DCAF Geneva Centre for Security Sector Governance

Institute for Democracy and Mediation
Instituti për Demokraci dhe Ndërmjetësim

TEJKALIMI I HENDEKUT MIDIS SIGURISË KIBERNETIKE DHE TË DREJTAVE TË NJERIUT

Megi Reçi dhe Sara Kelmendi | Instituti për Demokraci dhe Ndërmjetësim

Nismë e DCAF – Qendra në Gjenevë për Qeverisjen e Sektorit të Sigurisë, në kuadër të Projektit "Qeverisja e Mirë në Sigurinë Kibernetike në Ballkanin Perëndimor", mbështetur nga Zyra e Jashtme e Komonuelthit dhe Zhvillimit e Mbretërisë së Bashkuar (FCDO).

Nëntor 2022

TABELA E PËRMBAJTJES

HYRJE[1]

Ashtu si aksioma e biznesit sipas të cilës “nuk mund të menaxhosh diçka të cilën nuk mund ta matësh”, është gjithashtu e vërtetë se “nuk mund të ndryshosh diçka pa e hartëzuar apo identifikuar më parë” – një realitet i rëndësishëm ky për ndërlidhjen mes sigurisë kibernetike dhe të drejtave të njeriut.

Përkufizimet e sigurisë kibernetike zakonisht e vendosin theksin tek mbrojtja e aseteve të shtetit, institucioneve dhe mjedisit digjital[2]. Megjithatë, këto përkufizime neglizhojnë shumë sfida të sigurisë me të cilat përballen individët në internet. Ky publikim, shqyrton politikat kombëtare të sigurisë kibernetike në Shqipëri përmes një qasjeje me në qendër individin dhe vlerëson nivelet e sigurisë kibernetike për sa i përket mbrojtjes së të drejtave të njeriut. E thënë ndryshe, siguria kibernetike meriton një qasje analitike më të përqendruar tek individi, që nxjerr në pah jo vetëm çështjet që prekin aktorët shtetërorë, por edhe çështje që këta aktorë mund të shkaktojnë tek qytetarët.

Kjo qasje ndaj sigurisë kibernetike me në qendër individin, rrjedh nga teoria më e gjerë e qeverisjes së mirë të sektorit të sigurisë.[3] Qeverisja e mirë e këtij sektori përqëndrohet jo vetëm në mbrojtjen e rrjeteve, sistemeve dhe stabilitetit të shtetit, por edhe të të drejtave të njeriut në një shoqëri demokratike. Ajo përfshin parime të tilla si përgjegjshmëria, pjesëmarrja, gjithëpërfshirja, efektiviteti, efikasiteti dhe transparenca. Kjo çon në ofrim më të mirë të sigurisë dhe lejon mbikëqyrjen demokratike të saj, e cila nga ana tjetër parandalon abuzimin me pushtetin nga ofruesit e sigurisë. Kështu, siguria kibernetike mund të përkufizohet si siguria e individëve dhe të drejtave të njeriut në internet, si dhe e rrjeteve dhe shërbimeve që janë thelbësore për këtë objektiv, të cilat së bashku mbrojnë rendin demokratik dhe sundimin e ligjit.

Tashmë ekzistojnë një sërë kërkimesh mbi lidhjen mes sigurisë kibernetike dhe të drejtave të njeriut.[4] Për dekada, aktivistët, akademikët, përfaqësuesit e qeverive dhe sektorit privat kanë punuar për të përcaktuar kuptimin e “të drejtave të njeriut online”, “të drejtave të njeriut në internet” dhe “sigurisë kibernetike dhe të drejtave të njeriut”.[5] Vlerësimet kombëtare mbi sigurinë kibernetike zakonisht vlerësojnë mënyrat se si qeveritë i kanë inkorporuar standardet ekzistuese të të drejtave të njeriut në sferën online.[6]

Në këtë publikim, vlerësohet niveli i zbatimit të të drejtave të njeriut në kontekstin shqiptar duke hulumtuar

---

1 Kjo pjesë është shkruar nga Laylo Merali dhe Ena Bavčić në kuadër të *botimit rajonal* dhe është përshtatur në shqip nga autorët.

2 *Përkufizimi i sigurisë kibernetike sipas Unionit Ndërkombëtar të Telekomunikacionit*

3 DCAF, *Udhëzues për Qeverisjen e mirë të Sigurisë Kibernetike*

4 Publikimet e Global Partners Digital në *CybilPortal*.

5 *Nisma e Microsoft mbi teknologjinë dhe të drejtat e njeriut*

6 Freedom House: *Liria në rrjet*.

sfidat e evidentuara dhe përmbushjen e parimit të qeverisjes së mirë. Në veçanti, ekzaminohen ligjet, praktikat dhe kapacitetet e aktorëve të sigurisë kibernetike dhe të drejtave të njeriut dhe aktorëve mbikëqyrës. Pse vazhdojnë të ndodhin shkelje, duke përfshirë edhe në nivel sistemik, nëse tashmë kemi standarde ndërkombëtare për zbatimin e të drejtave të njeriut në nivel kombëtar? A nuk janë standardet mjaftueshëm të qarta apo të detajuara për të mundësuar zbatimin e tyre në kontekste të ndryshme kombëtare? Si shpjegohet që edhe pse një vend i ka transpozuar standardet në ligj, ato nuk njihen/zbatohen?

Rrjeti Kërkimor i Sigurisë Kibernetike në Ballkanin Perëndimor, pjesë e të cilit është edhe Instituti për Demokraci dhe Ndërmjetësim (IDM), ka ndërmarrë hulumtime novatore në këtë fushë, duke filluar me këtë studim të parë. Kjo është nga nismat kryesore të projektit të Qendrës së Gjenevës për Qeverisjen e Sektorit të Sigurisë (DCAF) "Qeverisja e mirë e Sigurisë Kibernetike në Ballkanin Perëndimor", i cili mbështetet nga Zyra e Jashtme e Komonuelthit dhe Zhvillimit e Mbretërisë së Bashkuar. Ky kapitull për Shqipërinë është pjesë e një botimi më të gjerë rajonal i cili mbulon gjashtë shtetet e Ballkanit Perëndimor: Shqipërinë, Bosnjen dhe Hercegovinën, Kosovën*, Malin e Zi, Maqedoninë e Veriut dhe Serbinë. Ky publikim fokusohet në hartëzimin e mundësive dhe sfidave të të drejtave të njeriut në lidhje me sigurinë kibernetike, dhe përfaqëson një fushë të pa eksploruar në Shqipëri dhe rajon.

