Prof. Asoc. **Fabian Zhilla**
Dr. **Iv Rokaj**
Dr. **Ivas Konini**

STUDIME NË KRIMINOLOGJI

Vëllimi I

STUDIME
NË
KRIMINOLOGJI

Vëllimi I

Autorët:
Prof. Asoc. Dr. Fabian Zhilla
Dr. Iv Rokaj
Dr. Ivas Konini

Drejtuese e Projektit: Alba Jorganxhi

ISBN:

Ky botim u mundësua nga:

OSCE Organizata për Siguri dhe Bashkëpunim në Evropë
Prezenca në Shqipëri

Ky projekt mbështetet financiarisht nga:

Parathënie

Ky botim është mbështetur nga projekti "Për krijimin e programit 'Master në Kriminologji'" (2018-2024), i cili zbatohet nga Prezenca e OSBE-së në Shqipëri, në bashkëpunim të ngushtë me Fakultetin e Drejtësisë dhe Fakultetin e Shkencave Sociale të Universitetit të Tiranës, me mbështetjen financiare të Byrosë së Shteteve të Bashkuara të Amerikës për Çështjet Ndërkombëtare të Narkotikëve dhe Zbatimit të Ligjit.

Prezenca e OSBE-së në Shqipëri falënderon autorin për punën e tij dhe shpreh përkushtimin e saj të vijueshëm për promovimin e hulumtimit shkencor dhe debatit akademik në fushën e kriminologjisë.

PËRMBAJTJA

Prof. Asoc. Fabian Zhilla

JURISPRUDENCA NDËRKOMBËTARE VLEFSHMËRIA E PROVAVE TË KOMUNIKIMEVE TË KODUARA

(EncroChat dhe SKY ECC)

Profesor i Asocuar Fabian Zhilla

Pedagog i të Drejtës, Instituti Kanadez i Teknologjisë (CIT)

Fabian.Zhilla@cit.edu.al

Abstrakt:

Ky artikull bën një radiografi të të gjithë jurisprudencës së gjykatave më të larta të disa vendeve të Bashkimit Evropian (BE) dhe Mbretërisë së Bashkuar duke u përpjekur të sjell në mënyrë të përmbledhur argumentet kryesore të këtyre gjykatave në lidhje me vlefshmërinë e përdorimit të mesazheve të koduara të marra nga EncroChat dhe SKY ECC. Në këtë artikull është përfshirë edhe mendimi i Avokatit të Përgjithshëm të Gjykatës së Drejtësisë së Bashkimit Evropian. Formati i këtij studimi është organizuar në mënyrë të tillë që të ndihmojë të gjithë palët e interesuara në hetimin, gjykimin dhe analizimin të këtyre materialeve hetimore që është një risi në procesin penal. Duhet cilësuar vështirësia e hasur në përkthimin e vendimeve të gjykatave, e cila nuk është kryer nga përkthyes të certifikuar dhe në këtë kontekst, ky aspekt duhet konsideruar si një kufizimi i këtij artikulli. Nga ana tjetër, duke qenë se fenomeni i përdorimit të telefonave dhe aplikacioneve që ofrojnë komunikime të koduara është një çështje e re ligjore, punimet akademike në këtë drejtim janë shumë të limituara, dhe për këtë arsye i gjithë studimi është fokusuar në organizimin dhe sjelljen në formë sistematike të jurisprudencës aktuale të gjykatave të sipër cituara, pa përfshirë në të një qëndrim specifik të autorit.

Fjalët kyçe: Komunikimet e koduara (EncroChat dhe SKY ECC), përdorshmëria e provave, ndihma e ndërsjelltë juridike, e drejta për një proces të rregullt ligjor, e drejta për respektimin e jetës private dhe familjare.

HYRJE

Në dekadën e fundit ka pasur një rritje të përdorimit të pajisjeve telefonike të cilat ofrojnë komunikime të koduara të cilat ju mundësojnë përdoruesve anonimitetin dhe konfidencialitetin e mesazheve të tyre. Ky lloj funksioni specifik i tyre solli një kërkesë në rritje të përdorimit të këtyre pajisjeve nga krimi i organizuar por dhe zyrtarëve me funksione të larta publike. Nga ana tjetër, përdorimi i tyre solli një zhvillim të ri edhe në sofistikimin e kryerjes së veprave penale në kuadër të krimit të organizuar dhe korrupsionit, duke sjellë edhe vështirësi të konsiderueshme në hetimin e tyre. Sidoqoftë, pas një periudhë gati pesë vjeçare të përdorimit të tyre, autoritetet ligjzbatuese franceze dhe holandeze arritën që të aksesojnë dhe bëjnë të mundur dekodimin e mijëra mesazheve të komunikimeve nëpërmjet EncroChat në vitin 2020, duke sjellë edhe arrestimin e një numri të konsiderueshëm të anëtarëve të organizatave kriminale në Bashkimin Evropian (BE)[1] por dhe në Ballkanin Perëndimor[2], ku përfshihen edhe grupet kriminale shqiptare.[3]

Pas dekodimit të këtyre mesazheve, sfida tjetër e agjencive ligjzbatuese ishte përdorimi i tyre si mjete prove në kërkesat për masat e

1 Shih njoftimin zyrtar të Europol datë 02 korrik 2022 këtu: https://www.eurojust.europa.eu/news/dismantling-encrypted-netëork-sends-shockëaves-through-organised-crime-groups-across-europe

2 Shh njoftimin zyrtar të Europol datë 13 maj 2023 këtu: https://www.europol.europa.eu/media-press/neësroom/news/balkans-biggest-drug-lords-arrested-after-investigation-encrypted-phones

3 Shi Ivana Jeremic, Milica Stojanovic and Samir Kajosevic "*Encrypted Phone Crack No Silver Bullet against Balkan Crime Gangs*", BIRN, 25 prill, 2022, këtu: https://balkaninsight.com/2022/04/25/encrypted-phone-crack-no-silver-bullet-against-balkan-crime-gangs/

sigurimit dhe gjykimit në themel të çështjeve gjyqësore. Tashmë çështje të cilat përfshijnë prova të mbështetura në komunikimet e EncroChat dhe Sky ECC janë gjykuar dhe po gjykohen në gjykata të ndryshme të disa vendeve të BE-së dhe jashtë saj në rajon, si Francë, Gjermani, Itali, Mbretëri e Bashkuar, Norvegji, Serbi etj.

Hetime dhe kërkesa për gjykim të cilat janë mbështetur në komunikimet e EncroChat dhe Sky ECC janë kryer edhe nga Prokuroria e Posaçme kundër Krimit të Organizuar dhe Korrupsionit (Prokuroria e Posaçme) ku më i njohuri ndër to është hetimi për të ashtuquajturin "*Operacioni Metmorfoza*" në të cilin u kërkuan masa sigurimi "arrest me burg" për 15 persona, ku ndër të tjera përfshihen si të dyshuar anëtarë dhe drejtues të një prej organizatave kriminale më të fuqishme në rrethin e Shkodrës, biznesmen të njohur, punonjës të policisë së shtetit të nivelit të lartë drejtues, dhe përfaqësues të sistemit të drejtësisë.[4]

Duke u nisur nga përdorimi gjithnjë e më në rritje të këtyre materialeve hetimore nga agjencitë ligjzbatuese në BE dhe Struktura e Posaçme Hetimore kundër Korrupsionit dhe Krimit të Organizuar (SPAK), ky punim synon të sjellë në vëmendje jurisprudencën e deritanishme të gjykatave në shtete të ndryshme të BE por dhe ato të Mbretërisë së Bashkuar për të kuptuar më qartë qasjet e ndryshme të mbajtura nga këto gjykata në lidhje me standardin e provueshmërisë për këto materiale hetimore. Për vetë natyrën deri diku të pazakontë të këtyre materialeve hetimore, ky studim do të ndahet në dy pjesë kryesore. Në pjesën e parë, do të bëhet një përmbledhje e pretendimeve të ngritura nga palët mbrojtëse dhe qëndrimet që kanë mbajtur gjykatat e ndryshme të vendeve të BE dhe ato të Britanisë së Madhe në kundërshtimin apo miratimin e tyre në lidhje me përdorimin dhe vlefshmërinë e komunikimeve EncroChat dhe Sky ECC në gjykimin penal. Pjesa e dytë i referohet zhvillimeve më të fundit në Gjykatën e Drejtësisë së Bashkimit Evropian. Pjesa e tretë do të konkludojë më një përmbledhje të të gjitha argumenteve të jurisprudencës të cituar në

4 Shih njoftimin zyrtar të SPAK, datë 28 korrik 2023, këtu: https://spak.gov.al/njoftim-per-shtyp-date-28-07-2023/

këtë punim, duke i organizuar ato sipas çështjeve kryesore juridike të ngritura nga palët mbrojtëse.

Nga pikëpamja metodologjike, ky studim do të aplikojë një nga metodat cilësore të kërkimit shkencor në fushën e jurisprudencës, siç është ajo që njihet si "metoda analitike" ligjore. Duke qenë se objekti i këtij studimi është të analizojë dhe sintetizojë interpretimet e ndryshme të gjykatave të shteteve të ndryshme dhe atyre të brendshme, kjo lloj metode shkencore ofron mundësinë e ekspozimit të argumenteve ligjore mbi aspekte të paqarta të ligjit siç në rastin konkret është ajo e standardit të provës për komunikimet telefonike të koduara. [5]

I. JURISPRUDENCA NDËRKOMBËTARE

Që në krye të herës duhet cilësuar se ka një qëndrim që sa vjen edhe konsolidohet nga gjykatat më të larta të disa prej vendeve të BE, të cilat janë ballafaquar më gjykimin e pranueshmërisë si mjete prove të materialeve hetimore të cilat rrjedhin nga të dhënat e marra prej bisedave të koduara, kryesisht nga telefonat EncroChat dhe aplikacioni SKY ECC.[6] Argumentet thelbësore të këtyre gjykatave do të trajtohen në seksionin në vijim.

Në ndryshim nga seksioni i parë i këtij punimi, formati i këtij seksioni do të organizohet duke u orientuar në argumentet kryesorë të vendimeve të gjykatave sipas shteteve përkatëse të BE. Kjo strukturë është organizuar e tillë, në mënyrë atipike për një punim akademik, me qëllim që ti vij në ndihmë jo vetëm studiuesve të kësaj fushe por dhe praktikuesve të ligjit, kryesisht gjyqtarëve, prokurorëve, avokatëve

5 Shih Ishaara, P, Bhat, 'Analytical Legal Research for Expounding the Legal World', Idea and Methods of Legal Research (Delhi, 2020; online edn, Oxford Academic, 23 Jan. 2020), https://doi.org/10.1093/oso/9780199493098.003.0006.

6 Një përmbledhje e disa vendimeve mund të gjendet në një studim të Parlamentit Evropian në dhjetor 2022 që mund të aksesohet këtu: https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/739268/EPRS_ATA(2022)739268_EN.pdf

mbrojtës, oficerëve nga shërbimet e policisë gjyqësore, hetuesve të Byrosë Kombëtare të Hetimit, etj.

FRANCË

Vendimi i mëposhtëm i Gjykatës së Kasacionit në Francë është vendimi kyç prej të cilit rrjedhin më pas të gjitha argumentet e gjykatave në vendet e tjera të BE. Për këtë qëllim, në trajtimin e këtij vendimi do të përfshihen si pretendimet e mbrojtjes por dhe argumentet përkatës të gjykatës.

Dhoma Penale, Gjykata e Kasacionit, çështje nr. 21-85.148, datë 11 tetor 2022

Rasti ka të bëjë me një hetim penal në shtetin francez në kuadër të krimit të organizuar. Gjatë hetimit, autoritetet franceze vendosen një pajisje në disa telefona e EncroChat dhe serverët e kompanisë në të cilën mblidheshin të dhënat (a) të ruajtura në çdo aparat celular apo server në atë kohë dhe (b) dërgoheshin ose merreshin nga çdo aparat celulari më pas. Agjencitë ligjzbatuese zbuluan se të akuzuarit përdornin komunikime të koduara për veprimet e tyre kriminale.[7] Të akuzuarit identifikoheshin gjithashtu me kodet e tyre përkatëse. Nga të dhënat e mbledhura u vërtetua se disa nga të hetuarit ishin përfshirë në trafikun e narkotikëve dhe armëve.[8] Një nga të akuzuarit e apeloi çështjen duke ngritur disa pretendime të cilat janë përmbledhur në vijim[9]:

7 Mundësia e instalimit të një pajisjeje të tillë u mundësua nga autoritetet franceze me ligjin e 14 marsit 2011 me qëllim për të bërë të mundur çmontimin e grupeve kriminale që përdorin teknika i sofistikuar komunikimi. Konkretisht, kjo pajisje, e cila përfshin instalimin e spyëare brenda një sistemi kompjuterik, duhet të bëjë të mundur kapjen, nëse është e nevojshme nëpërmjet monitorimit, jo vetëm të skedarëve të kompjuterit nga një hard disk ose media e lëvizshme (siç është çelësi USB), por edhe të teksteve të shtypura në tastierë ose imazheve që shfaqen në ekran.

8 Lexo vendimin e Gjykatës këtu: https://www.conseil-constitutionnel.fr/les-decisions/decision-n-2022-987-qpc-du-8-avril-2022-decision-de-renvoi-cass

9 Ibid,

Pretendimi i parë i mbrojtjes:

Mbrojtja argumentoi se kapja e të dhënave digjitale nga një rrjet i koduar ishte e paligjshme, në shkelje të së drejtës së jetës private dhe familjare si dhe në kundërshtim të nenit 706-102-1 të Kodit të Procedurës Penale,[10] veçanërisht në lidhje me marrjen e të dhënave të ruajtura në kompjuter dhe përgjimin e të dhënave në transit.[11] Mbrojtja

10 Neni 706-102-1 i Kodit të Procedurës Penale Franceze ndodhet në Seksionin 6 të Kapitullit 6 të Titullit 2 të Kodit të Procedurës Penale të Francës. Ky neni rregullon çështjet që lidhen me kapjen dhe regjistrimin e të dhënave kompjuterike në kuadër të hetimit penal. Ky nen rregullon mënyrën se si organet hetimore mund të kryejnë kapjen e të dhënave kompjuterike në kuadër të hetimit penal, duke caktuar kufizimet dhe procedurat që duhet të ndiqen në këtë proces. Me poshtë përafrimi i nenit te përkthyer:
Neni 706-102-1 (Për Kapjen e të Dhënave Kompjuterike):
"Kur është e nevojshme për hetime për veprat penale të përcaktuara në nenet 706-102 dhe 706-102-2, organet e hetimit, nën autoritetin e autoriteteve kompetente gjyqësore, kanë të drejtë të marrin masat e nevojshme për kapjen e të dhënave të ruajtura në një kompjuter ose një sistem të të dhënave elektronike.
Kapja e të dhënave të tjera, të veprimit ose të dërguara me anë të një sistemi të komunikimit elektronik, lejohet vetëm nëse janë të lidhura me të dhëna të ruajtura.
Për qëllimet e këtij neni, të dhëna të ruajtura janë të dhënat që janë ruajtur, të regjistruara, ose të regjistruara dhe ruajtura brenda një sistemi kompjuterik ose elektronik, për të cilin është kryer një kapje teknike për qëllimet e hetimit.
Kapja dhe përdorimi i të dhënave të kapura janë të ndaluar në qoftë se organi hetimor informohet se te dhënat janë krijuar ose përdorur në mënyrë të paditur.
Kjo kapje dhe përdorim nuk mund të përdoren për qëllime tjera se ato të shprehura në urdhrin e autorizuar nga gjyqtari i udhëtimit.
.....
Hyrja në mjetet e tjera të ruajtura të cilat janë të lidhura me sigurinë kombëtare është e ndaluar. Megjithatë, për qëllimet e të dhënave të kapura, dhe përkatësisht të çfarëdo informacioni të duhur, ato mund të përdoren nga struktura përkatëse e Ministrisë së Brendshme në pajtim me dispozitat e Kodit të Mbrojtjes Kombëtare dhe me miratimin e Ministrisë së Brendshme."

11 Këto dispozita u përfshin në me ligjin e 3 qershorit të vitit 2016 për forcimin e luftës kundër krimit të organizuar.

pretendonte se disa veprime teknike të kryera nga agjencitë ligjzbatuese, si bllokimi i operacioneve së të dhënave (block operations) i cili bllokon qarkullimin e të dhënave ndërmjet ofruesve të ndryshëm dhe veprimeve që bëjnë ridrejtimin e të dhënave (data flow redirection), konsiston nga pikëpamja teknike, në ndryshimin e rregullave të rrugëzimit të rrjetit (network routing rules), dhe sipas saj kjo ndërhyrje konsiderohet "përgjim" i të dhënave dhe si rrjedhojë është në tejkalim të nenit të mësipërm.

E drejta për respektimin e jetës private dhe familjare

Argumentimi i Gjykatës:

Gjykata hodhi poshtë argumentin e mbrojtjes, duke deklaruar se ligji nuk bën dallime midis llojeve të ndryshme të të dhënave digjitale nga një rrjet i koduar. Gjykata thekson se veprimet e organit hetimor në kapjen e këtyre të dhënave kishin si qëllim që të parandalonin administratorët e bisedave të koduara për të kryer kodimin e mesazheve të subjekteve nën hetim. Gjykata arsyetoi se veprimet e organit hetimor ishin në kuadër të masave teknike të cilat kishin si qellim mbledhjen e këtyre të dhënave dhe në këtë kontekst, këto veprime ishin tërësisht në përputhje me ligjin.

Sipas gjykatës vendosja e pajisjes për kapjen e të dhënave sipas nenit të mësipërm lejohet vetëm për vepra penale të kryera në kuadër të krimit të organizuar, dhe nëse te dhënat e mbledhura kanë lidhje me vepra penale të tjera ato nuk mund të jenë të përdorshme përballë gjykatës [12]. Në rastet e hetimit të krimit të organizuar, gjyqtari hetues lejon vendosjen e pajisjeve për "kapjen e të dhënave" vetëm pasi merr një mendim nga prokurori i çështjes. Pajisja lejon aksesin në të dhëna, regjistrimin, ruajtjen dhe transferimin e tyre pa nevojën e marrjes së pëlqimit e palëve të interesuara ose nën vëzhgim. Këto pajisje teknike

12 Lexo opinionin ligjor të avokatit Olivier Gutkes "Digital Evidence in Criminal Law", këtu: https://www.ecba.org/extdocserv/conferences/tallinn2012/recdev_france.pdf

mund të instalohen në një kompjuter ose një telefon celular por mund të vendosen edhe në distancë.

Pretendimi i dytë:

Mbrojtja pretendoi se në gjykim nuk ishin shqyrtuar të gjitha provat pasi nuk ishin përfshirë të gjitha dokumentet që duheshin shqyrtuar që në fazën e gjykimit në themel dhe si rrjedhojë, mungesa e tyre kishte cenuar procesin e drejtë ligjor.

Argumentimi i Gjykatës:

Gjykata deklaroi se ky pretendim nuk qëndronte pasi i gjithë dokumentacioni i duhur ishte përfshirë në gjykim. Gjykata gjithashtu nënvizoi se mbrojta ka pasur të gjitha mundësitë dhe të drejtat për të kërkuar përfshirjen dhe vlerësimin e ligjshmërisë së tyre që në fazën e gjykimit në themel.

Pretendimi i tretë (këtu do ndalemi më shumë për shkak të rëndësisë):

Përpara së të parashtrojmë pretendimin e tretë të mbrojtjes duhet të sqarojmë bazën ligjore mbi të cilat mbrojtja ngre pretendimin e saj siç parashikohet në nenin 230 të Kodit të Procedurës Penale Franceze. Në paragrafin e parë të tij (neni 230-1), ligji i jep të drejtë organit procedues që në rastet kur duket se të dhënat e sekuestruara ose të marra gjatë procesit të hetimit janë ndryshuar, duke penguar aksesin ose kuptimin që përmbajnë të dhënat e mbledhura, organi procedues mund të caktojë një ekspert të licencuar për të kryer veprimet e nevojshme teknike për të mundësuar marrjen e një versioni të lexueshëm të tij dhe gjithashtu, kur është përdorur një metodë kodimi, të mundësoj gjithashtu çelësin sekret për dekodimin e tij. Organi procedues, për vepra penale të dënueshme me burgim mbi dy vjet por edhe në rastet kur kompleksiteti i hetimit e justifikon, gjithashtu mund të urdhërojë dhe përdorimin e mjeteve të konsideruar si sekret shtetëror për ta marrë këtë informacion sipas procedurave të parashikuara në nenin 230-2. Në varësi të detyrimeve të sekretit shtetëror, rezultatet shoqërohen me udhëzime teknike që mundësojnë kuptimin dhe përdorimin e tyre, si dhe me lëshimin e një

raporti/certifikate vërtetësie i cili vërteton autencitetin e rezultateve të përgatitura nga eksperti i caktuar prej organit procedues (neni 230-3).[13]

(Argumenti i parë i mbrojtjes):

Mbrojtja argumentoi se përdorimi i mjeteve shtetërore që i nënshtroheshin sekretit shtetëror ishte i parregullt dhe shkelte të drejtat dhe liritë e njeriut, kjo për faktin se nuk kishte asnjë kontroll *apriori* ose *posteriori* që rregullonte këtë vendim diskrecional që ligji i jep organit procedues. Sipas mbrojtjes, këto veprime ishin të pajustifikuara dhe jo proporcionalë ndaj të drejtave dhe lirive kushtetuese.

(Argument i dyte-Informacioni Teknik dhe Certifikata e Vërtetësisë):

Mbrojtja argumentoi se edhe nëse janë përdorur mjete që i nënshtrohen sekretit shtetëror, rezultatet e marra duhet të shoqërohen me tregues teknike të dobishme për kuptimin dhe përdorimin e tyre, si dhe një certifikate të nënshkruar nga eksperti i licencuar që vërteton vërtetësinë e mesazheve të transmetuara. Mungesa e kësaj certifikate përbente shkelje të nenit 230-3 të Kodit të Procedurës Penale Franceze.

Kushtetutshmëria

Arsyetimi i Gjykatës mbi Kushtetutshmërinë:

Gjykata vuri në dukje se testi i kushtetutshmërisë se nenit 706-102-1 të Kodit Francez të Procedurës Penale dhe se Këshilli Kushtetues e kishte gjetur fjalinë e dytë të paragrafit të dytë të nenit 706-102-1 në përputhje me Kushtetutën, ashtu siç dilte edhe në ligjin nr. 2019-222 i datës 23 mars 2019.

Arsyetimi i Gjykatës mbi Informacionin Teknik dhe lëshimin e Certifikatës:

Gjykata u shpreh se ligji i parashikon këto kërkesa, por ato i

13 Shiko Kodin Procedural Penal Francez në anglisht këtu: https://sherloc.unodc.org/cld/uploads/res/document/fra/2006/code_of_criminal_procedure_en_html/France_Code_of_criminal_procedure_EN.pdf

nënshtrohen detyrimeve që rrjedhin në kuadër të ruajtjes së sekretit shtetëror. Gjykata shtoi se sipas procedurës së parashikuar në ligj Qendra për Luftën kundër Krimit Kibernetikë ka të drejtë të kundërshtojë kufizimet që lidhen me mbrojtjen e sekretit shtetëror në ato pika që lidhen me kërkesat për shpjegime të natyrës teknike. Megjithatë, Gjykata vërejti se ky pretendim nuk ishte objekt i gjykimit të saj, duke pranuar se certifikata e vërtetësisë duhej të ishte përfshirë në dosjen hetimore komfor ligjit procedural.

Si përfundim Gjykata e Kasacionit nuk e konsideroi "kapjen e të dhënave" si përgjim, dhe nuk e konsideroi përfshirjen e certifikatës së vërtetësisë si instrument thelbësor procedural i cili cenonte thelbin e vlefshmërisë së të dhënave të marra nga organi procedues.

GJERMANI

Vendimi i Gjykatës së Lartë Federale Gjermane, 2 mars 2022, çështja nr. 5 StR 457/21

Gjykata Rajonale e Hamburgut dënoi një të akuzuar për kryerjen e veprave penale në fushën e narkotikëve më të paktën 5 vite burgim dhe urdhëroi dhe konfiskimin e produkteve të veprës penale me vlerë prej më shumë se 70.000 euro. I akuzuari e apeloi vendimin në Kolegjin e Pestë Penal të Gjykatës Federale në Leipzig në vitin 2021. I dënuari gjatë veprimtarisë kriminale kishte komunikuar duke përdorur EncroChat për të organizuar trafikun e drogës. Këto mesazhe u përdorën në gjykatë si provë thelbësore për provueshmërinë e akuzave. Në apelin e tij, i akuzuari ngrinte pretendimin se mesazhet nëpërmjet EncoChat, të cilat i ishin përcjelle organit të akuzës nga autoritetet franceze nuk mund të pranoheshin prej tyre dhe të përdoreshin si mjete prove.

Me kërkesë të Prokurorit të Përgjithshëm Publik Federal, çështja kaloi për gjykim në Gjykatën e Lartë Federale Gjermane e cila rrezoi pretendimet e mbrojtjes. Gjykata e Lartë u shpreh se të dhënat e ofruesit EncroChat të përcjella nga autoritet franceze mund të përdoren si provë,

nëse i shërbejnë qëllimit të hetimit të veprave penale të rënda. [14]

Gjykata shprehet prerë duke thënë se "*Përjashtimi i provave që pretendohet në ankim të jenë marrë në mënyrë të parregullt dhe në shkelje të ligjit nuk qëndron nga çdo këndvështrim juridik*", duke argumentuar si me poshtë:

Kushtetushmëria

Gjykata shprehet se:

- "*Përdorimi i të dhënave të marra në një mënyrë të ngjashme me këtë rast mund të përfshijë një shkelje të respektimit të jetës private i cili mbrohet nga neni 10 i Ligjit Bazë (Grundgesetz, GG); prandaj, për arsye kushtetuese duhet që me kujdes të merret parasysh parimi i propocionalitetit. Duke iu referuar kufizimeve të përdorimit të provave sipas seksionit 100e (6) nr. 1 StPO, të dhënat e marra në këtë mënyrë mund të përdoren për të dënuar autorët që kanë kryer vepra penale veçanërisht të rënda, për hetimin e të cilëve, gjykata mund të lejojë përdorimin e teknikave hetimore të cilat mund të jenë edhe më ndërhyrëse se zakonisht në jetën private të të dyshuaritt dhe të cilat janë të parashikuara nga legjislacioni procedural penal, siç mund të jenë përkatësisht një kërkim në internet ose një vëzhgim zanor në ambientet private të personit nën hetim. Dhe në çështjen konkrete, kemi të bëjmë me një hetim të një vepre penale të rëndë siç është trafiku i lëndëve narkotike*".

Ndihma e ndërsjelltë juridike

Gjykata shprehet se:

- "*Mbledhja e provave nuk cenon vlerat themelore të të drejtave të njeriut, ato evropiane ose parimet themelore kushtetuese në kuptimin*

14 Shiko vendimin e plotë të Gjykatës këtu: https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/EN/2022/2022038.html

e një "ordre public" (urdhër që mund të cenonte moralin dhe rendin publik-shënimi i autorit) që duhet të marr parasysh në ndihmën e ndërsjelltë juridike. Sipas informacionit që autoritetet franceze kishin marrë nga aksesi i tyre i parë në këto të dhëna, hetimet nuk kishin të bënin me një vëzhgim masiv/të përgjithshëm të kryer pa shkak dhe që përfshinte një numër të madh përdoruesish të telefonave celularë dhe për të cilat nuk ekzistonte asnjë dyshim për ta. Në fakt, për autoritetet franceze EncroChat rezultoi të ishte një platformë që ishte ndërtuar që në krye të herës për të lehtësuar veprimtarinë e grupeve kriminale të cilët vepronin në fshehtësi. Për shkak të konstatimeve fillestare se këta telefona përdoreshin pothuajse ekskluzivisht për qëllime kriminale, një përdorues, vetëm nëpërmjet përdorimit të EncroChat i cili kushton shumë dhe nuk mund të blihet si telefonat e zakonshëm, dyshohej se po kryente vepra penale në kuadër të krimit të organizuar, si trafik të lëndëve narkotike, trafik armësh apo pastrim të produkteve penale".

Testi i përputhshmërisë me legjislacionin e brendshëm

Gjykata shprehet se në rastin konkret:

- "*Nuk do të kryhet një vlerësim i ligjshmërisë sipas legjislacionit të huaj të teknikave të hetimit të përdorura nga autoritetet franceze. Si rezultat, nuk ka shumë rëndësi nëse një mjet hetimor i ndërmarrë në Francë sipas legjislacionit francez mund të ishte lejuar ose jo edhe në Gjermani. Kjo nuk përbën një parakusht për transferimin në procedimin penal gjerman të provave të marra nga autoritetet franceze sipas legjislacionit francez. Kërkesat e ndryshme për urdhërimin e një mase të tillë në Francë dhe Gjermani mund të kompensohen me vlerësimin që mund ti bëhet përdorimit të provave në gjykatë. Për këtë arsye, siç edhe u citua më lartë në paragrafin a), për vepra penale të rënda zbatohen kërkesat veçanërisht të larta për përdorimin e kësaj prove".*

Detyrimi për të njoftuar autoritetet gjermane dhe mbizotërimi i interesit shtetëror

Në këtë pikë Gjykata nënvizon se:

- "*Nuk do të konsiderohet shkak për përjashtimin e marrjes së provave detyrimi që mund të kenë autoritetet franceze për të informuar në kohë autoritetet gjermane në lidhje me veprimet hetimore të vëzhgimit në territorin federal, duke pasur parasysh miratimin e mëvonshëm të përdorimit të të dhënave nga të gjitha palët. Pavarësisht kësaj, është e diskutueshme nëse detyra për të njoftuar palën gjermane do t'i shërbejë individualisht personave të interesuar për të diskutuar ligjshmërinë e përdorshmërisë së provave në gjykatë. Megjithatë, në çdo rast, në një çështje penale, një gjykim i duhur mbi përplasjen e interesave të ndryshme do të duhet të çoj në dhënien përparësi interesit të shtetit. Nuk ngre asnjë shqetësim ligjor fakti që Zyra e Prokurorisë në Frankfurt ka kërkuar një transferim të të gjithë provave në procedimet kundër personave të panjohur (pra jo vetëm për rastin konkret-shënim i autorit) bazuar në një dyshim që ishte i përgjithshëm, por që në fund të fundit do të zbatohej për përdoruesit specifik për secilin rast*".

Shkelje të procedurës në marrëdhëniet juridiksionale me autoritetet e huaja

Gjykata shprehet se pala mbrojtëse:

- "*nuk ka argumentuar ndonjë shkelje të rregullave që lidhen me ndihmën e ndërsjelltë ligjore gjatë procesit të shkëmbimit të të dhënave ose ndryshe gjatë bashkëpunimit midis autoriteteve policore franceze dhe gjermane përpara se të lëshohej Urdhri Evropian i Hetimit. Prandaj është e parëndësishme që, për shkak se pëlqimi është marrë më pas, mbi të gjitha, nuk vërehet ndonjë gabim drastik ligjor i dukshëm, pasi rregulloret evropiane mbi ndihëm e ndërsjelltë juridike e lejojnë transferimin ndërkufitar të gjetjeve për qëllime të ndjekjes penale edhe në mungesë të një kërkese zyrtare në formë shkresore. Në çdo rast, përdorimi i të dhënave që rrjedhin nga kjo formë shkëmbimi të dhënash nuk mund t'i nënshtrohet kërkesave më të rrepta se ato që zbatohen për përdorimin e të dhënave të marra nëpërmjet një Urdhri Evropian*

Hetimi. Një shmangie e synuar apo sistematike nga autoritetet franceze ose gjermane e rregulloreve të cilat do ti shërbenin mbrojtjes ligjore të të akuzuarve as nuk është ngritur nga mbrojtja në mënyrë të qartë dhe as nuk është realisht e dukshme."

NORVEGJI

Vendimi i Gjykatës së Lartë Norvegjeze, datë 04 nëntor, 2022, çështja nr. 22-156788STR-HRET[15]

Në këtë çështje tre persona akuzohen për trafik të lëndëve narkotikë në kuadër të grupit të strukturuar kriminal. Prokuroria e ka mbështetur provueshmërinë e faktit penal kryesisht në të dhënat e marra nga autoritetet Franceze, nga bisedat e koduara nëpërmjet të kryera nga të akuzuarit nëpërmjet EncroChat. Pala mbrojtëse ka kërkuar që këto materiale të mos administroheshin duke filluar me këtë pretendim që në shkallën e parë dhe duke e apeluar me të njëjtin pretendim edhe në gjykatën e apelit si dhe në Gjykatën e Lartë. Qoftë, Gjykata e Shkallës së Parë në Oslo por dhe Gjykata e Apelit të Borgarting në vitin 2022 i rrëzuan këto pretendime duke i konsideruar materialet e marrë nga autoritetet franceze të vlefshme.

Pretendimet e palës mbrojtëse për dërgimin e çështjes në Gjykatën e Lartë ishin se Gjykata e Apelit ka supozuar gabimisht se provat ishin të ligjshme dhe të marra në zbatim të legjislacionit penal francez, duke argumentuar se Gjykata e Apelit ka keqinterpretuar vendimin e Gjykatës së Kasacionit në Francë. Mbrojtja gjithashtu pretendonte edhe shkelje të nenit 6 të Konventës Evropiane për të Drejtat e Njeriut (KEDNJ), duke argumentuar se avokatit mbrojtës iu mohua aksesi në të gjithë zinxhirin e lëvizjes së provave materiale.

15 Shih v**endimin e plotë të Gjykatës këtu:** https://www.domstol.no/globalassets/upload/hret/decisions-in-english-translation/hr-2022-2125-u.pdf

Kriteret e pranueshmërisë së provave nga autoritetet e huaja

Gjykata e Lartë i rrëzon pretendimet e palës mbrojtëse duke sqaruar fillimisht se kriteret që duhet të plotësohen që materialet hetimore e përcjella nga autoritetet e huaja të jenë të pranueshme janë:

- " i) *Materialet hetimore duhet të jenë marrë në përputhje me legjislacionin në fuqi në vendin përkatës (Francë), (ii) i pandehuri duhet të ketë akses në të gjitha të dhënat e marra dhe (iii) të dhënat nuk duhet të jenë marrë sipas një procedure e cila bie ndesh me vlerat themelore të shoqërisë norvegjeze. Një ndalim i përdorimit të materialeve të marra nga autoritetet e huaja si provë do të ishte veçanërisht i rëndësishëm kur procedura e mbledhjes se provave kryhet nga shtete në të cilat traditat procedurale penale ndryshojnë nga tonat*."[16]

Legjitimiteti i provave

Pretendimi kryesor i palës mbrojtëse lidhej me legjitimitetin e administrimit të atyre provave, procedura e të cilave sipas legjislacionit procedural të vendit dërgues (Franca), nuk është e qartë ose nuk ka një parashikim të shprehur ligjor për to. Për ti dhënë përgjigje kësaj pyetje, Gjykata e Lartë nënvizoji argumentet e Gjykatës së Apelit që ajo i gjente të drejta dhe në përputhje me legjislacionin penal norvegjez. Kështu Gjykata e Apelit shprehet se:

- "*Nuk përbën rëndësi për këtë çështje, nëse të njëjtat materiale mund të paraqiten si prova në një gjykatë franceze. Pranimi i materialeve si provë në një gjykatë franceze varet nga një sërë faktorësh procedural të ndryshëm nga vetë marrja e tyre. Nuk ka rëndësi vendimtare për këtë çështje, cilido qoftë rezultati në çështjen gjyqësore franceze në lidhje me përjashtimin ose jo të këtyre materiale si prova. Referuar jurisprudencës norvegjeze, edhe vetë Gjykata e Apelit nuk ka shumë hapësirë interpretimi në lidhje me ligjshmërinë e provueshmërinë*

16 Ibid, paragrafi 26 i Vendimit të Gjykatës së Apelit të Borgarting, datë 21 tetor 2022.

së provave, e tillë që të kërkojë pajtueshmëri me procedurën penale franceze në trajtimin e mëvonshëm të provave që tashmë janë marrë prej këtyre autoriteteve. Sipas mendimit të Gjykatës së Apelit, marrja e provave nuk mund të konsiderohet e paligjshme, sepse një rregull shkelet në një fazë të mëvonshme siç është moslëshimi i një certifikate vërtetësie. Në mendimin e Gjykatës së Apelit, termi "kapje/marrje" të dhënash sipas legjislacionit penal francez (që është përdorur për këto biseda-shënimi i autorit) nuk ka të bëjë me (procedurën ku kërkohen-shënimi i autorit) lëshimet e mëvonshme të certifikatave të vërtetësisë ose çdo vërtetim tjetër të nevojshëm sipas ligjit francez."[17]

ITALI

Gjykata e Kasacionit, datë 5 prill 2023, nr. 16347

Në këtë çështje, gjykata e themelit të rajonit të Kalabrisë ka dhënë vendimin e masës së sigurimit personal "arrest me burg" duke u mbështetur në përmbajtjet e komunikimeve të koduara nëpërmjet aplikacionit SKY ECC. Këto të dhëna ishin marrë nga prokurori publik italian prej autoritetit gjyqësore franceze nëpërmjet një Urdhri Evropian Hetimi. Mbrojtja e kundërshtoi vendimin e gjykatës ku ndër të tjera pretendoi se **i)** janë shkelur ligjet që rregullojnë shkëmbimin e dokumentacionit mbi të cilat organi procedues mbështeti kërkesën për ndihmë të ndërsjelltë juridike **ii**) aktet e marra nga autoritetet franceze janë të papërdorshme pasi janë në shkelje të Konventës së Budapestit dhe është shkelur gjithashtu procedura dekodimit të bisedave nga autoritetet franceze, si mungesa e lëshimit të një certifikate vërtetësie për dekodimin e bisedave **iii**) pamundësia e mbrojtjes për tu njohur me procesin e dekodimit të bisedave dhe **iv**) mungesa e dyshimit i arsyeshëm për kryerjen e një krimi, bazuar në fakte dhe të dhëna objektive.

