arkitekturat dhe Topologjitë e Rrjeteve

1. Arkitektura Klient-Server

Në këtë model, një pajisje (serveri) ofron shërbime dhe të dhëna për klientët që lidhen me të përmes rrjetit.

- **Përparësia Kryesore:** Ofron një menaxhim dhe siguri qendrore të lehtë, pasi të gjitha të dhënat ruhen në një vend (server).
- **Mangësia Kryesore:** Nëse serveri qendror dështon (Single Point of Failure), i gjithë rrjeti ndalon së funksionuari. Gjithashtu kërkon harduer të shtrenjtë serveri.

2. Arkitektura Peer-to-Peer (P2P)

Në këtë model, të gjitha pajisjet në rrjet mund të komunikojnë drejtpërdrejt me njëra-tjetrën pa nevojën e një serveri qendror.

- **Përparësia Kryesore:** Është më e lirë dhe më e qëndrueshme (fault tolerance), pasi dështimi i një pajisjeje nuk e ndikon rrjetin tjetër.
- **Mangësia Kryesore:** Siguria është e vështirë për t'u menaxhuar në mënyrë qendrore dhe performanca varet nga ngarkesa e çdo pajisjeje individuale.

3. Topologjitë e Rrjetit

- Topologjia Yll (Star) – Të gjitha pajisjet lidhen në një qendër të vetme (p.sh., një switch ose router). Përparësia kryesore është se dështimi i një pajisjeje nuk ndikon në rrjet.
- Topologjia Unazë (Ring) – Pajisjet lidhen në një strukturë rrethore ku të dhënat qarkullojnë në një drejtim. Zakonisht përdor sinjale *token* për të shmangur përplasjet, por është e ndjeshme ndaj dështimit të një pajisjeje.

- Topologjia Rrjetë (Mesh) – Secila pajisje lidhet me të tjerat për të krijuar një rrjet të dendur lidhjesh. Ofron qëndrueshmërinë më të lartë (fault tolerance) sepse ka shumë rrugë, por është shumë e shtrenjtë dhe e vështirë për t'u implementuar.

- Topologjia Autobus (Bus) – Të gjitha pajisjet lidhen me një kabllo të vetme, ose "bus" qendror. Kjo topologji është e thjeshtë për t'u instaluar, por ka një mangësi kritike: nëse kablloja kryesore ndërpritet, i gjithë rrjeti dështon.

Përfundim

Rrjetet kompjuterike janë thelbësore për shkëmbimin e informacionit në botën moderne. Teknologjitë e rrjetit po evoluojnë vazhdimisht për të përmirësuar sigurinë, shpejtësinë dhe efikasitetin e komunikimit. Megjithatë, menaxhimi i tyre kërkon një kuptim të thellë të protokolleve dhe arkitekturave, pasi sfidat e sigurisë dhe kërkesa në rritje për performancë mbeten prioritete kyçe për zhvilluesit dhe administratorët e rrjeteve.

8.3 Serverët

Serverët janë kompjuterë ose sisteme të fuqishme të rrjetit që ofrojnë shërbime, burime dhe të dhëna për pajisjet dhe përdoruesit e tjerë të rrjetit. Ata luajnë një rol kritik në funksionimin e rrjeteve kompjuterike dhe internetit, duke përpunuar kërkesat dhe shpërndarë informacionin në mënyrë efikase. Ekzistojnë lloje të ndryshme serverësh, dhe ate (si Web Server, Mail Server, ose File Server), të cilët janë specializuar për të përmbushur detyra të caktuara, duke shërbyer si shtylla kurrizore për çdo arkitekturë Klient-Server.

8.4 Llojet e Serverëve

1. Serverët e Fajllave (File Servers)

- Përdoren për të ruajtur dhe menaxhuar dokumentet dhe të dhënat e përdoruesve në një rrjet.
- Lejojnë akses të centralizuar dhe ndarje të skedarëve.

- Menaxhimi i të Drejtave të Qasjes (Access Rights): Serverët e fajlave përdorin një sistem të të drejtave të qasjes për të kontrolluar se cilët përdorues mund të shikojnë, modifikojnë ose fshijnë skedarët, duke siguruar kështu integritetin dhe konfidencialitetin e të dhënave.

2. Serverët e Bazave të të Dhënave (Database Servers)

- Menaxhojnë dhe përpunojnë të dhëna për aplikacione dhe përdorues.
- Shërbejnë si pika qendrore për ruajtjen e të dhënave në sisteme si MySQL, PostgreSQL dhe Oracle.
- Optimizimi i Performancës dhe Qëndrueshmëria (Reliability): Këta serverë janë shpesh të optimizuar me memorie RAM të bollshme dhe disqe të shpejta (si SSD në konfigurime RAID) për të siguruar kohë të shpejtë përgjigjeje (latency të ulët) dhe ruajtje të sigurt, duke garantuar integritetin e transaksioneve (ACID properties).