Botimi ofron një vështrim të përgjithshëm konceptual në lidhje me sigurinë kibernetike dhe të drejtat e njeriut në Shqipëri, duke hartëzuar legjislacionin, masat e sigurisë kibernetike, kuadrin politik dhe institucional përkatës. Në këtë seksion, analizohen përputhshmëria e këtyre të fundit me standardet ndërkombëtare, por edhe mangësitë sa i përket bashkëpunimit ndërinstitucional dhe kapaciteteve teknike. Më pas ekzaminohen katër çështje thelbësore tematike: siguria kibernetike dhe e drejta për privatësi, siguria kibernetike dhe liria e shprehjes, siguria kibernetike dhe mbrojtja nga diskriminimi, siguria kibernetike dhe liria e tubimit paqësor. Në lidhje me **të drejtën për privatësi**, ekzaminohen raste të shkeljeve të shkaktuara nga aktorë publikë ose jo publikë, mënyrat si mund të kontribuojë higjiena kibernetike në mbrojtjen e të drejtës për privatësi, dhe niveli i reagimit ndaj këtyre shkeljeve. Në lidhje me **lirinë e shprehjes**, trajtohen raste të censurës online, shpifjes, kërcënimeve ndaj gazetarëve dhe shoqërisë civile si dhe reagimi apo përfshirja e aktorëve publikë në këto shkelje. Në lidhje me **mbrojtjen nga diskriminimi**, shqyrtohen rastet kur shkeljet e të drejtave të njeriut në hapësirën kibernetike targetojnë grupe specifike apo të nënpërfaqësuara, si dhe aksesin që kanë këto grupe në mekanizmat mbrojtës përkatës. Në lidhje me **lirinë e tubimit**, ekzaminohet niveli i mbrojtjes që gëzon kjo e drejtë në nivel kombëtar, mënyrat se si përdorimi i teknologjive apo kufizimeve të ndryshme ndikojnë tek veprimtaria e aktivistëve dhe organizimi i tubimeve, si dhe reagimin përkatës ndaj shkeljeve.

Së fundi, paraqiten rekomandime konkrete të cilat i drejtohen aktorëve publikë (qeveria, Parlamenti dhe autoritetet ligjzbatuese) dhe atyre jo-publikë (shoqëria civile, akademia, media, donatorët ndërkombëtarë). Në përgjithësi, ky botim ka për qëllim të ndihmojë në përmirësimin e të kuptuarit të kapaciteteve të sigurisë kibernetike për një zbatim më të mirë të normave të sigurisë kibernetike në lidhje me të drejtën për privatësi, lirinë e shprehjes, mbrojtjen nga diskriminimi dhe lirinë e tubimit.

* Ky shënim është pa paragjykim ndaj qëndrimeve mbi statusin dhe është në përputhje me Rezolutën 1244 të Këshillit të Sigurimit të OKB-së dhe Opinionin e GJND-së për shpalljen e pavarësisë së Kosovës

METODOLOGJIA

Për këtë hulumtim të dhënat parësore janë mbledhur me metoda cilësore të kërkimit. Procesi i kërkimit kaloi nëpër tre faza të cilat përfshinë mbledhjen e të dhënave, analizën dhe konsultimin/validimin e gjetjeve kryesore. Instrumentet metodologjike të përdorura për mbledhjen e të dhënave janë shqyrtimi i literaturës, një pyetësor anonim, intervistat e thelluara dhe takimet validuese.

Shqyrtimi i literaturës përfshiu kuadrin ligjor dhe strategjik, vendime të gjykatave dhe institucioneve të pavararua, raporte të institucioneve të qeverisjes qendrore, institucioneve të pavarura dhe agjencive ligjzbatuese, raporte dhe studime të organizatave vendase dhe ndërkombëtare, artikuj të ndryshëm, dërgimin e kërkesave zyrtare për informacion etj. Të dhënat e mbledhura i shërbyen analizës cilësore.

Pyetësori anonim targetoi aktivistë, gazetarë dhe përfaqësues të organizatave të shoqërisë civile dhe u plotësua elektronikisht në mënyrë anonime nga 19 persona. Pyetësori kishte qëllim vetëm identifikimin e rasteve të shkeljeve të katër të drejtave objekt studimi dhe reagimin institucional për çdo rast.

15 intervista të thelluara u zhvilluan me ekspertë të të drejtave të njeriut, aktivistë, gazetarë, juristë, përfaqësues të institucioneve të sigurisë kibernetike, përfaqësues të institucioneve të pavarura, përfaqësues të organizatave të shoqërisë civile. Informacioni i mbledhur nga intervistat i shërbeu analizës cilësore, pasurimit të mëtejshëm të studimit me raste studimore dhe hartimit të rekomandimeve.

4 takime validuese u zhvilluan pas hartimit të draftit të parë të studimit dhe përfshinë aktorë të ndryshëm publikë dhe jo publikë. Qëllimi i këtyre takimeve ishte konsultimi/validimi i gjetjeve paraprake dhe rekomandimeve kryesore para publikimit të studimit.

Konsiderata etike

Të dhënat e mbledhura në kuadër të studimit ruhen në ambientet e Institutit për Demokraci dhe Ndërmjetësim. Të dhënat personale të mbledhura në kuadër të studimit janë përpunuar në përputhje me Ligjin nr. 9887, datë 10.03.2008 “Për Mbrojtjen e të Dhënave Personale”. Të dhënat personale të të intervistuarve dhe individëve të referuar në studim janë anonimizuar me qëllim mbrojtjen e privatësisë.

Para kryerjes së intervistave, të intervistuarve iu shpjegua në detaje çfarë synon hulumtimi. Pjesëmarrësit u angazhuan vullnetarisht dhe iu kërkua pëlqimi verbal përpara se të intervistoheshin, ndërsa për plotësimin e anketave iu kërkua pëlqimi me shkrim. Pjesëmarrësit dhe institucionet publike ishin plotësisht të informuar mbi qëllimin e studimit dhe rolin e tyre në të, duke iu mundësuar të gjithë të përfshirëve të kontribuojnë me komente mbi draftin e studimit gjatë fazës së validimit.

Kufizimet e hulumtimit

Kufizimi kryesor i këtij hulumtimi lidhet me kohëzgjatjen e mbledhjes së të dhënave. Meqenëse hulumtimi është realizuar në periudhën dhjetor 2021 - maj 2022, publikimi nuk adreson një sërë çështjesh të rëndësishme që kanë ndodhur pas këtij afati kohor, siç janë sulmet kibernetike ndaj qeverisë shqiptare nga aktorë të huaj dhe rrjedhje të mëtejshme të të dhënave sensitive. Gjithashtu, studimi nuk analizon mangësitë në kuadrin ligjor për të dhënat personale, duke qenë se ky i fundit ishte duke u amenduar gjatë periudhës së shkrimit të studimit. Duke iu përmbajtur objektivave të studimit rajonal, hulumtimi për Shqipërinë është i kufizuar në ekzaminimin e ligjeve, praktikave dhe kapaciteteve të aktorëve të sigurisë kibernetike dhe të drejtave të njeriut dhe ilustron me shembuj shkelje të të drejtave të njeriut në hapësirën kibernetike, të cilat mund të shërbejnë si një pikë reference për të përmirësuar më tej kuadrin ligjor dhe politik; kapacitetet dhe bashkëpunimin institucional; ndërgjegjësimin dhe llogaridhënien; kapacitetet dhe mbështetjen e OSHC-ve dhe medias. Ky studim nuk synon kurrsesi të paraqesë një hartëzim të plotë dhe sasior të shkeljeve të të drejtave të njeriut në hapësirën kibernetike në Shqipëri.