Disa nga argumentet e gjykatës të cilat rrëzojnë kundërshtimin e palës mbrojtëse nënvizojnë se:

17 Ibid, paragrafi 26 i Vendimit të Gjykatës së Apelit.

Legjitimiteti i të dhënave

- "*Të dhënat e marra janë plotësisht të përdorshme..... Në këtë rast, të dhënat nuk janë kërkuar nga një subjekt privat (për shembull, SKY GLOBAL i cili menaxhonte platformën në fjalë përpara shkeljes së saj nga policia e huaj), por nga një autoritet gjyqësor i cili, në kuadër të një procedimi tjetër dhe të pavarur, i kishte marrë këto të dhëna nga serveri ku ishin ruajtur si pjesë e një hetimi tjetër..... Në lidhje me këtë rindërtim, pra, duket krejtësisht e papërshtatshme të flitet për pëlqim, më tepër që duhet të verifikohet nëse, në lidhje me legjislacionin e brendshme, kushdo që ka transmetuar të dhënat mund t'i disponojë në mënyrë legjitime ato. Dhe përgjigja nuk mund të jetë tjetër veçse pozitive, gjithmonë në kufijtë e vlerësimit të përputhshmërisë me parimet themelore të sistemit tonë ligjor, pasi veprimtaria e marrjes së të dhënave është zhvilluar nën drejtimin e një gjyqtar*i (Gjykata e Parisit)"...

Gjykata për këtë argument konkludon se:

- *"Në përfundim, duhet theksuar se ... nuk ka rëndësi për vlerësimin e legjitimitetit të urdhrit të ankimuar nëse këto të dhëna janë mbledhura nga autoritetet gjyqësore franceze ex post ose në kohë reale (d.m.th. si të "të dhëna të ftohta" ose si "rrjedha komunikimi") . Në fakt, kur autoritetet italiane kërkuan marrjen e këtyre të dhënave dhe (aq më tepër) kur ato të dhëna iu transmetuan, flukset e komunikimit sigurisht që nuk ishin më të vazhdueshme. Situata, pra, nuk ishte e ndryshme nga ajo që ndodh kur një rrjedhë komunikimesh, të shkruara ose në imazhe, të ruajtura në kujtesën e një telefoni merret ex poste. Në këto raste, jurisprudenca ka vlerësuar vazhdimisht se dispozitat e neneve 266 e në vazhdim të Kodit të Procedurës Penale nuk mund të aplikohen (pasi këto nene aktivizohen) vetëm kur synohet të veprohet duke iu referuar flukseve të vazhdueshme të komunikimit.."* (paragrafi 3.3. i Vendimit*).*

Marrja e të dhënave në ruajtje statike (të ftohta)

Gjykata shprehet se mbrojta:

- **"***ngatërron çështjen e autenticitetit të të dhënave të deshifruara me atë të garancisë së integritetit të zinxhirit të procedurës së ndjekur. Në këtë pikë është e rëndësishme të ritheksohet atë që tashmë është bërë e qartë në vendime të tjera të kësaj Gjykate në rastet e hetimit paraprak se: procedura e marrjes së të dhënave në ruajtje (të përcaktuara si të ftohta) ose përgjimi i të dhënave telematike në tranzit lejon marrjen, nëse të dhënat elektronike të mesazhit kodohen përmes përdorimit të një algoritmi ose një çelësi enkriptimi dhe shndërrohen në të dhëna të thjeshta kompjuterike, një varg kompjuterik i përbërë nga një kod binar. Në këtë rast - siç është thënë tashmë – ligjshmëria e mesazhit i nënshtrohet veprimtarisë së dekodimit, që presupozon disponueshmërinë e algoritmit që lejon kthimin e kodit binar në një përmbajtje të lexueshme, por çdo mesazh të enkriptuar që lidhet me çelësin e tij të dekriptimit, pasi vetëm çelësi i saktë do të prodhojë një dekodim të saktë ....*

- *tashmë është bërë e njohur, si në lidhje me deshifrimin e mesazheve me sistemin Blackberry (d.m.th. , "pin to pin" dhe jo "end to end"), si në rastin konkret që përdorimi i algoritmit përjashton mundësinë e ndryshimeve ose manipulimit të teksteve të marra, pasi, sipas shkencës kompjuterike, ai lejon riprodhimin besnik të tyre, me përjashtim të lidhjes së elementeve specifike dhe konkrete me të kundërtën. Për më tepër, pikërisht për mesazhet e shkëmbyera nëpërmjet sistemit të koduar "SKY ECC" dhe "EncroChat", është theksuar se dekodimi i bisedave dhe komunikimeve është një aktivitet i ndryshëm nga grumbullimi i tyre , këto të dhëna përbëjnë shpërfaqen e komunikimeve në një bazë materiale digjitale, d.m.th. janë të dhëna kompjuterike që lejojnë kuptueshmërinë e përmbajtjes së fjalëve të shkruara në vargje në një sistem binar*. " (paragrafi 4 i Vendimit).

Ndihma e ndërsjelltë juridike

Siç theksuam më lart, një ndër argumentet thelbësore të mbrojtjes ishte shkelja e procedurave të marrjes se provave në kuadër të Urdhrit Evropian të Hetimit.

Në këtë pikë gjykata argumenton se:

- "*Prokurori publik italian nuk i ka kërkuar autoritetit gjyqësor të një shteti tjetër anëtar të BE-së që të zhvillojë një hetim, por ka vepruar në përputhje me nenin 45 të dekretit të përmendur (Kërkesë për dokumentacion në lidhje me telekomunikacionet), me qëllim të kufizuar për të kërkuar dhënien e dokumentacionit të grumbulluar, i cili është kërkuar nëpërmjet Urdhrit Evropian të Hetimit. Këto të dhëna janë mbledhur me iniciativën e pavarur të autoritetit lëshues për një procedim që kryhej në atë vend.*

- *Në kuadër të një procedimi që lidhet me një Urdhër Evropian Hetimi garantimi i të drejtave themelore të njeriut i takon kryesisht shtetit anëtar lëshues, i cili presupozohet se është respektues i legjislacionit të BE, sidomos të të drejtëve themelore të njeriut.*

- *Në çështjen në shqyrtim, Urdhri Evropian i Hetimit duhet të përmbajë vetëm kërkesën për provën specifike, duke ia lënë në kompetencë shtetit ekzekutues, procedurën e brendshme të marrjes së provës. ... Gjykata e hetimit paraprak vuri në dukje se nga dokumentacioni i përcjellë ishte e mundur verifikimi i mënyrës së marrjes dhe e ruajtjes së të dhënave nga autoriteti gjyqësor francez* (paragrafi 3 i Vendimit)..

- *.... është e rëndësishme të risillet në vëmendje parimi i përgjithshëm i prezumimit të legjitimitetit të provave të marra nga autoriteti gjyqësor i një shteti tjetër anëtar të BE.. përdorimi i dokumenteve të transmetuara, në fakt, nuk kushtëzohet nga një vlerësim i gjyqtarit italian në lidhje me rregullsinë e mënyrës së marrjes së të dhënave të kryera nga autoriteti i huaj, pasi në këtë rast zbatohet prezumimi i legjitimitetit të veprimtarisë së kryer. Dhe ky proces është në kompetencën e gjyqtarit të huaj për të bërë verifikimin e korrektësisë*

së ndjekjes së procedurës dhe zgjidhjen e mundshme të çdo çështjeje në lidhje me parregullsitë e kundërshtuara ne apel në fazën e hetimit paraprak.... Prandaj, duhet ripërsëritur ajo që tashmë është shprehur nga Gjykata e Themelit se barra e provës u takon atyre që kundërshtojnë mungesën e përputhshmërisë së procedurave të autoriteteve gjyqësore të huaja me ato të sistemit të brendshëm, sidomos kur bëhet fjalë, si në rastin konkret, me legjislacioni e një vendi anëtar të BE të mbështesin pretendimin e tyre .."(paragrafi 5 i Vendimit).

MBRETËRIA E BASHKUAR

Vendimi i Gjykatë së Apelit A, B, D & C dhe REGINA datë 05/02/2021[18]

Çështja thelbësore që shtrohej përpara gjykatës ishte nëse komunikimet u përgjuan në momentin kur ato po transmetoheshin ose, siç konstatoi gjyqtari në gjykatën e themelit, u nxorën (përgjuan) nga ruajta (storage) qoftë e pajisjes telefonike të përdoruesit por dhe serverëve. Për qëllimin e këtij punimi do të ndalojmë vetëm në analizën që Gjykata i ka bërë procesit të "përgjimit" dhe "ruajtjes", në paragrafët 63-69 të vendimit të gjykatës.

Procesi i ruajtjes së të dhënave

Sipas gjyqtarit në gjykimin e themelit, kuptimi i "ruajtjes" nënkupton se:

- "*komunikimet janë ekstraktuar drejtpërdrejt nga pajisja e përdoruesit dhe jo gjatë lëvizjes së tyre, përmes ose nga ndonjë pjesë tjetër e sistemit të komunikimit. Ky është një proces i ngjashëm me çdo mënyrë tjetër të shkarkimit të përmbajtjes së të dhënave në një celular. Kjo bëhet në distancë, por bëhet edhe duke i dhënë komandën përkatëse RAM-it e celularit (memorjes), pa qenë e nevojshme të kryhet përgjimi*

18 Shih vendimi e plotë të Gjykatës së Apelit këtu: https://www.bailii.org/ëë/cases/EËCA/Crim/2021/128.pdf

i komunikimit pasi ai ka lënë telefonin. Në rastin e dërguesit, materialet u rikthyen në formë mesazhesh të dekoduara të ruajtura në RAM të pajisjes në një formë në të cilën ekzistonin para se të dërgoheshin nga telefoni në serverat që ndodhesin në Roubaix (të Francës-shënimi i autorit), përmes sistemit të telekomunikacionit."

Me tej Gjykata e Apelit sqaron se:

- "*duke pasur parasysh këtë interpretim për kuptimin e procesit të "ruajtjes", nuk është e nevojshme të përcaktohet kur fillon dhe përfundon procesi i transmetimit. Ne nuk e pranojmë se transmetimi i mesazhit filloi kur përdoruesi shtypi komandën "Dërgo". Ky ishte një veprim që shkaktoi pajisjen të përgatisë mesazhin në formën e tij përfundimtare dhe pastaj të nisë procesin e transmetimit. Një celular është një kompjuter dhe një transmetues. Transmetimi ndodh pasi mesazhi është vendosur nga kompjuteri në formën e tij përfundimtare. Në rastin e tanishëm, kjo përfshin edhe procesin e kodimit. Ky (kodim) ndodh pasi përdoruesi shtyp komandën "Dërgo", e cila ndodh përpara se mesazhi të transmetohet nga pajisja. Pas pranimit nga pajisja e pranuesit, ai dekriptohet në RAM dhe mund të ndodhë që në disa raste të shtohet një emër i përdoruesit në mesazhin që është transmetuar, i cili ruhet në bazën e të dhënave (Realm) në atë pajisje. Ne mendojmë që transmetimi është i plotë kur komunikimi mbërrin në pajisjen e pranuesit, kështu që pajisja mund të fillojë punën për ta dekriptuar dhe bërë mesazhin të lexueshëm. Edhe në këtë sistem të pazakontë, transmetimi ndodh, në lidhje me çdo komunikim, kur një pajisje është në kontakt me pjesën tjetër të sistemit për qëllimin e dërgimit ose marrjes së një komunikimi, dhe kur komunikimi lëviz nëpër pjesë të tjera të sistemit*.[19]

- *Mesazhi është ai që transmetohet. Ajo që mbetet në pajisje nuk është ajo që është transmetuar, por një kopje e saj ose ajo që, në format më të hershme të mesazheve, mund të përshkruhet si "draft". Kjo ndodh menjëherë pas transmetimit kur merret kopja, ose edhe nëse kopja është*

19 Gjyqtari i themelit bën një shpjegim teknik të të gjithë procesit i cili gjendet në paragrafin 14 të vendimit të Gjykatës së Apelit.

ekstraktuar ndërsa transmetimi i mesazhit origjinal të koduar vazhdon ende. Fakti që ajo që u mor është një mesazh i paprekur, do të thotë se ajo që ishte në telefon, dhe ajo që është kapur, nuk janë të njëjta me atë që është transmetuar, sepse ajo që është transmetuar është e koduar. Prandaj (mesazhi i intereferuar nga autoritetet franceze-shënimi i autorit) nuk ishte në procesin e "transmetimit" kur është kapur por ka qenë vetëm në "ruajtje"....

Gjykata konkludon se:

- *"....pyetja e vetme thelbësore ...është nëse materialet e EncroChat ishin të ruajtura në sistemin e telekomunikacionit kur ato u interferuan. ... ne mendojmë se këto mesazhe nuk po transmetoheshin por ishin të ruajtura (gjatë kohës së ndërhyrjes nga autoritetet franceze-shënim i autorit)"*

HOLANDË

Referuar dy profesorëve të ligjit në Universitetin e Utrecht, (Oerlemans dhe D.A.G. van Toor), autoritetet gjyqësore holandeze janë shprehur se gjykatat e brendshme nuk kanë pse gjykojnë legjitimiteti i provave që janë marrë nga organet e huaja të zbatimit të ligjit, përveç se jemi përballë shkeljes së procesit të rregullt ligjor. Si shembull autorët sjellin vendimin e Gjykatës së Roterdamit e cila nënvizon se:

- " *Autoritetet gjyqësore franceze kanë autorizuar përdorimin e mjetit të përgjimit dhe kanë marrë garancitë e nevojshme. Ndërkohë Prokuroria holandeze theksoi vazhdimisht se procedimi penal i ishte drejtuar një kompanie në territorin francez'. (...) Për këtë arsye, dhe duke iu referuar parimit të besimit në këto çështje, Gjykata nuk do të shqyrtojë legjitimitetin e urdhrit të një gjyqtari francez*".[20]

20 .J. Oerlemans and D.A.G. van Toor (2022) "Legal Aspects of the EncroChat Operation: A Human Rights Perspective", *European Journal of Crime, Criminal Law and Criminal Justice*, 30(3-4), 309-328.

II. QASJA SIPAS TË DREJTËS NDËRKOMBËTARE PENALE

Është ende herët të konkludohet se kush do të jetë interpretimi e gjykatave evropiane, Gjykatës së Drejtësisë së Bashkimit Evropian (GJDBE) dhe Gjykatës Evropiane për të Drejtat e Njeriut (GJEDNJ) mbi vlefshmërinë e përdorimit të të dhënave të marra nga platformat e komunikimit të koduar si ato të EncroChat dhe SKY ECC. Një kërkesë e është drejtuar GJDBE nga Gjykata Rajonale e Berlinit datë 19 tetor 2022, (525 KLs) 279 Js 30/22 (8/22) dhe një kërkesë i është drejtuar GJEDNJ nga dy shtetas britanik në dt. 5 tetor 2020 (aplikimi nr.44715/20) dhe 20 shtator 2021(aplikimi nr.47930/21).[21] Më poshtë do të trajtojmë kërkesat e Gjykatës Rajonale të Berlinit dhe parashtrimet e Avokatit të Përgjithshëm të GJDBE për këtë çështje.

Kërkesa drejtuar Gjykatës së Drejtësisë së Bashkimit Evropian (GJDBE)

Menjëherë pas vendimit të dhënë të Gjykatë së Lartë Federale Gjermane në datë 25 mars të vitit 2022 që cituam më sipër, 7 muaj më pas, Gjykata Rajonale e Berlinit do ti drejtohet GJDBE bazuar në parimin e supremacisë së ligjit të BE.[22] Gjykata më e ulët e justifikoi këtë qasje duke arsyetuar se:

"*Ishte fshehtësia e komunikimit (të autoriteteve gjermane-shënim i autorit) me Europolin dhe Eurojust-in që solli që shumë gjykata të larta rajonale gjermane të përfshiheshin në dhënien e masave të sigurimit me "arrest me burg", duke supozuar gabimisht se të dhënat u ishin transmetuar autoriteteve gjermane "spontanisht" dhe pa nxitjen ose pjesëmarrjen gjermane në nxjerrjen e këtyre të dhënave ....Gjykatat nuk ishin në dijeni paraprakisht për përfshirjen e autoriteteve gjermane.... Dokumentet në lidhje me këtë - si procesverbalet e konferencës dhe*

21 Shih të gjithë pretendimet e ngritura në njoftimin e bërë zyrtar në faqen e GJEDNJ këtu: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-214862%22]}

22 Shiko nenin 19 dhe nenin 267 paragrafi 3 të Traktatit të Funksionimit të Bashkimit Evropian.

mesazhet e SIENA-s - u morën vetëm më pas nga avokatët mbrojtës; Prandaj, ato nuk u morën parasysh në vendimin e Gjykatës Federale të Drejtësisë të datës 2 mars 2022 (5 StR 457/21 - juris Rn. 21 ff.) dhe ende nuk merren parasysh nga zyra e prokurorit publik.....”[23]

Gjykata Rajonale e Berlinit (Landgericht Berlin) me vendimin **datë 19 tetor 2022, (525 KLs) 279 Js 30/22 (8/22)** pezulloi gjykimin ndaj një të pandehuri, i cili ishte subjekt i ndjekjes penale për trafik narkotikësh bazuar në të dhënat e EncroChat. Gjykata ngrinte dyshimin nëse marrja e të dhënave nga autoritetet gjermane prej autoriteteve franceze, nëpërmjet një Urdhrit Evropian te Hetimit (UEH/EIO), ishte e ligjshme ose jo dhe nëse këto të dhëna mund të përdoreshin si prova gjatë procedimit penal të rastit konkret. Kështu Gjykata Rajonale e Berlinit i drejtoi 14 pyetje GJDBE ku për qëllim të këtij artikulli, do ti grupojmë ato sipas çështjeve ligjor që kanë nevojë për interpretim.[24] Ndër të tjera Gjykata Rajonale e Berlineit ngre këto pyetje:

- A mund të mbështetet në ligj aktivizimi i nenit 6(1)(b) i Direktivës UEH/EIO e cila njeh të drejtën e lëshimit të një UEH/EIO në rastet kur kemi të bëjmë më të dhëna të transmetuara nëpërmjet komunikimeve telefonike, kur procedura e mbledhjes së këtyre të dhënave mund të jetë në kundërshtim me legjislacionin e shtetit kërkues (Gjermanisë) për një çështje të ngjashme? [25]

- Bazuar në **parimin e efektivitetit** sipas ligjit të BE-së[26] a mund

23 Shih Vendimin e Gjykatës LG Berlin, Beschl. 19.10.2022 – (525 KLs) 279 Js 30/22 (8/22), paragrafi 31, këtu: https://www.burhoff.de/asp_weitere_beschluesse/inhalte/7384.htm

24 Shih analizën e plote të Fairtrails “German courts refer the legality of EncroChat evidence to the CJE”, të përditësuar në 08 nëntor 2022, këtu: https://www.fairtrials.org/articles/legal-analysis/german-courts-refer-the-legality-of-encrochat-evidence-to-the-cjeu/#background-98

25 Shih, Ibid, këtu: https://www.fairtrials.org/articles/legal-analysis/german-courts-refer-the-legality-of-encrochat-evidence-to-the-cjeu/

26 Parimi i efektivitetit, ose mbrojtja gjyqësore efektive, detyron gjykatat e shteteve anëtare të sigurojnë që mjetet juridike kombëtare dhe rregullat procedurale nuk i bëjnë kërkesat e bazuara në ligjin e BE-së të pamundura në praktikë ose tepër të vështira për t’u zbatuar. Ky parim një parim

të kërkohet përjashtimi i provave të marra me anë të një UEH/EIO që është në kundërshtim me ligjin e BE-së?

- Sipas **parimit të ekuivalencës** të legjislacionit të BE-së[27] a mundet përdorimi i provave të konsiderohet i paligjshëm nëse mënyra (masa) me të cilën është marrë kjo provë në shtetin ekzekutues do të ishte e paligjshme për një çështje të njëjtë sipas procedurës penale të brendshme të shtetit lëshues, përkatësisht Gjermanisë?

- A mund të konsiderohet shkelje e legjislacionit të BE-së, veçanërisht **parimit të efektivitetit**, nëse përdorimi i provave të marra në kundërshtim me legjislacionin e BE-së në procedimet penale justifikohet në kontekstin e një balancimi të interesave duke u nisur nga rëndësia e veprës penale, fakt që nuk dihej fillimisht përgjatë mbledhjes së provave?

- Si alternativë, **bazuar në parimin i efektivitetit** të ligjit të BE-së, nëse marrja e provave nuk mund të përjashtohet, a duhet të merren parasysh shkeljet e mësipërme së paku në nivelin e vlerësimit të provave ose të merren në konsideratë në dhënien e dënimit nga gjykata në procesin penal të brendshëm, kjo edhe në rastin e hetimeve për vepra penale të rënda? [28]

---

përdoret shpesh nga GjED për të siguruar autoritetin e ligjit të BE-së mbi ligjin kombëtar. Për më shumë shih M. Elvira Mendez-Pinedo, 2021. "The principle of effectiveness of EU law: a difficult concept in legal scholarship," *Juridical Tribune (Tribuna Juridica*), Bucharest Academy of Economic Studies, Law Departament, vol. 11(1), pages 5-29, March. .

27 Parimi i ekuivalencës kërkon që shtetet anëtare të mos i trajtojnë çështjet sipas ligjit të BE-së në mënyrë më pak të favorshme sesa çështjet e trajtuara sipas legjislacionit të brendshëm. Pra një shtetas i BE duhet të përdori të njëjtat instrumente procedural sikurse ata vendas në legjislacionin e brendshëm. Ky parim u sanksionua në vitin 1976 në cështjen *Rewe-Zentralfinanz eG and Rewe-Zentral AG v Landwirtschaftskammer für das Saarland*, nr. 33/76 që mund të aksesohet këtu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61976CJ0033

28 Shih analizen e plote të Fairtrails "German courts refer the legality of EncroChat evidence to the CJE", të përditësuar në 08 nëntor 2022, këtu: https://www.fairtrials.org/articles/legal-analysis/german-courts-refer-the-legality-of-encrochat-evidence-to-the-cjeu/#background-98

Për përgjimin e komunikimit telefonik pa ndihmën e një Shteti Anëtar (neni 31 i Direktivës së UEH/EIO**)**

- Sipas kuptimit të nenit 31 të Direktivës së UEH/EIO, a mund të konsiderohet "përgjim i komunikimit telefonik", kur në rastin konkret përfshihet infiltrimi i terminaleve (pajisjeve) për mbledhjen e trafikut, vendndodhjes dhe të dhënave të komunikimit të një shërbimi komunikimi të bazuar në internet?

- A duhet që njoftimi i parashikuar në nenin 31(1) të Direktivës së UEH/EIO t'i drejtohet gjithmonë një gjyqtari ose të paktën nëse sipas ligjit të shtetit të njoftuar (Gjermania), masa e parashikuar nga shteti monitorues (Franca) mund të urdhërohej vetëm nga një gjyqtar në një çështje të ngjashme të brendshme?

- Përderisa neni 31 i Direktivës së UEH/EIO i shërben gjithashtu mbrojtjes individuale të përdoruesve të telekomunikacionit në fjalë, a shtrihet kjo mbrojtje edhe në përdorimin e të dhënave për qëllime të ndjekjes penale në shtetin e njoftuar (Gjermani)? Përveç kësaj, nëse po, a është ai qëllim i barabartë me objektivin tjetër të mbrojtjes së sovranitetit të Shtetit Anëtar të njoftuar?

Kur bëhet fjalë për pasojat e një shkelje të mundshme të ligjit të BE, në mënyrë të përmbledhur Gjykata Rajonale e Berlinit , nënvizon se principet themelore të BE-së, si efikasiteti dhe ekuivalenca, të interpretuara më parë nga vendimet e GJDBE, kufizojnë autonominë procedurale të vendeve anëtare, veçanërisht në lidhje me çështjet që kanë të bëjnë me marrjen dhe pranimin e provave.

Në rastin konkret që po shqyrtohet, gjykata ka përcaktuar se shkelja e këtyre parimeve të BE mund të çoj në mos pranimin e këtyre provave. Arsyetimi i gjykatës rajonale për këtë vendim është i fokusuar tek mungesa e transparencës e organeve hetimore në mënyrën dhe procedurën e ndjekur për nxjerrjen e këtyre të dhënave. *Së pari*, mungesa e transparencës nga ana e agjencive ligjzbatuese franceze të cilat nuk kanë treguar formën teknike të ndërhyrjeve në pajisje e cila e ka bërë të pamundur vlerësimin e vërtetësisë së të dhënave. *Së dyti*,

refuzimi i agjencive të BE dhe autoriteteve gjermane të zbatimit të ligjit për ti dhënë akses mbrojtjes në një pjesë të dosjes.[29]

OPINIONI I AVOKATIT TË PËRGJITSHËM TË GJDBE

Një qasje paraprake duket se do të merret nga GJDBE pas Opinionit të Avokatit të Përgjithshëm, znj. Tamara Ćapeta, të lëshuar në datë 26 tetor 2023, argumentet e të cilit do të përmblidhen më poshtë. Duhet cilësuar se parashtrimet e Avokatit të Përgjithshëm nuk janë të detyrueshme për Gjykatën por ato kanë një ndikim shumë të rëndësishëm në orientimin e vendimit të saj. Për më tepër, parashtrimet e Avokatit të Përgjithshëm ndjekin të njëjtat parime të dhënies së një vendimi gjykate si paanshmëria, pavarësia dhe arsyetimi.[30]

Që në krye të herës, Avokati i Përgjithshëm sqaron se nuk ishin UEH/EIO të lëshuara nga autoritetet gjermane ato të cilat nxitën autoritetet franceze për të përgjuar komunikimet e kryera nëpërmjet EncroChat. Këto të dhëna u kapën nga autoritetet franceze në mënyrë të pavarur dhe sfida në lidhje me legjitimtetin e procesit të përgjimit të këtyre të dhënave i takon gjykatave kompetente franceze. Si rrjedhim UEH/EIO e lëshuara nga autoritetet gjermane, nuk kishin si objekt mbledhjen e të dhëna përmes përgjimit telefonik në Francë, por synimi i tyre ishte vetëm që të kryhej transferimi i provave të mbledhura tashmë nëpërmjet përgjimit të kryer nga autoritetet franceze në mënyrë autonome. Dhe ky synim është në përputhje të plotë me nenin neni 1(1) i Direktivës së UEH/EIO. Me pak fjalë "*një UEH/EIO mund të lëshohet ose për mbledhjen e provave të reja ose për transferimin e provave ekzistuese"* dhe në rastin konkret UEH/EIO *"u lëshua për rastin e dytë*"(paragrafët 16-20; shiko gjithashtu paragrafët 56-57 të konkluzionit të ndërmjetëm).

Më pas Avokati i Përgjithshëm cilëson se "*Do të doja ta bëja të qartë*

29 Shih Thomas Wahl, "EncroChat Turns into a Case for the CJEU", *EUCRIM*, Issue 3/2022, p.197-198, këtu: https://eucrim.eu/news/encrochat-turns-into-a-case-for-the-cjeu/

30 Shiko nenin 253 të Traktatit të Funksionimit të Bashkimit Evropian.

që në fillim, dhe do ta shtjelloj këtë më vonë, se në një skenar të tillë, autoriteti lëshues nuk mund të vërë në dyshim ligjshmërinë e masave me të cilat shteti ekzekutues kryen mbledhjen e provave."(paragrafi 22 i Opinionit). Në mbështetje të këtij argumenti, Avokati i Përgjithshëm nënvizon se "*Megjithëse sistemet e së drejtës penale të Shteteve Anëtare ndryshojnë ndjeshëm, kjo nuk do të thotë se një sistem penal i mbron të drejtat themelore të të dyshuarve dhe të akuzuar ndërsa një tjetër i shkel ato. Përkundrazi, bashkëpunimi i ndërsjëlltë gjyqësor në BE-së në çështjet penale mbështetet në supozimin se të gjitha Shtetet Anëtare respektojnë të drejtat themelore. Ndërsa ky supozim mund të rrëzohet para gjykatës kompetente në një rast të caktuar, kjo nuk mund të vërë në pikëpyetje parimin e besimit të ndërsjellë që qëndron në themel të UEH/EIO dhe instrumenteve të tjera të bashkëpunimit në çështjet penale*"(paragrafi 51).

Avokati i Përgjithshëm konkludon duke interpretuar nenet përkatëse të Direktivës së UEH/EIO si më poshtë:

Kushtet dhe autoriteti kompetentet për lëshimin e një UEH/EIO (neni 6 i Direktivës)

- Kur në shtetin ekzekutues një masë është autorizuar nga një gjyqtar, një UEH/EIO për transferimin e provave të tilla nuk kërkon që ajo të lëshohet domosdoshmërisht gjithashtu nga një gjyqtar, edhe nëse sipas ligjit të shtetit lëshues mbledhja e provave do të duhej të urdhërohej fillimisht me vendim gjykate.

- Fakti që përgjimi është kryer në territorin e një shteti tjetër anëtar nuk përbën ndonjë kusht për përcaktimin e institucionit autorizues në shtetin lëshues.

- Ligji i BE-së nuk kërkon që një UEH/EIO për transferimin e provave ekzistuese të mbledhura përmes përgjimit të telekomunikacionit të lëshohet nga një gjykatë, nëse ligji i brendshëm parashikon që një prokuror publik të mund të urdhërojë një transferim të tillë në një çështje të ngjashme vendase (lexo nga një gjykatë vendase në tjetrën

brenda sistemit të brendshëm gjyqësor).

- Vlerësimi i domosdoshmërisë dhe proporcionalitetit të një UEH/EIO që kërkon transferimin e provave ekzistuese është një çështje që i takon autoritetit lëshues që ta kryejë nëpërmjet shqyrtimit nga një gjykatë e brendshme kompetente. Një vlerësim i tillë duhet të marrë parasysh se qasja e autoritetit kombëtar në të dhënat e komunikimit të përgjuar përfaqëson ndërhyrje serioze në jetën private të personave në fjalë. Kjo ndërhyrje duhet të kundër-balancohet nga interesi serioz publik në hetimin dhe ndjekjen penale të krimeve.

- Kur lëshohet një UEH/EIO për transferimin e provave tashmë në posedim të një shteti tjetër, referenca për një çështje të ngjashme të brendshme sipas nenit 6(1)(b) të Direktivës 2014/41/BE të Parlamentit Evropian dhe të Këshillit të 3 prill 2014 në lidhje me UEH/EIO në çështjet penale kërkon që autoriteti lëshues të përcaktojë nëse dhe në cilat kushte ligji i brendshëm procedural penal lejon transferimin e provave të mbledhura përmes përgjimit të komunikimit.

- Kur vendoset nëse mund të lëshohet një UEH/EIO për transferimin e provave ekzistuese, autoriteti lëshues nuk mund të vlerësojë ligjshmërinë e mbledhjes së provave në shtetin ekzekutues, transferimi i të cilave kërkohet nga UEH/EIO përkatëse.

- Fakti që masat u ndërmorën në territorin e shtetit lëshues, ose ishin në interes të atij shteti, nuk ndikon në përgjigjen e mësipërme.

Interpretimi i nenit 31(1) dhe (3) i Direktivës (Njoftimi i shtetit anëtar)

- Një Shtet Anëtar i cili, gjatë hetimit ose procedurës së tij të njëanshme penale, përgjon telekomunikacionet në territorin e një Shteti tjetër Anëtar, duhet të njoftojë atë shtet tjetër për kryerjen e këtij përgjimi.

- Ky njoftim mund t'i dërgohet çdo autoriteti që shteti anëtar i përgjimit e konsideron të përshtatshëm, pasi ai shtet nuk mund të dijë se cili autoritet është kompetent në një çështje të ngjashme të brendshme.

• Neni 31 i Direktivës 2014/41 ka për qëllim të mbrojë si përdoruesit individualë të telekomunikimit në fjalë, si dhe sovranitetin e Shtetit Anëtar të njoftuar.

Përdorimi i provave

• Legjislacioni i BE, në këtë fazë të zhvillimit të tij, nuk rregullon pranueshmërinë e provave të cilat janë marrë nëpërmjet një UEH/ EIO të lëshuar në kundërshtim me kërkesat e Direktivës 2014/41. Pranueshmëria e provave është një çështje e ligjit të brendshëm, i cili, megjithatë, duhet të jetë në përputhje me nenet 47 dhe 48 të Kartës së të Drejtave Themelore të Bashkimit Evropian.

III. KONKLUZION

Më poshtë do të bëjmë një përmbledhje të standardeve të vendosura deri tani nga jurisprudenca e gjykatave të cituara më lart duke i organizuar ato sipas çështjeve ligjore të pretenduara nga palët mbrojtëse:

Ndryshimi midis marrjes/kapjes së të dhënave dhe përgjimit

• Komunikimet janë ekstraktuar drejtpërdrejt nga pajisja e përdoruesit dhe jo gjatë lëvizjes së tyre, përmes ose nga ndonjë pjesë tjetër e sistemit të komunikimit. Ky është një proces i ngjashëm me çdo mënyrë tjetër të shkarkimit të përmbajtjes së të dhënave nga një telefon celular (Angli).

• Mesazhi është ai që transmetohet. Ajo që mbetet në pajisje nuk është ajo që është transmetuar, por një kopje e saj ose ajo që, në format më të hershme të mesazheve, mund të përshkruhet si "draft".(Angli);

• Mesazhet që ndodhen në telefon dhe mesazhet që janë kapur, nuk janë të njëjta me ato që janë transmetuar, sepse mesazhi i transmetuar është i koduar. Prandaj mesazhi i intereferuar nga autoritetet francezenuk ishte në procesin e "transmetimit" kur është kapur por ka qenë vetëm në "ruajtje"....(Angli).

- Të dhënat janë marrë kur nuk ka pasur fluks transmetimi por kur ato kanë qenë statike (Itali).

- Dekodimi i bisedave dhe komunikimeve është një aktivitet i ndryshëm nga grumbullimi i tyre, këto të dhëna përbëjnë shpërfaqen e komunikimeve në një bazë materiale digjitale, d.m.th. janë të dhëna kompjuterike që lejojnë kuptueshmërinë e përmbajtjes së fjalëve të shkruara në vargje në një sistem binar (Itali).

Kriteret e marrjes së të dhënave

1. Provat duhet të jenë marrë në përputhje me legjislacionin në fuqi në vendin lëshues (Norvegji).

2. I pandehuri duhet të ketë akses në të gjitha të dhënat e marra (Norvegji).

3. Të dhënat nuk duhet të jenë marrë sipas një procedure e cila bie ndesh me vlerat themelore të shoqërisë norvegjeze(Norvegji).

Legjitimiteti i marrjes së të dhënave nga autoriteti i huaj

- Marrja e provave nuk mund të konsiderohet e paligjshme, sepse një rregull shkelet në një fazë të mëvonshme siç është moslëshimi i një certifikate vërtetësie(Norvegji).

- Procesi i "kapjes/marrjes" së të dhënave sipas legjislacionit penal francez (nuk ka të bëjë me kërkesën për lëshimin e certifikatës së vërtetësisë) (Norvegji).

- Të dhënat nuk janë kërkuar nga një subjekt privat (për shembull, SKY GLOBAL i cili menaxhonte platformën në fjalë përpara shkeljes së saj nga policia e huaj), por nga një autoritet gjyqësor i cili, në kuadër të një procedimi tjetër dhe të pavarur, i kishte marrë nga serveri ku ishin ruajtur këto të dhënat si pjesë e një hetimi tjetër (Itali).

Testi i përputhshmërisë me legjislacionin e brendshëm

- Nuk ka shumë rëndësi nëse një mjet hetimor i ndërmarrë në Francë sipas legjislacionit francez mund të ishte urdhëruar ose jo edhe në Gjermani. Kjo nuk përbën një parakusht për transferimin e provave

të marra nga autoritetet franceze sipas ligjit francez në procedimin penal gjerman (Avokati i Përgjithshëm i GJDBE; Gjermani).

- Kërkesat e ndryshme për urdhërimin e një mase të tillë në Francë dhe Gjermani mund të kompensohen me vlerësimin që mund ti bëhet shqyrtimit të përdorimit të provave në gjykatë (Gjermani).

- Nuk do të konsiderohet shkak për përjashtimin e marrjes së provave detyrimi që mund të kenë autoritetet franceze për të informuar në kohë autoritetet gjermane në lidhje me veprimet hetimore të vëzhgimit në territorin federal, duke pasur parasysh miratimin e mëvonshëm të përdorimit të të dhënave nga të gjitha palët (Avokati i Përgjithshëm i GJDBE; Gjermani).

- Nuk ngre asnjë shqetësim ligjor fakti që Prokuroria e Përgjithshme në Frankfurt ka kërkuar një transferim të të gjithë provave në procedimet kundër personave të panjohur (pra jo vetëm për rastin konkret-shënim i autorit) bazuar në një dyshim që ishte i përgjithshëm, por që në fund të fundit do të zbatohej për çdo rast konkret për secilin përdorues (Gjermani).

- Pranueshmëria ose jo e materialeve si provë në gjykatën e vendit lëshues si Franca nuk përbën kusht për marrjen e tyre nga vendi pritës (Norvegji);

- Përdorimi i dokumenteve të transmetuara, në fakt, nuk kushtëzohet nga një vlerësim i gjyqtarit te brendshëm në lidhje me rregullsinë e mënyrës së marrjes së të dhënave të kryera nga autoriteti i huaj, pasi në këtë rast zbatohet prezumimi i legjitimitetit të veprimtarisë së kryer(Avokati i Përgjithshëm i GJDBE; Itali, Holandë).

- Garantimi i të drejtave themelore të njeriut i takon kryesisht shtetit anëtar lëshues, i cili presupozohet se është respektues i legjislacionit të BE, sidomos të të drejtëve themelore të njeriut (Avokati i Përgjithshëm i GJDBE; Itali).

- Mbrojtja ka barrën e provës të provojë mungesën e përputhshmërisë së procedurave të autoriteteve gjyqësore të huaja

me ato të sistemit të brendshëm, sidomos kur bëhet fjalë, si në rastin konkret, me legjislacionin një vendi anëtar të BE (Itali).

Ndihma e Ndërsjelltë Juridike

- Mbledhja e provave nuk cenon vlerat themelore të të drejtave të njeriut ose evropiane ose kërkesave themelore kushtetuese në kuptimin e një "*ordre public*" që duhet të marr parasysh në ndihmën e ndërsjelltë juridike (Gjermani).

- Mungesa e një kërkese zyrtare në formë shkresore për transferimin e të dhënave midis agjencive ligjzbatuese sipas Urdhrit Evropian të Hetimit nuk konsiderohet shkelje ligjore (Gjermani).