3. Serverët e Uebit (Web Servers)

- Përdoren për të pritur dhe shërbyer faqe interneti përmes protokolleve si HTTP dhe HTTPS.
- Shembuj përfshijnë Apache, Nginx dhe Microsoft IIS.
- Përpunimi i Përmbajtjes: Serverët e Uebit mund të shërbejnë përmbajtje statike (skedarë HTML, imazhe) ose të bashkëpunojnë me serverë aplikacionesh (Application Servers) për të gjeneruar përmbajtje dinamike bazuar në ndërveprimet e përdoruesit (p.sh., kur hyni në një llogari ose kryeni një blerje).

4. Serverët e Postës Elektronike (Mail Servers)

- Menaxhojnë dërgimin dhe pranimin e e-mail-eve përmes protokolleve si SMTP, IMAP dhe POP3.
- Funksionet e Sigurisë dhe Filtrimit: Përveç dërgimit/pranimit, serverët e postës elektronike luajnë një rol kritik në filtrimin e mesazheve të padëshiruara (spam) dhe mbrojtjen nga kërcënimet (malware), duke përdorur mekanizma të sigurisë si shifrimi (encryption) dhe autentifikimi i dërguesit.

5. Serverët e Aplikacioneve (Application Servers)

- Përdoren për të pritur dhe ekzekutuar aplikacione të bazuara në rrjet.
- Ofrojnë shërbime për aplikacione si ERP dhe CRM (Stallings, 2013).
- Roli në Arkitekturën 3-Shtresore (3-Tier Architecture): Serveri i aplikacioneve shërben si shtresa e mesme (Business Logic Tier), duke vepruar si ndërmjetës midis Serverit të Uebit (Web Server) që menaxhon kërkesat e përdoruesit dhe Serverit të Bazës së të Dhënave (Database Server) që menaxhon të dhënat.

6. Serverët Proxy dhe Serverët e Cache-it

- Proxy serverët veprojnë si ndërmjetës midis klientëve dhe burimeve të rrjetit për të rritur sigurinë dhe optimizimin e trafikut.
    - Për Sigurinë! : Proxy serverët shpesh përdoren për të maskuar adresat IP të klientëve, për të zbatuar politika të kontrollit të qasjes dhe për të bllokuar përmbajtjen e dëmshme (malicious content).
- Cache serverët ruajnë kopje të të dhënave të aksesuara shpesh për të përmirësuar performancën dhe zvogëluar latencën.

    - Për Optimizimin: Nëpërmjet ruajtjes së kopjeve (cache) të faqeve ose skedarëve, ata shmangin nevojën për të kërkuar vazhdimisht informacionin nga burimet origjinale, duke i bërë shfletimet e përsëritura më të shpejta.

8.5 Komponentët Kryesorë të një Serveri

- **Procesori (CPU)** – Përdoret për përpunimin e të dhënave.
- **Memoria RAM** – Lehtëson operacionet dhe përmirëson shpejtësinë e aksesit në të dhëna.
- **Hapësira e Ruajtjes (Storage)** – Disket HDD ose SSD për ruajtjen e të dhënave.
- **Sistemi Operativ i Serverit** – Windows Server, Linux (Ubuntu Server, CentOS), etj.
- **Kartat e Rrjetit (NICs)** – Përdoren për lidhjen e serverëve me rrjetet kompjuterike.

8.6 Siguria e Serverëve

- **Firewall dhe IDS/IPS** – Mbrojnë serverët nga sulmet kibernetike.
- **Kriptimi dhe SSL/TLS** – Sigurojnë të dhënat gjatë transmetimit.
- **Autentifikimi me shumë faktorë (MFA)** – Rrit sigurinë e aksesit në serverë.
- **Backup dhe Redundanca** – Parandalojnë humbjen e të dhënave dhe ndërprerjet e shërbimit.
- **Menaxhimi i Vulnerabilitetit:** Përditësimi i rregullt i Sistemit Operativ dhe aplikacioneve (patching) është kritik për të mbyllur pikat e dobëta (vulnerabilities).