KREU 1

VËSHTRIM I PËRGJITHSHËM MBI SIGURINË KIBERNETIKE NË SHQIPËRI

1.1 Kuadri ligjor për sigurinë kibernetike

Indeksi Global i Sigurisë Kibernetike i vitit 2020 e renditi Shqipërinë në vendin e 80-të nga 132 shtete në nivel global dhe të 40-in nga 46 shtete në nivel evropian, sa i përket vlerësimit të masave të sigurisë kibernetike të marra në vend. Sipas këtij Indeksi, Shqipëria ka performancën më të mirë sa i përket masave ligjore, të cilat konsiderohen si fushë relativisht e fortë, ndërsa pikët më të ulëta u shënuan tek masat e bashkëpunimit dhe ngritjes së kapaciteteve.[7] Kuadri ligjor për sigurinë kibernetike në Shqipëri, është zhvilluar kryesisht në kuadër të harmonizimit të legjislacionit kombëtar me direktivat e Bashkimit Evropian (BE) dhe aderimit në Konventat e Këshillit të Evropës (KiE). Ratifikimi i Konventës për Krimin në Fushën e Kibernetikës dhe i protokollit shtesë të saj, kanë ndikuar në përafrimin e legjislacionit penal kombëtar me standardet që ajo përcakton në lidhje me krimet kibernetike dhe provat elektronike. Në vitin 2022, Shqipëria nënshkroi protokollin për ndryshimin e Konventës për Mbrojtjen e Individëve nga Përpunimi Automatik i të Dhënave Personale. Duke qenë një dokument i miratuar së fundi, ndikimi i tij në sistemin ligjor shqiptar mbetet për t'u vlerësuar në vitet në vijim. Sipas Komisionit Evropian[8], Shqipëria është mesatarisht e përgatitur në fushën e shoqërisë së informacionit dhe duhet të përmirësojë më tej kuadrin ligjor dhe politikat përkatëse, të harmonizojë legjislacionin për sigurinë kibernetike dhe komunikimet elektronike me legjislacionin e BE-së si dhe të përmirësojë mbledhjen e të dhënave statistikore për performancën digjitale dhe konkurrencën.

Në vijim paraqitet një analizë e akteve kryesore legjislative që përbëjnë kuadrin ligjor kombëtar për sigurinë kibernetike.

Ligji nr. 7895/1995, **"Kodi Penal i Republikës së Shqipërisë"**, (Kodi) parashikon veprat penale në fushën e teknologjisë së informacionit dhe komunikimit (TIK) dhe në përgjithësi është në përputhje me Konventat e sipërpërmendura të KiE-së. Kodi mbron të drejtën e jetës private nëpërmjet dispozitave të ndryshme, disa prej të cilave kriminalizojnë ndërhyrjen në jetën private të dikujt, përhapjen e sekreteve vetjake dhe cënimin e korrespondencës private. Në lidhje me kërcënimet, fyerjet dhe shpërndarjen elektronike të përmbajtjeve diskriminuese, Kodi i kufizon motivet vetëm tek racizmi ose ksenofobia dhe nuk trajton motive të tjera të mundshme. Sa i përket nxitjes së urrejtjes apo grindjeve, Kodi konsideron si motiv racën, përkatësinë etnike, fenë dhe orientimin seksual duke lënë jashtë përkatësinë gjinore. Kodi parashikon që akte të tilla mund të kryhen duke përdorur çdo mjet apo formë, pra duke përfshirë edhe ato elektronike. Kodi trajton edhe ngacmimin seksual të kryer me çdo mjet apo formë, ndërkohë që për sa i

7 Unioni Ndërkombëtar i Telekomunikacionit (2021) *Indeksi Global i Sigurisë Kibernetike 2020.*

8 Komisioni Evropian (2021) *Raporti për Shqipërinë 2021.*

përket përndjekjes Kodi nuk i mbulon rastet kur ajo ndodh/kryhet online. Megjithatë, motivet diskriminuese konsiderohen si rrethanë rënduese për çdo vepër penale. Së fundi, shpifja dhe përhapja e informacionit të rremë që ngjall panik janë penalisht të dënueshme dhe në praktikë janë zbatuar si për artikujt mediatikë, statuset e mediave sociale apo opinionet e publikuara në internet. Rregullat procedurale për hetimin dhe ndjekjen penale të krimeve dhe kundërvajtjeve të përcaktuara në këtë Kod përcaktohen me Ligjin nr. 7905/1995, **"Kodi i Procedurës Penale"**. Po ashtu, Ligji nr. 2/2017, **"Për Sigurinë Kibernetike"**, garanton sigurinë në hapësirën kibernetike dhe zbatohet për rrjetet e komunikimit dhe sistemet e informacionit, shkelja ose shkatërrimi i të cilave do të ndikonte në shëndetin, sigurinë, mirëqenien ekonomike të shtetasve dhe funksionimin efikas të ekonomisë në vend. Nga ana tjetër, Ligji nr. 9918/2008, **"Për Komunikimet Elektronike"**, siguron sekretin e komunikimeve elektronike dhe mbrojtjen e të dhënave personale, ndërsa përgjimi i komunikimeve lejohet vetëm kur kërkohet ligjërisht (p.sh. në kuadër të një hetimi penal). Ky ligj parashikon masat juridike në rast shkeljesh dhe siguron akses të barabartë në komunikimet dhe shërbimet elektronike, pa diskriminim, duke i vënë theksin përshtatjes ndaj nevojave të personave me aftësi të kufizuara. Ligji nr. 18/2017, **"Për të Drejtat dhe Mbrojtjen e Fëmijës"**, trajton forma të ndryshme të dhunës ndaj fëmijëve, si bulizmin, abuzimin seksual, trafikimim, etj., si dhe sigurinë e fëmijëve në internet. Më tej, Vendimi nr. 465/2019 i Këshillit të Ministrave përcakton masat konkrete për mbrojtjen e fëmijëve nga aksesi në përmbajtje të paligjshme dhe/ose të dëmshme në internet, duke përcaktuar edhe detyrime për aktorë të ndryshëm. Së fundi, ligje të tjera që ndikojnë në këtë sektor janë edhe Ligji nr. 9880/2008, **"Për Nënshkrimin Elektronik"**, i cili përcakton rregullat për njohjen dhe përdorimin e nënshkrimeve elektronike; Ligji nr. 107/2015, **"Për Identifikimin Elektronik dhe Shërbimet e Besuara"**, i cili përcakton rregullat për identifikimin elektronik, vulat elektronike, shërbimet e transmetimit elektronik, dhe autentifikimin e faqeve në internet; dhe Ligji nr. 10128/2009, **"Për Tregtinë Elektronike"**, i cili përcakton rregullat për zhvillimin e tregtisë elektronike, privatësinë e konsumatorëve, gjobat për shkeljet, dhe ndër të tjera, ky ligj zbatohet edhe për mediat online që ofrojnë shërbime abonimi për të gjeneruar të ardhura.