- Përdorimi i të dhënave që rrjedhin nga kjo formë shkëmbimi të dhënash nuk mund t'i nënshtrohet kërkesave më të rrepta se ato që zbatohen për përdorimin e të dhënave të marra nëpërmjet një Urdhri Evropian Hetimi (Gjermani).

- Kërkesa për të këto të dhëna nga autoritetet vendase nuk është bërë për hetimet që do të zhvillohen në një shtetet tjetër të BE (Avokati i Përgjithshëm i GJDBE; Itali).

E drejta për një proces të rregullt ligjor (Neni 6 i KEDNJ

- Procesi i rregullt ligjor kërkon që mbrojtja të ketë akses në dokumentacionin i cili shpjegon mënyrën e marrjes se mesazheve të koduara (Itali).

E drejta për respektimin e jetës private dhe familjare (neni 8 i KEDNJ)

- Nuk jemi përballë shkeljes se nenit 8 të KEDNJ pasi nuk kemi të bëjmë me përgjim por me kapje të dhënash (Francë).

- Pajisja është vendosur jo për të përgjuar por për të parandaluar lëvizjen e mesazheve të koduara (Francë).

- Vendosja e pajisjeve të tilla lejohet vetëm kur kemi të bëjmë më hetime të veprave penale në kuadër të krimit të organizuar (Francë).

- Në marrjen e të dhënave duhet të merret të merret parasysh parimi i proporcionalitetit i cili duhet të vlerësohet nga gjykatat e brendshme të shtetit lëshues (Avokati i Përgjithshëm i GJDBE, Gjermani).

- Hetimet nga autoritetet franceze nuk kishin të bënin me një vëzhgim masiv/të përgjithshëm të kryer pa shkak dhe që përfshinte një numër të madh përdoruesish të telefonave celularë dhe për të cilat nuk ekzistonte asnjë dyshim për ta (Gjermani).

- Të dhënat e marra në këtë mënyrë mund të përdoren për të dënuar autorët që kanë kryer vepra penale veçanërisht të rënda, për hetimin e të cilëve, gjykata mund të lejojë përdorimin e teknikave hetimore të cilat mund të jenë edhe më ndërhyrëse në jetën private dhe të cilat janë të parashikuara nga legjislacioni procedural penal (Gjermani).

Dr. Iv Rokaj

VËSHTRIM KRAHASUES MBI ASPEKTE KRIMINALOGJIKO-PENALE TË KRIMEVE KIBERNETIKE: CYBER-BULLYING DHE CYBER-STALKING

HYRJE

Zona dixhitale ka ndihmuar në avancimin e teknologjisë me përfitime të shumta në jetën e përditshme, por kjo mënyrë dixhitale e komunikimit i ka bërë edhe "ngacmimet dhe shqetësimet" më të shpeshta dhe të pazbuluara. Në përgjithësi, termi bullizëm barazohet me konceptin e ngacmimit, i cili është një formë e agresionit i paprovokuar që shpesh drejtohet në mënyrë të përsëritur ndaj një individi ose grupi tjetër individësh. Ngacmimi kibernetik është një ngacmim që ndodh nëpërmjet përdorimit të pajisjeve dixhitale, si telefonat celularë, kompjuterët dhe tabletët. Ngacmimi kibernetik mund të dëmtojë reputacionin online të të gjithëve atyre që janë të përfshirë – jo vetëm të personit që ngacmohet, por edhe atyre që bëjnë ngacmimin ose marrin pjesë në të. Nga ana tjetër, sulmi kibernetik është një lloj krimi kibernetik që përdor internetin dhe teknologjinë për të ngacmuar ose përndjekur një person. Mund të konsiderohet një shtrirje e bullizmit kibernetik dhe ndjekjes personale.

Termi bullizëm barazohet me konceptin e ngacmimit, megjithatë ngacmimi tenton të bëhet më "tinëzar" pasi vazhdon me kalimin e kohës dhe mund të barazohet më mirë me dhunën sesa me ngacmimin. Prandaj, Erling Roland shprehet se ngacmimi është "dhunë e gjatë, fizike ose psikologjike, e kryer nga një individ ose një grup i drejtuar kundër një individi që nuk është në gjendje të mbrohet në situatën aktuale"[1].

1 Roland, E. (1989). "Bullying: The Scandinavian Research Tradition." In Bullying in Schools, edited by Delwyn P. Tattum and David A. Lane, 21–32. Stroke-on-Trent, UK: Trentham, faq 11.

STRUKTURA E PUNIMIT

Ky punim do të strukturohet në kapituj dhe nënkapituj si më poshtë. Pas pjesës hyrëse, ku do të jepet një prezantim i përgjithshëm i punimit, pasqyrës së lëndës, metodologjisë së përdorur në punim dhe identifikimit të pyetjeve kryesore të cilat shtrohen për përgjigjie, tema do të zhvillohet më tej me ndarje me kapituj dhe nënkapituj.

Kapitulli i parë do të synojë të identifikojë, përshkruajë bullizmin kibernetik dhe përndjekjen kibernetike si vepër penale dhe gjithashtu si fenomene të reja dixhitale që kërkojnë mjete të reja për identifikimin dhe parandalimin e tyre.

Kapitulli i dytë do të trajtojë pse përndjekja kibernetike dhe bullizmi kibernetik nuk mund të shmangen dhe të luftohen me metoda tradicionale, të cilat me sa duket nuk janë më efikase. Ky kapitull do të trajtojë natyrën dhe ndikimin e saj në mendësinë e viktimës, në mënyrë që ky studim mund të ndihmojë në gjetjen e disa mjeteve më efikase për parandalimin e një sulmi të tillë në internet.

Kapitulli i tretë do të fokusohet kryesisht në aspektet kriminalogjike të këtyre krimeve kibernetike, por duke analizuar motivet dhe qëllimet e autorëve, ndryshimet sociale në jetën e viktimave, amplitudën e përhapjes së këtyre dukurive dhe përfitimet sociale që mund të arrihen nëpërmjet burgimit apo formave të tjera të dënimit penal, etj.

Kapitulli i katërt do të përpiqet të krahasojë dhe analizojë legjislacione të ndryshme në lidhje me bullizmin kibernetik dhe përndjekjen kibernetike, për të krijuar udhëzues më të mirë në luftën kundër këtyre fenomeneve. Legjislacione të ndryshme kanë zhvilluar arsyetime dhe perceptime të ndryshme për këto krime kibernetike dhe për rrjedhojë një studim krahasues i tyre mund të nxisë diskutime të reja për ndryshime të mundshme dhe të nevojshme legjislative në legjislacionin shqiptar, duke pasur parasysh faktin qe aktualisht po punohet për një draft për miratimin e Kodit te Ri Penal të Republikës së Shqipërisë pas më shumë se 18 vitesh që prej miratimit të kodit aktual në vitin 1995.

Në fund do të përfundojmë duke theksuar aspektet kryesore dhe duke identifikuar disa rekomandime legjislative dhe praktike për luftën në të ardhmen ndaj këtyre krimeve kibernetike.

METODOLOGJIA E PERDORUR

Metodologjia e përdorur për këtë punim shkencor mbi cyber-bullying dhe cyber-stalking, përfshin disa nga metodat e mëposhtme:

1. Metoda analitike: Përdorimi i saj për të shqyrtuar më në detaje elementët e bullzmit kibernetik dhe përndjekjes kibernetike duke analizuar më në thellësi aspektet ligjore, kriminalogjike, si dhe fenomenin, nëpërmjet identifikimit të elementëve thelbësorë dhe marrëdhëniet ndërmjet tyre.

2. Metodologjia intervistuese (për aq sa mund të jetë e mundur): Realizimi i intervistave me viktimat e cyber-bullying dhe cyber-stalking për të kuptuar përvojën e tyre, ndikimin e këtyre fenomeneve dhe strategjitë e përdorura për t'i përballuar ato. Gjithashtu në këtë metode përfshihet edhe studimi i rasteve, pra analiza e rasteve konkrete të cyber-bullying dhe cyber-stalking për të identifikuar mënyrat e veprimit, pasojat dhe masat e ndërmarra nga autoritetet ose individët për të mbrojtur viktimat.

3. Metoda kualitative përmbajtësore: Analiza e materialeve të shkruara, si forume online, blogje dhe komente në artikuj që lidhen me cyber-bullying dhe cyber-stalking, për të nxjerrë tema, tendenca dhe opinionet e ndryshme të shoqërisë. Gjithashtu këtu përfshihet edhe analiza e mediave sociale (për aq sa është e mundur): Hulumtimi i komenteve, postimeve dhe sjelljeve në platforma të ndryshme të mediave sociale për të kuptuar shprehjen e cyber-bullying dhe cyber-stalking në këto mjedise dhe për të ndërtuar një perceptim të gjerë të fenomeneve.

4. Metoda kuantitative: Kërkimet kuantitative përdorin shifrat dhe statistika për të shpjeguar dhe provuar hipoteza duke përdorur anketa,

studime ndërkombëtare, dhe analiza të ndryshme statistikore.

5. Metoda komparative: Përfshin krahasimin e disa rasteve apo legjislacioneve për të identifikuar ngjashmësi dhe dallimet, duke kërkuar të gjejë shkaqet dhe pasojat e tyre.

Kombinimi i disa prej këtyre metodologjive do të ofroje një perspektivë të pasur dhe të kompletuar mbi cyber-bullying dhe cyber-stalking.

Disa pyetje shkencore që mund të adresohen për të eksploruar dhe analizuar cyber-bullying dhe cyber-stalking janë:

1. Si përcaktohet cyber-bullying dhe cyber-stalking? Çfarë ndryshimesh ka ky format digjital me formën tradicionale të bullizmit dhe perndjekjes?

2. Cilat janë formët më të zakonshme të cyber-bullying dhe cyber-stalking? Si ndikojnë ato në individët dhe shoqërinë në përgjithësi?

3. Cilat janë karakteristikat e viktimave dhe të autorëve të cyber-bullying dhe cyber-stalking? Çfarë i shtyjnë ata të bëjnë këto veprime?

4. Si ndryshojnë kulturat dhe konteksti social në manifestimin dhe trajtimin e cyber-bullying dhe cyber-stalking?

5. Cilat janë pasojat e cyber-bullying dhe cyber-stalking në shëndetin mendor dhe emocional të viktimave? Si ndikojnë këto fenomene në përgjithësi në marrëdhëniet sociale?

6. Cilat janë strategjitë dhe mjetet e përdorura për të parandaluar, monitoruar dhe trajtuar cyber-bullying dhe cyber-stalking? A janë efikase ato dhe si mund të përmirësohen?

7. Si ndikojnë ligjet dhe politikat e ndryshme në nivel vendi dhe ndërkombëtar, në trajtimin e cyber-bullying dhe cyber-stalking? A janë të përshtatshme për t'u kundërpërgjigjur këtyre fenomeneve?

8. Si është e lidhur çështja e privatësisë me cyber-bullying dhe

cyber-stalking? Çfarë politikash dhe masash mund të ndërmerren për të garantuar mbrojtjen e privatësisë në këtë kontekst?

9. Cilat mund të jenë ndryshimet e mundshme dhe të nevojshme legjislative në legjislacionin shqiptar në lidhje me këto vepra penale dhe fenomene, duke pasur parasysh faktin që aktualisht po punohet për një draft për miratimin e Kodit të Ri Penal në Republikën e Shqipërisë?

KAPITULLI I

Studiuesi skandinav Dan Olweus, një nga studiuesit më në zë në këtë fushë, e përkufizon bullizmin si "sjellje agresive e qëllimshme dhe që përfshin një çekuilibër fuqie, e cila shpesh, përsëritet me kalimin e kohës."[2] Tonja Nansel e përkufizon ngacmimin si sjellje agresive ose "dëmtim" të qëllimshëm nga një person ose një grup personash, i kryer në përgjithësi në mënyrë të përsëritur dhe me kalimin e kohës përfshin një diferencim të fuqisë[3]. Së fundi, Departamenti i Arsimit i Minesotës arsyeton se "përkufizimet e ngacmimit ndryshojnë, por shumica pajtohen se ngacmimi përfshin qëllimin për të dëmtuar, përsëritjen dhe një çekuilibër fuqie midis viktimës dhe agresorit."[4]

Ngacmimi kibernetik është ngacmim që ndodh nepërmjet pajisjeve dixhitale si telefonat celularë, kompjuterët dhe tabletët. Ngacmimi kibernetik mund të ndodhë përmes SMS-ve, tekstit dhe aplikacioneve, ose në internet në media sociale, forume ose lojëra ku njerëzit mund të shikojnë, marrin pjesë ose ndajnë përmbajtje. Ngacmimi kibernetik përfshin dërgimin, postimin ose ndarjen e përmbajtjes negative, të dëmshme, të rreme ose të keqe për dikë tjetër. Mund të përfshijë ndarjen e informacionit personal ose privat për dikë tjetër që shkakton siklet ose poshtërim ndërsa disa ngacmime kibernetike e kalojnë kufirin në sjellje të paligjshme ose kriminale.

Nga ana tjetër, përndjekja kibernetike është një lloj krimi kibernetik që përdor internetin dhe teknologjinë për të ngacmuar ose përndjekur një person. Mund të konsiderohet një shtrirje e bullizmit kibernetik dhe ndjekjes personale. Megjithatë, ajo merr formën e mesazheve me tekst, e-mail, postime në mediat sociale dhe mediume të tjera dhe shpesh

2 Olweus, D., & Limber, S., & Mihalic, S. (1999). "Bullying Prevention Program." In Fight Crime: Invest in Kids. Blueprints for Violence Prevention: Book Nine, edited by Delbert S. Elliott. Boulder, CO: Center for the Study and Prevention of Violence, faq 56.

3 Olweus, D. (1990). "Bullying Among School Children." In Health Hazards in Adolescence, 259–297. Berlin: De Gruyter,faq 234.

4 Minnesota Department of Education. (2014). "Bullying and Cyber-Bullying."

është këmbëngulëse, e qëllimshme dhe metodike.

Përndjekja kibernetike shpesh fillon me ndërveprime në dukje shfaqen si të padëmshme dhe që vazhdojnë të bëhen sistematike në një mënyrë të bezdisshme ose të frikshme. Disa madje e shohin fazën fillestare të ndjekjes kibernetike si argëtuese dhe të padëmshme, por ajo pushon së qeni argëtuese kur ndërveprimet nuk mbarojnë edhe pasi personi ka shprehur pakënaqësinë e tij dhe ka kërkuar që ndërveprimi të ndalet. Përmbajtja që i drejtohet viktimës është shpesh e papërshtatshme dhe shqetësuese. Një sulmues kibernetik mund të terrorizojë një viktimë duke dërguar mesazhe disa herë në ditë dhe nga llogari të ndryshme.

Përndjekja kibernetike nuk përfshin domosdoshmërisht komunikim të drejtpërdrejtë dhe disa viktima mund të mos e kuptojnë se janë viktima të përndjekjes në internet. Viktimat mund të monitorohen me metoda të ndryshme dhe informacioni i mbledhur mund të përdoret më vonë për krime të tilla si vjedhja e identitetit, shantazhi, denigrimi etj.

Disa karakteristika të zakonshme të sjelljes së përndjekjes kibernetike janë gjurmimi i vendndodhjeve, shkelja e privatësisë së të dhënave, monitorimi i aktiviteteve në internet dhe të botës reale, gjurmimi me obsesion i vendndodhjes së viktimave, frikësimi i viktimave, etj. Përndjekja e mediave sociale mund të përfshijë dërgimin e mesazheve kërcënuese private ose falsifikimin e fotografive.

Shpesh, sulmuesit kibernetikë bëjnë akuza të rreme, përhapin thashetheme keqdashëse, krijojnë profile ose bloge të rreme në mediat sociale, ose krijojnë dhe publikojnë imazhe seksuale hakmarrëse, etj.

Shpesh këto sjellje mund të keqkuptohen për shkak se nuk përfshin kontakt fizik dhe përndjekja kibernetike nuk është aq e rëndë sa forma fizike e përndjekjes. Kjo nuk është e vërtetë në të gjitha rastet. Interneti është bërë pjesë integrale e pashmangshme e jetës tonë, qoftë personale apo profesionale dhe bota online vetëm sa ka lehtësuar mënyrën se si zhvillohen komunikimet së bashku me rritjen e aksesit në informacionin personal.

Së dyti, ngacmimi përfshin domosdoshmërisht keqdashje nga

ana e agresorit, dhe se keqdashja është një lloj dhune. Studiuesit janë përpjekur të kategorizojnë lloje të ndryshme të dhunës ngacmuese në mënyra të shumta. Disa janë fokusuar në dallimin midis agresionit të drejtpërdrejtë dhe agresionit indirekt[5]. Agresioni i drejtpërdrejtë përfshin dhunën fizike goditjen, shkelmimin, marrjen e sendeve me forcë dhe dhunën verbale tallje, ngacmim, kërcënim ndersa agresioni indirekt përfshin akte më delikate, manipuluese, të tilla si izolimi, frikësimi ose kontrolli i një personi tjetër. Të tjerë janë fokusuar në dallimin midis formave të hapura dhe të fshehta (relacionale) të ngacmimit[6]. Ngacmimi i hapur mund të përfshijë thirrjen, shtyrjen ose goditjen, ndërsa ai relacional përfshin thashethemet, përhapjen e thashethemeve, sabotimin social, përjashtimin dhe sjellje të tjera shkatërruese për marrëdhëniet ndërpersonale.

Së treti, ngacmimi nuk mjaftohet me një rast sporadik për t'u kualifikuar si bullizëm, pra sjellja duhet të ndodhë, ose të përsëritet[7]. Kjo është një nga veçoritë që e dallon bullizmin nga format e tjera të ngacmimit, megjithatë për shkak se një sjellje lënduese ndodh vetëm një herë, nuk do të thotë se duhet të injorohet ne kuptim social e parandalues, por thjesht do të thotë se nuk është e saktë t'i referohemi atij si bullizëm në kuptimin klasik të tij. Pra arsyeja pse ngacmimi mund të jetë kaq i dëmshëm emocionalisht ose psikologjikisht dhe meriton ndeshkim penal është sepse ai është i përsëritur. Natyra e përsëritur e ngacmimit krijon një dinamikë ku viktima shqetësohet vazhdimisht për atë që ngacmuesi do të bëjë më pas. Në të vërtetë, viktima shpesh ndryshon sjelljet e tij ose të saj të përditshme për të shmangur kontaktin personal me dhunuesin, sepse supozohet se diçka e keqe do të ndodhë

5 Roland, E. (1980). Terror i skolen. Stavanger, Norway: Rogaland Research Institute, faq 45.

6 Po aty

7 Olweus, D., & Limber, S., & Mihalic, S. (1999). "Bullying Prevention Program." In Fight Crime: Invest in Kids. Blueprints for Violence Prevention: Book Nine, edited by Delbert S. Elliott. Boulder, CO: Center for the Study and Prevention of Violence, faq 341.

nëse ata ndërveprojnë[8].

Së katërti, është e natyrshme që në çdo koncept të bullizmit shfaqet demonstrimi ose interpretimi i pushtetit nga autori mbi viktimen. Nëse të dyja palët do të ishin shoqërisht apo fizikisht të barabarta, nuk mund të mendohet se asnjëra ka përparësi mbi palën tjetër. Shumë karakteristika mund t'i japin dhunuesit perceptimin e një pushtet mbi viktimën, duke përfshirë popullaritetin, forcën fizike, kompetencën sociale, zgjuarsinë, besimin, inteligjencën, moshën, seksin, racën, përkatësinë etnike ose statusin socio-ekonomik. Akoma më e rëndësishme në lidhje me këtë punim janë edhe aftësitë teknologjike të cilat në ditët e sotme mund t'i japin një personi pushtet mbi një tjetër. Të rinjtë që janë në gjendje të lundrojnë në internetit ose që dinë të mbulojnë gjurmët e tyre virtuale, janë një hap para atyre që nuk kuptojnë plotësisht ose nuk dinë si t'i konfigurojë siç duhet llogaritë e tyre online ose si të identifikojë autorët e cyber-bullying.

Autorët e këtyre krimeve përdorin një sërë taktikash dhe teknikash për të poshtëruar, ngacmuar, kontrolluar dhe frikësuar viktimat e tyre. Disa shembuj se si mund të ndodh cyber-bullying janë:

- Postimi i komenteve ofenduese, sugjestive ose ofenduese në internet.
- Dërgimi i emaileve ose mesazheve kërcënuese, të turpshme ose fyese për viktimën.
- Anëtarësimi në të njëjtat grupe dhe forume si viktima.
- Publikimi i informacionit konfidencial të viktimës në internet.
- Ndjekja e të gjitha lëvizjeve online të viktimës përmes pajisjeve gjurmuese.
- Përdorimi i teknologjisë për shantazhimin ose kërcënimin e

8 Limber, S., & Nation, M. (1998). "Bullying Among Children and Youth." In Combating Fear and Restoring Safety in Schools, edited by June L. Arnette and Marjorie C. Walsleben. Office of Juvenile Justice and Delinquency Prevention (1998), faq 78.

viktimës.

- Etiketimi i tepërt i viktimës në postime të parëndësishme.
- Angazhimi me të gjitha postimet në internet të bëra nga viktima.
- Krijimi i profileve false në rrjetet sociale për të ndjekur viktimën.
- Postimi ose shpërndarja e fotove reale ose false të viktimës.
- Dërgimi i fotografive eksplicite të viktimës.
- Bërja e postimeve false me qëllim turpërimin e viktimës.
- Dërgimi i mesazheve në mënyrë të përsëritur viktimës.
- Hakimi në llogaritë online të viktimës.
- Përpjekja për të zhvatur foto eksplicite të viktimës.
- Dërgimi i dhuratave apo sendeve të padëshiruara për viktimën.
- Përdorimi i mjeteve të hakerimit për të hyrë në kamerën e laptopit ose të smartfonit të viktimës dhe për t'i regjistruar ato fshehurazi.

Llojet e ndryshme të ndjekjes kibernetike që janë të përhapura janë krijimi i profileve të rreme ose kopjimi i atyre ekzistuese në mediat sociale për t'iu afruar viktimave; monitorimi i kontrolleve në mediat sociale; vëzhgimi i aktiviteteve të një viktime në mediat sociale për të vlerësuar me saktësi modelin e sjelljes së tyre; spiunimi nëpërmjet Google Maps dhe Google Street View; duke përdorur Street View për të spiunuar një viktimë dhe për të gjetur vendndodhjen e saj nga postimet ose fotot në mediat sociale; hakerimi i kamerës nepërmjet internetit; instalimi i stalker-ware për të gjurmuar vendndodhjen, mundësimin e aksesin në historikun e viktimës, bërja e regjistrimeve audio, etj., pa dijeninë e viktimës; gjurmimi i vendndodhjes me gjeo-lokacionit e fotove dixhitale gjë që e bën më të lehtë për autorët qasjen në informacionin duke përdorur aplikacione të veçanta.

Përndjekja kibernetike nuk ndryshon nga ndjekja dhe çon në pasoja që mund të jenë të dëmshme për viktimat si fizikisht ashtu

edhe mendërisht. Viktimat që ngacmohen në internet përjetojnë frikë, zemërim, konfuzion dhe pagjumësi së bashku me çështje të tjera shëndetësore. Përndjekja kibernetike ndikon në mirëqenien e përgjithshme të viktimave. Ata shpesh vuajnë nga ankthi, shqetësimi, depresioni, PTSD[9] dhe idetë vetëvrasëse.

Në përgjithësi, ngacmimi kibernetik përfshin dërgimin ose postimin e teksteve dhe/ose imazheve të dëmshme ose mizore duke përdorur internetin ose pajisje të tjera komunikimi dixhitale, si telefonat celularë. Ngacmimi kibernetik mund të ndodh në faqet e internetit personale ose mund të transmetohet nëpërmjet postës elektronike, faqeve të rrjeteve sociale, tabelave të mesazheve dhe mesazheve të çastit ose telefonave celularë.

Llojet e bulizmit kibernetik[10].

Shumica e ngacmimeve kibernetike bien në një ose më shumë nga kategoritë e mëposhtme:

1. Flaming: Lufton online duke përdorur mesazhe elektronike me gjuhë urretje dhe vulgare.
2. Ngacmimi dhe ndjekja: Dërgimi i vazhdueshëm i mesazheve mizore, të egra dhe/ose kërcënuese.
3. Denigrim: Dërgimi ose postimi i thashethemeve rreth një personi për të dëmtuar reputacionin e tij ose të saj.
4. Imitim: Depërtimi në llogarinë e postës elektronike të dikujt dhe përdorimi i tij për të dërguar të mbrapshtë ose të turpshëm materiale për të tjerët.
5. Mashtrime të ndryshme: Angazhimi i dikujt në mesazhe të çastit, duke e mashtruar atë për të zbuluar ndjeshmërinë informacion, dhe përcjellja e atij informacioni te të tjerët
6. Përjashtim: Përjashtimi i qëllimshëm i dikujt nga një grup në internet.

9 Post Traumatic Stress Disorder- Çrregullime të stresit post-traumatik

10 Willard, 2007.

Ngacmuesit kibernetikë kanë po aq gjasa të jenë femra sa meshkuj dhe kanë më shumë gjasa të jenë adoleshente më të moshuar sesa më të rinj. Në mënyrë të ngjashme me ngacmuesit tradicionalë, ngacmuesit kibernetikë priren të kenë marrëdhënie të dobëta me kujdestarët e tyre. Ata kanë më shumë gjasa se jo ngacmuesit të jenë objektiva të ngacmimit tradicional dhe të përfshihen në sjellje delikuente dhe në përdorimin më të shpeshtë të substancave. Ata gjithashtu kanë më shumë gjasa të jenë përdorues të shpeshtë të përditshëm të internetit.

Një ngacmues kibernetik mund të jetë ose jo një person që viktima njeh. Ngacmuesit kibernetikë shpesh mund të mbeten anonim, duke e bërë të vështirë nëse jo të pamundur të dallosh se kush është dhunuesi. Ata mund të punojnë në grup me miqtë e tyre, duke e bërë edhe më të vështirë përcaktimin se kush po sulmon. Megjithëse nuk ka prova të qarta që të rinjtë që përfshihen në ngacmime tradicionale janë gjithashtu të prirur ndaj ngacmimit kibernetik, duket se disa viktima të ngacmimit fizik përfshihen në bullizëm kibernetik si një formë hakmarrjeje ndaj torturuesve të tyre.

Programi STOP Cyberbullying[11] përshkruan katër lloje kryesore të bullizmit kibernetik:

1. "Engjëlli hakmarrës" nuk e sheh veten si një ngacmues, por më tepër si një vigjilent, pasi ai ose ajo shpesh përfshihet duke u përpjekur të mbrojë një mik që po ngacmohet ose ngacmohet në internet.
2. Ngacmuesit kibernetikë "të uritur për pushtet" duan të ushtrojnë autoritetin e tyre dhe të kontrollojnë të tjerët me frikë, dhe ata shpesh janë viktima të ngacmimeve tradicionale. Disa njerëz e quajnë këtë "Hakmarrja e Nerds" bullizëm kibernetik, sepse këta ngacmues janë shpesh aq fizikisht të vegjël dhe të shënjestruar nga bashkëmoshatarët e tyre për shkak se nuk janë „cool" ose të aftë teknologjikisht.
3. Ngacmimi kibernetik i "Vajzave të këqija" ndodh shpesh në një grup. Autorët zakonisht mërziten dhe kërkojnë argëtim.

11 Wired Kids, Inc.

4. “Ngacmuesit e paqëllimshëm” kibernetikë nuk synojnë të shkaktojnë dëm, ata thjesht përgjigjen pa menduar për pasojat e veprimeve të tyre.

Në lidhje me dallimet midis bullizmit kibernetik dhe bullizmit tradicional themi se ato nuk janë shumë të dukshme për shkak të ngjashmërive në teknika. Edhe pse ngacmimi kibernetik dhe ngacmimi tradicional sjellin dëm dhe trajtim ndaj viktimave, ngacmimi kibernetik lejon që dhunuesi të fshihet pas një ekrani dhe të kryejë bullizmin pa u identifikuar lehtësisht, gjë që lejon anonimitetin. Më pas, ngacmimi kibernetik gjithashtu lejon që informacioni të përhapet me shpejtësi dhe i lejon autorit të aksesojë ngacmimin kudo dhe në çdo kohë. Prandaj, disponueshmëria dhe qasja ndaj ngacmimit janë më të përshtatshme dhe në përgjithësi ndihmojnë aktin.

Në përgjithësi, ngacmimi tradicional ka një shkallë më të lartë prevalence në krahasim me ngacmimin kibernetik. Kjo për shkak se ngacmimi kibernetik është relativisht i ri për shoqërinë dhe kërkimet e bëra janë të kufizuara. Çështja e bullizmit kibernetik pritet të rritet pasi adoleshentët rritën kohën e tyre të kaluar në internet dhe përdorimin e telefonit celular.

Përveç kësaj, shumë e kanë të vështirë të bëjnë dallimin midis një shakaje të pafajshme dhe ngacmimit kibernetik. Meta-analiza e fundit tregoi se ngacmimi kibernetik lidhet fuqishëm me idetë vetëvrasëse në krahasim me ngacmimet tradicionale, duke shkaktuar më shumë efekt negativ tek viktimat.

Përveç kësaj, vëmendja e prindërve luan një rol jetik në identifikimin e bullizmit kibernetik dhe bullizmi tradicional. Gjeneratat e vjetra janë kryesisht më pak të aftë për teknologjinë në krahasim me gjeneratat e reja, gjë që më pas ndikon në efikasitetin në zbulimin dhe realizimin e aktiviteteve të ngacmimit kibernetik. Për shkak të kësaj, mungon frika ndaj ndëshkimeve për bullizmin, gjë që mund të kontribuojë në rritjen e shkallës së bullizmit kibernetik.

KAPITULLI II

Kapitulli i dytë do të trajtojë pse përndjekja kibernetike dhe bullizmi kibernetik nuk mund të shmangen dhe të luftohen me metoda tradicionale, të cilat me sa duket nuk janë më efikase. Ky kapitull do të trajtojë natyrën dhe ndikimin e saj në mendësinë e viktimës, në mënyrë që ky studim mund të ndihmojë në gjetjen e disa mjeteve më efikase për parandalimin e një sulmi të tillë në internet.

Në vazhdimësi të rrezikut, disa të rinj janë më të ndjeshëm ndaj rasteve të bullizmit kibernetik se të tjerët. Ashtu si me ngacmimet kibernetike, viktimat kanë gjasa të jenë po aq femra sa meshkuj dhe kanë më shumë gjasa të jenë adoleshente më të rritur sesa fëmijët më të vegjël. Përafërsisht gjysma e viktimave të bullizmit kibernetik janë gjithashtu objektiva të bullizmit tradicional. Viktimat janë përgjithësisht jopopullore, të izoluara, të dëshpëruara, të shqetësuara dhe të frikësuara në krahasim me bashkëmoshatarët e tyre. Ata që janë në rrezik kanë më shumë gjasa të jenë në kërkim të pranimit dhe vëmendjes në internet, më të prekshëm ndaj teknikave manipuluese, më pak të vëmendshëm ndaj mesazheve të sigurisë në internet, më pak elastikë në trajtimin e një situate të vështirë, më pak të aftë ose të gatshëm për të mbështetuni te prindërit për ndihmë dhe më pak gjasa për të raportuar një situatë të rrezikshme në internet tek një i rritur. Të rinjtë më të rrezikuar nga bulizmi kibernetik përfshijnë adoleshentë të cenueshëm, të papjekur ose jo social të cilëve mund t'u mungojnë njohuritë dhe aftësitë e mjaftueshme për t'u përfshirë në vendimmarrje efektive; adoleshentë më të rinj që mund të kenë prindër tepër mbrojtës ose jo, por që ka të ngjarë të kenë marrëdhënie të shëndetshme me bashkëmoshatarët dhe vlera të mira; të rinj që kanë përkohësisht të dëmtuara marrëdhëniet me prindërit dhe/ose bashkëmoshatarët dhe aktualisht janë shumë të mërzitur emocionalisht dhe të rinj që përballen me sfida të mëdha të vazhdueshme në lidhje me shëndetin mendor personal dhe ndërprerje në marrëdhëniet me prindërit, shkollën dhe/ose bashkëmoshatarët.

NDIKIMI

Dëmi emocional që mund të rezultojë nga ngacmimi kibernetik është i rëndësishëm. Viktimat e bullizmit ballë për ballë shpesh përjetojnë depresion, ankth, dështim në shkollë dhe shmangie nga shkolla. Objektivat e ngacmimit kibernetik pësojnë dëme psikologjike të barabarta, nëse jo më të mëdha, sepse informacioni lëndues është i disponueshëm për publikun 24 orë në ditë, agresorët janë shpesh anonim, viktimizimi është i vazhdueshëm dhe i pashmangshëm dhe duke qenë se shpesh është e vështirë të hiqet materiali i postuar, informacioni mund të jetë i aksesueshëm publikisht për një kohë të gjatë. Adoleshentët mund të hezitojnë t'u tregojnë të rriturve për abuzimin që po u ndodh sepse janë të traumatizuar emocionalisht, mendojnë se është faji i tyre, kanë frikë nga ndëshkimi ose shqetësohen se aktivitetet e tyre në internet ose përdorimi i celularit do të kufizohen. Në ekstrem, ngacmimi kibernetik mund të çojë në vetëvrasje të të rinjve dhe dhunë të jashtme.

Viktimat e ngacmimeve kibernetike dhe sulmeve kibernetike mund të përjetojnë një gamë të gjerë pasojash emocionale, psikologjike dhe ndonjëherë fizike. Disa nga efektet e zakonshme tek këto viktima është shqetësimi emocional, pra viktimat mund të përjetojnë ndjenja frike, ankthi, zemërimi, trishtimi dhe pafuqie; ngacmimi dhe frikësimi i vazhdueshëm mund të kontribuojnë në depresionin klinik, i cili mund të kërkojë trajtim professional; viktimat mund të përjetojnë ankth të shtuar, duke përfshirë simptoma si sulmet e panikut, ankthin e përgjithësuar dhe ankthin social; në përpjekje për të shmangur burimin e ngacmimit, viktimat mund të izolohen nga miqtë, familja dhe aktivitetet shoqërore, duke çuar në ndjenjën e vetmisë; ngacmimi i vazhdueshëm mund të dëmtojë vetëvlerësimin dhe vetëvlerësimin e një personi, duke çuar në një imazh negativ për veten.

Gjithashtu mund të kenë problemet në shkollë ose në punë, në probleme akademike dhe shmangie të shkollës ose rënie të performancës. Në rastin e të rriturve, kjo mund të ndikojë në performancën e tyre të punës dhe kënaqësinë në punë. Një tjetër aspekt është shëndeti fizik pasi stresi i zgjatur nga ngacmimi në internet dhe sulmi në internet mund të

ketë pasoja fizike, duke përfshirë dhimbje koke, shqetësime të gjumit dhe probleme të tjera shëndetësore të lidhura me stresin ose vetëdëmtim dhe mendime vetëvrasëse. Në raste ekstreme, viktimat e bullizmit dhe sulmit në internet mund të përjetojnë sjellje të vetëdëmtimit ose mendime vetëvrasëse, si dhe çrregullime dhe stres post-traumatik (PTSD), të tilla si makthe dhe hipervigjilencë.

Një tjetër aspekt është ndikimi në marrëdhëniet me të tjerët pasi viktimat mund të kenë marrëdhënie të tensionuara me miqtë, anëtarët e familjes ose partnerët si rezultat i përvojave të tyre, si dhe mund të ndihen sikur kanë humbur ndjenjën e privatësisë, pasi aktivitetet e tyre në internet dhe informacioni personal mund të ekspozohet.

Një aspekt i fundit, por jo nga rëndësia janë edhe pasojat financiare pasi disa here përndjekja kibernetike mund të shtrihet në vjedhje identiteti ose ngacmim financiar, duke rezultuar në humbje të konsiderueshme financiare për viktimat.

Aspektet sociale të ngacmimit kibernetik dhe sulmit kibernetik janë kritike për të kuptuar se si këto sjellje ndikojnë jo vetëm tek individët, por edhe tek komuniteti dhe shoqëria më e gjerë. Këtu janë disa nga aspektet sociale të këtyre çështjeve.

Një ndër aspektet e para është izolimi social. Viktimat e ngacmimit kibernetik dhe sulmit në internet mund të tërhiqen nga ndërveprimet sociale, si në internet ashtu edhe jashtë linje, për shkak të frikës dhe ankthit. Ky izolim mund të çojë në vetmi dhe një ndjenjë të reduktuar të përkatësisë. Së dyti parashikohet dëmtimi i reputacionit. Ngacmimi në internet mund të dëmtojë reputacionin e një personi, duke e bërë të vështirë ruajtjen e marrëdhënieve shoqërore, duke përfshirë ato personale, akademike dhe profesionale.

Gjithashtu, ngacmimi kibernetik dhe sulmi kibernetik ngrenë pyetje në lidhje me vlerat shoqërore, duke përfshirë çështjet që lidhen me ndjeshmërinë, respektin dhe sjelljen e përgjegjshme në internet. Ato sfidojnë aftësinë e shoqërisë për të zbatuar sjelljen etike në hapësirat dixhitale.

Një aspekt shumë i rëndësishëm është edhe dinamika e bashkëmoshatarëve. Në rastet e bullizmit kibernetik që përfshijnë të rinjtë, roli i bashkëmoshatarëve është i rëndësishëm. Kalimtarët e rastit ose mund të përforcojnë ose zbusin dëmin duke marrë pjesë ose duke mbështetur ngacmimin ose duke mbrojtur dhe mbështetur viktimën.

Gjithashtu, komunitetet në internet, duke përfshirë platformat e mediave sociale, përballen me sfida në trajtimin e bullizmit dhe sulmit kibernetik. Përgjigja e këtyre komuniteteve mund të ndikojë se sa të sigurt dhe gjithëpërfshirës janë ata për përdoruesit e tyre, si dhe ndikimi në shkollë dhe në vendin e punës mund të prish mjediset arsimore dhe të punës. Shkollave dhe punëdhënësve mund t'u duhet t'i adresojnë këto çështje për të mbajtur një atmosferë pozitive dhe produktive.