Përfundim

Serverët janë themeli i rrjeteve moderne dhe internetit, duke mundësuar shpërndarjen e burimeve dhe shërbimeve në mënyrë të organizuar dhe të sigurt. Teknologjitë e serverëve vazhdojnë të zhvillohen për të ofruar performancë më të lartë dhe siguri më të madhe. Në këtë kontekst, avancimet në "cloud computing" dhe virtualizim kanë transformuar mënyrën e menaxhimit të serverëve dhe mënyrën se si ata i shërbejnë nevojave globale të të dhënave.

9. Software i Dëmshëm (Malware)

Software-i dëmshëm, i njohur ndryshe si malware, përfshin programe të krijuara për të dëmtuar, ndërhyrë, ose fituar akses të paautorizuar në sistemet kompjuterike. Ky lloj software-i mund të përdoret për qëllime të ndryshme keqdashëse, duke përfshirë vjedhjen e të dhënave, shkatërrimin e skedarëve dhe mbikëqyrjen e aktiviteteve të përdoruesve. Motivimi kryesor është përfitimi financiar, i lehtësuar nga anonimiteti dhe shtrirja globale që ofron interneti.

9.1 Llojet Kryesore të Malware-it

1. Viruset

- **Përshkrimi:** Programe të dëmshme që ngjiten në skedarë legjitimë dhe përhapen kur ekzekutohen.
- **Shembuj:** Michelangelo, CIH (Chernobyl virus).

- **Dëmet:** Shkatërrimi i skedarëve, ngadalësimi i sistemit dhe ndërhyrja në funksionimin e kompjuterit.
- **Kërkojnë Host**: Viruset kanë nevojë të bashkëngjiten në një program ose dokument ekzistues (host) dhe nuk mund të përhapen pa ndihmën e përdoruesit (p.sh., hapjen e skedarit të infektuar).

2. Krimbat (Worms)

- **Përshkrimi:** Programe që replikohen vetë dhe përhapen në rrjete pa pasur nevojë për ndërhyrjen e përdoruesit.
- **Shembuj:** Code Red, WannaCry.
- **Dëmet:** Konsumimi i burimeve të sistemit dhe rrjetit, hapja e vrimave të sigurisë.
- **Autonomi e Lartë:** Ndryshe nga Viruset, krimbat nuk kanë nevojë t'i bashkëngjiten një skedari (host) dhe përdorin dobësitë e rrjetit për t'u shpërndarë në mënyrë të pavarur.

3. Trojanët (Trojan Horses)

- **Përshkrimi:** Software që maskohet si program legjitim, por përmban funksione të dëmshme.
- **Shembuj:** Zeus Trojan, Emotet.
- **Dëmet:** Vjedhja e të dhënave të ndjeshme, krijimi i backdoors për akses të paautorizuar.
- **Mungesa e Ri-prodhimit:** Trojanët zakonisht nuk replikohen vetë (si krimbat ose viruset); shpërndarja e tyre varet nga mashtrimi i përdoruesit për të instaluar softuerin.

4. Ransomware

- **Përshkrimi:** Malware që enkripton skedarët e viktimës dhe kërkon pagesë për rikthimin e tyre.
- **Shembuj:** CryptoLocker, REvil.
- **Dëmet:** Humbja e të dhënave, kërkesa për shpërblim financiar, ndërprerja e operacioneve të organizatave.
- **Kërkesa për Kriptovaluta:** Pagesat e shpërblimit pothuajse gjithmonë kërkohen në kriptovaluta (si Bitcoin), sepse ofrojnë anonimitet të lartë për sulmuesit.

5. Spyware dhe Keyloggers

- **Përshkrimi:** Programe që mbikëqyrin aktivitetet e përdoruesit dhe mbledhin informacione pa dijeninë e tij.
- **Shembuj:** FinSpy, DarkComet.
- **Dëmet:** Vjedhja e fjalëkalimeve, informacioneve bankare dhe të dhënave personale.
- **Fokus te Keyloggers:** Një Keylogger është një nën-tip i Spyware që fokusohet në regjistrimin e saktë të të gjitha goditjeve të tastierës (keystrokes) të bëra nga përdoruesi, si fjalëkalimet dhe mesazhet.

6. Adware

- **Përshkrimi:** Software që shfaq reklama të padëshiruara dhe mund të monitorojë aktivitetin e përdoruesit.
- **Shembuj:** Fireball, Gator.
- **Dëmet:** Shfaqja e reklamave të shumta, ngadalësimi i sistemit dhe ekspozimi ndaj malware të tjerë.
- **Modeli i Të Ardhurave:** Shpesh instalohet së bashku me softuer legjitim (p.sh., si 'program i paketuar') dhe i shërben shpërndarësve të tij për të fituar para nga klikimet (Pay-Per-Click) dhe shfaqjet (Impressions) e reklamave.