1.2 Kuadri politik për sigurinë kibernetike

Angazhimet e qeverisë shqiptare përmes dokumenteve të ndryshëm strategjikë fokusohen në ngritjen e infrastrukturës dhe kapaciteteve të institucioneve publike, përmirësimin e shërbimeve publike dhe e-qeverisjes, si dhe në rregullimin e tregut për shërbimet online dhe aktivitetet ekonomike online. Sektori i sigurisë kibernetike i konsideron sistemet dhe infrastrukturën si asete që duhen mbrojtur, rregulluar dhe mirëmbajtur, por duke i parë si të shkëputura nga dimensioni i sigurisë njerëzore.[9] Për rrjedhojë, hapësira kibernetike në Shqipëri trajtohet gjerësisht si treg dhe hapësirë shërbimesh. Qytetarët shihen ngushtësisht si klientë dhe vlerësimet e riskut dhe masat mitiguese për kërcënimet e të drejtave të tyre në këtë mjedis mungojnë. Përjashtimi i vetëm nga kjo normë në këtë sektor duket se është bërë në lidhje me mbrojtjen e fëmijëve në internet, për të cilën, siç u theksua më lart, ofrohet një nivel i caktuar rregullimi dhe vëmendje nga ana e politikave. Vëmendja e politikave që me të drejtë i është dhënë mbrojtjes së fëmijëve nga abuzimi në internet dhe nevojës për të rritur sigurinë e tyre, duhet të shtrihet edhe në çështje të tjera urgjente të të drejtave të njeriut që prekin grupe të ndryshme të cenueshme si dhe publikun në përgjithësi. Në këtë aspekt, qeverisjes së sigurisë kibernetike do t'i duhet të zhvillojë një qasje më të ndjeshme ndaj të drejtave të njeriut, për të adresuar rreziqet që shoqërojnë digjitalizimin.

Në vijim paraqitet një analizë e dokumenteve kryesore strategjikë të sigurisë kibernetike nga këndvështrimi i të drejtave të njeriut.

---

9 DCAF (2021) *Dhuna kibernetike ndaj grave dhe vajzave në Ballkanin Perëndimor: Raste Studime të Përzgjedhura dhe një Qasje e Qeverisjes së Sigurisë Kibernetike*

Strategjia Kombëtare për Sigurinë Kibernetike dhe Plani i saj i Veprimit 2020–2025 mbulojnë fusha të ndryshme të cilat kërkojnë ndërhyrje në fushën e krimit kibernetik, radikalizmit, ekstremizmit të dhunshëm, mbrojtjes së fëmijëve në internet, etj. Përveç fokusit në mbrojtjen e fëmijëve, strategjia nuk ndërthuret me asnjë çështje tjetër të të drejtave të njeriut dhe nuk trajton mbrojtjen e grupeve të tjera të rrezikuara në hapësirën kibernetike, si gratë, apo pakicat etnike, racore dhe seksuale. Kur u hartua kjo strategji, në konsultim morën pjesë organizatat e shoqërisë civile (OSHC) që punojnë për të drejtat e fëmijëve, por gjithsesi nuk u konsultua asnjë nga institucionet e pavarura[10] që mbulojnë të drejtat e njeriut.[11] Nga ana tjetër, **Strategjia për Mbrojtjen Kibernetike 2021-2023** është e fokusuar në mënyrë rigoroze në çështjet e mbrojtjes kombëtare, prandaj nuk ka asnjë lidhje të drejtpërdrejtë me çështjet e të drejtave të njeriut. Po ashtu, në **Strategjinë Ndërsektoriale "Agjenda Digjitale e Shqipërisë" 2015-2020** trajtohej digjitalizimi i proceseve ekonomike, sociale, institucionale dhe administrative. Strategjia ishte më tepër e orientuar drejt shërbimeve sesa drejt qytetarëve dhe në asnjë nga objektivat e saj nuk kishte lidhje të drejtpërdrejtë me çështjet e të drejtave të njeriut. Vlen të theksohet se për Agjendën e re Digjitale dhe Planin e Veprimit 2022-2026 raportohet të jenë bërë konsultime gjatë periudhës tetor-nëntor 2021, ndërkohë që institucionet e pavarura që mbulojnë të drejtat e njeriut nuk janë përfshirë në këtë proces dhe raporti mbi rezultatet e konsultimit publik është shumë i paqartë në lidhje me aktorët që janë përfshirë në këtë konsultim.[12] I vetmi dokument strategjik për çështjet e sigurisë kibernetike në vend me një qasje tek të drejtat e njeriut ishte **Plani i Veprimit për një Internet më të Sigurt për Fëmijët në Shqipëri 2018-2020**, i cili mund të shërbejë si praktikë e mirë për këtë sektor.

1.3 Kuadri institucional për sigurinë kibernetike

Aktualisht nuk ka asnjë institucion në qeverinë shqiptare, me kompetenca të centralizuara dhe politikëbërëse për çështjet e sigurisë kibernetike, teknologjisë së informacionit dhe komunikimit (TIK), komunikimeve elektronike apo medias. Institucioni i fundit i tillë për nga natyra ishte Ministria e Inovacionit dhe Administratës Publike[13], e cila u shpërbë në vitin 2017 për shkak të ristrukturimit të qeverisë. Aktualisht, aktorët kryesorë për qeverisjen e sigurisë kibernetike janë agjencitë e një natyre më shumë teknike se sa politikëbërëse. Ato përbëhen nga institucionet e qeverisë qendrore (Kryeministria dhe ministri të linjës), agjencitë në varësi të tyre si dhe institucionet e pavarura. Gjithashtu, qeveria planifikon të krijojë një Qendër Kombëtare të Operacioneve të Sigurisë Kibernetike si dhe një Qendër Ekselence për Sigurinë Kibernetike[14] dhe mbetet për t'u parë se si këto institucione do të ndikojnë në qeverisjen dhe politikëbërjen e sigurisë kibernetike. Në këtë proces, qeveria do të marrë ndihmë nga Jones International Group, një kompani me qendër në SHBA, kontrata me të cilën ishte duke u negociuar në kohën e shkrimit të këtij raporti. Vlen të theksohet se Komisioni i krijuar për negocimin e kësaj kontrate nuk përfshin asnjë nga institucionet e pavarura që mbulojnë të drejtat e njeriut.[15] Natyra e larmishme e punës së aktorëve të përfshirë në çështjet e sigurisë kibernetike mund të sjellë vështirësi në koordinim dhe të shkaktojë zbehjen e kufijve tradicionalë mes llogaridhënies dhe mbikëqyrjes. Prandaj, nevojitet koordinim më i mirë ndërinstitucional, si dhe adresim i riskut të lënies së disa fushave me mbikëqyrje të pamjaftueshme ose pa mbikëqyrje, në momentin e krijimit ose ristrukturimit të institucioneve.