Një aspekt shumë i rëndësishëm lidhet me përgjigjet ligjore dhe politike ndaj bullizmit dhe sulmit kibernetik. Legjislacioni shpesh zhvillohet për të mbrojtur individët nga këto forma ngacmimi. Në këtë kuadër media luan një rol në formësimin e perceptimeve publike dhe ndërgjegjësimi për bullizmin kibernetik dhe sulmin kibernetik. Rastet e profilit të lartë mund të çojnë në rritjen e ndërgjegjësimit dhe diskutimit publik duke përfshirë miqtë, familjen dhe organizatat e komunitetit, luajnë një rol vendimtar për të ndihmuar viktimat të përballen dhe të shërohen nga pasojat sociale dhe emocionale të këtyre formave të ngacmimit nëpërmjet promovimit të sigurisë në internet dhe shkrim-leximit dixhital është bërë një përgjegjësi sociale, me institucionet arsimore, prindërit dhe organizatat që punojnë për të edukuar individët, veçanërisht të rinjtë, rreth rreziqeve dhe strategjive për të qëndruar të sigurt në internet.

Së fundmi ngacmimi kibernetik dhe sulmi kibernetik kanë implikime në shëndetin publik, pasi ato mund të kontribuojnë në çështjet e shëndetit mendor, stresin dhe mirëqenien. Kuptimi i këtyre efekteve është i rëndësishëm për shoqërinë në tërësi.

Aspektet sociale të ngacmimit kibernetik dhe sulmit kibernetik theksojnë nevojën për një përpjekje kolektive për të parandaluar dhe

adresuar këto çështje. Promovimi i një kulture ndjeshmërie, respekti dhe përgjegjësie në hapësirat online dhe offline është thelbësor për të reduktuar përhapjen dhe ndikimin e këtyre sjelljeve të dëmshme.

STRATEGJITË PËR NDËRHYRJE DHE PARANDALIM

Hulumtimet e fundit sugjerojnë se pothuajse të gjithë të rinjtë në shkollën e mesme dhe të mesme me akses në një kompjuter në shtëpi ose shkollë do të përdorin internetin dhe se kjo përfaqëson një rritje të shpejtë gjatë dekadës së fundit[12]. Numri i adoleshentëve me profile në internet, duke përfshirë ato në faqet e rrjeteve sociale si Facebook dhe Instagram, është rritur gjithashtu dhe ka dëshmi se shumë prej këtyre adoleshentëve që hyjnë në internet në shtëpi bëjnë përpjekje për të mbajtur aktivitetin e tyre larg kontrollit të prindërve[13].

Askush nuk duhet të durojë ngacmimin kibernetik sepse pasojat i lënë fëmijët dhe adoleshentët të frikësuar, të mërzitur dhe të hutuar. Ata priren të mos e dinë pse u ndodh ky sulm dhe shpesh nuk janë të sigurt se kush mund t'i ndihmojë ata të zgjidhin këtë situatë të mundimshme dhe shpesh të frikshme. Përpjekjet e kombinuara të shkollës dhe shtëpisë nevojiten për të parandaluar, reduktuar ose eliminuar bullizmin kibernetik.

Viktimat e ngacmimit kibernetik nuk duhet të hakmerren, pasi kjo mund të nxisë ngacmime më intensive nga dhunuesi kibernetik dhe mund ta bëjë të paqartë se kush e nxiti fillimisht këtë sjellje agresive dhe lënduese.

Në varësi të ashpërsisë së ngacmimit kibernetik, viktimat dhe prindërit e tyre duhet të marrin parasysh disa nga hapat[14], të cilat përfshijnë injorimin ose bllokimin e komunikimet, kopjimi i materialit

12 "Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying", Sameer Hinduja dhe Justin W. Patchin, faq 87.

13 McQuade & Sampat, 2008, faq 145.

14 Gladden, M., & Vivolo-Kantor, A., & Hamburger, M., & Lumpkin, C. (2014). Bullying, faq 35.

që ngacmuesi kibernetik e postoi dhe ua dërgoi të tjerëve, pastrimi nga lista e miqve të mesazheve të çastit për të ndihmuar në uljen e numrit të njerëzve të tjerë që kanë akses në vendndodhjen e emailit të viktimës. Ndër të tjera është shumë e rëndësishme që të kërkohet edhe ndihmë e specializuar duke paraqitur një ankesë në faqen e internetit dhe tek ofruesi i shërbimit (ISP)[15] ose kompania e telefonisë celulare.

Meqenëse ngacmimi kibernetik ndodh më shpesh ndërsa fëmijët dhe adoleshentët janë në shtëpi, prindërit mund të jenë një burim i madh në parandalimin e rasteve të këtij lloji të ngacmimit. Duhet të merren parasysh mbajtja e kompjuterit të shtëpisë në vende lehtësisht të dukshme, si p.sh. dhoma e familjes ose kuzhina, komunikimi me femijët rregullisht për aktivitetet e tyre në internet dhe rregullat e etikës në internet në përgjithësi[16]. Ka një rëndësi shumë të madhe e foluar me fëmijën në mënyrë specifike për bullizmin kibernetik dhe inkurajimi që të njoftojnë menjëherë të rriturit nëse bëhen viktima të bullizmit në internet, si dhe ndihma që fëmijët të kuptojnë se ngacmimi në internet është i dëmshëm.

15 Kompania që ofron shërbimin e internetit.

16 "Cyberstalking: Harassment in the Internet Age and How to Protect Your Family", Paul Bocij.

KAPITULLI III

Punimi fokusohet kryesisht edhe në aspektet kriminalogjike të këtyre krimeve kibernetike, duke analizuar motivet dhe qëllimet e autorëve, ndryshimet sociale në jetën e viktimave, amplitudën e përhapjes së këtyre dukurive dhe përfitimet sociale që mund të arrihen nëpërmjet burgimit apo formave të tjera të dënimit penal.

Janë një sërë problematikash të cilat shfaqen në kësi lloj rastesh dhe ato janë të shumëllojshme. Disa nga këto aspekte lidhen me sfidat e mos-raportimit dhe zbulimit, pasi viktimat shpesh nuk raportojnë përndjekjen kibernetike dhe ngacmimin kibernetik për shkak të frikës, turpit ose mungesës së vetëdijes. Zbulimi i këtyre krimeve mund të jetë sfidues, duke e bërë të vështirë matjen e saktë të prevalencës dhe ndikimit të tyre të vërtetë.

Një tjetër problematik lidhet me çështjet juridiksionale pasi natyra pa kufij e internetit paraqet sfida juridiksionale. Përcaktimi i juridiksionit të duhur ligjor për hetimin dhe ndjekjen penale të rasteve të përndjekjes kibernetike dhe ngacmimit kibernetik mund të jetë komplekse, veçanërisht kur autori dhe viktima janë në vende të ndryshme.

Gjithashtu, përparimet teknologjike dhe përshtatshmëria u ofrojnë autorëve mjete të reja për t'u përfshirë në përndjekje kibernetike dhe ngacmime kibernetike, duke e bërë të vështirë për ligjet dhe zbatimin e ligjit që të vazhdojnë me taktikat dhe platformat në zhvillim. Një aspekt tjetër është ndikimi psikologjik dhe emocional duke qenë se përndjekja kibernetike dhe ngacmimi në internet mund të kenë efekte të rënda psikologjike dhe emocionale te viktimat, duke përfshirë ankthin, depresionin, vetëdëmtimin dhe tendencat për vetëvrasje. Kuptimi dhe adresimi i ndikimit psikologjik është thelbësor për strategjitë efektive të parandalimit dhe ndërhyrjes.

Autorët shpesh fshihen pas anonimitetit ose pseudonimeve në internet, duke e bërë të vështirë identifikimin dhe mbajtjen e tyre përgjegjës për veprimet e tyre. Mjetet teknologjike që lehtësojnë anonimitetin mund të keqpërdoren për aktivitete të dëmshme. Shumë

individë, veçanërisht brezat e rinj, mund të mos jenë plotësisht të vetëdijshëm për rreziqet dhe pasojat e mundshme të përfshirjes në ndjekje kibernetike dhe ngacmim kibernetik. Edukimi dhe ndërgjegjësimi për sjelljen e përgjegjshme në internet janë thelbësore për të parandaluar këto krime. Gjithashtu shpërndarja jo konsensuale e imazheve intime, e njohur edhe si "pornografi hakmarrëse", është një shqetësim në rritje. Ai përfshin shpërndarjen e përmbajtjes eksplicite pa pëlqimin e individëve të përfshirë, duke çuar në dëmtim shkatërrues emocional dhe reputacion.

Përndjekja kibernetike dhe ngacmimi kibernetik prekin në mënyrë disproporcionale gratë dhe vajzat, shpesh duke marrë formën e ngacmimit në internet, kërcënimeve dhe bullizmit në internet. Trajtimi i dhunës kibernetike me bazë gjinore është kritike për krijimin e një mjedisi më të sigurt në internet.

Gjithashtu balancimi i nevojës për të luftuar përndjekjen kibernetike dhe ngacmimin kibernetik me të drejtat e privatësisë dhe konsideratat etike paraqet një sfidë komplekse. Arritja e ekuilibrit të duhur gjatë mbrojtjes së lirive civile është thelbësore në adresimin e këtyre problemeve kriminalistike.

Kuptimi dhe adresimi i këtyre sfidave kriminologjike është thelbësore për zhvillimin e politikave efektive, kornizave ligjore dhe strategjive parandaluese për të luftuar përndjekjen kibernetike dhe bullizmin kibernetik dhe për të siguruar një hapësirë dixhitale më të sigurt për të gjithë.

Ngacmimi kibernetik është një çështje komplekse me aspekte kriminalistike që përfshijnë studimin e sjelljes kriminale, viktimizimit dhe dinamikës sociale që rrethon këto akte. Këtu janë disa aspekte kriminalistike të bullizmit në internet si psh qëllimi kriminal. Ngacmimi kibernetik zakonisht përfshin veprime të qëllimshme, të përsëritura dhe të dëmshme të drejtuara ndaj një individi përmes mjeteve dixhitale. Kriminologët analizojnë qëllimin e këtyre veprimeve për të kuptuar motivimet dhe modelet e sjelljes. Së dyti veçojmë faktorët psikologjikë

që i shtyjnë individët të përfshihen në ngacmime kibernetike, duke përfshirë çështjet që lidhen me pushtetin, kontrollin dhe dëshirën për të dëmtuar ose frikësuar të tjerët.

Një aspekt i rëndësishëm është edhe ndikimi i bullizmit kibernetik tek viktimat është një shqetësim kritik kriminalistik. Hulumtimi[17] vlerëson pasojat emocionale, psikologjike dhe fizike të bullizmit kibernetik mbi viktimat, duke përfshirë ankthin, depresionin dhe tendencat vetëvrasëse. Gjithashtu një pjesë e konsiderueshme e bullizmit kibernetik përfshin të rinjtë. Kriminologët shpesh hetojnë shkaqet dhe pasojat e bullizmit kibernetik të të miturve, si dhe efektivitetin e programeve të ndërhyrjes dhe parandalimit. Kriminologët duhet të eksplorojnë dallimet gjinore si te autorët ashtu edhe te viktimat e bullizmit kibernetik dhe se si normat dhe pritshmëritë shoqërore të cilat kontribuojnë në këtë sjellje si dhe në zhvillimin dhe vlerësimin e strategjive për parandalimin e bullizmit kibernetik, si për viktimat ashtu edhe për shkelësit[18].

Të kuptuarit e aspekteve teknike të ngacmimit kibernetik, si përdorimi i anonimitetit dhe teknologjisë për kryerjen e këtyre akteve, është thelbësor për kriminologët që të kuptojnë natyrën në zhvillim të kësaj forme agresioni, si dhe ekzaminimi i rolit të komuniteteve dhe nënkulturave online në lehtësimin ose dekurajimin e bullizmit kibernetik është një fushë tjetër me interes për kriminologët.

Hulumtimi kriminalistik mbi bullizmin kibernetik ndihmon politikëbërësit, zbatuesit e ligjit dhe edukatorët të kuptojnë më mirë fenomenin, të zhvillojnë strategji efektive për ta luftuar atë dhe për të mbështetur viktimat. Ai gjithashtu kontribuon në kuptimin më të gjerë të ndikimit të epokës dixhitale në sjelljen kriminale dhe viktimizimin.

Ndërsa cyberstalking është një formë e ngacmimit ose ndjekjes në internet që përfshin përdorimin e mjeteve dixhitale për të synuar,

17 Ericson, N. (2001). "Addressing the Problem of Juvenile Bullying." OJJDP Fact Sheet, 27. Washington, DC: US Department of Justice, Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention, faq 56.

18 "Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress", Nancy E. Willard, faq 78.

ngacmuar ose frikësuar një individ. Një këndvështrim kriminologjik i cili lidhen me sulmin kibernetik parashikon se kërkimi në internet zakonisht përfshin një model të përsëritur dhe të vazhdueshëm të sjelljes së padëshiruar në internet.

Kjo sjellje mund të përfshijë dërgimin e mesazheve kërcënuese, monitorimin e pranisë së viktimës në internet ose përhapjen e informacionit të rremë. Kriminologët shpesh studiojnë motivet psikologjike që qëndrojnë pas sulmeve kibernetike[19]. Këto mund të përfshijnë një dëshirë për kontroll, pushtet, hakmarrje ose një obsesion apo ndikim mbi viktimën. Ndikimi emocional dhe psikologjik tek viktimat është një shqetësim i rëndësishëm për kriminologët. Përndjekja kibernetike mund të shkaktojë shqetësime të rënda emocionale, ankth, depresion dhe madje edhe dëmtim fizik për viktimat.

Të kuptuarit e aspekteve teknologjike të sulmit kibernetik është thelbësor. Kjo përfshin ekzaminimin se si ndjekësit përdorin mjetet në internet, mediat sociale dhe platforma të tjera dixhitale për të kryer aktivitetet e tyre. Studiuesit mund të eksplorojnë dallimet gjinore si te autorët ashtu edhe në viktimat e sulmit kibernetik dhe se si normat dhe pritshmëritë shoqërore kontribuojnë në këtë sjellje. Kriminologët shpesh vlerësojnë gjasat e recidivizmit midis sulmuesve kibernetikë. Kuptimi i potencialit për përsëritjen e shkeljeve është thelbësor për hartimin e strategjive efektive të parandalimit dhe ndërhyrjes.

Cyberstalking mund të ketë një ndikim më të gjerë në komunitetet online dhe rrjetet sociale. Hulumtimi mund të shqyrtojë se si këto komunitete reagojnë ndaj incidenteve të sulmit kibernetik dhe rolin e platformave në adresimin e një sjelljeje të tillë.

Gjithashtu kriminologët kontribuojnë në zhvillimin dhe vlerësimin e strategjive për parandalimin dhe ndërhyrjen në rastet e sulmit kibernetik. Kjo mund të përfshijë praktikat e zbatimit të ligjit, programet për

19 Tattum, D. (1989). "Violence and Aggression in Schools." In Bullying in Schools, edited by Delwyn P. Tattum and David A. Lane, 17–19. Stroke-on-Trent, UK: Trentha, faq 97.

mbështetjen e viktimave dhe fushatat e ndërgjegjësimit publik, si dhe anonimiteti në internet, pra aftësia për të ruajtur anonimitetin në internet përdoret shpesh nga sulmuesit kibernetikë. Kriminologët studiojnë se si ky anonimitet dixhital ndikon në kryerjen e sulmit kibernetik dhe sfidat që ai paraqet për zbatimin e ligjit.

Kuptimi i këtyre aspekteve kriminalogjike të sulmit kibernetik është thelbësor për zbatimin e ligjit, politikëbërësit dhe mbrojtësit e viktimave për të luftuar në mënyrë efektive këtë formë të ngacmimit në internet dhe për të ofruar mbështetje për viktimat. Ligjet në lidhje me sulmin kibernetik vazhdojnë të zhvillohen për të adresuar sfidat e paraqitura nga epoka dixhitale pasi shumë pak vende paraqesin mbrojte efektive dhe figura veprash penale të përshtatshme për të adrsuar drejtë këto aspekte të digjitalizmit.

ASPEKTI STATISTIKOR

Në lidhje me aspektet statistikore të ketij punimi, paraqitet një situate më e veshtirë për sa i përket aspektit kombëtar, por disi më e lehtë dhe e strukturuar në aspektin ndërkombëtar. Janë marrë në referencë disa statistika zyrtare, duke u bazuar në literaturën dhe në institucionet e besuara. Disa prej tyre të cilat do të prevalojnë në këtë punim lidhen me prevalencën tek adoleshentët. Sipas një sondazhi të vitit 2019 nga Qëndra Kombëtare për Statistikat e Arsimit (NCES) në Shtetet e Bashkuara[20], rreth 20.8% e nxënësve të moshës 12-18 vjeç raportuan se ishin ngacmuar në shkollë gjatë vitit shkollor. Nga këto, 15.7% raportuan se ishin ngacmuar në internet ose përmes të shkruarit.

Kategoritë kryesore të shkeljeve që u raportuan gjatë 2022 ishin: CSAM (44 raste), përbëjnë ankesën kryesore të raportimeve. Në vend të dytë rezultonte vjedhja dhe postimi i fotove/videove personale (37 raste) ndjekur nga përndjekjet, shantazhet apo kërcënimet.

20 Surveillance Among Youths: Uniform Definitions for Public Health and Recommended Data Elements

Shkalla e prevalencës së bullizmit kibernetik është brenda intervalit 30% - 55%. Shkalla më e ulët e prevalencës është 15.8% në mesin e nxënësve të shkollave të mesme. Shkalla më e lartë e prevalencës raportohet nga një meta-analizë e fundit e cila tregoi një shkallë të lartë të përhapjes së kësaj çështjeje në të gjitha vendet, afërsisht 40% deri 55% e studentëve janë të përfshirë në një farë mënyre qoftë si viktima, autorë apo vëzhgues.

Prandaj, pothuajse një nga dy studentët ka qenë ose është i përfshirë në bullizëm kibernetik. Midis tyre, prevalenca e viktimave është më e larta, rreth 10% deri në 27% e të përfshirëve janë viktima të bullizmit kibernetik.

Dy motivime të tjera të cituara shpesh dhe të ndërlidhura përfshijnë anonimitetin. Ndryshe nga ngacmimi tradicional ku është personalisht, ngacmuesit kibernetikë nuk identifikohen nga vëzhguesit dhe viktimat. Kjo distancë i mbron ata nga përballja me pasojat e veprimeve të tyre; reduktimi i vetëkontrollit për ngacmuesit e mundshëm për të bërë atë që nuk do ta bëjnë personalisht.

Ndërsa një studim i vitit 2019 nga Patchin dhe Hinduja[21] zbuloi se në mesin e nxënësve të shkollave të mesme dhe të mesme në SHBA, 37% përjetuan bullizëm kibernetik gjatë jetës së tyre. Format e zakonshme përfshijnë thirrjet me emra tallës (26.3%), përhapjen e thashethemeve (21.0%) dhe kërcënimin (16.4%). I njëjti studim nga Patchin[22] dhe Hinduja theksoi se 33.7% e viktimave të ngacmimit kibernetik raportuan se ndjeheshin të trishtuar, 27.8% përjetuan depresion dhe 20.8% kishin mendime vetëvrasëse[23].

Sipas ketyre studimeve vetëm rreth 40% e studentëve që kanë përjetuar ngacmim kibernetik ia kanë raportuar një të rrituri, gjë që tregon se shumë raste nuk raportohen. Mekanizmat dhe ndërhyrjet

21 Hinduja, S. & Patchin, J. W. (2015). Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying (2nd Ed.). Thousand Oaks, CA: Sage Publications, faq 98.

22 Po aty

23 Pa aty

adekuate të raportimit janë thelbësore për të trajtuar në mënyrë efektive bullizmin kibernetik[24].

Për më tepër përhapja e përndjekjes kibernetike ndryshon sipas rajonit dhe popullsisë, por është një çështje e përhapur në të gjitha vendet. Gratë shpesh preken në mënyrë disproporcionale nga ndjekja kibernetike, me raste që variojnë nga ngacmimet në internet deri te ndjekja përmes platformave të ndryshme dixhitale. Studimet kanë treguar një lidhje shqetësuese midis përndjekjes kibernetike dhe dhunës nga partneri e cila u pasqyrua në 71% e viktimave të dhunës në familje të cilat kanë përjetuar gjithashtu ndjekje kibernetike[25].

Mosha kryesore dhe më e prekur nga dhuna online dhe gjuha e urrejtjes në internet ishte 18-30 vjeç, e ndjekur kjo nga grup mosha 15-17 vjeç dhe përndjekja kibernetike mund të ketë pasoja të rënda emocionale dhe psikologjike, duke përfshirë ankthin, depresionin, humbjen e gjumit dhe uljen e përgjithshme të mirëqenies. Viktimat shpesh raportojnë se ndihen të dhunuar, të frikësuar dhe të shqetësuar për sigurinë e tyre. TikTok dhe Instagram përbënin dy platformat kryesore të ankesave të fëmijëve dhe adoleshentëve për dhunën online dhe gjuhën e urrejtje.

Ligjet dhe dënimet në lidhje me ndjekjen kibernetike ndryshojnë në nivel global. Shumë vende e kanë njohur përndjekjen kibernetike si një krim dhe kanë ligje specifike për ta trajtuar atë. Megjithatë, zbatimi dhe përgjigjia ligjore mund të jenë sfiduese për shkak të natyrës transnacionale të internetit.

Disa nga aspektet që parashikojnë lidhjen me ngacmimin kibernetik, pavarësisht nga rolet janë:[26]

---

24 "Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying", Sameer Hinduja dhe Justin W. Patchin, faq 89.

25 Journal of Interpersonal Violence.

26 Wolke, D., & Woods, S., & Bloomfield, L., & Karstadt, L. (2000). "The association Between Direct and Relational Bullying and Behaviour Problems among Primary School Children." Journal of Child Psychology and Psychiatry 41, No. 8, faq 994.

1. Lidhja pozitive me veprën
2. Lidhja pozitive me viktimizimin
3. Mjedis shkollor jo mbështetës
4. Imazhi i dobët i trupit për vajzat
5. Sjelljet e rrezikshme në internet
6. Obeziteti
7. Perceptimi i bashkëmoshatarëve që sillen në mënyrë të ngjashme
8. Rinia e identifikuar joheteronormative
9. Narcisiste shfrytëzuese
10. Koha më e gjatë e shpenzuar në aktivitete sociale të bazuara në kompjuter
11. Ndikimi i ngacmimit kibernetik

Të gjitha format e bullizmit kanë ndikime negative tek personat e përfshirë. Ngacmimi kibernetik ka disa faktorë, të cilët mund të intensifikojnë ndikimet e tij negative, duke përfshirë vështirësinë për të shpëtuar nga bullizmi, madhësinë e audiencës së mundshme, anonimitetin e ngacmuesit dhe aftësinë për të sulmuar në çdo kohë dhe në çdo vend[27].

Një zbulim interesant është se statusi i ngacmimit kibernetik është i lidhur me vështirësitë e perceptuara, dhimbje koke dhe ndjenjën e pasigurisë në shkollë.

Përveç kësaj, ngacmimi kibernetik është parë si një modulues i statusit social. Ekziston një marrëdhënie pozitive midis ngacmimit kibernetik dhe popullaritetit të perceptuar. Kjo peshon më shumë për femrat ku mund të matin popullaritetin dhe statusin e tyre social përmes mediave sociale. Ngacmuesit mund ta përdorin këtë si një avantazh për

27 Crick, N., & Grotpeter, J. (1995). "Relational Aggression, Gender, and Social-Psychological Adjustment." Child Development, faq 716.

të ngacmuar të tjerët për të fituar një pozicion më të lartë të statusit social. Në të gjitha hulumtimet, një gjetje e zakonshme është se grupi më i cenueshëm ndaj ndikimeve negative të ngacmimit kibernetik janë viktimat e dhunimit dhe kjo duhet të merret parasysh në ndërhyrjen kryesore të synuar të problemit.

Ashpërsia e ndikimeve varet edhe nga forma e bullizmit kibernetik. Ngacmimi kibernetik i cili është publik (si rrjetet sociale) dhe jo privat (siç janë mesazhet tekstuale abuzive) dhe autorët anonimë më shumë sesa jo-anonimë paraqesin peshë specifike më të rëndë. Ngacmimi kibernetik me fotografi dhe video, veçanërisht të skenave intime ose të dhunshme janë dhe perceptohet si më të rënda perkundrejt thirrjeve telefonike në formë shakaje ose fyerje në tekstet e mesazheve të shkurtra (SMS)[28].

28 Slee, P., & Rigby, K. (1993). "The Relationship of Eysenck's Personality Factors and Self-Esteem to Bully-Victim Behaviour in Australian School Boys." Personality and Individual Differences 14, faq 371.

KAPITULLI IV

Kapitulli i katërt do të përpiqet të krahasojë dhe analizojë legjislacione të ndryshme në lidhje me bullizmin kibernetik dhe përndjekjen kibernetike, për të krijuar udhëzues më të mirë në luftën kundër këtyre fenomeneve. Legjislacione të ndryshme kanë zhvilluar arsyetime dhe perceptime të ndryshme për këto krime kibernetike dhe për rrjedhojë një studim krahasues i tyre mund të nxisë diskutime të reja për ndryshime të mundshme dhe të nevojshme legjislative në legjislacionin shqiptar, duke pasur parasysh faktin qe aktualisht po punohet për një draft për miratimin e Kodit te Ri Penal të Republikës së Shqipërisë pas më shumë se 18 vitesh që prej miratimit të kodit aktual në vitin 1995.

Aspektet kriminale të bullizmit në internet përfshijnë veprime dhe sjellje që mund të konsiderohen të paligjshme sipas ligjeve dhe rregulloreve të ndryshme. Ndërsa ligjet dhe përkufizimet specifike mund të ndryshojnë sipas juridiksionit, disa aspekte ngelen të njëjta për të gjitha legjislacionet[29].

Së pari ngacmimi kibernetik pothuajse në të gjitha rastet përfshin komunikim ose sjellje të përsëritur, të padëshiruar dhe keqdashëse drejtuar një individi, që mund të përbëjë ngacmim. Ligjet që lidhen me ngacmimin mund të zbatohen për ngacmimin në internet dhe shkelësit mund të përballen me akuza penale. Një aspekt tjetër është kërcënimi, qoftë i drejtpërdrejtë apo i tërthortë, nëpërmjet komunikimit elektronik përbën vepër penale. Në këtë kontekst trajtojmë edhe shpifjen. Përhapja e informacionit të rremë dhe dëmtuese për dikë në internet mund të konsiderohet shpifje, e cila është një vepër penale në shumë juridiksione por edhe me pasoja civile. Nëse ngacmimi kibernetik përfshin gjuhë urrejtjeje, diskriminim ose kërcënime bazuar në racën, fenë, gjininë ose karakteristika të tjera të mbrojtura të një personi, ai mund të

29 Limber, S., & Nation, M. (1998). "Bullying Among Children and Youth." In Combating Fear and Restoring Safety in Schools, edited by June L. Arnette and Marjorie C. Walsleben. Office of Juvenile Justice and Delinquency Prevention (1998), faq 113.

konsiderohet një krim urrejtjeje në disa juridiksione. Krimet e urrejtjes[30] shpesh mbartin dënime më të rënda. Shumë vende kanë ligje që synojnë posaçërisht mbrojtjen e të miturve nga ngacmimi kibernetik, si dhe ata që shpallen fajtorë për shënjestrimin e të miturve në internet.

Ndër të tjera, kur të miturit përfshihen në ngacmim kibernetik, kjo vepër ndërthuret me veprat penale të e shfrytëzimit të fëmijëve etj[31].

Ligjet që lidhen me sulmin kibernetik ndryshojnë sipas vendit dhe në disa raste, sipas shteteve ose rajoneve individuale brenda një vendit. Këto ligje janë krijuar për të trajtuar çështjen e ngacmimit, ndjekjes dhe frikësimit në internet.

Ligjet kundër sulmit kibernetik shpesh kërkojnë që dhunuesi të ketë qëllimin të shkaktojë frikë, dëmtim ose shqetësim tek viktima. Vërtetimi i qëllimit është një element kyç në këto raste. Shumë ligje kërkojnë që sjellja të jetë e përsëritur ose e vazhdueshme, në krahasim me një incident të vetëm të izoluar. Kjo i dallon mosmarrëveshjet e zakonshme ose argumentet në internet nga sulmet kibernetike. Ligjet e ndjekjes kibernetike përfshijnë një sërë metodash të komunikimit elektronik, duke përfshirë emailet, mesazhet me tekst, postimet në mediat sociale dhe ndërveprime të tjera në internet.

Një aspket veçanërisht i rëndësishëm janë viktimat e sulmit kibernetik të cilat kërkojnë urdhra mbrojtjeje ose urdhra ndalimi kundër autorëve për të ndaluar ndjekësin të kontaktojë ose t'i afrohet viktimës fizikisht por edhe virtualisht. Mbrojtja ndaj dhunës në familje, në zbatim të ligjislacionit shqiptar[32], do të sigurohet duke urdhëruar menjëherë të padituri/ën (dhunuesin/en) që të mos kryejë ose të mos kërcënojë se do të kryejë vepër të dhunës në familje ndaj paditësit/es (viktimës) apo pjesëtarëve të tjerë të familjes së viktimës, siç përcaktohet në nenin 3 pika 3 të këtij ligji apo siç emërtohet në urdhër duke urdhëruar menjëherë të padituri/ën (dhunuesin/en) që të mos cenojë, ngacmojë,

30 Hate crimes.

31 "Hate Crimes in Cyberspace", Danielle Keats Citron, faq 67.

32 Ligji Nr. 9669, datë 18.12.2006, i ndryshuar.

kontaktojë apo të komunikojë drejtpërdrejt ose tërthorazi me viktimën apo pjesëtarë të familjes së viktimës, siç përcaktohet në nenin 3 pika 3 të këtij ligji apo siç emërtohet në urdhër, duke larguar menjëherë të padituri/ën (dhunuesin/en) nga banesa për një afat kohor të caktuar me urdhër të gjykatës dhe të mos e lejojë të rihyjë në banesë pa autorizimin e gjykatës, duke ndaluar menjëherë të padituri/ën (dhunuesin/en) që t'i afrohet përtej një distance të caktuar viktimës apo pjesëtarëve të familjes së viktimës, siç përcaktohet në nenin 3 pika 3 të këtij ligji apo siç emërtohet në urdhër; duke ndaluar menjëherë të padituri/ën (dhunuesin/en) që t'i afrohet shtëpisë, vendit të punës, banesës së familjes së origjinës apo banesës së çiftit të ardhshëm ose të personave të tjerë dhe për më tepër shkollës së fëmijëve, ose vendeve të cilat frekuentohen më tepër nga viktima, me përjashtim të rasteve kur frekuentimi bëhet për arsye pune; duke vendosur menjëherë viktimën/at dhe të miturit në strehime të përkohshme, duke mbajtur parasysh në çdo rast interesin më të lartë, atë të të miturit; duke kufizuar ose duke ndaluar të padituri/ën (dhunuesin/en) të takohet me fëmijën e viktimës, sipas kushteve të cilat mund të jenë të përshtatshme; duke i ndaluar të padituri/ës (dhunuesit/es) hyrjen ose qëndrimin në banesën e përkohshme apo të përhershme të viktimës, ose në ndonjë pjesë të saj, pavarësisht nga të drejtat e pronësisë apo të posedimit të dhunuesit, duke urdhëruar një person të autorizuar nga gjykata (punonjës i rendit ose përmbarues gjyqësor) që të shoqërojë viktimën ose të padituri/ën (dhunuesin/en) deri në banesën e viktimës dhe të mbikëqyrë largimin e pasurisë personale, duke urdhëruar organet zbatuese të ligjit që të sekuestrojnë çdo armë që i përket dhunuesit gjatë kontrollit të kryer apo të urdhërojë dhunuesin për të dorëzuar çdo armë që i përket atij, duke urdhëruar të padituri/ën (dhunuesin/en) që të lejojë viktimën të posedojë banesën të cilën e përdorin së bashku viktima dhe dhunuesi/ja ose ndonjë pjesë të saj, duke urdhëruar të padituri/ën (dhunuesin/en) që të paguajë qeranë e banesës së përhershme apo të përkohshme të viktimës, si dhe detyrimin ushqimor për viktimën, fëmijët apo pjesëtarë të tjerë të familjes që ka në ngarkim; duke i hequr dhunuesit, përkohësisht, përgjegjësinë prindërore ose nëse është rasti, kujdestarinë

mbi të miturin, kujdestarinë për personin me aftësi të kufizuara, ose për personin që i është hequr ose kufizuar zotësia për të vepruar.

Kur gjykata vendos të heqë ushtrimin e përgjegjësisë prindërore nga të dy prindërit ose nga prindi i vetëm, ajo cakton kujdestarinë e përkohshme mbi fëmijët, duke zbatuar rregullat e parashikuara në Kodin e Familjes dhe legjislacionin procedural në fuqi; duke urdhëruar organet kompetente, shërbimet sociale të njësive përkatëse të vetëqeverisjes vendore dhe/ose organizatat që ofrojnë shërbime, që, sipas rastit, të mbështesin me ndihmë psikosociale, shëndetësore e financiare personat e dhunuar në familje, si dhe të monitorojnë respektimin e urdhrave të mbrojtjes nga palët, duke paraqitur raportet përkatëse përpara koordinatorit vendor për referimin e rasteve të dhunës në marrëdhëniet familjare; duke urdhëruar të padituri/ën (dhunuesin/en) që të bëjë një pagesë periodike në favor të personave bashkëjetues, të cilët, për efekt të masës së mësipërme, mbeten të privuar nga mjetet e jetesës.

Për të siguruar pagesën, gjykata mund të vendosë që shuma të derdhet nga punëdhënësi në favor të përfituesit. Një vendim i tillë përbën titull ekzekutiv; duke përfshirë viktimën e dhunës në familje në programe rehabilitimi; duke urdhëruar dhunuesin/en, nëse është rasti, të marrë pjesë në programe rehabilitimi psikosociale dhe/ose në programe të aftësimit prindëror, të organizuara nga subjekte publike ose private; duke urdhëruar të padituri ose dhunuesin/en, nëse është rasti, të marrë pjesë në programe rehabilitimi, pranë qendrave spitalore, qendrave ambulatore ose qendrave komunitare, që japin shërbime të shëndetit mendor, shërbime të alkoologjisë ose shërbime të toksikologjisë. Përgjegjësit e programit të rehabilitimit vënë në dijeni koordinatorin vendor pranë Mekanizmit të Koordinuar të Referimit të rasteve të dhunës në familje për pjesëmarrjen e të paditurit në program dhe ecurinë e tij.

Gjykata, kryesisht, në urdhrin e menjëhershëm të mbrojtjes ose/dhe në urdhrin e mbrojtjes, mund të parashikojë masa mbrojtëse për fëmijët që kanë pësuar dhunë ose kanë qenë të pranishëm kur është ushtruar dhunë në familje. Gjykata, sipas vlerësimit të saj, mund të zbatojë edhe masa mbrojtëse e procedura të parashikuara nga legjislacioni në fuqi për

të drejtat dhe mbrojtjen e fëmijës, derisa nuk cenohen afatet e procesit gjyqësor të parashikuara nga ky ligj.

Një aspekt tjetër i rëndësishëm janë çështjet ndër-juridiksionale. Kur ndjekësi dhe viktima janë në juridiksione të ndryshme, ligjet mund të kenë dispozita për të trajtuar çështjet që kalojnë kufijtë shtetërorë ose kombëtarë.

Në lidhje me mekanizmat e raportimit, shumë juridiksione kanë krijuar mekanizma raportimi që viktimat të raportojnë sulmin kibernetik tek forcat e rendit ose platformat online, të cilat më pas mund të ndërmarrin veprime kundër shkelësit.

Kodi ynë Penal nuk parashikon aktualisht asnjë vepër penale mirëfilltazi në lidhje me cyber-bullying apo cyber-stalking dhe besojmë se kjo është edhe një nga problematikat kryesore që qëndrojnë në gjenezë të mos pasjes se instrumentave të duhur ligjor për luftë kundër këtyre krimeve kibernetike. Megjithate mendoj se veçimi i disa veprave të tjera penale të lidhura disi me këto forma të krimit kibernetik janë psh:

Neni 99[33] i cili parashikon se "shkaktimi i vetëvrasjes ose i tentativës së vetëvrasjes të një personi, si rrjedhojë e trajtimit të keq sistematik ose nga sjellje të tjera sistematike që prekin rëndë dinjitetin, të kryera nga personi që e ka në varësi apo nga personi me të cilin ka marrëdhënie familjare ose bashkëjetese, dënohet me burgim nga tre deri në shtatë vjet". Në këtë kontekst kjo vepër lidhet me krimet në fjalë pasi e gjithë frika dhe paniku i shkaktuar si dhe trajtimi i keq dhe sistematik ose sjelljet e tjera sistematike që prekin rëndë dinjitetin në kohët e sotme kur ndërveprimi kryesor mes njerëzve bëhet nëpërmjet internetit dhe sistemit kompjuterik, krimet e tilla kibernetike janë drejpërdrejtë të lidhura me veprën në fjalë të vetëvrasjes.

Ndërsa neni 119[34] parashikon se "fyerja e qëllimshme e personit përbën kundërvajtje penale dhe dënohet me gjobë nga pesëdhjetë mijë

33 Kodi Penal i Republikës së Shqipërisë

34 Po aty

gjer në një milion lekë".

Po kjo vepër, kur kryhet botërisht, në dëm të disa personave ose më shumë se një herë, përbën

kundërvajtje penale dhe dënohet me gjobë nga pesëdhjetë mijë gjer në tre milionë lekë. Në këtë rast mendojmë se vetë fyerja përben një nga elementët e anës objektive me anë të së cilës shfaqet krimi kibernetik i bullizmit, pasi fyerja e dikujt është një ndër tiparet kryesore të shfaqjes së bullizmit në internet.

Në vijim të parashikimeve të këtij seksioni të Kodit Penal, neni 119/a parashikon "ofrimi në publik ose shpërndarja e qëllimshme publikut, nëpërmjet sistemeve kompjuterike, e materialeve me përmbajtje raciste ose ksenofobike përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim deri në dy vjet. Në këtë rast mendojmë se lidhja qëndron pikërisht tek përdorimi i sistemeve kompjuterike, i cili në rastin konkret nuk përbën më element të anës objektive të kryerjes së veprës siç është veprimi, por përbën elemnetin e anës objektive të mënyrës, pra se si konkretisht kryhet vepra.