7. Rootkits

- **Përshkrimi:** Software që fsheh praninë e malware-it dhe lejon akses të fshehtë në sistem.
- **Shembuj:** Stuxnet, Sony BMG Rootkit.
- **Dëmet:** Modifikimi i kernelit të sistemit operativ, fshehja e aktiviteteve keqdashëse.
- **Modeli i Të Ardhurave:** Shpesh instalohet së bashku me softuer legjitim (shembull, si 'program i paketuar') dhe i shërben shpërndarësve të tij për të fituar para nga klikimet (Pay-Per-Click) dhe shfaqjet (Impressions) e reklamave.
- **Vjedhja e Kredencialeve:** Krijimi i dyqaneve të rreme (fake storefronts) për të vjedhur informacionet e kartave të kreditit gjatë procesit të pagesës.

8. Botnets

- **Përshkrimi:** Rrjete kompjuterësh të infektuar që kontrollohen nga një hacker për të kryer sulme kibernetike.
- **Shembuj:** Mirai, Storm Botnet.
- **Dëmet:** Sulme DDoS, spam, vjedhje të informacionit.
- **Zbulueshmëria e Ulët:** Rootkits fshihen në nivelet më të thella të sistemit operativ (si kernel space), duke i bërë ato praktikisht të padallueshme nga softueri standard i antivirusit dhe i zbulimit të kërcënimeve.

9.2 Mënyrat e Infektimit me Malware

- Email-et me phishing dhe attachment të infektuar.
- Shkarkimi i software-it nga burime të pasigurta.
- Vizitimi i faqeve të internetit të infektuara.
- Përdorimi i pajisjeve USB të kompрometuara**.**

9.3 Masat e Sigurisë për të Parandaluar Malware-in

- Përdorimi i antiviruseve dhe software-it të sigurisë.
- Përdorimi i autentifikimit me shumë faktorë (MFA).
- Verifikimi i burimit të skedarëve para shkarkimit dhe hapjes.
- Përditësimi i rregullt i sistemit operativ dhe aplikacioneve.
- Edukimi i përdoruesve për të shmangur mashtrimet në internet**.**

Përfundim

Software-i dëmshëm përbën një kërcënim serioz për sigurinë kibernetike dhe privatësinë e përdoruesve, pasi mund të shkaktojë humbje të dhënash, ndërprerje të shërbimeve dhe ekspozim të informacionit personal. Përballimi i këtyre kërcënimeve kërkon masa të forta mbrojtëse dhe një edukim të vazhdueshëm të përdoruesve për të njohur rreziqet dhe për të vepruar në mënyrë të sigurt në mjedisin dixhital. Aplikimi i zgjidhjeve antivirus, përdorimi i firewall-eve, përditësimi i rregullt i softuerit dhe monitorimi i aktiviteteve të dyshimta janë shtyllat kryesore të mbrojtjes kibernetike, të cilat duhet të kombinohen me politika dhe praktika të sigurta brenda organizatave dhe komuniteteve online. Vetëm me një qasje të integruar dhe vigjilencë të

vazhdueshme mund të minimizohen rreziqet dhe të ruhet siguria e informacionit në një botë gjithnjë e më dixhitale.

BIBLOGRAFIA

Libra dhe botime tjera :

- Forouzan, B. A. (2012). "Data Communications and Networking." McGraw-Hill.
- Kurose, J. F., & Ross, K. W. (2017). "Computer Networking: A Top-Down Approach." Pearson.
- Stallings, W. (2013). "Computer Networking with Internet Protocols and Technology." Pearson.
- Tanenbaum, A. S., & Wetherall, D. (2011). "Computer Networks." Pearson.
- Casey, E. (2011). Digital Evidence and Computer Crime. Academic Press.
- Mitnick, K., & Simon, W. (2005). The Art of Intrusion. Wiley.
- Schneier, B. (2015). Secrets and Lies: Digital Security in a Networked World. Wiley.
- Stallings, W. (2015). Cryptography and Network Security. Pearson.
- Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). "A view of cloud computing." Communications of the ACM, 53(4), 50-58.
- Codd, E. F. (1970). "A relational model of data for large shared data banks." Communications of the ACM, 13(6), 377-387.
- Patterson, D. A., & Hennessy, J. L. (2017). "Computer Organization and Design RISC-V Edition: The Hardware Software Interface." Morgan Kaufmann.

+383 38 200 68 000
infoad@rks-gov.net
Rr. "Murat Mehmeti" nr. 1-3 - Prishtinë