---

10 Komisioneri për Mbrojtjen nga Diskriminimi; Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale; Avokati i Popullit

11 Informacion i dhënë nga AKCESK përmes kërkesës për informacion datë 28/7/2022.

12 Informacion i dhënë nga AKSHI përmes kërkesës për informacion datë 10/5/2022.

13 Vendim i Këshillit të Ministrave nr.943/2013.

14 Vendim i Këshillit të Ministrave nr.1/2022.

15 Ligj nr. 34/2022 për përcaktimin e procedurës së veçantë për negocimin dhe zbatimin e kontratës me shoqërinë Jones Group International për forcimin e sigurisë kibernetike.

Në vijim përshkruhet roli i aktorëve kryesorë të sigurisë kibernetike në vend.

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK), agjenci në varësi të Kryeministrisë, është përgjegjës për vendosjen e masave kombëtare të sigurisë kibernetike dhe mbikëqyrjen e zbatimit të ligjeve për nënshkrimet elektronike, identifikimin elektronik, shërbimet e besuara dhe sigurisë kibernetike. AKCESK shërben si pika kryesore e kontaktit në rastet e sulmeve dhe incidenteve që lidhen me sigurinë kibernetike dhe është institucioni kryesor përgjegjës për zbatimin e Strategjisë Kombëtare për Sigurinë Kibernetike dhe Planin e saj të Veprimit. Nga ana tjetër, janë dy njësi të posaçme përgjegjëse për hetimin e krimit kibernetik brenda **Drejtorisë së Policisë së Tiranës** dhe **Drejtorisë së Përgjithshme të Policisë**, në varësi të Ministrisë së Brendshme. Drejtoritë Vendore të Policisë nuk kanë njësi apo oficerë të dedikuar për krimin kibernetik, prandaj këto dy njësi me qendër në Tiranë mbulojnë raportimet e krimit kibernetik në nivel kombëtar.[16] Për t'u mundësuar qytetarëve të raportojnë krimin kibernetik, Policia ka krijuar një rubrikë të posaçme në faqen e saj të internetit, ndonëse aktualisht kjo rubrikë është jashtë funksionit.[17] Po ashtu, njësia përkatëse e **Prokurorisë** për hetimin e krimit kibernetik merret me ndjekjen penale të krimeve kibernetike. Një tjetër aktor vendimtar në sektorin e TIK-ut është **Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI)** - agjenci në varësi të Kryeministrisë. Kjo agjenci është përgjegjëse për bazat e të dhënave shtetërore, administrimin dhe mirëmbajtjen e shërbimeve të qeverisjes elektronike të ofruara nëpërmjet portalit e-Albania, sportelet me një ndalesë për shërbimet online të administratës publike.[18] AKSHI është përgjegjës edhe për administrimin e sistemeve TIK të institucioneve publike dhe është institucioni kryesor për hartimin dhe zbatimin e Strategjisë së Agjendës Digjitale. Më tej, **Autoriteti i Komunikimeve Elektronike dhe Postare (AKEP)** është organi i pavarur rregullator që mbikëqyr komunikimet elektronike dhe shërbimet postare dhe ka autoritetin të japë sanksione administrative në rast shkeljesh. AKEP mund të kërkojë nga Ofruesit e Shërbimeve të Internetit (ISP) heqjen e përmbajtjes së paligjshme në bazë të vendimeve të autoriteteve kompetente, megjithëse nuk ka një përkufizim të njëjtësuar të asaj që konsiderohet përmbajtje e paligjshme dhe/ose e dëmshme, apo të autoriteteve kompetente që mund të kërkojnë heqjen e një përmbajtje të tillë.[19] Për të adresuar këtë, ligji për komunikimet elektronike nuk është i mjaftueshëm dhe duhet të bëhen referenca në ligje të tjera. Përsa i përket mbrojtjes së fëmijëve nga përmbajtjet e dëmshme ose të paligjshme në internet, **Agjencia Shtetërore për të Drejtat dhe Mbrojtjen e Fëmijëve** është agjencia përgjegjëse e cila mbikëqyr zbatimin e masave mbrojtëse/parandaluese nga ISP-të, institucionet arsimore dhe çdo institucion tjetër publik apo privat. Së fundi, **Ministria e Mbrojtjes (MM)** është përgjegjëse për trajtimin e incidenteve kibernetike të lidhura me Ministrinë e Mbrojtjes dhe Forcat Ajrore dhe mbikëqyr zbatimin e Strategjisë për Mbrojtjen Kibernetike.

16 Intervistë me përfaqësues të Njësisë C për Hetimin e Krimeve Kompjuterike, Policia e Tiranës, datë 26/5/2022.

17 Aksesuar për herë të fundit më datë 13/6/2022.

18 *e-Albania*. Aksesuar për herë të fundit më datë 13/06/2022.

19 Birn Shqipëri (2020). *Qeverisja e internetit në Shqipëri dhe roli i saj në lirinë e medias.*

KREU 2

SIGURIA KIBERNETIKE DHE KUADRI I TË DREJTAVE TË NJERIUT[20]

Në përgjithësi, Shqipëria aplikon standardet ndërkombëtare të të drejtave të njeriut dhe ka ratifikuar pjesën më të madhe të konventave ndërkombëtare për mbrojtjen e të drejtave themelore.[21] Sipas Kushtetutës së Shqipërisë, kufizimet e të drejtave të njeriut nuk mund të tejkalojnë kufizimet e parashikuara nga Konventa Evropiane për të Drejtat e Njeriut (KEDNJ) - duke i dhënë kësaj Konvente një status të veçantë brenda sistemit ligjor vendas. KEDNJ siguron mbrojtjen e të drejtave dhe lirive themelore duke përfshirë ato të analizuara në këtë raport: të drejtën për respektimin e jetës private dhe familjare, lirinë e shprehjes, ndalimin e diskriminimit dhe lirinë e tubimit dhe organizimit. Tashmë pranohet gjerësisht se ligji ndërkombëtar zbatohet edhe për hapësirën kibernetike,[22] prandaj, standardet e vendosura nga KEDNJ si dhe praktika gjyqësore e Gjykatës Evropiane për të Drejtat e Njeriut (GJEDNJ) zbatohen edhe për rastet kur shkeljet e të drejtave ndërthuren me sigurinë kibernetike, qoftë kur këto shkelje kryhen në hapësirën kibernetike, apo edhe kur mundësohen/lehtësohen prej saj.