Po ashtu neni 119/b parashikon se "fyerja e qëllimshme publike, nëpërmjet sistemit kompjuterik, që i bëhet një personi, për shkak të përkatësisë etnike, kombësisë, racës apo fesë, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim deri në dy vjet. Në këtë kontekst kjo vepër lidhet me krimet në fjalë pasi vlen e njëjta llogjikë arsyetimi si në rastin e në nenin 119/a.

Po në këtë llogjikë neni 120 parashikon se "përhapja e qëllimshme e thënieve, si dhe çdo informacion tjetër, duke e ditur se janë të rreme, që cënojnë nderin dhe dinjitetin e personit, përbën kundërvajtje penale dhe dënohet me gjobë nga pesëdhjetë mijë gjer në një milion e pesëqind mijë lekë. Në këtë kontekst kjo vepër lidhet me krimet në fjalë pasi vlen e njëjta llogjikë arsyetimi si në rastin e fyerjes. Fyerja dhe shpifja janë dy vepra penal të cilat kombinohen shumë here me njëra tjetrën në shfaqjet e tyre në komunikimet apo postimet online.

Në vijim të sa më sipër citojmë nenin 121, i cili parashikon se

"vendosja e aparaturave që shërbejnë për dëgjim apo regjistrim të fjalëve ose të figurave, dëgjimi ose regjistrimi i fjalëve, fiksimi ose regjistrimi figurave, si dhe ruajtja për publikim i të dhënave që ekspozojnë një aspekt të jetës private të personit, pa pëlqimin e tij, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim deri në dy vjet". Konkretisht vendosja e aparaturave përben një tjetër element të anës objektive, pra mjetin me anë të të cilës shpeshherë realizohen një pjesë e veprave penale kibernetike.

Neni 121/a parashikon se "kërcënimi ose ngacmimi i personit me anën e veprimeve të përsëritura, me qëllimin për t'i shkaktuar një gjendje të vazhdueshme dhe të rëndë ankthi apo frike për sigurinë vetjake, të një të afërmi ose të një personi, me të cilin ka lidhje shpirtërore, apo për ta detyruar të ndryshojë mënyrën e tij të jetesës, dënohet me burgim nga gjashtë muaj gjer në katër vjet. Kur kjo vepër kryhet nga ish-bashkëshorti, ish-bashkëjetuesi apo personi që ka pasur lidhje shpirtërore me të dëmtuarin, dënimi rritet me një të tretat e dënimit të dhënë. Në këtë rast kjo vepër përbën formën fizike të shfaqjes së krimit kiberetik të cyber-stalking, pasi në legjislacionin shqiptar dispozita në fjalë titullohet si "përndjekja".

Një ndër nenet më të lidhura me krimet kibernetike në fjalë është edhe neni 122 i Kodit Penal, i cili parashikon se "përhapja e një sekreti që i përket jetës private të një personi nga ai që e siguron atë për shkak të detyrës ose të profesionit, kur detyrohet të mos e përhapë pa qenë i autorizuar, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim gjer në një vit.

Po kjo vepër, e kryer me qëllim fitimi ose për të dëmtuar një person tjetër, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim gjer në dy vjet. Në këtë kontekst kjo vepër lidhet me krimet kibernetike në fjalë pasi një nga format se si këto krime kibernetike kryhen është edhe përhapja e një sekreti që i përket jetës private të një personi.

Së fundmi mund të veçojmë nenin 123 të Kodit Penal i cili lidhet me pengimin ose shkelja e fshehtësisë së korrespondencës nëpërmjet

kryerjes me dashje e veprimeve të tilla si asgjësimi, mosdorëzimi, hapja dhe leximi i letrave apo çdo korrespondencë tjetër, si dhe ndërprerja ose vënia nën kontroll, dëgjimi i bisedave telefonike, telegrafike ose i çdo mjeti tjetër telekomunikimi, përbën kundërvajtje penale dhe dënohet me gjobë ose burgim gjer në dy vjet. Në këtë kontekst kjo vepër lidhet me krimet kibernetike në fjalë pasi një nga format se si këto krime kibernetike kryhen është edhe pengimin ose shkelja e fshehtësisë së korrespondencës nëpërmjet kryerjes me dashje e veprimeve të tilla si asgjësimi, mosdorëzimi, hapja dhe leximi i letrave apo çdo korrespondencë tjetër, si dhe ndërprerja ose vënia nën kontroll, dëgjimi i bisedave telefonike.

Ndërsa ligji Nr. 2/2017 "Për Sigurinë Kibernetike", lidhet në mënyrë thelbësore me krimet kibernetike në përgjithësi pasi parashikon zbatimin për rrjetet e komunikimit dhe sistemet e informacionit, cenimi apo shkatërrimi i të cilave do të kishte impakt në shëndetin, sigurinë, mirëqenien ekonomike të qytetarëve dhe funksionimin efektiv të ekonomisë në Republikën e Shqipërisë.

Autoriteti përgjegjës ka këto kompetenca në fushën e sigurisë kibernetike pasi përcakton masat e sigurisë kibernetike; vepron si pikë qendrore kontakti në nivel kombëtar për operatorët përgjegjës në fushën e sigurisë kibernetike dhe bashkërendon punën për zgjidhjen e incidenteve të sigurisë kibernetike; administron raportet e incidenteve në fushën e sigurisë kibernetike dhe siguron ruajtjen e regjistrimin e tyre; siguron ndihmë dhe mbështetje metodike për operatorët përgjegjës në fushën e sigurisë kibernetike; kryen analiza për dobësitë e konstatuara në fushën e sigurisë në internet; kryen aktivitete ndërgjegjësimi dhe edukimi në fushën e sigurisë kibernetike; vepron në cilësinë e CSIRT-së kombëtare.

Autoriteti në fjalë koordinon veprimtaritë e tij me institucionet e sigurisë dhe të mbrojtjes dhe bashkëpunon me CSIRT-të sektoriale dhe autoritetet ndërkombëtare në fushën e sigurisë kibernetike, nëpërmjet marrëveshjeve të përbashkëta, në përputhje me legjislacionin në fuqi.

Sipas ligjit subjekte të tjera përgjegjëse në fushën e sigurisë kibernetike janë operatorët e infrastrukturës kritike të informacionit; operatorët e

infrastrukturës së rëndësishme të informacionit. Këshilli i Ministrave, me propozimin e ministrit përgjegjës, miraton listën e infrastrukturave kritike të informacionit dhe të infrastrukturave të rëndësishme të informacionit, e cila përditësohet të paktën një herë në dy vjet.

Ligji parashikon gjithashtu Ekipin e Përgjigjes ndaj Incidenteve të Sigurisë Kompjuterike (CSIRT)[35]

Ekipet e përgjigjes ndaj incidenteve të sigurisë kompjuterike (CSIRT) përbëhen nga specialistë të fushës së sigurisë kompjuterike pranë çdo operatori që administron infrastrukturën kritike të informacionit. Operatorët e infrastrukturave të rëndësishme të informacionit duhet të kenë të paktën një person përgjegjës për incidentet e sigurisë kompjuterike. Ministri përgjegjës nxjerr udhëzim për metodologjinë e punës, detyrat që duhet të zbatojnë ekipet ose personat përgjegjës dhe kriteret e përgjithshme që duhet të respektojnë operatorët në përzgjedhjen tyre.

Konkretisht me rastet e problemeve në internet merret Njësia C– Hetimi i krimeve kibernetike në Departamentin e Policisë Kriminale në Drejtorinë e Përgjithshme të Policisë së Shtetit. Kjo është struktura përgjegjëse për krimet kibernetike dhe merret në mënyrë të përditshme edhe ndër të tjera me cyber-bullying dhe cyber-stalking.

Shumica e ligjeve kundër bullizmit përfshijnë në mënyrë eksplicite një element qëllimi. Për shembull, ligji i Delaware[36] e karakterizon ngacmimin si një "akt të qëllimshëm me shkrim, elektronik, verbal ose fizik. Ne shtetin e Luizianës[37] bullizimi përkufizohet si transmetimin e çdo komunikimi elektronik tekstual, vizual, të shkruar ose gojor me qëllimin keqdashës dhe të qëllimshëm për të detyruar, abuzim, munduar ose frikësuar një person. Në të vërtetë, perveç fajit edhe qëllimi është përgjithësisht një komponent themelor i ligjit penal. Për të mbajtur dikë penalisht përgjegjës, jo vetëm që duhet të vërtetojmë se personi ka kryer

35 Ligji Nr.2/2017 "Për Sigurinë Kibernetike".

36 Delaware State Code. (2014). Education, Free Public Schools, § 4112D School Bullying Prevention.

37 Louisiana State Legislature. (2014). La. Rev. Stat. § 14:40.7 Cyberbullying

një veprim të padrejtë e në kundërshtim me ligjin, por se ai ose ajo e ka bërë këtë me "*mens rea*"[38], pra me faj.

KONKLUZIONE

Përpjekjet për të luftuar sulmin kibernetik dhe bullizmin në internet vazhdojnë të zhvillohen, me nisma dhe strategji të reja që shfaqen për të adresuar këto çështje. Disa iniciativa të kohëve të fundit që synojnë parandalimin dhe luftimin e sulmeve kibernetike dhe bullizmit në internet paraqiten si më poshtë:

1. Duhen krijuar mekanizma të përmirësuar të raportimit në internet: Platformat e mediave sociale, faqet e internetit dhe komunitetet online po përmirësojnë sistemet e tyre të raportimit dhe moderimit. Përdoruesit mund të raportojnë më lehtë përmbajtje abuzive dhe platformat po investojnë në teknologji për të identifikuar dhe hequr shpejt përmbajtjen e dëmshme.
2. Reformat ligjore: Disa shtete po zbatojnë ose përditësojnë ligje për të trajtuar në mënyrë më efektive cyber-bullying dhe cyber-stalking. Këto reforma mund të rezultojnë në dënime më të ashpra për shkelësit dhe rritje të mbrojtjes ligjore për viktimat.
3. Fushata të ndërgjegjësimit publik: Qeveritë, organizatat jofitimprurëse dhe grupet e avokimit duhet të bëjnë fushata ndërgjegjësimi publik për të edukuar njerëzit rreth rreziqeve të ngacmimit kibernetik dhe sulmit kibernetik, si dhe se si të mbrohen dhe të mbështesin viktimat.
4. Edukimi për qytetarinë dixhitale: Shkollat dhe institucionet arsimore duhet të bëjnë fushata për edukimin e qytetarisë dixhitale në kurrikulat e tyre. Kjo i ndihmon studentët të mësojnë sjellje të përgjegjshme në internet dhe përdorimin etik të teknologjisë.
5. Mbështetje e Shëndetit Mendor: Organizatat e shëndetit mendor duhet të ofrojnë burime dhe mbështetje për ata që preken nga

38 Faji në kuptimin penal

ngacmimi kibernetik dhe sulmi kibernetik, duke njohur ndikimin psikologjik që këto veprime mund të kenë tek viktimat.

6. Trajnimi për ndërhyrjen e "vëzhguesve" nëpërmjet iniciativave për të inkurajuar individët që të bëhen "kalimtarë active" duke ndërhyrë ose raportuar kur ata janë dëshmitarë të bullizmit kibernetik ose sulmit kibernetik.

7. Mjetet e sigurisë në internet: Kompanitë duhet të zhvillojnë dhe promovojnë mjete sigurie në internet, të tilla si cilësimet e privatësisë dhe veçoritë kundër ngacmimit, për të ndihmuar përdoruesit të mbrohen nga ngacmimet dhe ndjekjet.

8. Linjat e ndihmës dhe shërbimet mbështetëse: Linjat e ndihmës, qendrat e krizave dhe shërbimet mbështetëse posaçërisht për viktimat e bullizmit dhe sulmit në internet duhet të krijohen për të ofruar ndihmë dhe udhëzime të menjëhershme.

9. Partneritetet Bashkëpunuese: Palë të ndryshëm të interesuar, duke përfshijnë agjensitë qeveritare, organet e zbatimit të ligjit, kompanitë e teknologjisë dhe grupet e avokimit, për të bashkëpunuar për të zhvilluar strategji gjithëpërfshirëse për të adresuar këto çështje.

10. Kërkimi dhe mbledhja e të dhënave: Hulumtimi i vazhdueshëm ndihmon për të kuptuar më mirë natyrën cyber-bullying dhe cyber-stalking, gjë që nga ana tjetër, informon zhvillimin e masave më efektive parandaluese dhe ndërhyrjeje.

11. Iniciativat e udhëhequra nga të rinjtë: Të rinjtë po marrin një rol aktiv në adresimin e këtyre çështjeve përmes nismave të udhëhequra nga të rinjtë, avokimit dhe programeve të mbështetjes së bashkëmoshatarëve.

12. Bashkëpunimi Ndërkombëtar: Meqenëse cyber-bullying dhe cyber-stalking mund të kalojnë kufijtë ndërkombëtarë, bashkëpunimi ndërkombëtar është gjithnjë e më i rëndësishëm për të adresuar këto probleme në mënyrë efektive.

LITERATURA E PERDORUR

1. "Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying", Sameer Hinduja dhe Justin W. Patchin.
2. "Computers in Human Behavior", "Journal of Cybersecurity", "Cyberpsychology, Behavior, and Social Net-working".
3. "Cyberbullying: Bullying in the Digital Age", Robin M. Kowalski, Susan P. Limber, and Patricia W. Agatston
4. "Cyberstalking: Harassment in the Internet Age and How to Protect Your Family", Paul Bocij.
5. "Hate Crimes in Cyberspace", Danielle Keats Citron.
6. "Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress", Nancy E. Willard.
7. Besag, V. (1989). Bullies and Victims in Schools. Milton Keynes, UK: Open University Press.
8. California Penal Code (1872). https://leginfo.legislature.ca.gov/faces/codesTOCSelected.xhtml?tocCode=PEN&tocTitle=+Penal+Code+-+PEN.
9. Crick, N. (1996). "The Role of Relational Aggression, Overt Aggression, and Prosocial Behavior in the Prediction of Children's Future Social Adjustment." Child Development 67, 2317–2327.
10. Crick, N., & Grotpeter, J. (1995). "Relational Aggression, Gender, and Social-Psychological Adjustment." Child Development 66, 710–722.
11. Delaware State Code. (2014). Education, Free Public Schools, § 4112D School Bullying Prevention.
12. Ericson, N. (2001). "Addressing the Problem of Juvenile Bullying." OJJDP Fact Sheet, 27. Washington, DC: US Department of Justice, Office of Justice Programs, Office of Juvenile Justice and

Delinquency Prevention.

13. F. van der Wal, M., & M. de Wit, C., & Hirasing, R. (2003). "Psychosocial Health Among Young Victims and Offenders of Direct and Indirect Bullying." Pediatrics 11, 1312–1317.
14. Gladden, M., & Vivolo-Kantor, A., & Hamburger, M., & Lumpkin, C. (2014). Bullying
15. Hawker, D., & Boulton, M. (2000). "Twenty Years' Research on Peer Victimization and Psychosocial Maladjustment: A Meta-Analytic Review of Cross-Sectional Studies." Journal of Child Psychology and Psychiatry 41, No. 4, 441–445.
16. Hinduja, S. & Patchin, J. W. (2015). Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying (2nd Ed.). Thousand Oaks, CA: Sage Publications.
17. Kodi Penal i Republikës së Shqipërisë.
18. Leckie, B. (1997). "Girls, Bully Behaviours and Peer Relationships: The Double Edged Sword of Exclusion and Rejection." Presented at Annual Conference of Australian Association for Research in Education, Brisbane, Australia.
19. Ligj Nr.2/2017 "Për Sigurinë Kibernetike".
20. Ligji Nr. 9669, datë 18.12.2006, i ndryshuar.
21. Limber, S., & Nation, M. (1998). "Bullying Among Children and Youth." In Combating Fear and Restoring Safety in Schools, edited by June L. Arnette and Marjorie C. Walsleben. Office of Juvenile Justice and Delinquency Prevention (1998).
22. Louisiana State Legislature. (2014). La. Rev. Stat. § 14:40.7 Cyberbullying.
23. Manning, M., & Heron, J., & Marshal, T. (1978). "Style of Hostility and Social Interactions at Nursery, at School, and at Home: An Extended Study of Children." In Aggresion and Antisocial Behavior in Childhood and Adolescence, edited

by Lionel A. Hersov, M. Berger, and David R. Shaffer, 29–58. Oxford: Pergamon.

Minnesota Department of Education. (2014). "Bullying and Cyber-Bullying." http://education.state.mn.us/MDE/StuSuc/SafeSch/BullyiCyberBullyPrev/index.html.

Nansel, T., & Overpeck, M., & Pilla, R., & Ruan, J., & Simons-Morton, B., & Scheidt. P. (2001). "Bullying Behaviors Among U.S. Youth: Prevalence and Association With Psychosocial Adjustment." Journal of the American Medical Association 285, No. 16: 2094–2100.

Olweus, D. (1978). Aggression in the Schools. Bullies and Whipping Boys. Washington, DC: Hemisphere Press.

Olweus, D. (1990). "Bullying Among School Children." In Health Hazards in Adolescence, 259–297. Berlin: De Gruyter.

Olweus, D. (1993). Bullying at School. Oxford, UK: Blackwell.

Olweus, D., & Limber, S., & Mihalic, S. (1999). "Bullying Prevention Program." In Fight Crime: Invest in Kids. Blueprints for Violence Prevention: Book Nine, edited by Delbert S. Elliott. Boulder, CO: Center for the Study and Prevention of Violence.

Prinstein, M., & Boergers, J., & Vernberg, M. (2001). "Overt and Relational Aggression in Adolescents: Social-Psychological Adjustment of Aggressors and Victims." Journal of Clinical Psychology 30, 479–491.

Rigby, K., & Slee, P. (1993). "Dimensions of Interpersonal Relating Among Australian School Children and Their Implications for Psychological Well-Being." The Journal of Social Psychology 133, no. 1, 33–42.

Roland, E. (1980). Terror i skolen. Stavanger, Norway: Rogaland Research Institute.

24. Roland, E. (1989). "Bullying: The Scandinavian Research

Tradition." In Bullying in Schools, edited by Delwyn P. Tattum and David A. Lane, 21–32. Stroke-on-Trent, UK: Trentham.

25. Sharp, V. (1995). "How Much Does Bullying Hurt? The Effects of Bullying on the Personal Well-Being and Educational Progress of Secondary Aged Students." Educational and Child Psychology 12, 81–88.
26. Slee, P., & Rigby, K. (1993). "The Relationship of Eysenck's Personality Factors and Self-Esteem to Bully-Victim Behaviour in Australian School Boys." Personality and Individual Differences 14, 371–373.
27. Surveillance Among Youths: Uniform Definitions for Public Health and Recommended Data Elements.
28. Tattum, D. (1989). "Violence and Aggression in Schools." In Bullying in Schools, edited by Delwyn P. Tattum and David A. Lane, 17–19. Stroke-on-Trent, UK: Trentha.
29. Wolke, D., & Woods, S., & Bloomfield, L., & Karstadt, L. (2000). "The association Between Direct and Relational Bullying and Behaviour Problems among Primary School Children." Journal of Child Psychology and Psychiatry 41, No. 8, 989–1002.

Dr. Ivas Konini

CYBERCRIME INVESTIGATION

TABLE OF CONTENTS

ABSTRACT

As we navigate the digital age, cybercrimes have become a growing concern, challenging traditional methods of law enforcement. This research paper sheds light on the world of cyber investigation, aiming to explore its significance in tackling modern-day crimes that occur in the virtual realm.

In a nutshell, cyber investigation involves unraveling the mysteries of cybercrimes, understanding how they occur, and identifying those responsible. By using a mix of research methods, we've delved into official crime data, reports from law enforcement agencies, and government statistics to grasp the true extent and nature of cybercrimes.

Through our study, we've come to realize that cybercrimes are more prevalent than ever before, posing unique challenges for law enforcement agencies. To combat these ever-evolving threats effectively, it's crucial for them to strengthen their expertise in cyber investigation.

Our findings highlight the pressing need for collaboration between public and private sectors to tackle cybercrimes as a unified force. This joint effort can lead to more efficient and successful outcomes.

In conclusion, understanding cybercrimes and the significance of cyber investigation is vital in protecting individuals and organizations from the perils of the digital world. By advancing our knowledge and improvement of the methodologies, we can better prevent, investigate, and resolve cybercrimes, ensuring a safer and more secure society for everyone. Therefore, it is imperative for all stakeholders to invest in strengthening the capabilities and capacities of cybercrime investigation to effectively combat the evolving cyber threats.

Keywords: Cybercrime, Criminology, Artificial Intelligence, Law Enforcement, Albania.

Author: IVAS KONINI*

*Dr. Ivas Konini is an effective lecturer at the Department of Criminal Law of the Faculty of Law - University of Tirana (Albania). She is skilled in Criminal Law, Penology and Criminology, Criminal Justice and Legal Research. She has completed her doctoral studies on Eavesdropping. She is an active lawyer. During her career she has also worked at the Police Academy, Faculty of Public Security and Crime Investigation, Department of Criminal Law. She is the author of scientific works and publications in the criminal field.

Email: ivas.konini@fdut.edu.al

1. INTRODUCTION

In our fast-paced digital world, technology has opened up new opportunities for criminals to exploit vulnerabilities, leading to a surge in cybercrimes. These digital offenses pose significant threats to individuals, businesses, and governments, as well as to international peace and stability, and they have a major social and economic impact, prompting the field of criminology to recognize the critical importance of cyber investigation in tackling these emerging challenges and in maintaining law and order in the digital sphere.

This research paper delves into the realm of criminology, focusing on the essential role of cyber investigation, highlighting its importance, methodologies, challenges, and future perspectives. We aim to explain why cyber investigation has become so vital in countering the ever-evolving landscape of cybercrimes.

Traditional crime-fighting methods fall short when dealing with intricate digital offenses. Cyber investigation has emerged as an indispensable tool, combining criminology, computer science, and cybersecurity expertise to combat these modern-day crimes effectively[1]. We want to highlight how cyber investigation enhances our

1 Maimon, D. and Louderback, E. R. (2019). Cyber-dependent crimes: an

ability to detect, investigate, and prosecute cybercriminals, ultimately safeguarding our digital ecosystem[2].

Addressing cybercrimes requires international cooperation and collaboration between law enforcement agencies and other stakeholders. By understanding the challenges involved, we can develop effective strategies and policies to tackle this ever-growing threat. We also explore the potential impact of cyber investigation on broader crime prevention and law enforcement. Equipped with advanced data analytics and cutting-edge technologies, cyber investigation has the power to revolutionize how we combat cyber threats.

In conclusion, our research aims to contribute to criminology's knowledge, specifically focusing on cyber investigation. By understanding its significance, methodologies, and potential outcomes, we hope to pave the way for a safer and more secure digital future. This knowledge can guide policymakers, law enforcement agencies, and academics in their efforts to protect our digital realm from malicious actors.

2. LITERATURE REVIEW

The evolution of cybercrime investigation has been shaped by the rapid advancement of technology and the increasing sophistication of cybercriminals. Early literature on cybercrime investigation primarily focused on traditional investigative techniques, such as digital forensics and network analysis (Goodman, 2010). Digital forensic techniques, tools, and methodologies are related to the collection and analysis of electronic evidence from digital devices and networks. The integration of digital forensics in the investigative process has proven crucial in identifying cybercriminals, preserving evidence, and ensuring the

interdisciplinary review. *Annual Review of Criminology, 2(1)*, 191-216.

2 Wu, W., Harrou, F., Bouyeddou, B., Senouci, S., & Sun, Y. (2021). A stacked deep learning approach to cyber-attacks detection in industrial systems: application to power system and gas pipeline systems. *Cluster Computing, 25(1)*, 561-578.

admissibility of digital evidence in legal proceedings (Casey, 2011). However, as cybercriminals have become more adept at exploiting technological vulnerabilities, the literature has shifted towards more advanced investigative techniques, such as machine learning and artificial intelligence (Chen, 2018).

These studies highlight the potential of AI and machine learning in cybercrime investigation. AI-based tools can assist in analyzing large datasets, detecting patterns of cyberattacks, and automating certain aspects of digital forensics (Kosba et al., 2016). Machine learning algorithms can aid in identifying anomalies and predicting potential cyber threats, enhancing the speed and accuracy of investigations.

The literature acknowledges the challenges faced by law enforcement agencies and investigators in cybercrime cases, including the rapidly evolving nature of cyber threats, the global and cross-border aspects of cybercrimes, encryption and anonymization techniques used by cybercriminals, and the lack of standardized investigative procedures (Kshetri, 2010). Therefore, it is important to focus on the frameworks and initiatives that facilitate effective cooperation among nations in combating cybercrimes (Broadhurst, 2019).

3. METHODOLOGY

The research involved a thorough analysis using a comprehensive approach with two main steps for gathering data:

1. Analyzing the current state of cyber investigation, examining the methods, techniques, and tools used worldwide[3] and in Albania to combat cybercrime.

2. Tailoring cybercrime investigation practices to the Albanian context, with an emphasis on utilizing Artificial Intelligence, machine

3 Javed, A., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. (2022). A comprehensive survey on computer forensics: state-of-the-art, tools, techniques, challenges, and future directions. *Ieee Access, 10*, 11065-11089.

learning, and international collaboration. This approach is expected to have a broad impact, including the following benefits[4]:

- Making cybercrime investigations in Albania better by using modern technology and global best practices.
- Making the police and cybersecurity experts in the country more skilled.
- Encouraging countries to work together and share information to prevent cybercrimes.
- Creating a safer online space in Albania, so people trust it more and it helps the country's online business.
- Helping the world be safer online by sharing what we know.
- Adapting a multi-dimensional approach to combating cybercriminal activities, thereby reducing their impact on individuals and organizations in Albania.

The following Figure, presents the steps of the research for this report:

Figure 1 - Research process

In addition, the methodology is based on the following questions:

a. Which is the importance of research in cybercrime investigation?

b. Which are the most common forms of cyber-crime and emerging trends and tactics used by cybercriminals in conducting cyber-crime?

c. How can investigators accurately identify and locate

4 Velasco, C. (2022, February 22). Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum*.

cybercriminals considering the anonymous nature of the internet?

d. Which are the techniques and methods used by investigators to ensure the accurate collection, preservation, and interpretation of digital evidence?

e. How can the application of Artificial Intelligence (AI) techniques contribute to the identification and understanding of patterns, behaviors, and indicators associated with a criminal mind in the context of cyber investigation within criminology?

f. How can digital evidence be effectively presented in court to ensure its admissibility and reliability in cybercrime prosecutions?

g. What are the key differences and similarities between cybercrime investigation in the private sector versus law enforcement agencies, and how can knowledge-sharing between these sectors be improved?

Cybercrime investigation methodologies have undergone significant evolution over the years. Traditional approaches, such as digital forensics, involve the collection and analysis of digital evidence to identify and prosecute cybercriminals[5]. However, these methods can often be time-consuming and demand substantial technical expertise. Consequently, recent literature has explored the utilization of automated techniques, such as machine learning and artificial intelligence, to enhance the efficiency and effectiveness of cybercrime investigations[6]. These automated methods employ algorithms to analyze vast amounts of data and detect patterns that may indicate cybercriminal activity

Considering the impact that cybercrime has on the society especially their increase in the recent years makes it a challenging task

5 Casey, E. (2011, April 12). Digital Evidence and Computer Crime. *Academic Press*. Retrieved October 16, 2023 from Digital Evidence and Computer Crime: Forensic Science, Computers, and the ... - Eoghan Casey - Google Books

6 Chen, C. (2018). Cybercrime Investigation Methodologies: Machine Learning & Artificial Intelligence.

for the investigators on identifying and locating cybercriminals due to the anonymous nature of the internet adding also the fact that technology evolves, so do the methods used by cybercriminals. As traditional crimes even cybercrime has their own techniques and tools to track down and apprehend cybercriminals. Cybercrime investigations often require specialized skills, extensive resources, and time. Moreover, legal and jurisdictional challenges can complicate the process, especially when dealing with international cases.

The strategies or techniques used so far are as follows:

i. **Digital Forensics[7]:** The digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information to reconstruct past events. This can include examining compromised systems, network logs, and other digital artifacts to uncover clues about the identity and location of the attacker. The content is most often for the usage of data in a court of law, though digital forensics can be used in other instances.

ii. **IP Address Tracking[8]**: Cybercriminals often use various tools and techniques to hide their IP addresses. However, skilled investigators can still trace these addresses back to the source, providing valuable information about the attacker's location. Tracing an IP address involves finding the device that an IP address was assigned to at a specific time, the location of the device and the user of the device at that specific time. IP tracing is an important aspect used in tracking the name and location of Cybercriminals.

---

7 RecFaces. (n.d.). *Digital Forensics*. Retrieved October 16, 2023, from What Is Digital Forensics: Process, Tools, and Types | Computer ForensicsOverview | RecFaces

8 CANDDi. (2020, September). *IP Tracking: The Ultimate Guide*. Retrieved October 16, 2023, from https://www.canddi.com/blog/2020/09/ip-tracking/

iii. **Malware Analysis**[9]: Malware analysis is the study of the unique features, objectives, sources, and potential effects of harmful software and code, such as spyware, viruses, advertising, and ransomware. If a cybercriminal uses malware to conduct their attacks, experts can analyze the malware to identify patterns, signatures, or other clues that may help identify the author or the source of the attack. The malware analysis is compiled by 4 stages: static properties analysis, interactive behavior analysis, fully automated analysis and manual code reversing.

iv. **Honeypots**[10]: A honeypot is a security mechanism that creates a virtual trap to lure cyber attackers and detect, deflect and study hacking attempts to gain unauthorized access to information systems. Setting up honeypots or decoy systems that attract cybercriminals can help investigators gather information about the attacker's methods and potentially their location. Large enterprises and companies involved in cybersecurity research are common users of honeypots to identify and defend against attacks from advanced persistent threat (APT) actors.

v. **Social Engineering**[11]: Social engineering refers to all techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons. Law enforcement agencies may use social engineering techniques to gather information about suspects. This might involve pretending to be the victim of a cyberattack and engaging with the attacker to obtain information.

vi. **Cooperation with ISPs and Hosting Providers**[12]: Investigators

9 Fortinet. (n.d.). *Malware Analysis*. Retrieved October 16, 2023, from What is Malware Analysis? Types and Stages of Malware Analysis | Fortinet

10 Fortinet. (n.d.). *What Is Honeypot?* Retrieved October 16, 2023, from What Is a Honeypot? Meaning, Types, Benefits, and More | Fortinet

11 IBM. (n.d.). *Social Engineering*. Retrieved October 16, 2023, from What is Social Engineering? | IBM

12 TechTarget. (n.d.). *ISP (Internet Service Provider).* Retrieved October 16, 2023, from What is an Internet Service Provider (ISP)? - WhatIs.com (techtarget.com)

can collaborate with internet service providers (ISPs) and hosting providers to obtain information about users who may have been involved in criminal activities. ISPs may provide subscriber information, which can lead to identifying the user behind a specific IP address.

vii. **International Cooperation**[13]: Many cybercriminals operate across borders. International cooperation among law enforcement agencies is essential for tracking down and apprehending cybercriminals. The international cooperation does not consist only of providing support on specific cases but also organizations like Interpol, Europol etc. define policies which aim to boost countries for cyber defense capabilities and strengthen coordination and cooperation between the military and civilian cyber communities.

viii. **Open Source Intelligence (OSINT)**[14]**:** Open-Source Intelligence (OSINT) is defined as intelligence produced by collecting, evaluating and analyzing publicly available information with the purpose of answering a specific intelligence question. Investigators can use publicly available information from social media, forums, and other online sources to gather information about cybercriminals. Sometimes, cybercriminals reveal information about themselves inadvertently.

13 United Nations Office on Drugs and Crime (UNODC). (2019). *International Cooperation on Cybersecurity Matters*. Retrieved October 16, 2023, from Cybercrime Module 8 Key Issues: International Cooperation on Cybersecurity Matters (unodc.org)

14 SANS Institute. (n.d.). *What Is Open Source Intelligence?* Retrieved October 16, 2023, from What is OSINT (Open-Source Intelligence?) | SANS Institute

Different entities and professionals use these techniques for various purposes related to cybercrime prevention and investigation:

- **Sting Operations**[15]:
  - *Law Enforcement Agencies*: Police and other law enforcement agencies use sting operations to catch cybercriminals in the act. They set traps or decoys to lure criminals into revealing their identity or engaging in illegal activities.
  - *Security Experts*: Some cybersecurity professionals may collaborate with law enforcement in setting up sting operations to identify and apprehend cybercriminals. They often specialize in ethical hacking and digital forensics.
- **Behavioral Analysis**[16]:
  - *Cybersecurity Experts*: Security professionals, including threat analysts and researchers, use behavioral analysis to detect abnormal or malicious behavior within computer networks. They employ machine learning and artificial intelligence algorithms to identify potential threats.
  - *Law Enforcement:* Behavioral analysis can also be used by law enforcement to profile the behavior of cybercriminals. This can help in understanding their modus operandi and motives.
- **Encryption and Anonymity Services**[17]:
  - *Cybercriminals*: Many cybercriminals use encryption and

15 Hay, B. L. (2005). Sting Operations, Undercover Agents, and Entrapment. *Missouri Law Review, 70.*

16 Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020, April 21). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity, 3(1).*

17 National Institute of Justice. (2020). *Taking on the Dark Web: Law Enforcement Experts ID Investigative Needs.* Retrieved October 16, 2023, from Taking on the Dark Web: Law Enforcement Experts ID Investigative Needs | National Institute of Justice (ojp.gov)

anonymity services to hide their activities and identities, making it difficult for law enforcement to trace them. They use these services to carry out illicit activities, such as communicating about cyberattacks or selling stolen data.

- *Cybersecurity Experts and Law Enforcement*: Cybersecurity professionals and law enforcement agencies work to counter the use of encryption and anonymity services by cybercriminals. They may employ experts in cryptography and digital forensics to decrypt communications and uncover vulnerabilities in these services. This is crucial for tracking and prosecuting cybercriminals.

These methods are part of a broader effort to combat cybercrime and protect individuals, organizations, and nations from online threats. Sting operations and behavioral analysis help identify and catch cybercriminals, while efforts to address encryption and anonymity services aim to mitigate the tools they use to evade law enforcement.

4. CYBERCRIME LANDSCAPE: GLOBAL TRENDS AND IMPACT

4.1. The Present State of Cybercrime on a Global and Albanian Scale

Cybercrime, as digital offenses, poses significant threats to society. The timely detection, investigation, and punishment of cybercriminals hold a crucial place in the realm of law enforcement. The characteristics of cybercrime set it apart from traditional criminal cases in various ways, including the methods used to commit the crime, the time it takes to discover it, the types of victims targeted, the legal foundations, clue discovery, and case filing[18].

18 Nicholls, J., Kuppa, A., & Le-Khac, N. (2021). Financial cybercrime: a comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access, 9,* 163965-163986.

The research outcomes are expected to contribute to the advancement of cybercrime investigation practices within the Albanian context. This effort focuses on harnessing the capabilities of Artificial Intelligence, machine learning, and collaborative international efforts. This framework is projected to have a multifaceted impact, including improvements in investigation techniques, on-site assessment and protection, evidence collection and preservation, evidence analysis, legal identification, and legal procedures.

A cybercrime investigation involves the process of scrutinizing, analyzing, and recovering digital evidence from devices such as computers, cellphones, automobile navigation systems, video game consoles, or other networked devices found at the scene of a crime. This evidence assists cybercrime investigators in identifying the individuals responsible for cybercrimes and understanding their intentions.

According to the FBI's Internet Crime Complaint Center and Norton PNC Insights, the most frequently reported cybercrimes in the United States include phishing, extortion, identity theft, debit and credit card fraud, and personal data breaches. In Europe, as reported by the European Union Agency for Cybersecurity, the most common types of cyber threats are ransomware attacks, phishing attempts, and malware incidents[19].

The COVID-19 pandemic situation put online security to the test worldwide. Social distancing measures led to an increase in people's online presence for maintaining personal and professional relationships. Unfortunately, this situation was exploited by hackers and malicious actors, resulting in a surge in cybercrimes[20].

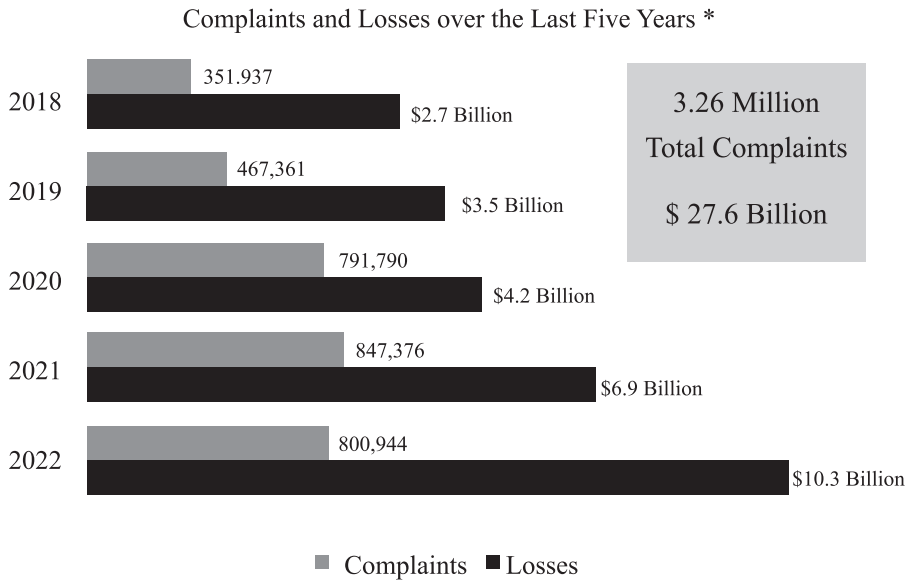
According to Internet Crime Complaint Crime[21] report the

19 Iqbal, F., Fung, B. C. M., Debbabi, M., Batool, R., & Marrington, A. (2019). Wordnet-based criminal networks mining for cybercrime investigation. *IEEE Access, 7*, 22740-22755.

20 Naidoo, R. (2020). A multi-level influence model of covid-19 themed cybercrime. *European Journal of Information Systems, 29(3)*, 306-321.

21 Retrieved October 16, 2023, from Cybercrime Statistics Worldwide - 2023 -

ICS3[22] has received an average of 652,000 complaints per year. These complaints address a wide array of Internet scams affecting victims across the globe.



Also referring to same institution data (IC3) report the top five crime types for the last 5 year are tech support scams[23], extortion[24], nonpayment/non delivery[25], personal data breach[26], phishing,[27]. It shows clearly that phishing is the most applied cybercrime.

Cybersecurity For Me

22 Retrieved October 16, 2023, from 2022_IC3Report.pdf

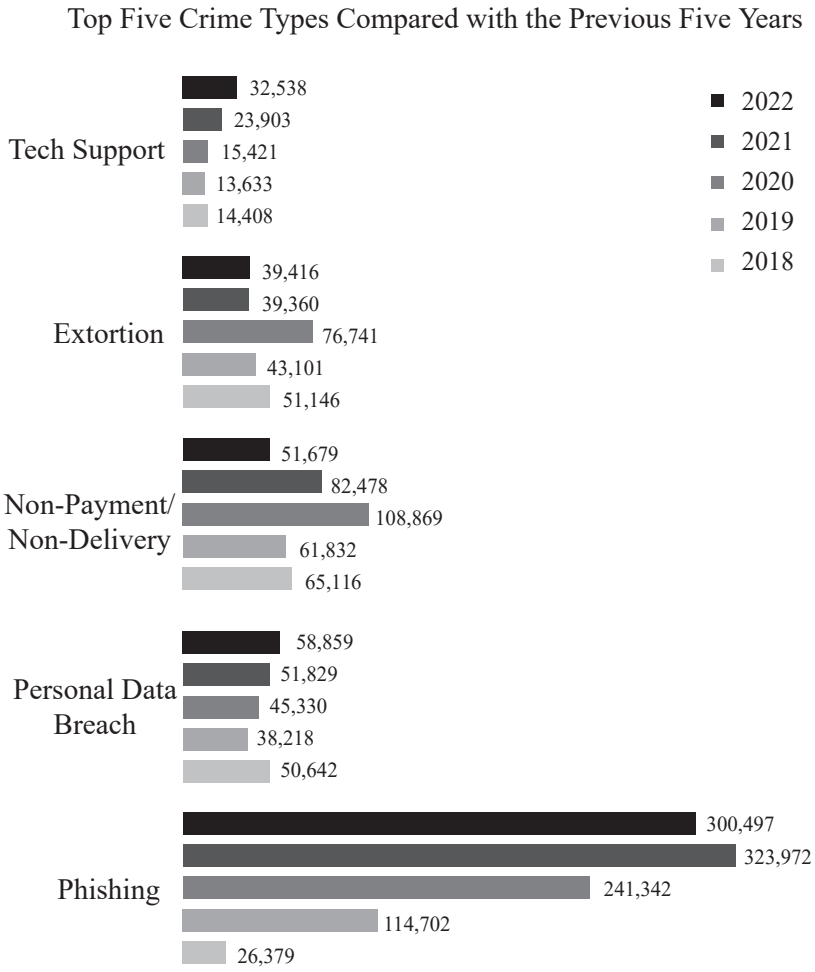
23 Tech support scams are fraudulent activities in which scammers pose as legitimate technical support representatives and use social engineering and fear tactics to persuade victims to pay for fictitious computer problems.

24 Cyber extortion is a type of cybercrime in which a hacker illegally accesses an organization's sensitive data or systems and then demands money in return for allowing the organization to either regain control or stop the attack.

25 It is a type of cybercrime in which a victim pays for goods or services but does not receive them, or a seller ships goods but does not receive payment.

26 A personal data breach is a security incident in which sensitive, protected, or confidential data is accessed, viewed, stolen, or used by an unauthorized individual or entity.

27 Phishing is a cybercrime where scammers use social engineering and fear tactics to trick individuals into revealing sensitive data, banking details, and passwords.



As reported by the Council of the EU and the European Council, the top cyber threats in EU[28] are:

a) ransomware attacks,

b) Distributed Denial of Service (DDoS) attacks,

c) malware,

d) social engendering threats,

e) threats against data's,

28 Retrieved October 16, 2023, from Top cyber threats in the EU - Consilium (europa.eu)

f) internet threats,

g) disinformation /misinformation

h) supply chain attacks.

If we refer to the most recent Internet Organized Crime Threat Assessment (IOCTA)[29], near EUROPOL, cybercrime is becoming more aggressive and confrontational across various form of it, including high-tech crimes, data breaches and sexual extortion.

So, as per Internet Organized Crime Threat Assessment (IOCTA), the cybercriminals have expanded their illicit activities, including:

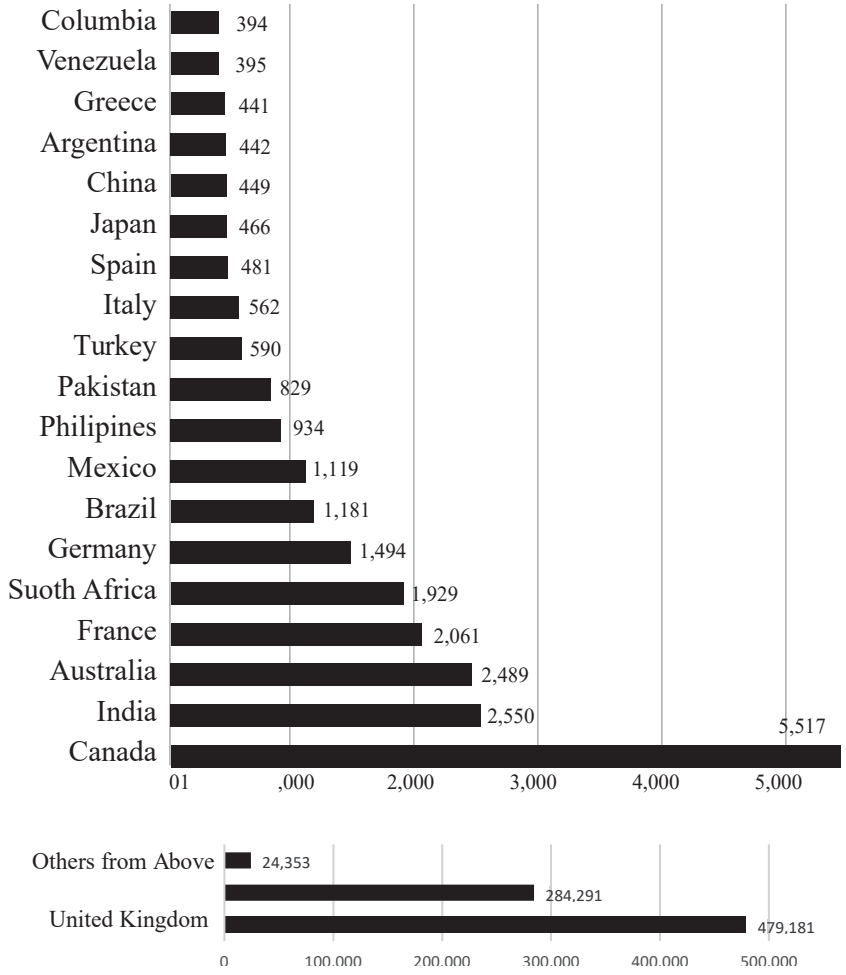
- using botnets—networks of devices infected with malware without their users' knowledge—to transmit viruses that gain illicit remote control of the devices, steal passwords and disable antivirus protection;
- creating "back doors" on compromised devices to allow the theft of money and data, or remote access to the devices to create botnets;
- creating online fora to trade hacking expertise;
- bulletproof hosting and creating counter-anti-virus services;
- laundering traditional and virtual currencies;
- committing online fraud, such as through online payment systems, carding and social engineering;
- various forms of online child sexual exploitation, including the distribution online of child sex-abuse materials and the live-streaming of child sexual abuse
- the online hosting of operations involving the sale of weapons, false passports, counterfeit and cloned credit cards, and drugs, and hacking services.

In this analysis, we delve into the most prevalent cyberattacks and crimes in Europe and the USA. Additionally, we emphasize the critical need to understand the distribution of cyberattack victims worldwide.

29 Retrieved October 16, 2023, from Cybercrime | Europol (europa.eu)

Specifically, we explore which countries have experienced the highest number of victims.

Furthermore, we present data obtained from the FBI's Internet Crime Report 2022, which indicates that the United States and the United Kingdom have the highest count of victims of cyber-attacks. Conversely, countries such as Colombia, Venezuela, and Greece have the lowest count of victims.



In another dataset published by Statista[30] and AAG[31], which examines the prevalence of cyber-attacks and crimes, with a specific focus on the distribution of victims across different countries, the findings are as follows:

1. **Global Cybercrime Trends[32]**:

- **Phishing Attacks**: Phishing remains the most common form of cybercrime globally. In 2021, **323,972 internet users** reported falling victim to phishing attacks, accounting for half of all data breach victims.
- **Email Exposure**: Nearly **1 billion emails** were exposed in a single year, affecting **1 in 5 internet users**.
- **Ransomware Threat**: Ransomware attacks continue to pose a serious threat. Around **236.1 million ransomware attacks** were reported worldwide in the first half of 2022

2. **Countries with High Cybercrime Rates[33]**:

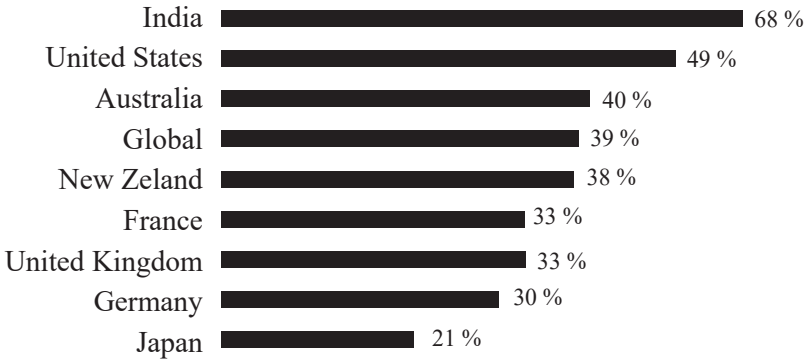
- India**: India stands out as the country with the highest cybercrime encounter rate. Nearly** 70% of Indian respondents **claimed to have ever experienced cybercrime.**
- United States**:Approximately** 49% of U.S. respondents **reported experiencing internet crime.**
- Australia**: Around** 40% of Australian internet users **fell victim to cybercrime.**
- United Kingdom**: Roughly** 33% of UK respondents **reported suffering from cyber attacks**

30 Statista is a statistics portal that provides market data, consumer survey results, and industry studies.

31 AAG stands for American Airlines Group, which is a publicly traded holding company.

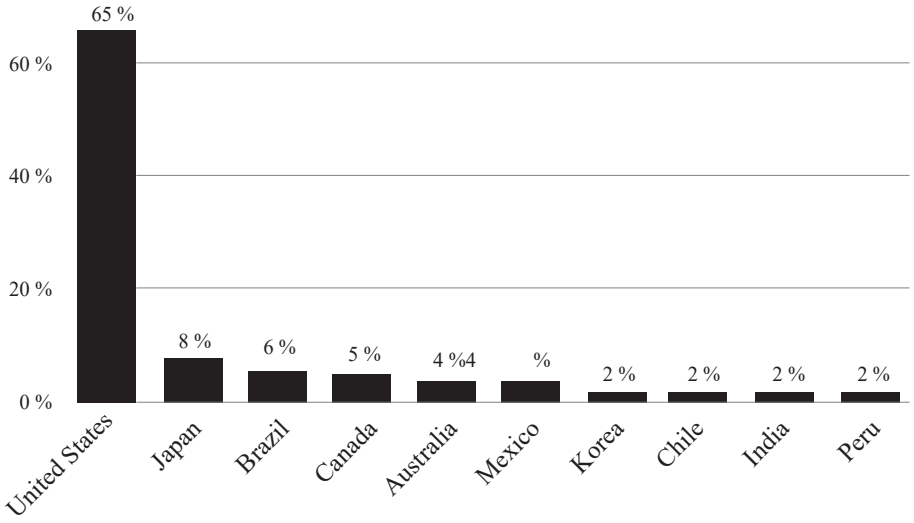
32 Retrieved October 16, 2023, from The Latest Cyber Crime Statistics (updated January 2024) | AAG IT Support (aag-it.com)

33 Retrieved October 16, 2023, from Cybercrime rate by country 2022 | Statista



3. Countries Most Targeted by Cyber Attacks[34]:

- United States**: A significant** 65% of detected cyber-attacks **worldwide targeted U.S. organizations.**
- Japan**: Japan ranked second, targeted by approximately** 8% of the attacks**.**
- Brazil**: Brazil came in third, with** 6% of the attacks**.**



34 Retrieved October 16, 2023, from Cyber attacks most targeted countries 2022 | Statista

4. Cybersecurity Awareness and Action[35]:

The rising threat globally has prompted organizations to take cybersecurity seriously, **73%** of Small and medium-sized businesses recognize the need for action, with **78%** planning to increase investment in cybersecurity in the next 12 months

As a response to cybercriminal activity, each state has its own institution or agency responsible for combating cybercrime and takes its own measures. Determining the countries with the strongest cybersecurity can be subjective and may vary based on different criteria and assessments. However, several countries are often recognized for their robust cybersecurity capabilities, even though the cybersecurity landscape is dynamic and rankings may change over time.

As a trusted reference that measures countries' commitment to cybersecurity on a global scale, the **Global Cybersecurity Index** [36](GCI) assesses each country's level of development or engagement across five pillars:

- Legal Measures
- Technical Measures
- Organizational Measures
- Capacity Development
- Cooperation

The GCI aggregates these dimensions into an overall score, providing a comprehensive view of cybersecurity efforts worldwide as per International Telecommunication Union.

Notably, the United States, United Kingdom, and Saudi Arabia have demonstrated strong commitment to cybersecurity.[37]

---

35 Retrieved October 16, 2023, from The Latest Cyber Crime Statistics (updated January 2024) | AAG IT Support (aag-it.com)

36 Retrieved October 16, 2023, from Global Cybersecurity Index (itu.int)

37 Retrieved October 16, 2023, from Index page for Global Cyber Security Index | Composite Indicators & Scoreboards Explorer (europa.eu)

Another index used to measure the cyber security of the countries is **GRWI (Global Risk and Well-Being Index[38])** to assess the appeal of remote work in 66 countries. This index provides insight for comparing countries in terms of cybersecurity, digital infrastructure, cybercrime threat response and legal measures.

According to the GRWI, the best countries in terms of cybersecurity include:

- Slovakia
- Lithuania
- Germany
- Estonia

Greece

The **National Cyber Security Index (NCSI)** is a global measure that assesses the preparedness of 160 nations in preventing cyber threats and effectively managing cyber incidents. Each country's

38 Retrieved October 16, 2023, from The World's Most Cybersecure Countries (And How To Protect Yourself When You're Not In One) (forbes.com)

performance is evaluated based on a variety of available data, including criteria such as crisis management planning, cybersecurity legislation, and educational and professional development. This comprehensive index serves as both a database of publicly available evidence materials and a valuable tool for enhancing national cyber security capabilities.

The top 10 cyber-secure countries according to the NCSI:[39]

Rank	Country	National Cyber Security Index	Digital Development Level	Difference
1.	Belgium	94.81	74.07	20.74
2.	Lithuania	93.51	67.34	26.17
3.	Estonia	93.51	75.59	17.92
4.	Czech Republic	90.91	69.21	21.70
5.	Germany	90.91	80.01	10.90
6.	Romania	89.61	59.84	29.77
7.	Greece	89.61	64.02	25.59
8.	Portugal	89.61	68.46	21.15
9.	United Kingdom	89.61	79.96	9.65
10.	Spain	88.31	72.21	16.10

The cybercrime in Albania, despite the fact that it has a low weight compared to other crimes, specifically 0.99% of the total number of criminal proceedings registered nationwide, has its own importance considering also that there is an increase in their trend compared to the year 2021, which was 0.81%.

The crime coefficient per 100,000 inhabitants for this group of offenses in 2022 was 9.13, while in 2021 it was lower, or 8.16%.

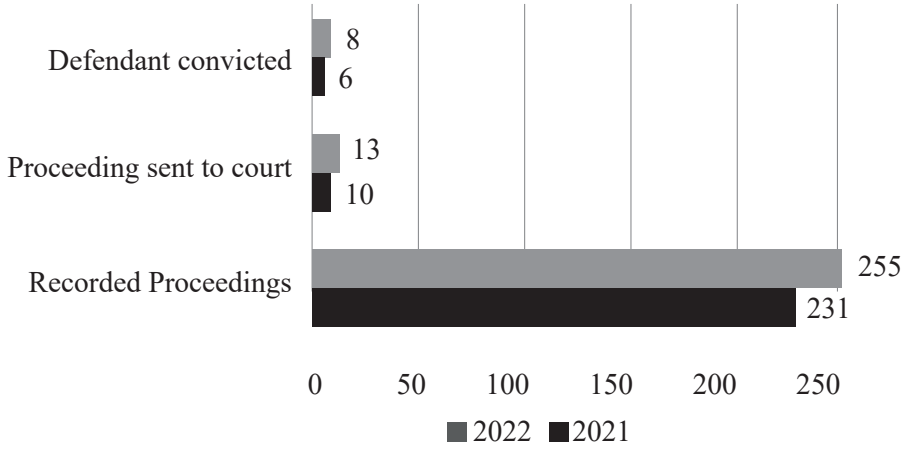
From the statistical data according to the Report of the General Prosecutor on the State of Crime in Albania[40], it appears that in 2022 the

39 Retrieved October 16, 2023, from NCSI :: Ranking (ega.ee)

40 Retrieved October 16, 2023, from Microsoft Word - Raporti Vjetor kriminaliteti 2022-Kuvendit Prokuroria e Pergjithshme.docx (pp.gov.al)

number of registered proceedings has increased by 10.39% compared to the previous year. There is an increase in the number of proceedings sent to the court, from 10 proceedings in 2021 to 13 proceedings sent to court in 2022, or 30%, and an increase in the number of defendants convicted of criminal offenses against computer crime, from 6 in 2021 to 8 in 2022, or 33.33%.

Graphically, the cybercrime trend for 2022 compared to 2021 is presented as follows:



The types of cybercrime recorded in Albania are:

Computer fraud[41]

From the statistical data in 2022, there is an increasing trend of 23.94% of proceedings registered for the criminal offense provided for by Article 143/b of the Criminal Code "Computer Fraud", compared to 2021.

Computer forgery[42]

From the statistical data, it can be observed that the number of

41 Computer fraud involves illegal activities like phishing, social engineering, viruses, and DDoS attacks, which disrupt service or access user funds through computers and the internet.

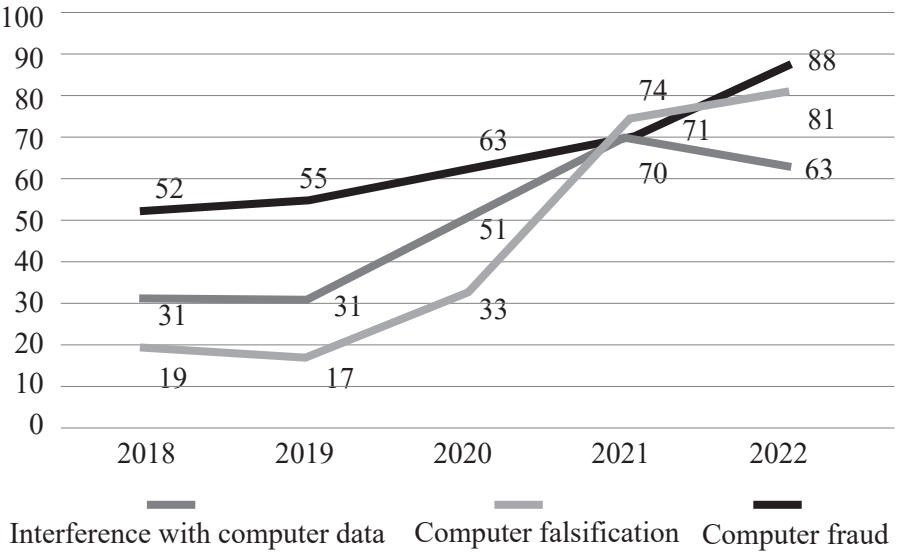
42 Computer forgery involves altering, erasing, or suppressing computer data or programs in a manner that would constitute forgery if committed against a traditional object.

proceedings registered in 2022 for the criminal offense provided for by Article 186/a of the Criminal Code, "Computer forgery", has increased by 9.46%

Interference with computer data[43]

From the statistical data, it can be observed that the number of proceedings registered in 2022 for the criminal offense provided for by Article 293/b of the Criminal Code, "Interference with computer data", has decreased by 10%.

The progress of these criminal offenses in five years, 2018-2022 is presented in the following chart (criminal proceedings registered at the prosecutor's office):



5. TYPES OF CYBERCRIMES

Cybercrime is vastly growing in the world of tech today. Criminals of the World Wide Web exploit internet users' personal information for their own gain. They dive deep into the dark web to buy and sell illegal

43 Interference with computer data refers to the intentional or reckless alteration, deletion, deterioration, or suppression of computer data without right, hindering system functioning.

products and services. They even gain access to classified government information[44].

Cybercrimes are at an all-time high, costing companies and individuals billions of dollars annually. What's even more frightening is that this figure only represents the last 5 years with no end in sight. The evolution of technology and increasing accessibility of smart tech means there are multiple access points within users' homes for hackers to exploit. While law enforcement attempts to tackle the growing issue, criminal numbers continue to grow, taking advantage of the anonymity of the internet[45].

What is Cybercrime?

Cybercrime is defined as a crime where a computer is the object of the crime or is used as a tool to commit an offense. A cybercriminal may use a device to access a user's personal information, confidential business information, government information, or disable a device. It is also a cybercrime to sell or elicit the above information online.

Cybercrimes can generally be divided into two categories[46]:

- **Crimes that target networks or devices;**
- **Crimes that target individuals or data.**

Mostly, the emerging trends and tactics used by cybercriminals in conducting cyber-crime are:

i. **Double Extortion Ransomware[47]:** In addition to encrypting data, cybercriminals are increasingly stealing sensitive information

44 Guinchard, A. (2008). Cybercrime: the transformation of crime in the information age. *Information Communication & Society, 11(7)*, 1030-1032.

45 Bossler, A. M. and Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. Policing: An International Journal of Police Strategies &Amp; *Management, 35(1)*, 165-181.

46 Powerhouse Forensics. (n.d.). *Intellectual property theft: What is intellectual property theft?* Retrieved December 5, 2023, from What is Cybercrime? Types, Prevention & Digital Forensics | EC-Council (eccouncil.org)

47 Zscaler. (n.d.). *What Is Double Extortion Ransomware?* Retrieved October 16, 2023, from What Is Double Extortion Ransomware? | Zscaler

before deploying ransomware. They then threaten to release the data unless a ransom is paid. These attacks can disrupt critical infrastructure and organizations. According to the European Council of European Union the 60% of affected organizations by this cyberattack may have paid ransom demands[48], whereas in 2022, as per the Federal Bureau of Investigation's Internet Crime Report, the Internet Crime Complaint Center (IC3) received 2,385 complaints related to ransomware. These incidents resulted in adjusted losses totaling over $34.3 million.

ii. **Distributed Denial-of-Service (DDoS)**. This attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. This can disrupt websites and online services. According to the European Council of European Union this form of cybercrime in July 2022 was recorded as the largest attack against European customers[49].

iii. **Malware[50]**, short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware. According to the European Council of European Union in June 2022 alone, adware trojans were downloaded around 10 million times[51].

---

48 Consilium. (n.d.). *Top Cyber Threats in the EU*. Retrieved October 16, 2023, from Top cyber threats in the EU - Consilium (europa.eu)

49 Akamai. (2022, July 21). *Largest European DDoS Attack Ever Detected*. Retrieved October 16, 2023, from Largest European DDoS Attack on Record | Akamai

50 Malwarebytes. (n.d.). *Malware*. Retrieved October 16, 2023, from https://www.malwarebytes.com/malware

51 Consilium. (n.d.). *Top Cyber Threats in the EU*. Retrieved October 16, 2023, from Top cyber threats in the EU - Consilium (europa.eu)

iv. **Social engineering**[52]is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. Phishing is one of the most common forms of social engineering attacks which involve the use of deceptive emails or websites to trick individuals or organizations into revealing sensitive information, such as login credentials or financial details. According to the European Council of European Union studies the 82% of data breached involved a human element[53].

v. **Data Breaches**[54]**:** Data breaches occur when unauthorized individuals gain access to sensitive data to manipulate and interfere with the behavior of the system. This can lead to the exposure of personal information, trade secrets, or financial data. As per the European Council of European Union studies the 90% of attacks are against the servers[55].

vi. **Web-based threats, or online threats**[56], are a category of cybersecurity risks that may cause an undesirable event or action via the internet. Web threats are made possible by end-user vulnerabilities, web service developers/operators, or web services themselves. These attacks have an impact on the availability of the internet like GDP (Border Gateway Protocol) border hijacking. According to the European Council of European Union in June 2022, 15% of the internet infrastructure

52 Proofpoint. (n.d.). *Social Engineering*. Retrieved October 16, 2023, from What Is Social Engineering? - Definition, Types & More | Proofpoint US

53 Consilium. (n.d.). *Top Cyber Threats in the EU*. Retrieved October 16, 2023, from Top cyber threats in the EU - Consilium (europa.eu)

54 IBM. (n.d.). *Data Breach*. Retrieved October 16, 2023, from What is a Data Breach? | IBM

55 Consilium. (n.d.). *Top Cyber Threats in the EU*. Retrieved October 16, 2023, from Top cyber threats in the EU - Consilium (europa.eu)

56 Kaspersky. (n.d.). *Web Threats*. Retrieved October 16, 2023, from What are web threats and online Internet threats? (kaspersky.com)

in Ukraine has been destroyed by Russia[57].

vii. **Disinformation and misinformation[58]**. An international attack of creating or sharing false and misleading information to manipulate public opinion. Mass disinformation campaigns were already targeting Ukraine before Russia launched its invasion as per European Council of European Union information.

viii. **Supply Chain attacks[59]**. A supply chain attack is a type of cyberattack carried out against an organization's suppliers as a means to gain unauthorized access to that organization's systems or data. According to European Council of European Union data the supply chain incidents accounted for 16% of intrusion for 2020 and 17% for 2021[60].

ix. **Intellectual Property (IP) Theft[61]**: IP theft includes the unauthorized use or theft of intellectual property, including copyrighted content, patented technology, and trade secrets.

6. CYBERCRIME INVESTIGATION AND PRIVACY

6.1. What is Cybercrime investigation

Cybercrime investigation is a process with multiple components that aims to find and stop illegal activities that happen online. At its

57 Consilium. (n.d.). *Top Cyber Threats in the EU*. Retrieved October 16, 2023, from Top cyber threats in the EU - Consilium (europa.eu)

58 EU DisinfoLab. (n.d.). *Why Disinformation is a Cybersecurity Threat*. Retrieved October 16, 2023 Why Disinformation is a Cybersecurity Threat - EU DisinfoLab

59 Investopedia. (n.d.). *Supply Chain Attack*. Retrieved October 16, 2023, from Supply Chain Attack: What It is, Example (investopedia.com)

60 Consilium. (n.d.). *Top Cyber Threats in the EU*. Retrieved October 16, 2023, from Top cyber threats in the EU - Consilium (europa.eu)

61 Powerhouse Forensics. (n.d.). *Intellectual Property Theft: What Is Intellectual Property Theft?* Retrieved October 16, 2023, from What Is Intellectual Property Theft? Understanding IP Theft (powerhouseforensics.com)

core, it uses specialized methods and tools to get around the difficulties of crimes committed on computer networks, the internet, and other digital platforms. With this project, the main goal is to gather strong evidence that can be used in court to find and prosecute people who commit cybercrimes[62].

Cybercrime investigations consist of:

- *Digital forensics*[63] is like a detective for the digital world. It's all about carefully collecting, looking at, and keeping electronic evidence, and it's super important for investigating cybercrimes. Imagine investigators using special tools to check digital stuff like computers, phones, and other devices to find important information related to a cybercrime. This step is crucial because it helps build a strong case and ensures there's a clear path showing who has the evidence.

  In simpler terms, digital forensics is all about gathering, analyzing, and keeping digital evidence to investigate and stop cybercrimes or other bad activities. It's like a digital detective that helps law enforcement, cybersecurity experts, and legal teams understand how cyber threats happen and catch people involved in cybercrimes.

- *Incident response*[64] includes the quick steps that are taken to contain and lessen the effects of a cyber incident. Responders work quickly to figure out what happened, shut down any systems that are affected, and put plans in place to stop the damage from getting worse. To respond to incidents effectively, many people

62 Cybercrime Investigations - Law Enforcement Cyber Center. (2018, January 3). *Law Enforcement Cyber Center*.
Retrieved October 16, 2023, from
Cybercrime Investigations - Law Enforcement Cyber Center (iacpcybercenter.org)

63 EC-Council. (2023, August 30). *What is Digital Forensics | Phases of Digital Forensics.* Retrieved October 16, 2023, from What is Digital Forensics | Phases of Digital Forensics | EC-Council (eccouncil.org)

64 IBM. (n.d.). *Incident Response*. Retrieved October 16, 2023, from What is incident response? | IBM

must work together, such as IT teams, legal authorities, and cybersecurity experts who know what they're talking about.

Incident response is like a well-organized plan that organizations use to deal with and reduce the impact of security problems, especially those linked to cybercrimes. This plan includes different steps[65]:

a) finding out what happened;

b) stopping the issue from getting worse;

c) getting rid of the problem;

d) getting things back to normal

e) learning from what happened.

In the world of crime investigations, this response plan is very important for dealing with cyber-related crimes.

In an incident response, the main aim is to figure out if a security problem, like a cyberattack or data breach, has really happened. This might mean keeping a close eye on computer systems, checking logs, and paying attention to alerts from security tools. Once they know what's going on, the next step is containment, where they quickly try to stop the problem from spreading more, like isolating affected systems or stopping harmful activities.

The eradication part is about completely getting rid of the threat and fixing the weaknesses that caused the problem, so it doesn't happen again. After that, the recovery step focuses on bringing things back to normal and making sure everything is secure to reduce downtime and go back to regular business activities.

In criminal investigations, incident response is like a superhero helping law enforcement collect important information and save evidence. It helps build a strong case against the bad guys by tracking where the attack came from, understanding how it happened, and collecting proof that can be used in legal situations.

65 Cisco. (n.d.). *Incident Response Plan.* Retrieved October 16, 2023, from What Is an Incident Response Plan for IT? - Cisco

Another important part of incident response is "lessons learned." This means looking back after an incident to see what can be improved in the response process. By learning from each incident, organizations and law enforcement enhance their security measures, so they're ready to handle and reduce future problems.

- *Malware analysis*[66] is critical tool in the world of cybersecurity, where investigators take apart malicious software, often referred to as malware, to understand its inner workings. The main goal is to figure out how these harmful programs, which can cause damage to computer systems, networks, and data, operate and where they come from. Cybersecurity professionals carefully dissect and examine malware, aiming to identify its characteristics, behavior, and the vulnerabilities it exploits. This knowledge is crucial for developing effective ways to counteract malware and strengthen overall cybersecurity defenses.

There are two main[67] approaches to malware analysis:

- Static analysis: investigators study the code and structure of the malware without actually running it. This approach provides insights into how the program is put together, its logic, and potential functionality
- Dynamic analysis. dynamic analysis involves running the malware in a controlled environment, like a sandbox, to observe how it behaves in real-time. This helps analysts understand the malware's capabilities and uncover any hidden functions that might not be apparent through static analysis alone.

66 Baker, K. (2023, April 17). Malware Analysis: Steps & Examples. *CrowdStrike*. Retrieved October 16, 2023, from Malware Analysis: Steps & Examples - CrowdStrike

67 DifferenceBetween.net. (n.d.). *Difference Between Static Malware Analysis and Dynamic Malware Analysis*. Retrieved October 16, 2023, from Difference Between Static Malware Analysis and Dynamic Malware Analysis | Difference Between

Malware analysis is a key player in cybersecurity investigations, aiding in the detection of cyber threats, responding to incidents, and developing strategies to proactively defend against future attacks. When a cybersecurity incident, like a malware infection, occurs, analysts use malware analysis to assess the extent of the threat and plan strategies to contain and remove the malicious software. Moreover, the insights gained from malware analysis contribute to creating updated antivirus signatures, rules for intrusion detection systems (IDS)[68], and other security measures to prevent similar malware from compromising systems in the future.

- *Network forensics* is a specialized field in cybersecurity that focuses on monitoring, analyzing, and investigating network traffic and activities to uncover evidence related to cybercrimes. Imagine it as a detailed check-up of network logs, packets, and digital info to understand the events leading to a cyber incident. The goal is to spot any suspicious or bad activities within the network.

In cybercrime investigations, network forensics is a big help:

- Firstly, it helps in spotting unauthorized access, data breaches, or any bad activities in the network. By checking how data moves through the network and looking for unusual patterns, investigators can find potential threats and weaknesses.
- Secondly, network forensics helps in understanding the tricks used by cybercriminals. Investigators can create a timeline of events, like how the attacker got in, moved around the network, and took sensitive data. This info is crucial to fully understand the cyberattack and figure out who's behind it.

68 An Intrusion Detection System (IDS) is a digital security guard for computer networks. It watches network traffic for signs of cyber threats, sounding an alarm if it detects anything suspicious. IDS tools can be software on computers, dedicated devices, or even work in the cloud, protecting data and systems online. In simple terms, an IDS is like a watchful guard keeping the digital space safe.

Network forensics is also a hero in incident response[69]. When a security incident happens, investigators use network forensics tools to quickly figure out what's going on, stop the threat, and reduce the damage. It's like a quick and smart response to cybercrimes using tools and methods, like deep packet inspection, log analysis, intrusion detection systems (IDS), and network traffic analysis tools. These tools help investigators recreate network activities, find bad behaviors, and collect evidence for legal actions.

To sum it up, network forensics gives us a peek into network activities, offers evidence to understand and respond to cybercrimes, and keeps our computer networks safe from evolving cyber threats.

- *Cyber threat intelligence*[70] is like a guide for cybersecurity, helping organizations gather, analyze, and understand information about potential cyber threats. It's a tool that reveals the tactics[71], techniques[72], and procedures[73] (TTPs) used by cyber adversaries, empowering organizations to detect, prevent, and respond to cyber threats effectively. Essentially, it gives insights into the ever-changing world of cybersecurity, helping organizations make informed decisions to safeguard their systems and data. Cyber threat intelligence is a proactive

69 GeeksforGeeks. (2022). *What is Network Forensics?* Retrieved October 16, 2023, from What is Network Forensics? - GeeksforGeeks

70 Splunk. (2023). *TTP (Tactics, Techniques, Procedures).* Retrieved October 16, 2023, from What Are TTPs? Tactics, Techniques & Procedures Explained | Splunk

71 Think of tactics as the big picture plans that cyber bad actors have. It's like their overall strategy, such as trying to sneak into a system, steal information, or cause trouble with online services

72 Techniques are like the specific tricks they use to carry out these plans. For example, if their tactic is trying to get into a system, their techniques could include things like finding and exploiting weak points in software or tricking people with fake emails.

73 Procedures are the detailed step-by-step guides they follow during an attack. It's like their playbook. Understanding these helps cybersecurity experts spot patterns and signs of trouble, making it easier to defend against these digital bad guys.

force, providing information about new threats and weaknesses, allowing investigators to stay ahead of cybercriminals' evolving methods and strategies.

In cybersecurity investigations, this intelligence is a treasure trove of information about specific threats, the actors behind them, and the methods they use. It includes details about malware, vulnerabilities, and indicators of compromise (IoCs). Analyzing this intelligence helps investigators spot patterns, identify trends, and assess potential risks to their systems.

One of the crucial roles of cyber threat intelligence in cybersecurity investigations is in proactive threat detection. Organizations use this intelligence to identify potential threats before they turn into major attacks. Early detection allows for a swift response and effective mitigation, minimizing the impact of cyber incidents.

Moreover, when a cybersecurity incident happens, investigators turn to threat intelligence to understand the attack's nature, motivations, and the specific techniques employed by threat actors. This information guides the development of response strategies, including identifying compromised systems, containing the threat, and facilitating recovery efforts[74].

Cyber threat intelligence contributes significantly to overall cybersecurity strength. By staying informed about emerging threats and vulnerabilities, organizations can proactively implement security measures, update defenses, and patch vulnerabilities to prevent potential attacks.

To obtain cyber threat intelligence, organizations monitor various sources such as open-source intelligence, dark web forums, industry reports, and information shared within the cybersecurity community. This collected intelligence is then carefully analyzed and put into context, providing actionable insights for cybersecurity investigations

74 CrowdStrike. (2023). *Threat Intelligence*. Retrieved October 16, 2023, from What is Cyber Threat Intelligence? [Beginner's Guide] (crowdstrike.com)

and defense strategies.

As a result, cyber threat intelligence is a vital component of cybersecurity investigations, offering organizations valuable information to comprehend, anticipate, and respond to cyber threats. By harnessing this intelligence, cybersecurity professionals can stay ahead of adversaries, fortify their defenses, and reduce the risks associated with the dynamic and complex landscape of cyber threats.

6.2. What is privacy?

The right to privacy is a fundamental human right that allows individuals to keep their personal information and activities private. It means that people have the right to control who gets their personal details and to be free from unwanted intrusions. It is protected by various international[75] and national[76][77][78] laws,

75 *European Convention of Human Rights*,Art.8 Right to respect for private and family life
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others
European Convention on Human Rights (coe.int)

76 *The Constitution of Republic of Albania*: Article 5
The Republic of Albania applies international law binding on it.
*On October 2, 1996, Albania ratified the European Convention on Human Rights, thereby obligating our country to adhere to the provisions of Article 8 of the Convention. Kushtetuta-2017.pdf (klp.al)

77 Penal Code of Republic of Albania, Art.121 Unlawful Interference in Private Life Installation of devices serving for listening or recording of words or images, listening, recording or transmitting of words, fixation, recording or transmitting of images, as well as the storage for publication or the publication of this data that expose an aspect of the private life of the person without his consent, constitutes a criminal offense and is punishable by a fine or imprisonment for up to two years. kodi_penal_2016_1033.pdf (pp.gov.al)

78 *Law No. 9887, dated 10.3.2008, "On Personal Data Protection"*

protocols[79] and treaties[80] emphasizing the importance of safeguarding individuals from unnecessary interference.

In simple terms, the right to privacy ensures that individuals can decide what information about them is collected, used, and shared. This protection is especially important today with the rise of technology, which can easily access and share personal data. Privacy rights help maintain a balance between personal freedom and the need for protection.