E drejta për privatësi përfshin mbrojtjen e të dhënave personale dhe detyrimin për t'i dhënë ato vetëm në rrethana/kritere strikte, siç parashikohet në ligj (p.sh. në kuadër të një hetimi penal). Pëlqimi kërkohet gjatë mbledhjes, përdorimit dhe publikimit të të dhënave, ndërkohë që secili ka të drejtë të dijë se çfarë të dhënash janë mbledhur rreth tij dhe ka të drejtë të kërkojë korrigjimin ose fshirjen e tyre nëse të dhënat janë të pavërteta, të paplota ose të mbledhura në kundërshtim me ligjin. Ligji nr. 9887/2008 për Mbrojtjen e të Dhënave Personale parashikon kriteret për përpunimin e ligjshëm të të dhënave, kufizimet, si dhe mjetet juridike në dispozicion në rastet kur ndodhin shkelje. Ky ligj, në kohën e shkrimit të këtij raporti ishte në procesin e harmonizimit me Rregulloren e Përgjithshme për Mbrojtjen e të Dhënave të BE-së (GDPR).[23] Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (KDIMDP) është një institucion i pavarur, përgjegjës për kryerjen e hetimeve administrative, dhënien e rekomandimeve dhe sanksioneve administrative ndaj aktorëve privatë ose publikë për shkelje të këtij ligji.

Liria e shprehjes, liria e shtypit, e drejta e informimit dhe ndalimi i censurës janë të garantuara. Në Shqipëri nuk ka një ligj specifik për mediat online dhe mungon përkufizimi ligjor i tyre. Përpjekja e fundit për të rregulluar mediat online u bë në vitin 2019 përmes paketës ligjore "anti-shpifje" që ngjalli mjaft debate.[24] Projektligjet e kësaj pakete u kundërshtuan gjerësisht nga organizatat kombëtare dhe ndërkombëtare të lirisë së medias, të cilat shprehën shqetësime për censurën, ndërkohë që Komisioni i

---

20 Për hartëzimin e rasteve individuale të analizuara në seksionet 2.1-2.4, u intervistuan 15 ekspertë të fushës së të drejtave të njeriut, medias dhe qeverisjes së sigurisë kibernetike, ndërsa 19 aktivistë dhe gazetarë dhanë informacion nëpërmjet një pyetësori anonim.

21 Komisioni Evropian (2021) *Raporti për Shqipërinë 2021.*.

22 DCAF (2021), *Udhëzues për qeverisjen e mirë të sigurisë kibernetike*.

23 Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (2021) *Njoftim për shtyp "Konsultimi publik për projektligjin e ri "Për mbrojtjen e të dhënave personale" dhe përmirësimet e Ligjit 'Për të drejtën e informimit'"*.

24 Kosovo 2.0 (2020) *Anti-shpifja lundron kundër rrymës demokratike*.

Venecias rekomandoi rishikimin e projektligjeve përkatëse.[25] Nga ana tjetër, mjedisi për mediat audiovizive rregullohet me Ligjin nr. 97/2013 për Mediat Audiovizive, i cili detyron mediat të respektojnë dinjitetin njerëzor dhe të drejtat themelore të njeriut gjatë transmetimit. Ligji ndalon transmetimin e materialeve që justifikojnë ose nxisin dhunën, urrejtjen, intolerancën dhe kryerjen e veprave penale. Autoriteti për Mediat Audiovizive (AMA), si një organ i pavarur rregullator që mbikëqyr mediat audiovizive, është përgjegjës për licencimin e tyre, për luftën kundër piraterisë së përmbajtjes së mbrojtur me të drejtë autori, shqyrtimin e ankesave dhe dhënien e sanksioneve administrative në raste shkeljesh. Mandati i AMA-s nuk mbulon mediat online dhe mbajtja e këtyre të fundit përgjegjëse për shkelje shpesh përbën sfidë. Pavarësisht kufizimeve të mandatit, AMA mund të ndikojë edhe tek mediat online, p.sh., në vitin 2019, AMA i kërkoi AKEP-it të bllokonte përmbajtjet online në 86 raste të lidhura me shkeljen e të drejtave të autorit.[26] Së fundi, Kodi Penal, Ligji për Mbrojtjen e të Dhënave Personale, Ligji për Mbrojtjen nga Diskriminimi, Ligji për të Drejtat e Autorit dhe të drejtat e tjera të lidhura me to, ndikojnë mbi mjedisin mediatik përmes kufizimeve që përmbajnë, ndërsa mungojnë plotësisht parashikimet ligjore për mbrojtjen nga Paditë Strategjike kundër Pjesëmarrjes Publike (SLAPPs).[27]

Parimi i barazisë dhe ndalimi i diskriminimit është i garantuar, ndërsa Ligji nr. 10221/2010 Për Mbrojtjen nga Diskriminimi ofron një listë të gjerë (dhe të hapur) të motiveve duke përfshirë racën, gjininë, orientimin seksual, përkatësinë gjinore etj. Gjithashtu, në ligj përcaktohen format e diskriminimit, ku përfshihen ndër të tjera gjuha e urrejtjes, shqetësimi, shqetësimi seksual, diskriminimi ndërsektorial dhe diskriminimi i shumëfishtë. Ligji zbatohet për shkeljet që ndodhin në çdo mjedis dhe me çdo mjet, pra është i zbatueshëm edhe për hapësirën kibernetike, por pa e përmendur shprehimisht atë. Megjithatë, ky ligj nuk trajton koncepte që lidhen me paragjykimet algoritmike, të cilat kanë të bëjnë me vendimmarrjen automatike diskriminuese. Ligje të tjera që trajtojnë diskriminimin si Ligji nr. 9970/2008 Për Barazinë Gjinore dhe Ligji Nr. 96/2017 Për Mbrojtjen e Pakicave Kombëtare nuk kanë asnjë dispozitë për shkeljet që ndodhin në hapësirën kibernetike. Dispozita e vetme e Ligjit për Barazinë Gjinore që mund të lidhet me hapësirën kibernetike është ndalimi i publikimit të përmbajtjeve diskriminuese, ofenduese ose me stereotipe gjinore. Megjithatë ky parashikim është ngushtësisht i zbatueshëm për median dhe jo për aktorët e tjerë. Komisioneri për Mbrojtjen nga Diskriminimi (KMD) është institucioni i pavarur që ka autoritetin të kryejë hetime administrative, të japë rekomandime dhe sanksione administrative ndaj aktorëve privatë ose publikë për rastet e diskriminimit. Ndërsa, kur veprimet diskriminuese përmbajnë elemente të një kundravajtje ose vepre penale, zbatohet Kodi Penal, siç është analizuar në seksionin më sipër.