People have the right to be protected from unauthorized surveillance, searches, and access to their personal data. This right is essential for promoting individual freedom, allowing people to express themselves without fear of unnecessary scrutiny. It also supports the development of personal identity.

However, it's crucial to understand that the right to privacy is not absolute. In certain situations, like matters of national security or public safety, there may be limitations to privacy rights. Striking a balance between protecting individual privacy and addressing collective interests is an ongoing challenge that requires careful consideration and adherence to legal principles.

The right to privacy is a vital human right that ensures individuals have control over their personal information, promoting autonomy and freedom in a world where technology can easily access and share data.

Microsoft Word - LDP english version amended_2014.docx (privacyconference2019.info)

79 *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Art. 2:
The purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy.
CETS 223 - Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (coe.int)

80 *Council of Europe Convention on Access to Official Documents*
CETS 205 - Council of Europe Convention on Access to Official Documents (coe.int)

6.3. Cybercrime investigation and the right to privacy

The relationship between cybercrime investigation and the right to privacy is complex, as law enforcement uses digital tools and surveillance methods to track cybercriminals[81]. However, these actions can potentially interfere with individuals' privacy rights, leading to ethical and legal concerns. Privacy is a fundamental human right protected by international and national laws, and cybercrime investigations must strike a balance between protecting privacy and maintaining public safety. To ensure privacy rights are not violated, safeguards like legal warrants, due process, and data collection must be implemented. Clear rules governing surveillance technologies and oversight mechanisms should be in place to prevent misuse and accountability. International cooperation is crucial in tackling cybercrimes while respecting privacy rights.

6.3.1. The positive aspect of this relationship

The connection between cybercrime investigations and the right to privacy can have positive aspects, promoting both security and individual freedoms[82]. Here are some positive elements:

- Boosting Online Safety: Effective cybercrime investigations make the online world safer. By looking into and stopping cybercrimes, authorities can protect people and organizations from digital dangers, making sure the internet is a secure place.
- Guarding People and Society: Cybercrime investigations are crucial for shielding individuals and society from online threats

81 Office of the United Nations High Commissioner for Human Rights (OHCHR). (2022, September). Spyware and surveillance: Threats to privacy and human rights growing - *UN report*. Retrieved October 16, 2023, from Spyware and surveillance: Threats to privacy and human rights growing, UN report warns | OHCHR

82 Hoven van Genderen, R. (2008). Cybercrime investigation and the protection of personal data and privacy. *Council of Europe*. Retrieved October 16, 2023, from HOVEN_VAN_GENDEREN_Octopus_2008 (coe.int)

like identity theft, fraud, and cyberattacks. This helps keep the public safe and maintains trust in digital systems.

^ Global Teamwork: When countries work together on cybercrime investigations, it promotes global cooperation. Sharing information and resources allows for a stronger response to cyber threats worldwide, creating a joint effort to protect digital spaces.

^ Setting Legal Examples: Cybercrime investigations often involve legal processes that set examples for future cases. These examples help create clear rules, ensuring that investigations follow the law and respect privacy rights.

^ Advancing Technology: Dealing with cybercrime challenges leads to technological advancements. As investigators adapt, new tools and methods emerge, improving not only investigations but also digital security as a whole.

^ Stopping Future Crimes: Successful cybercrime investigations can discourage potential offenders and prevent future crimes. Knowing that there are consequences for cybercrimes acts as a deterrent, making the digital world safer.

^ Public Awareness and Education: Cybercrime investigations raise awareness about online threats and the importance of digital safety. This knowledge empowers people to take steps to protect their online privacy.

^ Balancing Rights: Finding the right balance between cybercrime investigation and the right to privacy can result in guidelines that protect both. Clear rules ensure that investigations are done responsibly, reducing the risk of privacy violations.

6.3.2. The impact of cybersecurity investigations on privacy

The intersection of cybersecurity investigations and the right to privacy demands a delicate balance. On one side, these investigations are crucial for keeping our digital world safe from cyber threats. But on the other side, the techniques used can sometimes step on people's privacy toes.

When cybersecurity investigators do their job, they need a bunch of data to understand cyber threats. This data often comes from online sources, digital communications, and network activities. While the goal is to boost security, there's a challenge in finding the right balance between effective investigations and respecting people's privacy[83].

Surveillance is a common tool in cybersecurity. Keeping an eye on online activities helps spot potential threats. But too much surveillance can feel like someone peeking into your private space. People wonder if this monitoring is really necessary and if it's fair in the quest for cybersecurity without sacrificing individual privacy rights[84].

Sharing information is very important for global cybersecurity efforts[85]. Teaming up among different groups and nations can make us stronger against cyber threats. But it's crucial to make sure that shared information is handled responsibly to avoid invading people's privacy. Having clear laws and standards on how sensitive data is exchanged becomes really important.

Laws[86] also play a big role in making sure cybersecurity

83 Verma, A. K., & Ramanathan, K. (2021). *Data privacy preservation in digital forensics investigation*. Retrieved October 16, 2023, from Data privacy preservation in digital forensics investigation | AIP Conference Proceedings | AIP Publishing

84 Kowalski, R. (2017). Ethical and legal implications of internet surveillance. *Journal of Information Privacy and Security, 13(2),* 69-79.

85 Carlin, A. P. (2018). Sharing Cyber Threat Information in International Context. *Arizona Law Review, 60(2),* 387-438

86 Vasenina, I. A., & Selivanov, M. A. (2019). Legal and organizational portrayal of cyber-threats: concerns and possibilities. *Journal of Cybersecurity, 5(1),* 1-22.

investigations don't overstep privacy boundaries. Good laws provide checks and balances, making sure investigations stick to ethical standards and respect people's privacy rights. Having clear rules helps legitimize cybersecurity practices.

It's not just about laws; it's also about making sure people know what's going on. *Educating the public*[87] about why certain investigative measures are needed for everyone's safety helps build understanding. Being transparent about why and how cybersecurity investigations happen can get public support, even if it means some impact on individual privacy.

Ethics[88] matter a lot. Following ethical standards in cybersecurity investigations is a must to keep any negative impact on privacy in check. Being responsible and ethical in practices helps manage cyber threats effectively while also respecting people's rights.

Technology[89] is in the mix too. Using advanced tools in cybersecurity can make things better, but we need to be careful about how these technologies might affect privacy. Balancing the benefits of technology with the need to protect privacy is a big deal.

The link between cybersecurity investigations and the right to privacy is tricky. Finding that sweet spot between keeping our digital world safe and respecting people's privacy needs a careful approach. It's about keeping an eye on ethics, having good laws, making sure people know what's happening, and using technology responsibly in the world of cybersecurity.

---

87 Taylor, K. & Richardson, B. (2018). Educating the Next Generation of Cybersecurity Professionals. *Journal of Cybersecurity Education, Research and Practice, 1(1),* 21-31.

88 Georgiev, T. (2018). Disruptive Technologies and Ethical Challenges in Cybersecurity. Innovation, Entrepreneurship and Digital Ecosystems. *Springer Proceedings in Business and Economics*, pp 57-73.

89 Kanjolia, R., & Mookerjee, V. S. (2020). Privacy Respecting Technologies for Cybersecurity: *A Survey*

6.3.3. The negative aspect of this relationship

Here are some of the negatives of the relationship between cybersecurity investigations and privacy[90]:

- Too Much Monitoring: Sometimes, advanced technologies used for cybersecurity investigations can watch and collect more information than needed. This might make people feel like they are being surveyed all the time, even when they haven't done anything wrong.
- Mistakes in Data: While gathering data for cybersecurity, there's a chance of getting wrong or unreliable information. Depending on this kind of data can lead to investigations that are not correct, making innocent people look guilty and non-necessarily invading their privacy.
- Going Beyond the Plan: Cybersecurity investigations might start small but sometimes grow into something bigger, collecting more data than needed. This can mean getting information about people's lives that has nothing to do with the original reason for the investigation.
- Making People Afraid to Speak Up: Strict cybersecurity measures, especially watching what people do online, might make individuals scared to express their thoughts or do certain actions online. This fear of being watched can affect people's right to privacy and freedom of speech.
- Not Enough Protection for Shared Data: Cybersecurity investigations often involve sharing data with other groups. Without strong protection rules, this shared data might not be kept safe, putting people's privacy at risk.
- Accidentally Treating People Unfairly: The tools and technologies used in cybersecurity can unintentionally treat different groups

90 Shilton, K., & Farnham, S. D. (2019). Engaging with Privacy in Cybersecurity Threat Reporting. *The Information Society*

of people unfairly. If these tools are not designed carefully, they might focus more on certain types of people, making existing biases worse and threatening equal privacy for everyone.

- Keeping Data for Too Long: Holding onto data collected during cybersecurity investigations for a long time can be a privacy risk. If it's not managed well, keeping personal information for too long makes it more likely for someone to access or use it without permission, harming people's privacy.

Addressing these negatives requires a commitment to ethical practices[91], including regular audits[92], clear guidelines on data retention[93], and continuous efforts to minimize the unintended consequences[94] of

91 Ethical cybersecurity practices are crucial for protecting individual privacy. Transparency, accountability, informed consent, data minimization, fair practices, accuracy, robust security safeguards, and training programs are essential. These practices align with human rights standards, respecting privacy, freedom of expression, and protection from discrimination. By adopting these ethical principles, organizations maintain security while upholding privacy rights, fostering trust in the digital realm.

92 Regular audits in cybersecurity investigations involve systematic reviews of data collection and management processes to ensure compliance with ethical standards, legal regulations, and organizational policies. They help identify potential vulnerabilities and shortcomings, promote continuous improvement, and maintain a balance between cybersecurity measures and privacy protection. Regular audits enhance accountability and transparency in cybersecurity investigations, allowing organizations to address issues proactively.

93 Setting up a structured framework for cybersecurity investigations requires clear rules on how long to keep data. Taking into account legal, regulatory, and moral concerns, these guidelines spell out how long and under what conditions different types of data should be kept. They help stop storage that isn't needed, cut down on data breaches, and are in line with privacy principles. They spell out types of data and how long they should be kept, stressing how important it is to only store as much as is needed for investigations. Making sure there are clear rules encourages responsible data management, openness, and following privacy laws, which builds trust with people who are involved in cybersecurity investigations.

94 To minimize the unintended impacts of cybersecurity investigations on individual privacy, it is crucial to continuously improve methods and stay updated on new ways to protect privacy. This includes ongoing training for professionals, assessing risks and impacts, and maintaining open communication

cybersecurity investigations on individual privacy.

7. ARTIFICIAL INTELLIGENCE IN CRIMINAL INVESTIGATION

7.1. The usage of Artificial Intelligence in criminal investigation

In modern times Artificial Intelligence (AI) has impacted the field of criminal investigation, enhancing the efficiency and effectiveness of law enforcement processes[95]. Here's a brief introduction on how AI tools are/can be utilized in criminal investigations:

A. COMPAS (Correctional Offender Management Profiling for Alternative Sanctions)

COMPAS, is a software program used in the criminal justice system. The term "COMPAS" is commonly associated with a specific tool developed by a company called Northpointe (now known as Equivant). The software is designed to assess the risk of recidivism (the likelihood of a person reoffending) for individuals within the criminal justice system.

The COMPAS system utilizes various factors, such as criminal history, age, employment status, and substance abuse history, to generate a risk assessment score. This score is intended to assist judges and parole boards in making more informed decisions about sentencing, probation, and parole[96].

---

with privacy groups, legal experts, and the public. Feedback from those affected by investigations and learning from past situations also contribute to improving practices over time. In essence, continuous efforts to minimize unintended consequences involve continuously learning, adapting, and improving cybersecurity investigations while respecting privacy.

95 Atri, A., Kumar, M., Goyal, D., & Choudhary, V. (2020). An overview of artificial intelligence-based techniques used for criminal investigations. *Journal of Ambient Intelligence and Humanized Computing, 12(10)*, 9875-9886

96 Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science, 360(6396),* 243-247

The specific details of how COMPAS works are not publicly disclosed, as the algorithm and its workings are considered proprietary information[97].

However, here is a general overview of how risk assessment tools like COMPAS typically operate[98]:

Scenario: Sentencing Decision

- Defendant Information: A defendant, let's call them John Doe, is convicted of a crime. The court gathers information about John's criminal history, personal details, and other relevant factors.
- Data Input: John's information, including age, previous criminal convictions, employment history, and other pertinent details, is input into the COMPAS system.
- Training the COMPAS Model: The COMPAS model has been previously trained using historical data from individuals with similar profiles. The model has learned patterns associated with recidivism based on various features.
- Risk Assessment: The COMPAS system analyzes John's data and provides a risk assessment, indicating the likelihood of John reoffending within a specific timeframe. The assessment might categorize John's risk as low, medium, or high.
- Sentencing Consideration: The judge, prosecutor, or probation officer considers the COMPAS risk assessment as one factor among others when making decisions about sentencing or probation terms for John Doe.
- Decision Making: The court uses the COMPAS assessment alongside other relevant information to inform decisions. For example, if John is assessed as a high risk, the court might

97 *Bureau of Justice Assistance*. (n.d.) Retrieved October 16, 2023, from COMPAS (ojp.gov)

98 Mattu, J. A. L. K. (2023, December 20). Machine Bias. *ProPublica*. Retrieved October 16, 2023, from Machine Bias — ProPublica

consider a sentence with more emphasis on rehabilitation or supervision.

The use of COMPAS and similar tools has been a subject of controversy. Critics argue that these algorithms may introduce or perpetuate biases, as they are trained on historical data that may reflect existing disparities in the criminal justice system. Concerns have been raised about the potential for these tools to disproportionately impact certain demographic groups.

The ethical implications and potential bias in algorithmic decision-making within the criminal justice system have sparked debates and discussions about the responsible use of such technologies. It underscores the importance of continually evaluating and refining these tools to ensure fairness and justice in their application.

B. PSA (Public Safety Assessment)

The Public Safety Assessment (PSA) is a widely used risk assessment tool employed in the criminal justice system to assist judges in making informed decisions about pretrial release or detention. Developed by the Laura and John Arnold Foundation (now Arnold Ventures)[99], the PSA aims to provide an objective and data-driven approach to evaluating the risk posed by individuals awaiting trial. This tool primarily focuses on two key factors:

- the likelihood of a defendant failing to appear in court,
- the risk of committing new criminal activity if released before trial.

One of the distinguishing features of the PSA is its reliance on specific and objective risk factors. These factors typically include the defendant's criminal history, age at the time of the current offense, and

99 Arnold Ventures. (2021). *Public Safety Assessment*. Retrieved October 16, 2023, from Public Safety Assessment: A Risk Tool That Promotes… | Arnold Ventures

any prior instances of failing to appear in court. By utilizing a data-driven approach, the PSA analyzes large datasets to identify patterns and correlations between these factors and pretrial behavior. The goal is to generate risk assessment scores that categorize individuals into different risk levels, such as low, moderate, or high risk[100].

The information provided by the PSA is intended to inform pretrial decisions, offering judges valuable insights into the potential risks associated with releasing or detaining a defendant. Judges use the risk assessment scores, along with other relevant considerations, to make more informed decisions about the appropriate conditions for pretrial release. This may include imposing specific requirements or monitoring measures, such as electronic monitoring or regular check-ins with pretrial services[101].

While the PSA is designed to enhance fairness and objectivity in pretrial decisions, it has not been without controversy. Critics have raised concerns about the potential for algorithmic bias and the impact on certain demographic groups. Ongoing evaluation, transparency, and adjustments are crucial to addressing these concerns and ensuring that risk assessment tools like the PSA contribute positively to the criminal justice system's goals of fairness and public safety.

C. CNN (Convolutional Neural Network)[102]

The argument about how to tell the difference between criminals and non-criminals in mugshots began when photography was invented.

---

100 Stimson, C. D. (2020, June 8). The First Step Act's Risk and Needs Assessment Program: A Work in Progress. Edwin Meese III Center for Legal & Judicial Studies, Legal Memorandum No. 265. *The Heritage Foundation.* Retrieved October 16, 2023, from LM265_0.pdf (heritage.org)

101 National Institute of Justice. (2021). *The Public Safety Assessment (PSA).* Retrieved October 16, 2023, from Strengthening data-driven pretrial release in New Jersey | National Institute of Justice (ojp.gov)

102 LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature, 521(7553)*, 436-444.

Criminologists like Cesare Lombroso thought that criminals were "throwbacks" who were more like apes than law-abiding citizens. English criminologist Charles Goring, on the other hand, said that there was no statistical difference between criminals and non-criminals, which showed that he was wrong.

An experiment from 2011 at Cornell University showed that people could tell the difference between criminals and normal people just by looking at pictures of them. This is what Xiaolin Wu[103] and Xi Zhang from China's Shanghai Jiao Tong University did. They used machine-vision algorithms to look at the faces of criminals and normal people and tested it to see if it could tell the difference. They took ID pictures of 1856 Chinese men without beards who were between the ages of 18 and 55. Half of these men were criminals.

The researchers trained a convolutional neural network to tell the difference with 90% of these images. They then used the other 10% of the images to test the neural net. The results are scary because the neural network could tell the difference between criminals and normal people 89.5% of the time.

When the neural network sorts faces, it looks at three things[104]:

- The curve of the upper lip: This feature involves measuring the shape or curvature of the upper lip in a facial image. The curvature might be quantified by analyzing the contour or outline of the upper lip, potentially capturing variations in its shape.
- The distance between the inner corners of the eyes: This feature involves measuring the distance between the inner corners of the eyes. The distance might be quantified in pixels or other units,

103 Wu, X., & Zhang, X. (2016). Automated inference on criminality using face images. *IEEE Transactions on Information Forensics and Security, 11(8),* 1792-1806. Retrieved October 16, 2023, from 1611.04135v1.pdf (arxiv.org)

104 Emerging Technology from the arXiv. (2016, November 22). Neural Network Learns to Identify Criminals by Their Faces. *MIT Technology Review.* Retrieved October 16, 2023, from Neural Network Learns to Identify Criminals by Their Faces | MIT Technology Review

providing information about the relative positioning of the eyes in the facial image.

- The 20% smaller angle between two lines drawn from the nose tip to the corners of the mouth: This feature involves measuring the angle formed by two lines: one drawn from the tip of the nose to one corner of the mouth and the other to the opposite corner of the mouth. The angle could be used as a facial feature to capture the orientation or tilt of the mouth in relation to the nose.

Three samples in criminal ID photo set

Three samples in non-criminal ID photo set

The researchers used a simplified parameter space called a manifold to plot the differences in the data from criminal and noncriminal faces. This shows why the difference has been so hard to find. It shows that these datasets are centered, but the criminal faces dataset has a lot more variation. This could be the reason why some statistical tests can't tell the difference between these sets of data.

The most interesting aspect about the 2011 study on facial recognition was that it showed people could tell the difference between criminals and non-criminals just by looking at their faces. They did this without knowing anything about the criminals' pasts[105]. This finding is interesting because it makes us think about:

- The existence of an Inherent Human Ability: The study suggests that people may naturally be able to tell the difference between criminals and non-criminals, even when they are only shown pictures of their faces. This goes against the idea that making such decisions would require clear information about a person's background.
- Nonverbal Cues: The study shows how important some body language and facial expressions may be for sharing information about a person's background or traits. It makes me think that people may use small visual cues to make decisions without even realizing it.
- Base for Automation: The study's results from 2011 probably laid the groundwork for what later researchers like Xiaolin Wu and Xi Zhang built on. This made it possible to use machine-vision algorithms and neural networks to automatically tell the difference between criminals and normal people based on their faces.
- Implications for Ethics and Society: The study brings up important ethical questions about how facial recognition technology could be used in different situations, especially in the criminal justice system. It raises concerns about how this kind of technology could be used on a larger scale, like with photos on passports or driver's licenses, and what might happen if people are automatically marked as possible criminals.

105 McGoogan,C. (2016, November 24). Minority Report-style AI Learns to Predict People Criminals by Facial Features. *The Telegraph*. Retrieved October 16, 2023, from Minority Report-style AI learns to predict if people are criminals from their facial features (telegraph.co.uk)

- Complexity of Human Judgment: The fact that people can tell the difference between people based on their faces makes understanding human judgment even more difficult. It forces researchers and ethicists to look into the complexities of perception, bias, and how these judgments might affect social norms.

The worry[106] is how people might use these machines, since it's easy to see how this process could be used on sets of photos for passports and driver's licenses for the whole country. This would make it possible to catch criminals before they do anything illegal.

This work needs to be put on a much stronger foundation by being done again with people of different ages, genders, races, and with much bigger sets of data. The work makes us think about how we can tell the difference between criminal and normal faces and why criminal faces are so different from normal faces. Researchers shared how they taught a deep-learning machine to look at a picture of someone's face and decide if it was trustworthy in the same way that humans do. This starts a new era of anthropometry[107], whether it's used for wrong reasons or not.

D. Facial recognition Systems

Facial recognition technology has been around for decades. However, in recent years, it has seen more widespread adoption. Why? Artificial intelligence. Advances in deep learning and faster systems for

106 Vilvestre, J. (2016, November 28). Controversial New AI Can Tell Whether or Not You're a Criminal. *Futurism*. Retrieved October 16, 2023, from Controversial New AI Can Tell Whether or Not You're A Criminal (futurism.com)

107 In the context of criminals, anthropometry refers to the measurement and analysis of physical characteristics for identification purposes. While historically significant, traditional anthropometry has been largely replaced by more advanced biometric techniques, such as fingerprinting and DNA analysis, in modern criminal investigations. However, the term may still be used to describe the measurement of various physical features, including facial dimensions, for forensic identification.

processing enormous amounts of data has helped the technology come closer to reaching its full potential. This has led to higher accuracy and faster processing times. Governments and private companies are taking notice. The global market for facial recognition is expected to reach $12.92 billion by 2027[108].

Facial recognition is a biometric tool, as with other commonly used biometric technologies like fingerprint recognition, iris recognition, and finger vein pattern recognition. Facial recognition identifies a person based on specific aspects of their physiology. Though the software can vary, the process of facial recognition tends to follow three basic steps. First, your face is captured with a photo or video. It doesn't matter if you're alone or in a crowd. It can happen in real time. The software then measures a variety of facial features called landmarks or nodal points on the face. These could include the distance between the eyes, the width of the nose, depth of eye sockets, distance from forehead to chin. Each program uses different nodal points and may collect up to 80 different measurements. This information is then converted into a mathematical formula, which represents your unique facial signature. That facial signature is then compared to a database of known faces. This can all happen in a matter of seconds[109].

Facial recognition technology can be traced back[110] to the 1960s[111]. In the 1990s, the U .S. Defense Advanced Research Projects

---

108 Pascu, L. (2020, July 9). Video Surveillance to Drive Biometric Facial Recognition Market to $12.9B by 2027. *Biometric Update*. Retrieved October 16, 2023, from Video surveillance to drive biometric facial recognition market to .9B by 2027 | Biometric Update

109 BBC Newsround. (2020). *What is facial recognition and why are people talking about it?* Retrieved October 16, 2023, from What is facial recognition and why are people talking about it? - BBC Newsround

110 Thales Group. (2023). *History of Facial Recognition*. Retrieved October 16, 2023, from Facial recognition history (thalesgroup.com)

111 A research team led by Woodrow W Bledsoe ran experiments between 1964 and 1966 to see whether 'programming computers' could recognize human faces. The team used a rudimentary scanner to map the person's hairline, eyes, and nose.

Agency[112] and the National Institute of Standards and Technology[113] designed a face recognition program[114] which eventually led to more sophisticated automatic face recognition technology. One early version of this technology was tested at the 2002 Super Bowl, when law enforcement officials scanned the crowd and found several minor criminals. Although that experiment also yielded a high number of false positives[115]. However, the technology blossomed in the 2010s because of rapid developments in artificial intelligence.

By 2014, face recognition systems were being regularly used by police to identify suspects in the field.

However, since its inception, facial recognition has been polarizing. A significant use of facial recognition technology is in the area of safety and security. Law enforcement agencies use it to fight petty crime, help locate missing people, prevent terrorist attacks, and even uncover local criminals. Security checkpoints at airports worldwide are increasingly using such technology to protect flyers and to identify criminals trying to enter the country[116]. The Department of Homeland Security also uses facial recognition to find people who have overstayed visas or who are

112 Abbr. DARPA

113 Abbr. NIST

114 Adjabi, I., Ouahabi, A., Benzaoui, A., & Taleb-Ahmed, A. (2020, July 23). Past, Present, and Future of Face Recognition: A Review. *Electronics, 9(8)*. Retrieved October 16, 2023, from (PDF) Past, Present, and Future of Face Recognition: A Review (researchgate.net)

115 Thornburg,R. (2002). Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses Under the Fourth Amendment, 20 J. Marshall J. Computer & Info. L. 321. *UIC John Marshall Journal of Information Technology & Privacy Law*. Retrieved October 16, 2023, from "Face Recognition Technology: The Potential Orwellian Implications and " by Robert H. Thornburg (uic.edu)

116 Raposo, V. L. (2022, June 1). The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal. *European Journal on Criminal Policy and Research, 29(4),* 515–533. Retrieved October 16, 2023, from The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal | European Journal on Criminal Policy and Research (springer.com)

under criminal investigation[117].

Today, several companies are developing watch lists as a service, using face recognition data platforms to help prevent shoplifting and violent crime. Facial recognition technology is getting faster and more accurate every year. This means that it could also soon be used to make our lives more convenient.

One of the most used AI in facial recognition is Clearview AI[118].

Clearview AI is a facial recognition platform that contains more than 3 billion images from the public internet. It is used by law enforcement agencies to generate investigative leads.

May 2019, Las Vegas, Nevada. A web services provider alerted authorities after a user received images depicting the sexual abuse of a young girl. The only clue was an adult face visible in one image. Investigators turn to Clearview AI. Using this platform, a potential match was found. The suspect appeared in the background of an image. Detectives were able to positively identify the man. A search of his electronic devices revealed that he was creating child sex abuse material to share on the dark web. The seven -year -old victim had been under his supervisory control. The man was arrested and the child victim was rescued. Investigators said that without Clearview AI, there was no way that guy would have found. He pleaded guilty in February 2020 and was sentenced to 35 years in prison[119].

There are vocal arguments against facial recognition technology, with the biggest being its threat to an individual's privacy. Some cities across the world are already working towards banning real -time facial recognition. Why? Your facial data can be collected and stored without

117 U.S. Department of Homeland Security. (2020). Use of Facial Recognition Services. *Privacy Impact Assessment for the ICE.* Retrieved October 16, 2023, from DHS/ICE/PIA-054 ICE Use of Facial Recognition Services

118 Clearview AI *official website*. Retrieved October 16, 2023, from Clearview AI | Facial Recognition

119 More information available: Clearview AI Company Overview (youtube.com)

your permission[120]. There are also concerns regarding safety. Apps that allow individuals to use Facial Recognition Software to identify someone they see on the street or at a bar already exist[121].

Finally the technology is still far from perfect. Many algorithms produce far more false positives on non-white faces[122]. Is has also demonstrated that the system can be tricked: researchers have developed anti-facial recognition glasses[123] which make wearers undetectable. This has not stopped facial recognition from being widely adapted. From smartphones using it as a way to unlock the system, to retailers using it to stop theft.

7.2. Advantages and disadvantages of using AI in criminology

Here are some benefits of using AI in fighting and preventing crime:

- Predictive Policing[124]:

  Description: AI algorithms can analyze historical crime data to identify patterns and trends, helping law enforcement predict potential crime hotspots and allocate resources strategically.

120 Selinger, E., & Leong, B. (2022). The Ethics of Facial Recognition Technology. *In Oxford Handbook of Ethics of AI* (pp. 590–610). Retrieved October 16, 2023, from The Ethics of Facial Recognition Technology | Oxford Handbook of Digital Ethics | Oxford Academic (oup.com)

121 Trangotech. (2023). *Best Facial Recognition Apps*. Retrieved October 16, 2023, from 12 Best Facial Recognition Apps for iOS & Android in 2023 - Trango Tech

122 National Institute of Standards and Technology (NIST). (2019, December). NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software. *NIST News.* Retrieved October 16, 2023, from NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software | NIST

123 Reflectacles *official website*. Retrieved October 16, 2023, from Reflectacles Privacy Eyewear & Sunglasses: Anti Facial Recognition Glasses since 2015.

124 Lau, T. (2020, April 1). Predictive Policing Explained. *Brennan Center for Justice*. Retrieved October 16, 2023, from Predictive Policing Explained | Brennan Center for Justice

Benefit: This proactive approach enables law enforcement agencies to prevent criminal activities by deploying resources to areas with a higher likelihood of crime, ultimately reducing response times and enhancing overall public safety.

- Facial Recognition Technology[125]:

  Description: AI-driven facial recognition systems can identify and track individuals in public spaces by analyzing facial features captured through surveillance cameras or other imaging devices.

  Benefit: This technology aids in locating suspects, monitoring public spaces, and enhancing security by quickly identifying individuals of interest, providing valuable information for investigations and preventing potential threats.

- Cybercrime Detection[126]:

  Description: AI is used to detect and prevent cybercrimes by analyzing vast amounts of data to identify patterns, anomalies, and potential security threats in digital environments.

  Benefit: As cybercrimes become more sophisticated, AI helps law enforcement stay ahead by identifying and mitigating cyber threats, protecting individuals, businesses, and critical infrastructure from online criminal activities.

These benefits showcase how AI technologies contribute to more proactive, efficient, and effective crime prevention and law enforcement

125 Smart Eye Technology. (2022, January 3). *The Benefits of Facial Recognition – Full List of Advantages*. Retrieved October 16, 2023, from The Benefits of Facial Recognition - Full List of Advantages (getsmarteye.com)

126 Al-Khater, W. A., Al-Maadeed, S., & Ahmed, A & others. (2020). Comprehensive Review of Cybercrime Detection Techniques. *IEEE Access, 8*, 137293-137311.. Retrieved October 16, 2023, from Comprehensive Review of Cybercrime Detection Techniques | IEEE Journals & Magazine | IEEE Xplore

strategies.

While AI technologies offer various advantages in fighting and preventing crime, they also come with certain disadvantages and challenges. Here are some of them:

- Bias and Discrimination[127]:

  Description: AI algorithms can inherit biases present in training data, leading to discriminatory outcomes, especially if the data used to train the algorithms contain biases related to race, gender, or socioeconomic factors.

  Disadvantage: Unintentional biases in AI systems can result in unfair targeting of specific demographics, potentially leading to wrongful accusations or reinforcing existing social inequalities within the criminal justice system.

- Privacy Concerns[128]:

  Description: AI applications often involve extensive data collection, including surveillance footage, social media monitoring, and personal information, raising concerns about the invasion of privacy.

  Disadvantage: The use of AI in crime prevention may infringe on individuals' privacy rights, leading to debates about the balance between public safety and personal freedoms. Striking the right balance requires careful consideration of ethical and legal frameworks.

127 Thomas, M. (2023, October 31). 12 Risks and Dangers of Artificial Intelligence (AI). *Built In.* Retrieved October 16, 2023, from 12 Risks and Dangers of Artificial Intelligence (AI) | Built In

128 Thomas, M. (2023, October 31). 12 Risks and Dangers of Artificial Intelligence (AI). *Built In.* Retrieved October 16, 2023, from 12 Risks and Dangers of Artificial Intelligence (AI) | Built In

- Reliability and Accountability[129]:

  Description: AI systems are not infallible and can make errors, whether due to incomplete training data, algorithmic limitations, or unexpected scenarios.

  Disadvantage: Relying solely on AI for decision-making in law enforcement may result in inaccuracies and unintended consequences. Additionally, when AI systems make mistakes, accountability becomes a challenge, as it may be unclear who is responsible for errors in the system.

It's crucial to address these disadvantages through responsible AI development practices, ongoing monitoring, and a commitment to transparency and accountability. Balancing the benefits of AI in crime prevention with the ethical and legal considerations is essential for fostering trust in these technologies

7.3. AI Tools in the Fight Against Cybercrime

Cybercrime refers to criminal activities carried out in the digital space using computers, networks, and the internet. It encompasses a broad range of illicit activities that exploit vulnerabilities in information systems, compromise data integrity, and cause harm to individuals, organizations, or governments. Cybercriminals employ various techniques, such as hacking, malware, phishing, and other forms of cyber-attacks, to gain unauthorized access, steal sensitive information, commit fraud, or disrupt digital operations.

Artificial Intelligence (AI) is a powerful tool in the fight against cybercrime, offering advanced capabilities to detect, prevent, and respond to various cyber threats.

129 Novelli, C., Taddeo, M., & Floridi, L. (2022). Accountability in Artificial Intelligence: What It Is and How It Works. *SSRN Electronic Journal*. Retrieved October 16, 2023, from Accountability in artificial intelligence: what it is and how it works | AI & SOCIETY (springer.com)

Here are some AI tools to fight cybercrime:

Cybercrime refers to criminal activities carried out in the digital space using computers, networks, and the internet. It encompasses a broad range of illicit activities that exploit vulnerabilities in information systems, compromise data integrity, and cause harm to individuals, organizations, or governments. Cybercriminals employ various techniques, such as hacking, malware, phishing, and other forms of cyberattacks, to gain unauthorized access, steal sensitive information, commit fraud, or disrupt digital operations[130].

Artificial Intelligence (AI) is a powerful tool in the fight against cybercrime, offering advanced capabilities to detect, prevent, and respond to various cyber threats.

Here are some AI tools to fight cybercrime:

i. Darktrace[131]

Darktrace is an advanced AI-driven cybersecurity tool designed to combat cyber threats effectively. One key tool within Darktrace's arsenal is its unsupervised machine learning algorithms, which continuously monitor network traffic and analyze the behavior of all devices and users in real time. This capability allows Darktrace to establish a baseline of normal behavior for each user and device within a network.

In a practical scenario, let's consider an insider threat where an employee unwittingly falls victim to a phishing attack within a financial institution. Darktrace's machine learning algorithms quickly detect anomalous patterns associated with the compromised employee's account. By comparing the observed behavior to established baselines, Darktrace identifies the unusual data access and movement indicative

130 Ravichandran, H. (2023, March 15). How AI Is Disrupting and Transforming the Cybersecurity Landscape. *Forbes Technology Council*. Retrieved October 16, 2023, from How AI Is Disrupting And Transforming The Cybersecurity Landscape (forbes.com)

131 McCallion, J. (2017, August 01). What is Darktrace? *ITPro*. Retrieved October 16, 2023, from What is Darktrace? | ITPro

of a potential security breach. Upon detecting the anomaly, Darktrace generates real-time alerts for the security team. These alerts provide detailed insights into the deviations from the norm, such as irregular data access times or unfamiliar system interactions. The security team then uses Darktrace's intuitive interface to investigate the alert further, gaining visualizations of the attack path and understanding how the attacker is moving within the network.

Darktrace goes beyond detection; it enables automated responses integrated with the organization's security infrastructure. For instance, it can isolate the compromised user account, limiting access to critical systems and data. This automated response helps contain the threat swiftly, preventing further unauthorized access.

Following containment, the security team takes additional actions to mitigate the incident. This may involve resetting compromised credentials, enhancing security awareness training, and analyzing the phishing email to improve email filters.

Throughout this process, Darktrace continues to learn from the incident, adapting its models to better detect and respond to similar threats in the future.

In summary, Darktrace's AI-driven capabilities empower organizations to proactively detect and respond to cyber threats, especially insider threats. Its continuous learning and automated response features contribute to the swift containment of incidents, bolstering overall cybersecurity resilience.

ii. IBM Watson for Cyber Security[132]

This is an AI-powered platform designed to enhance cybersecurity by leveraging cognitive computing capabilities. This platform integrates

132 Security Intelligence Staff. (2017, February 13). Investigating Threats with Watson for Cyber Security. *Security Intelligence.* Retrieved October 16, 2023, from Investigating Threats with Watson for Cyber Security - Security Intelligence

advanced AI technologies, including machine learning and natural language processing, to analyze vast amounts of data and provide actionable insights for cybersecurity professionals.

In a practical example, let's consider a large financial institution using IBM Watson for Cyber Security to strengthen its defenses against evolving cyber threats. The platform continuously ingests and analyzes diverse data sources, such as security blogs, research papers, and real-time security feeds, to stay updated on the latest threats and vulnerabilities.

If a new strain of malware is identified in the wild, IBM Watson for Cyber Security can quickly process the information. Its natural language processing capabilities enable it to understand and extract relevant details about the malware, including its behavior, attack vectors, and potential impact. The platform also takes into account the specific industry and context of the financial institution, tailoring its analysis to prioritize threats that are most relevant to the organization.

In addition to external threat intelligence, IBM Watson for Cyber Security integrates with the institution's internal security data, such as logs from firewalls, intrusion detection systems, and endpoint protection. It correlates this internal data with external threat intelligence, creating a comprehensive view of the institution's cybersecurity posture.

When an employee unknowingly clicks on a phishing link, triggering an alert from the institution's security infrastructure, IBM Watson for Cyber Security comes into action. It analyzes the alert in real time, considering the user's historical behavior, the nature of the clicked link, and any potential indicators of compromise associated with the incident.

IBM Watson for Cyber Security doesn't stop at detection; it aids in the investigation process. The platform provides security analysts with detailed reports, highlighting the potential impact of the phishing attempt and offering suggestions for remediation. It helps the analysts understand the broader context of the incident and prioritize their

response efforts.

Moreover, the platform's machine learning capabilities enable it to learn from each incident. As the financial institution responds to and mitigates the phishing incident, IBM Watson for Cyber Security adapts its models, refining its understanding of phishing threats specific to the organization.

In summary, IBM Watson for Cyber Security empowers organizations to proactively analyze and respond to cyber threats. Its ability to integrate external threat intelligence, correlate with internal data, and provide contextualized insights supports effective decision-making in the ever-changing landscape of cybersecurity.

iii. BioCatch[133]

BioCatch is an advanced behavioral biometrics platform designed to detect and prevent various types of online fraud and cyber threats by analyzing user behavior. Unlike traditional authentication methods that rely on static credentials, BioCatch focuses on continuous monitoring of user interactions with online applications, leveraging behavioral patterns to identify anomalies and potential fraudulent activities.

Certainly, let's consider a practical example of how BioCatch can be applied in the context of securing an e-commerce platform.

Suppose an online retailer integrates BioCatch into its authentication and fraud prevention system. When a user logs in to make a purchase, BioCatch starts analyzing various behavioral attributes, including mouse movements, scrolling patterns, and interaction with the website interface.