Liria e tubimit dhe e organizimit paqësor rregullohet me Ligjin nr. 8773/2001 Për Tubimet, i cili është përgjithësisht në përputhje me Udhëzimet për Lirinë e Tubimit Paqësor të OSBE/ODIHR.[28] Gjithsesi, ligji nuk shtjellon të drejtën për tubime online, tubime spontane apo kundërtubime (kundër-protesta). Për më tepër, ky ligj i lejon policisë të mbikëqyrë tubimet (incizim audio/video, ose fotografim) kur ka arsye për të besuar se mund të ketë rrezik të drejtpërdrejtë për rendin dhe sigurinë publike. Një mundësi e tillë, nëse nuk balancohet siç duhet, mund të keqpërdoret si ndjekje penale ose kërcënim ndaj Mbrojtësve të të Drejtave të Njeriut (MDNj), organizatorëve të tubimeve dhe pjesëmarrësve, si në kontekstin e tubimeve fizike ashtu edhe atyre në internet. Kur bëhet fjalë për garantimin e lirisë së tubimit, aktorët kryesorë janë Avokati i Popullit dhe Policia e Shtetit. Edhe pse nuk ka një mandat specifik për t'u marrë me shkeljet e të drejtave të njeriut në hapësirën kibernetike, roli i Avokatit të Popullit mund të jetë me interes, inter alia, për

---

25 *Opinioni nr. 980/2022 i Komisionit të Venecias*.

26 Birn Shqipëri (2020), *Qeverisja e internetit në Shqipëri dhe roli i saj në lirinë e medias.*

27 Paditë Strategjike kundër Pjesëmarrjes Publike (SLAPPs) janë padi që përdoren nga politikanë, individë e korporata të pasura për të frikësuar dhe heshtur zërin e kritikëve publikë duke i përfshirë ata në beteja ligjore që nuk mund t'i përballojnë, derisa të ndalojnë kritikat ose kundërshtimet e tyre. Ligjet Anti-SLAPP janë krijuar për të mundësuar rrëzimin e këtyre padive në një fazë shumë të hershme nëse ato klasifikohen si "SLAPP".

28 OSCE/ODIHR (2010) *Udhëzues për Lirinë e Tubimeve Paqësore.*

trajtimin e shkeljeve që kryhen nga autoritetet publike në sektorin e sigurisë kibernetike – autoritete të cilat mbulohen nga mandati i Avokatit të Popullit. Megjithatë, mundësi të tilla nuk janë eksploruar ende pasi deri më sot, Avokatit të Popullit nuk i është drejtuar asnjë ankesë[29] për shkelje të të drejtave që lidhen me hapësirën kibernetike.

Për mbrojtjen e të drejtave të grupeve veçanërisht të cënuara janë zhvilluar disa **dokumente strategjike për të drejtat e njeriut**. Gjithsesi, këtyre dokumenteve u mungon perspektiva për sigurimin e mbrojtjes së këtyre grupeve në hapësirën kibernetike, ashtu siç u mungon qasja për të drejtat e njeriut strategjive të sigurisë kibernetike të analizuara më sipër. Më poshtë analizohen për ilustrim disa nga këto dokumente strategjike për të drejtat e njeriut.

Strategjia Kombëtare për Barazinë Gjinore 2021–2030, ndër të tjera, synon të përmirësojë mbrojtjen nga të gjitha format e dhunës me bazë gjinore, por nuk i referohet drejtpërsëdrejti dhunës me bazë gjinore në internet. Nga ana tjetër, Plani Kombëtar i Veprimit për personat LGBTI 2021-2027 njeh gjuhën e urrejtjes në internet dhe gjuhën diskriminuese ndaj komunitetit LGBTI+ si disa nga sfidat me të cilat përballet komuniteti, por nuk i trajton ato me ndonjë masë konkrete. Një nga objektivat specifikë, të Planit Kombëtar të Veprimit për Barazinë, Përfshirjen dhe Pjesëmarrjen e Romëve dhe Egjiptianëve 2021-2025, i cili përfaqëson angazhimin e parë politik të Shqipërisë në trajtimin e antigjipsizmit[30], ka të bëjë me eliminimin e gjuhës së urrejtjes dhe krimeve të urrejtjes ndaj këtyre pakicave. Ky dokument pranon disa sfida në lidhje me gjuhën e urrejtjes dhe krimet e urrejtjes (përfshirë ato që ndodhin online), ndër të cilat mekanizmat e dobët institucionalë, numrin e ulët të raportimeve për shkak të mungesës së besimit tek institucionet dhe mungesën e të dhënave statistikore dhe të disagreguara në lidhje me gjuhën e urrejtjes dhe krimet e urrejtjes. Ky Plan Veprimi parashikon financimin e OSHC-ve nga fondet publike për të monitoruar dhe raportuar rastet e gjuhës së urrejtjes, si dhe rritjen e kapacitetit të autoriteteve përkatëse për hetimin dhe monitorimin e krimeve të urrejtjes dhe gjuhës së urrejtjes. Së fundi, Plani Kombëtar i Veprimit për Personat me Aftësi të Kufizuara (PAK) 2021-2025, ndër të tjera, synon të sigurojë akses në teknologjinë e informacionit, tek shërbimet elektronike dhe ato publike online për PAK. Ministria e Shëndetësisë dhe Mbrojtjes Sociale është institucioni kryesor përgjegjës për zbatimin e katër dokumenteve strategjike të përmendura më sipër.

Një tjetër dokument i rëndësishëm në këtë drejtim është rezoluta e Kuvendit e vitit 2019[31] , e cila ofron njohje dhe mbështetje për MDNJ. Rezoluta njeh sfidat me të cilat përballen MDNJ, duke përfshirë kërcënimet, fushatat e shpifjeve dhe sulmeve, por nuk i referohet shkeljeve që ndodhin në hapësirën kibernetike. Sipas Rezolutës, Kuvendi duhet të hartojë një raport të detajuar me rekomandime për situatën e MDNJ në Shqipëri si dhe do të miratojë një plan veprimi, por deri më sot dokumente të tilla nuk janë miratuar.[32] Për këtë Rezolutë janë përgjegjës Komisioni Parlamentar për Çështjet Ligjore, Administratën Publike dhe të Drejtat e Njeriut dhe Nënkomisioni i tij për të Drejtat e Njeriut, të cilët, në përgjithësi luajnë rol kryesor në hartimin dhe mbikëqyrjen e kuadrit kombëtar të të drejtave të njeriut.