Now, imagine a scenario where a cybercriminal gains access to a user's account credentials and attempts to make unauthorized transactions on the e-commerce site. As the fraudster navigates through

133 BioCatch *official website*. Retrieved October 16, 2023, from Behavioral Biometrics: Prevent Fraud, Build Digital Trust (biocatch.com)

the website to add items to the cart and proceed to checkout, BioCatch is actively monitoring the session.

BioCatch establishes a baseline of the legitimate user's behavior during typical shopping sessions. This includes factors like the time spent browsing, the sequence of product selections, and the usual hesitation or confidence in the decision-making process. If the cybercriminal's behavior deviates significantly from these established patterns, BioCatch raises an alert.

For instance, if the legitimate user typically takes time to compare product details and suddenly the session shows rapid and erratic selections, BioCatch recognizes this as an anomaly. It may also consider additional factors such as the usual device used for transactions, the geographic location, and the regularity of purchases. If any of these parameters indicate a deviation from the norm, BioCatch triggers an alert in real-time.

BioCatch's ability to detect anomalies goes beyond simple transaction patterns. It can identify signs of automated scripts or bots attempting to manipulate the platform for fraudulent activities. For example, if the system observes unnatural and superhuman speeds in navigating through pages or filling out forms, it recognizes the potential threat and takes preventive measures.

In response to the detected anomaly, the e-commerce platform can dynamically adjust its security measures. It may prompt the user for additional verification steps, such as confirming identity through a multi-factor authentication process. Alternatively, the system could temporarily suspend the transaction and notify the user of the suspicious activity.

By incorporating BioCatch into its security infrastructure, the e-commerce platform gains a behavioral biometrics layer that adapts to evolving threats. BioCatch helps create a more secure and trustworthy environment for users, safeguarding against a variety of fraudulent activities that can occur during online transactions.

iv. Dark Web ID[134]

Dark Web ID is a cybersecurity tool designed to monitor the dark web for compromised credentials and sensitive information, providing businesses with proactive threat intelligence. The dark web is a hidden part of the internet where cybercriminals trade stolen data, and Dark Web ID helps organizations identify potential risks before they escalate.

In a practical example, let's consider a mid-sized enterprise that has implemented Dark Web ID as part of its cybersecurity strategy. The company stores a vast amount of sensitive customer data, including login credentials and personal information. Dark Web ID continuously scans the dark web, including forums, marketplaces, and other hidden corners where stolen data is exchanged.

Suppose an employee of this enterprise unknowingly falls victim to a phishing attack, resulting in the compromise of their corporate email credentials. The cybercriminal, aiming to monetize this information, intends to sell these stolen credentials on the dark web. This is where Dark Web ID comes into play.

Dark Web ID's monitoring system detects the appearance of the compromised email credentials on the dark web. It correlates this information with the enterprise's internal records, recognizing that the exposed credentials belong to an employee within the organization. In real-time, the system alerts the security team about the compromised credentials, providing details about the affected employee and the potential risks involved.

Armed with this intelligence, the enterprise's security team can swiftly take action to mitigate the threat. They may, for example, reset the compromised credentials, enforce multi-factor authentication, and conduct security awareness training to educate employees about phishing risks. Additionally, the security team can monitor for any suspicious activities related to the compromised account to prevent

134 Dark Web *official website*. Retrieved October 16, 2023, from Dark Web Monitoring for IT Professionals | ID Agent - Dark Web ID

unauthorized access or data breaches.

Dark Web ID not only identifies compromised credentials but also helps organizations understand the context of the exposure. It provides insights into which data is at risk, allowing for a targeted and effective response. By using Dark Web ID, businesses can stay one step ahead of cyber threats, safeguarding their sensitive information and maintaining the trust of their customers and stakeholders.

v. FireEye Helix[135]

FireEye Helix is a cloud-based security operations platform that integrates and analyzes data from various security products to provide organizations with a unified view of their cybersecurity posture. It streamlines the incident detection and response process, allowing security teams to effectively manage and mitigate threats. Here's a practical example of how FireEye Helix works.

Imagine a mid-sized e-commerce company facing a growing number of phishing attacks aimed at stealing customer login credentials. In this scenario, the organization utilizes FireEye Helix to enhance its cybersecurity defenses.

Upon integrating FireEye Helix into its security infrastructure, the platform begins to aggregate data from various sources, including email security solutions, network traffic logs, and endpoint protection systems. One day, an employee clicks on a seemingly innocent email link, unknowingly triggering a phishing attempt. The email security solution generates an alert, detecting suspicious activity related to this phishing incident.

FireEye Helix, through its correlation capabilities, links the email security alert with information from the network logs. It identifies that,

135 Lennon, M. (2016, November 30). FireEye Unveils Helix Platform to Streamline Security Operations. *SecurityWeek*. Retrieved October 16, 2023, from FireEye Unveils Helix Platform to Streamline Security Operations - SecurityWeek

around the same time, there was an uptick in outbound network traffic from the affected employee's workstation, suggesting a potential data exfiltration attempt. This correlation raises the severity level of the incident.

The centralized dashboard in FireEye Helix provides the security team with a detailed overview of the phishing incident. It shows the affected employee's workstation, the email content, and the associated network activity. The platform also cross-references threat intelligence feeds to determine if similar phishing campaigns have been observed elsewhere.

In response to the incident, the security team can leverage FireEye Helix's automated capabilities. The affected employee's workstation is immediately isolated from the network to prevent further data exfiltration. Simultaneously, the platform triggers alerts to other potential targets, such as employees who received similar phishing emails, advising them to be cautious.

Using the case management features of FireEye Helix, the security team documents their investigation process, including any indicators of compromise discovered. They collaborate within the platform to share insights and observations, fostering a coordinated response. Additionally, FireEye Helix provides post-incident reports, allowing the organization to analyze the incident thoroughly and enhance its security policies.

In this practical example, FireEye Helix empowers the e-commerce company to swiftly detect, respond to, and mitigate a phishing attack. By leveraging the platform's capabilities, the organization not only secures its current environment but also learns from the incident to bolster its cybersecurity defenses against similar threats in the future.

8. CYBERCRIME IN ALBANIA

8.1. Albania Cybercrime Attacks

Albania has been the target of several cyberattacks that have caused major problems and raised concerns about cybersecurity. The incidents were looked at using a variety of data collection methods, such as document analysis and case study examination.

- A cyber-attack on Albanian institutions (the TIMS system) caused queues on border points, causing manual registration of citizens and vehicles. Microsoft, which the Albanian government tasked with assisting in the recovery and investigation of the cyber-attack, found that the attacks began in May 2021 and were carried out by four groups linked to the Iranian government. The attack escalated until July 2022, when the attackers attempted to delete data on the server. Microsoft was able to prove with a high degree of certainty that a variety of Iranian groups were involved in this attack, with different actors responsible for different phases[136].
- Another major cyber event involved Credins Bank[137], one of Albania's biggest banks, which had to shut down its online services because of an attack planned by the Homeland Justice[138] group. The bank's business clients' data was compromised by Homeland Justice on January 9, 2022, leading to another file appearing under the name 'All Accounts Customers' and a

136 Microsoft Threat Intelligence. (2022, September 8). Microsoft Investigates Iranian Attacks Against the Albanian Government. *Microsoft Security Blog*. Retrieved October 16, 2023, from Microsoft investigates Iranian attacks against the Albanian government | Microsoft Security Blog

137 Sinoruka, F. (2023, January 25). Albanians Mull Options as Data Security Takes New Hit. *Balkan Insight*. Retrieved October 16, 2023, from Albanians Mull Options as Data Security Takes New Hit | Balkan Insight

138 The Iranian HomeLand Justice group, a cyber threat group, has been active since May 2021, known for cyber espionage, ransomware, and malware attacks on Albanian government networks.

message stating that "Credins Failed". The bank claimed a peripheral system had been affected but that the danger was isolated and the highest IT security measures were implemented. The bank urged that no private data be published and that the publication of personal information without authorization constitutes a legal violation. The bank's response to the incident highlights the importance of customer protection in data breaches.

The attackers said they chose the bank because the Albanian government backs the MEK[139], an Iranian opposition group. It's unclear whether the bank checked the leaked files with the name "ALLAccountsCustomers.zip."

❖ On July 15, 2022, Albania faced its most significant cyberattack to date when unauthorized individuals breached the government's centralized e-services system[140]. The attackers had prolonged access to the government's computer network for an entire year, during which they extensively explored the network, collected login credentials, and introduced harmful software. Notably, they even left a message criticizing a group known as Mujahideen E-Khalq (MEK) directly on the government's computers.

As the government's cybersecurity defenses began to respond to the threat, the attackers retaliated by deploying a destructive computer virus called ZeroCleare[141] on July 18, 2022. Openly

139 At one point the MEK was Iran's "largest and most active armed dissident group," and it is still sometimes presented by Western political backers as a major Iranian opposition group. More information here Mujahadeen-e-Khalq (MEK) | Council on Foreign Relations (cfr.org)

140 Anadolu. (2023, May 8). Iran's Foreign Ministry Confirms Cyberattack but Denies Leak of Documents. *The Nation.* Retrieved October 16, 2023, from Iran's Foreign Ministry confirms cyberattack but denies leak of documents (nation.com.pk)

141 Zerocleare is a destructive form of malware that targets industrial control systems and critical infrastructure. It is designed to erase data from infected systems, causing significant damage and disruption to operational technology networks in facilities such as manufacturing plants and power facilities

claiming responsibility for hacking the Albanian government's infrastructure, the attackers further escalated their actions. Between late July and mid-August 2022, they took to social media to share Albanian government documents, allowing users to choose which documents they wished to see. Subsequently, the selected documents were published as zip files or videos.

In response to this cyberattack attributed to the Iranian dissident group Mujahedeen-e-Khalq (MEK), the Albanian government took decisive measures. Temporary closures of online public services and government websites were implemented, accompanied by the deliberate destruction of government data to mitigate the impact. The MEK, in turn, responded by canceling a scheduled summit in Albania, citing terrorist threats and following the advice of the Albanian government.

The cybersecurity firm Mandiant[142] identified Iran as the likely source of the attack, a claim corroborated by the White House. In a robust response, the Albanian government chose to sever diplomatic relations with Iran and expel Iranian Embassy staff[143]. While Iran disputed Albania's claims and criticized the diplomatic decisions, cybersecurity experts commended the Albanian government's strong and public response, characterizing it as one of the most robust reactions to a cyberattack ever witnessed.

❖ There was a big event on January 30, 2023, when the LockBit[144]

142 Mandiant is a cybersecurity firm recognized for its expertise in incident response, threat intelligence, and cybersecurity services. The company offers a range of services, such as incident response, digital forensics, and threat detection, helping organizations detect and mitigate cyber threats effectively.

143 Gritten, D. (2022, September 7). Albania severs diplomatic ties with Iran over cyber-attack. *BBC News*. Retrieved October 16, 2023, from Albania severs diplomatic ties with Iran over cyber-attack - BBC News

144 Hackers with the name LockBit use ransomware to get into computers and hold them hostage. They demand money to unlock computers that have been hacked, and to get people to pay, they often threaten to leak stolen data. LockBit is a type of ransomware called a "crypto virus," and it is used to attack businesses and organizations very specifically. It works like ransomware-as-a-service (RaaS),

ransomware group attacked a well-known airline company, Air Albania[145]. They said they stole the company's data and encrypted it, then demanded money to get it back. The menacing message was uploaded onto the online platform for unauthorized information disclosure on the 30th of January. The due date for the payment of the ransom was 14 February[146]. Even though there had been an attack, Air Albania told the public that its data was still safe and that system updates were being made.

❖ On December 25,2023, The Iranian hacker group "Homeland Justice" says they broke into and deleted more than 2 petabytes of data from the phone company's network[147] and the networks of all companies that were connected to it[148].

The hackers also wrote a message "The mission has begun. The phone company was hacked by Homeland Justice. Ignoring our "humanitarian warnings" cost your corrupt politicians all this. But don't be fooled. This will continue until we completely clear the country of terrorists. In this operation, taken together, more than 2 petabytes of telecommunication network and internal network data of all related companies were deleted, and the

---

where people who want to pay for custom attacks can do so and make money through an affiliate system. Members of the attacking group get up to ¾ of the ransom money, which is split between the LockBit developer team and them.

145 Air Albania is a joint venture by the Albanian and Turkish governments, founded in 2018 as a public–private partnership. Founding partner Turkish Airlines owns 49.12% shares of the carrier. The remaining 50.88% is split between Albanian government body Albcontrol (10%) and privately held Albanian company MDN Investment (41%).

146 Khaitan, A. (2023, January 30). LockBit Ransomware Gang Hits Air Albania, Puts Payment Deadline as Feb 14. *The Cyber Express*. Retrieved October 16, 2023, from LockBit Targets Air Albania, Puts Payment Deadline As Feb 14 (thecyberexpress.com)

147 One Albania is an albanian mobile company: The One Network | One Albania

148 "Homeland Justice" hacks telephone company in Albania: We got the data.(2023, December 2023). *Euronews*. Retrieved October 16, 2023, from "Homeland Justice" hacks telephone company in Albania: We got the data | Euronews Albania

important data will be released soon. We just wanted to convey a message. Hope it worked! We have already proven that the eagle's claws are where the sparrow belongs".

8.2. The need to Fortify Cyber Infrastructure

These cyberattacks in Albania show how dangerous cybercrime is getting and how much better security is needed to protect businesses and important infrastructure. The government and institutions of Albania need to stay alert and work with other countries to improve their cybersecurity and lower the risks that could happen in the future.

Because cyber threats are getting worse, Albania needs to strengthen its cyber infrastructure right away. To fully fix these problems, it is essential to put invest into cybersecurity education and training programs. These programs should be aimed at IT professionals, government workers, and the general public to make sure that everyone is aware of new cyber threats and follows the best digital security practices.

Additionally, Albania should work together with cybersecurity groups and agencies from other countries. Partnering up with nearby countries and organizations around the world makes it easier to share important threat information, cybersecurity knowledge, and tried-and-true methods. When people work together in this way, Albania can stay ahead of new cyber threats by using its shared resources and knowledge.

Putting in place and following strong cybersecurity rules is an important first step. Albania needs strict rules that cover a lot of topics, like protecting data, handling incidents, and managing risks. Regular audits and assessments can make sure compliance and show areas that need improvement. Strict penalties for not complying can stop cybercriminals from doing bad things.

Also, making and testing recovery and incident response plans on a regular basis are important parts of a strong cybersecurity strategy.

Setting up backup systems, regular drills, and clear communication protocols to keep the public informed are all well-defined processes that can help lessen the damage and downtime caused by a cyberattack[149].

The most important thing is to put money into advanced threat detection and prevention systems that use AI and ML[150] technologies. The proactive detection and mitigation of potential threats before they can do a lot of damage is made possible by these systems. Protecting critical infrastructure should be a top priority. This includes building secure networks, encrypting communication channels, and putting strong cybersecurity measures in place for all essential services.

Another important way to improve Albania's cyber defenses is to form partnerships between the government and private companies. Working together, the government, the private sector, and academia can find new ways to solve problems, share information about threats, and get a lot of different kinds of expertise. Regular assessments and audits of cybersecurity are needed to find weaknesses in a planned way, which lets the cybersecurity posture be improved in specific ways.

9. LEGAL AND REGULATORY FRAMEWORK

To make our online world safer, it's not just about fancy tech and services. We also need solid laws that keep up with how the internet and online threats keep changing.

Different groups, both inside our country and worldwide, have been running campaigns to educate people about staying safe from

149 The state of cybersecurity in Albania: A comprehensive overview. *Gavin Dennis Blog*. (2023, May 11). Retrieved October 16, 2023, from The state of cybersecurity in Albania: A comprehensive overview - Blog | Gavin Dennis - Certified and Experienced Cyber Security Contractor

150 Machine Learning (ML) technologies, including supervised and unsupervised learning, are crucial in AI and automation, solving complex problems and extracting insights from large datasets across diverse industries. They include reinforcement learning, deep learning, natural language processing, computer vision, clustering algorithms, and ensemble learning.

online crimes and attacks that threaten internet security.

Having laws that protect us from electronic crimes and misuse is super important to make sure our online communication and transactions are reliable. There are some main laws about cybercrime in our country, like:

- Law No. 7895, dated 27.1.1995, "Criminal Code of the Republic of Albania151", as amended;
- Law No. 2/2017, "On cybersecurity152";
- Law No. 9918 dated 19.5.2014, "On Electronic Communications in the Republic of Albania153", as amended;
- Law No. 9887, dated 10.3.2008, "On Personal Data Protection154", as amended;
- Law No. 8457, dated 11.2.1999, "On Classified Information155", as amended;
- Law No. 9880, dated 25.02.2008 "On the Electronic Signature156", as amended;
- Law No. 107 dated 15.10.2015, "On Electronic Identification and Trusted Services157," as amended

A separate court structure or specialized judges for cybercrime cases and cases involving electronic evidence do not exist. As participants noted, judges are not currently being trained in cybercrime. Concerns were raised regarding the difficulties that the judiciary is having due to a lack of resources.

151 ALBANIA_Criminal Code.pdf (ohchr.org)

152 Law_No_22017_on_Cybersecurity.pdf (unodc.org)

153 Microsoft Word - ligji 9918 i ndryshuar versioni per publikim ne faqe 19.3.2013.docx (akdie.org)

154 Microsoft Word - LDP english version amended_2014.docx (privacyconference2019.info)

155 6.pdf (mod.gov.al)

156 Law (unodc.org)

157 ligj-2015-10-01-107.pdf (cesk.gov.al)

Albania has signed and ratified the Budapest Convention for Cyber Crime and has reflected in the Penal Code and Penal Procedure Code the requirements of the Convention.

The Constitution of Albania proclaims that fundamental human rights and freedoms are indivisible, inalienable, and inviolable and stand at the base of the entire juridical order. Moreover, Law No. 9887, Article 11 from March 10, 2008, "On protection of personal data'', speaks on the processing of personal data and freedom of expression.

Comprehensive legislation on the protection of children online has been adopted and enforced like the Article 117/2 of the Criminal Code[158] on Pornography.

Albania has also adopted an action plan for the protection of children's rights (DCM No. 182/2012).[159]

As mentioned above, the Law No. 8888 of 25 April 2002 "On Ratification of the Convention on Cyber Crime[160]" is reflected in the Criminal Code; and so is the Law No. 9262 of 29 July 2004 "On ratification of Additional Protocol of the Convention on Cyber Crime, for the criminalization of acts of racist and xenophobic nature that are committed via computer systems[161]". Similarly, procedural cybercrime legal provisions are fully implemented in the Criminal Procedural Law[162].

Within the criminal justice system in Albania, capacities are at a formative stage of development. A central forensics laboratory exists within the Cybercrime Unit of the State Police. However, there was a

158 Production, import, offering, making available, distribution, broadcasting, use, or possession of child pornography, as well as the conscious creation of access in it, by any means or form, shall be punishable by three to ten years of imprisonment.

159 Action Plan for protection children's rights

160 Albania (cybercrimelaw.net)

161 First Additional Protocol - Cybercrime (coe.int)

162 Criminal Procedural Law

general consensus among stakeholders that more resources are necessary to be provided to the cybercrime unit, as well as continuous training for the employees. A limited number of specialized cybercrime prosecutors have the capacity to build a case based on electronic evidence. According to the legislation, there is a requirement for the submission of evidence to the court by not only the prosecutor but also the victim. Therefore, legal authority is needed before any further action.

A separate court structure or specialized judges for cybercrime cases and cases involving electronic evidence do not exist. As participants noted, judges are not currently being trained in cybercrime. Concerns were raised regarding the difficulties that judiciary are having due to lack of resources.

Albania has established regional and international cooperation mechanisms. The country is one of the parties to the 1959 Council of Europe Convention on Mutual Legal Assistance in Criminal Matters[163]; it also ratified the First and Second Additional Protocols to the European Convention on Mutual Assistance in Criminal Matters, as well as the Convention on Extradition[164]. With regard to international cooperation, the Criminal Procedure Code (CPC) includes preservation and expedited disclosure of computer data, access to computer data, comprising search, seizure, and disclosure of data stored in the computer system located in Albania[165], when the search and seizure would be admissible, and interception of communications.

There is a strong collaboration mechanism with Interpol[166] and Europol[167], and there have been joint operations with Europol in the

163 Council of Europe – European Convention on Mutual Assistance in Criminal Matters (ETS No. 030) – Translations - Treaty Office (coe.int)

164 Council of Europe – European Convention on Extradition (ETS No. 024) – Translations - Treaty Office (coe.int)

165 Report on Cybersecurity Maturity Level in Albania

166 The International Criminal Police Organization (INTERPOL) *official page*. Retrieved October 16, 2023, from INTERPOL | The International Criminal Police Organization

167 European Union Agency for Law Enforcement Cooperation (EUROPOL)

past.

In addition, our cybersecurity laws should be in line with the ones in the European Union. We should put enough resources into this, according to what our country needs, and keep up with the latest technology while being fair and neutral.

10. NATIONAL CYBERSECURITY STRATEGY

Cybersecurity strategy is essential to mainstreaming a cybersecurity agenda across government because it helps prioritize cybersecurity as an important policy area, determines the responsibilities and mandates of key government and non-governmental cybersecurity actors, and directs the allocation of resources to emerging and existing cybersecurity issues and priorities.

Albania's commitment to cybersecurity and cyber-resilience has notably progressed since it recently adopted various national digital transformation security strategies[168]. The National Cross-Cutting Strategy "Digital Agenda of Albania 2015-2020"[169], is led by the Ministry of Infrastructure and Energy. The strategy superseded the National Cross-Cutting Strategy on Information Society (2008–2013)[170], a key document in stipulating cybersecurity at a high level. Prior to that, the first ICT strategy was adopted in 2003. The Digital Agenda of Albania (2015–2020) has interwoven the cybersecurity theme across the strategy. Guaranteeing high security levels for the information networks is a core element of the second objective of the strategy. Secure information society is a main section of the strategy,

official page. Retrieved October 16, 2023, from Home | Europol (europa.eu)

168 DCAF - Geneva Centre for Security Sector Governance. (2021). *National Cybersecurity Strategies in Western Balkan Economies*. Retrieved October 16, 2023, from NationalCybersecurityStrategiesWB_2021.pdf (dcaf.ch)

169 More information here: *The National Cross-cutting Strategy "Digital Agenda of Albania 2015-2020*

170 More information here: The National Cross-cutting Strategy on Information Society 2008-2013

which covers secure communications and electronic certifications; computer security; and safer internet practices.

In 2020, the Government of Albania endorsed a new five-year National Cybersecurity Strategy (2020 – 2025). The strategy is a comprehensive document that lays out the nation's strategy for enhancing its cybersecurity landscape. This strategy was crafted within the framework of the "National Security Strategy 2014–2020" and the "Cybersecurity Policy Paper 2014–2017". It encompasses key principles like safeguarding fundamental rights, upholding freedom of expression, protecting personal information and privacy, ensuring access for all, promoting democratic and effective governance, and fostering collective responsibility in upholding cybersecurity. Additionally, the strategy places special emphasis on the protection of children in the online sphere, dedicating a specific chapter to this vital objective.

The development and introduction of the specific chapter on children in the national strategy is a result of the intensive work of multiple stakeholders, including vested institutions, national regulators, law enforcement, and, more importantly, ICT industry representatives. The process was led by the National Authority for Cybersecurity and Electronic Certification (AKCESK)[171] and supported by UNICEF[172], which also ensured that children's opinions and experiences were taken into consideration.

Following the above line the Albanian Police Department have established the Computer Crime Investigation Unit to investigate cybercrime and developing officers' skills to undertake and assist in criminal investigations involving electronic/digital media and computer related crimes.

In fulfilling its mission and give efficient support to a public prosecutor in the cybercrime investigation and collection of electronic

171 More information here: Cybil Portal

172 United Nations Children's Fund *official website*. Retrieved October 16, 2023, from UNICEF

evidence, the Computer Crime Investigation Unit can develop capacities and being aware of number of additional activities, including the following ones:

- Pre-Planning an investigation where it relates to complex computer
- crime;
- Live Data or Volatile Data will be encountered;
- Information is required on Wireless networks;
- Advice on acquiring communication data from National or
- International partners (Data Preservation Requests);
- Communication Data investigation – Emails, Social Media, IP
- addresses, Phone and Internet Service providers;
- Open Source Intelligence (OSINT) advice – Research equipment and
- operational security when researching Social Media, Chatrooms, IRC,
- research of suspects or witnesses on-line;
- Covert Open Source Intelligence Research;
- Incidents affecting the National Critical Infrastructure of Albania.

11. LAW ENFOREMEND AGENCIES AND PRIVATE SECTOR

In both the private sector and law enforcement agencies, cybercrime investigations aim to address and mitigate online threats. However, there are key differences and similarities between these sectors in terms of their approaches, priorities, and resources.

While both sectors, private sector and law enforcement agencies,

share the common goal of addressing cybercrime, they differ in their approaches[173].

The key differences of private sector and law enforcement agencies are:

a) The mandate and authority:

Law enforcement agencies (Government agencies)[174] have the legal authority and a mandate to enforce laws and their focus extends beyond protecting individual organizations to maintaining public order and safety in contrast to law enforcement agencies, private companies are not authorized to investigate and prosecute cybercriminals. Instead, they focus on safeguarding their interests, which include protecting their assets, reputation, and customer data.

b) The scope of investigation:

Investigations in the private sector often focus on identifying and mitigating threats to the organization's systems, intellectual property, and sensitive data through on internal investigations and information sharing with other organizations to identify and mitigate cyber threats. While private sector investigations focus on identifying and mitigating threats to the organization's systems, intellectual property, and sensitive data, law enforcement investigations cover a wider spectrum of cybercrimes. This includes offenses with national security implications, organized cybercrime, and cases involving public safety.

173 Council of Europe. (n.d.). Criminal justice authorities and multi-national service providers. *Cybercrime*. Retrieved October 16, 2023, from Criminal justice authorities and multi-national service providers: enhancing public-private cooperation in cyberspace - Cybercrime (coe.int)

174 Law Explores. (n.d.). *Public and private law enforcement*. Retrieved October 16, 2023, from Public and Private Law Enforcement | (lawexplores.com)

c) The resources and expertise:

While law enforcement agencies have access to greater resources, including specialized cybercrime units and forensic experts, private companies may have limited resources and may lack the specialized skills required for comprehensive cybercrime investigations

The key similarities of private sector and law enforcement agencies are:

a. Technological Challenges:

Both sectors face similar technological challenges, including encryption, anonymization, and the rapid evolution of cyber threats. Encryption is the process of converting plain text into a coded message to prevent unauthorized access. Anonymization is the process of removing personally identifiable information (PII) from data sets to protect privacy and prevent unauthorized access. The rapid evolution of cyber threats refers to the increasing sophistication of cyberattacks and the need for better cyber information sources, standardized databases, mandatory reporting, and public awareness. These challenges are common to both the public and private sectors, and addressing them requires a comprehensive approach that includes technical, organizational, and human factors.

b. Information Sharing:

Recognizing the interconnected nature of cyber threats, both public and private sectors benefit from sharing information about emerging threats, vulnerabilities, and attack methodologies. Effective collaboration[175] is crucial in both sectors, and public-private partnerships allow for the exchange of expertise,

175 Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). *Partnerships and collaboration*. Retrieved October 16, 2023, from Partnerships and Collaboration | Cybersecurity and Infrastructure Security Agency CISA

resources, and threat intelligence.

c. Establishing Trust:

Building trust between private sector entities and law enforcement agencies is essential for effective information sharing. This involves ensuring data privacy, confidentiality, and legal compliance.

d. Legal Frameworks:

Sharing threat intelligence with law enforcement can help to combat cyber threats. However, it is essential to protect sensitive business information while doing so. Governments can create legal frameworks that enable the private sector to share threat intelligence with law enforcement while protecting sensitive business information.

e. Standardized Protocols:

Developing standardized protocols for sharing information, such as indicators of compromise (IoCs)[176] and best practices can enhance collaboration and streamline the exchange of critical data between public and private sectors. Indicators of compromise (IoCs) are pieces of information that can be used to identify a security incident or a potential security incident. They can include IP addresses, domain names, file hashes, and other technical details that can help security teams detect and respond to cyber threats.

f. Training and Education:

176 Sophos. (n.d.). Indicators of Compromise (IoC) - *Cybersecurity Explained*. Retrieved October 16, 2023, from Indicators of Compromise

Offering training programs and educational initiatives that bridge the gap between private sector professionals and law enforcement investigators can improve understanding and cooperation.

g. Joint Task Forces:

Establishing joint task forces or cybersecurity working groups that include representatives from both public and private sectors can facilitate ongoing collaboration and communication. These groups can help to identify common challenges, share best practices, and develop strategies to improve cybersecurity.

The National Institute of Standards and Technology (NIST)[177] has developed a framework for improving critical infrastructure cybersecurity that includes guidelines for establishing public-private partnerships. The framework provides a common language for discussing cybersecurity risk management and can help organizations to identify, assess, and manage cybersecurity risks.

h. Incentives:

Governments can offer incentives to encourage private sector entities to participate in cybercrime information sharing. These incentives may include legal protections, tax incentives, or access to additional resources.

The primary federal law enforcement agencies that investigate domestic cybercrime in the **United States** include:

i. The Federal Bureau of Investigation (FBI)[178].

177 National Institute of Standards and Technology. (n.d.). NIST, an *official website* of the United States government. Retrieved October 16, 2023, from National Institute and Standards and Technology

178 Federal Bureau of Investigation, *official website*. Retrieved October 16, 2023,

The FBI is the lead federal agency for investigating cyber-attacks and intrusions and is committed to combating the evolving cyber threat by developing innovative investigative techniques, using cutting-edge analytic tools, and forging new partnerships in our communities. The FBI has specially trained cyber squads in each of our 56 field offices, working hand-in-hand with interagency task force partners. The rapid-response Cyber Action Team can deploy across the country within hours to respond to major incidents. With cyber assistant legal attachés in embassies across the globe, the FBI works closely with the international counterparts to seek justice for victims of malicious cyber activity.

CyWatch[179] is the FBI's 24/7 operations center and watch floor, providing around-the-clock support to track incidents and communicate with field offices across the country.

ii. The United States Secret Service[180].

iii. The Department of Homeland Security[181].

iv. United States Department of Justice (DOJ)[182]

v. United States Secret Service (USSS)[183],

vi. National Cyber Investigative Joint Task Force (NCIJTF)[184],

---

from Welcome to fbi.gov — FBI

179 FBI official website. What we investigate. Retrieved October 16, 2023, from Cyber Crime — FBI

180 The United States Secret Service, *official website*. Retrieved October 16, 2023, from United States Secret Service

181 The Department of Homeland Security, *official website*. Retrieved October 16, 2023, from Homeland Security

182 United States Department of Justice, *official website*. Retrieved October 16, 2023, from US Department of Justice

183 United States Secret Service, *official website*. Retrieved October 16, 2023, from Home | United States Secret Service

184 National Cyber Investigative Joint Task Force (NCIJTF), *official website*. Retrieved October 16, 2023, from National Cyber Investigative Joint Task Force

vii. Internet Crime Complaint Center (IC3)[185].

The Internet Crime Complaint Center (IC3) collects reports of Internet crime from the public. Using such complaints, the IC3's Recovery Asset Team has assisted in freezing hundreds of thousands of dollars for victims of cybercrime.

The **European Union** law enforcement agencies are:

a) Europol[186].

It plays a key role in the European Cybercrime Task Force, which is an expert group made up of representatives from Europol, Eurojust, and the European Commission. The task force works together with the Heads of EU Cybercrime Units to facilitate the cross-border fight against cybercrime.

b) Europol established the EC3[187] in 2013 to enhance the EU's response to cybercrime. The EC3 serves as the focal point for coordination, cooperation, and intelligence-sharing among EU member states' law enforcement agencies. Its primary objective is to combat cyber threats effectively and protect European citizens, businesses, and governments.

Each year, the EC3 issues the Internet Organized Crime Threat Assessment (IOCTA), which sets priorities for the EMPACT[188] Operational Action Plan.

185 Internet Crime Complaint Center, *official website*. Retrieved October 16, 2023, from Internet Crime Complaint Center

186 EUROPOL *official website*. Retrieved October 16, 2023, from EUROPOL

187 European Cybercrime Center, *official website*. Retrieved October 16, 2023, from European Cybercrime Centre - EC3 | Europol (europa.eu)

188 EMPACT, or the European Multidisciplinary Platform Against Criminal Threats, is an integrated approach to EU internal security, involving border controls, police, customs, judicial cooperation, information management, innovation, training, prevention, and public-private partnerships. Retrieved October 16, 2023, from EU Policy Cycle - EMPACT | Europol (europa.eu)

c) Eurojust[189]:

Eurojust is an EU agency that supports judicial cooperation among EU member states. It plays a coordinating role in complex cross-border criminal cases, including those related to cybercrime, facilitating communication between national authorities.

d) European commission[190]:

The European Commission is the executive branch of the European Union, responsible for proposing legislation, implementing decisions, upholding the EU treaties, and managing the day-to-day business of the EU.

e) European Union Agency for Network and Information Security (ENISA)[191]: dedicated to enhancing cybersecurity across Europe. Despite that does not have law enforcement powers, it plays a key role in providing expertise, guidance, and recommendations to EU institutions and member states.

ENISA's primary objective is to ensure a high and effective level of network and information security within the European Union.

Albania's law enforcement agencies**:**

a. In 2015 was established a National Cybersecurity Agency[192], (The national Computer Incident Response Team for Albania

189 European Union Agency for Criminal Justice Cooperation, *official website*. Retrieved October 16, 2023, from Eurojust | European Union Agency for Criminal Justice Cooperation (europa.eu)

190 European commission, *official website*. Retrieved October 16, 2023, from European Commission, official website - European Commission (europa.eu)

191 European Union Agency for Network and Information Security, *official website*. Retrieved October 16, 2023, from ENISA

192 National Security Strategy. The official document is retrieved October 16, 2023, from National Cybersecurity Agency

–previously known as ALCIRT, now part of AKCESK[193]) to coordinate and respond to cyber threats across the country. CERT-Al[194] works in partnership with other government agencies, such as the Ministry of Interior, Ministry of Defense, and Ministry of Justice, to protect critical infrastructure and national security

b. The National Authority on Electronic Certification and Cyber Security (NAECCS) is another responsible authority for implementation and supervision of legislation on electronic signature, electronic identification, and the legislation on Cyber Security[195] in Albania.

CONCLUSION

The research provides a comprehensive exploration of the critical role of cyber investigation in addressing the ever-evolving landscape of cybercrimes. It highlights the profound impact of cybercrimes on individuals, businesses, governments, and international stability and the imperative need for advanced methodologies and collaboration to counter these digital offenses effectively. The paper underscores that traditional methods of combating crime fall short in the face of intricate cybercrimes, necessitating the emergence of cyber investigation as a vital tool.

The study emphasizes that cyber investigation is a multidisciplinary approach, fusing criminology, computer science, and cybersecurity expertise, equipped with cutting-edge technology to detect, investigate,

193 National Authority for Electronic Certification and Cyber Security, *official website*. Retrieved October 16, 2023, from About Us - AKCESK

194 CERT is not an acronym; it is a name and a registered service mark of Carnegie Mellon University. The CERT Coordination Centre was the first computer incident response team (CIRT) and although certain CIRT teams have been authorized to use the CERT name by Carnegie Mellon University, the term CIRT is used when referring to general incident response teams.

195 National Cyber Security Index of Albania as of October 2022. Retrieved October 16, 2023, from NCSI :: Albania (ega.ee)

and prosecute cybercriminals. It serves as a safeguard for our digital ecosystem, bolstering digital security. Moreover, the research highlights the significance of international cooperation in addressing cybercrimes and offers insights into the potential of cyber investigation to revolutionize broader crime prevention and law enforcement.

RECCOMENDATIONS

1. **Investment in Cyber Investigation Training and Resources**: Governments, law enforcement agencies, and cybersecurity organizations should invest in training programs and resources to enhance the capabilities of cyber investigators. The rapidly evolving nature of cyber threats necessitates continuous education and skill development to stay ahead of cybercriminals.
2. **International Collaboration**: Given the global nature of cybercrimes, fostering international collaboration and information sharing among countries and organizations is imperative. Encouraging the sharing of threat intelligence, best practices, and cybercrime-related data can help identify and combat cybercriminals operating across borders.
3. **Utilization of Advanced Technologies**: Embrace and integrate advanced technologies, such as artificial intelligence, machine learning, and automation, into cyber investigation practices. These technologies can assist in analyzing vast datasets, detecting patterns, and improving the speed and accuracy of investigations.
4. **Public Awareness and Education**: Governments and organizations should run public awareness campaigns to educate individuals and businesses about online threats and best practices for staying safe. Well-informed individuals are less likely to fall victim to cybercrimes.
5. **Consistent Cybersecurity Regulations**: Align national

cybersecurity laws and regulations with international standards, such as those set by the European Union, to ensure a comprehensive legal framework that can effectively address cybercrimes while maintaining fairness and neutrality.

6. **Open Source Intelligence (OSINT) Initiatives**: Foster initiatives that encourage the responsible use of open-source intelligence. Leveraging publicly available information from online sources can provide valuable insights into cybercriminal activities. Support and training for OSINT analysts should be promoted.
7. **Collaboration with Tech Industry**: Strengthen cooperation with technology companies, internet service providers (ISPs), and hosting providers. These entities can play a pivotal role in providing information and data that can aid in tracking and prosecuting cybercriminals.
8. **Comprehensive Cybersecurity Legislation**: Continuously update and refine existing cybersecurity laws to keep pace with evolving cyber threats. These laws should encompass aspects of data protection, digital signatures, electronic identification, and trusted services.
9. **Response to State-Sponsored Cyberattacks**: Develop clear strategies and policies for responding to state-sponsored cyberattacks, like those outlined in the case of the Albanian government's experience. This should include measures for diplomatic actions, sanctions, and international cooperation in addressing such incidents.
10. **Regular Cybercrime Research and Analysis**: Promote continuous research and analysis of emerging cyber threats and trends. Understanding the modus operandi of cybercriminals and their evolving tactics is vital for staying ahead of the curve.

By implementing these recommendations, stakeholders can strengthen their ability to combat cybercrimes, protect digital

ecosystems, and contribute to a safer and more secure digital future for individuals, businesses, and governments.