---

29 Informacion i dhënë nga zyra e Avokatit të Popullit përmes kërkesës për informacion datë 17/2/2022.

30 Term i përdorur referuar racizmit ndaj pakicave rome dhe egjiptiane.

31 *Rezoluta e datës 3/3/2019 e Kuvendit të Shqipërisë për njohjen dhe mbështetjen e veprimtarisë së Mbrojtësve të të Drejtave të Njeriut në promovimin, nxitjen dhe mbrojtjen e të drejtave të njeriut dhe lirive themelore, forcimin e shtetit të së drejtës dhe konsolidimin e demokracisë*

32 Informacion i dhënë nga Kuvendi i Shqipërisë përmes kërkesës për informacion datë 20/4/2022.

2.1 Siguria kibernetike dhe e drejta për privatësi

Në vitin 2021, **nxjerrja e të dhënave** kryesonte listën e kërcënimeve kibernetike në Shqipëri. Pak javë para zgjedhjeve parlamentare në muajin prill u publikuan të dhënat personale të 910,000 qytetarëve shqiptarë.[33] Baza e të dhënave, e cila u shpërnda tek qytetarët dhe mediat online, përmbante informacione sensitive për popullatën në moshë votimi në Tiranë, përfshirë të dhëna si numri personal i identifikimit, vendi i punës, adresa, numri i telefonit dhe hamendësime për preferencat e votimit. Të dhënat tregonin se çdo qytetari i ishte caktuar një patronazhist[34], i cili synonte monitorimin e preferencave të votimit dhe në disa raste, regjistronte edhe pikat e dobëta të qytetarëve që mund të ndikonin në votimin e tyre. Kështu, baza e të dhënave përmbante edhe komente shtesë në lidhje me të dhëna sensitive për shëndetin e individit, situatën familjare, pikëpamjet fetare ose përkatësinë etnike.

Reagimi institucional ndaj rrjedhjes së të dhënave ilustron më së miri se si trajtohet e drejta për privatësi në kuadrin e sigurisë kibernetike, duke vënë në dukje mundësitë për të trajtuar fragmentimin e qeverisjes së sigurisë kibernetike. Pas nxjerrjes së të dhënave, u hodhën akuza të cilat fajësonin Partinë Socialiste (PS) për krijimin e bazës së të dhënave. PS nuk e pranoi autorësinë e bazës së të dhënave, por pranoi se kishte mbledhur të dhëna personale gjatë viteve derë-më-derë për qëllime zgjedhore.[35] Kjo u konfirmua më vonë edhe nga Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (KDIMDP), i cili vlerësoi se disa të dhëna ishin siguruar nga patronazhistët. Megjithatë, KDIMDP[36] arriti në përfundimin se nuk kishte prova të mjaftueshme që baza e të dhënave të ishte krijuar nga PS apo se kishte dalë në mënyrë të paligjshme nga bazat e të dhënave shtetërore.

Përveç të dhënave të mbledhura nga patronazhistët, baza e të dhënave përmbante informacione personale të përditësuara nga vetë qytetarët në e-Albania, faqe interneti e e-qeverisjes që përdorej shpesh për të kërkuar leje për të qarkulluar në rrugë gjatë izolimit për shkak të pandemisë Covid-19. Kjo bëri që shumica e qytetarëve ta lidhin nxjerrjen e të dhënave me AKSHI-in, si përgjegjëse për administrimin e portalit shumë-funksional. Megjithatë, që nga skandali i nxjerrjes së të dhënave, AKSHI pohon se e-Albania nuk ruan, administron apo përpunon asnjë të dhënë[37], por shërben si portë hyrëse e qeverisë që u mundëson përdoruesve të ndërveprojnë me institucionet publike. Kështu, të dhënat ruhen dhe administrohen në databazat e institucioneve përkatëse, në këtë rast Drejtorisë së Përgjithshme të Gjendjes Civile. Hetimet administrative të kryera nga KDIMDP në ambientet e PS-së, AKSHI-it dhe Drejtorisë së Përgjithshme të Gjendjes Civile nuk arritën në përfundime të mirëfillta për këtë çështje, duke mos nxjerrë përgjegjës. Ndonëse rezultatet e këtyre hetimeve nxjerrin në pah probleme serioze për mbrojtjen dhe sigurinë e të dhënave, institucioni përgjegjës për shkeljen nuk evidentohet qartë.

Konkretisht, hetimet administrative ndaj AKSHI-t dhe Drejtorisë së Përgjithshme të Gjendjes Civile zbuluan se sipas KDIMDP të dhënat mund "të jenë mbledhur nga institucionet përkatëse ose autoritetet e (nën) kontraktuara që menaxhojnë dhe/ose përpunojnë këto të dhëna, që merren me mirëmbajtjen e infrastrukturës së rëndësishme, për shkak të mungesës së masave të sigurisë".[38] Në ndryshim nga qëndrimi zyrtar i AKSHI-it, në raportin në kuadër të Rezolutës së Kuvendit të Shqipërisë 2020, KDIMDP

---

33 Exit.al (2021) *Rrjedhja e të dhënave personale të mbi 910,000 shqiptarëve tek politikanët dhe publiku*.

34 Termi ''patronazhist'' përdoret duke iu referuar individëve të caktuar nga partia në pushtet për të gjurmuar çdo votues dhe për të regjistruar të dhënat e tyre personale në një databazë kombëtare.

35 Balkan Insight (2021) *Rrjedhjet masive të të dhënave në Shqipëri shtrojnë pikëpyetje mbi sigurisë publike*.

36 Rekomandimi nr. 44, datë 19/08/2021 i Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale.

37 Informacion i dhënë nga AKSHI përmes kërkesës për informacion datë 10/5/2022.

38 Rekomandimi nr. 43, datë 19/08/2021 i Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale. Shih edhe: Monitor.al (2021), *Patronazhistët, Komisioneri: Përgjigjet e AKSHI-t jo shteruese, Tatimet mungesë bashkëpunimi, PS përpunues por jo krijues*

zbuloi se AKSHI ka rol të rëndësishëm në mbrojtjen e të dhënave. KDIMDP rekomandoi që AKSHI në kuadrin e privatësisë së të dhënave të përfshijë protokolle që mbulojnë të gjitha procedurat e përpunimit të të dhënave.[39] Kur u kontaktua për këtë raport, AKSHI nuk u përgjigj nëse kishte marrë ndonjë masë për adresimin e rekomandimeve të KDIMDP. Raporti i KDIMDP për vitin 2020 vuri në dukje se edhe pse masat ekzistuese për Informacionin Personal të Identifikueshëm (IPI) përfshijnë disa parime themelore mbrojtëse, si të drejtat e subjekteve e të dhënave personale, kuadri institucional ua vështirëson individëve të kuptojnë se cilat kategori të IPI ruhen dhe cili është qëllimi i përpunimit të tyre. Për çdo lloj informacioni sensitiv, siç janë numrat personalë të identifikimit, institucionet nevojitet të përcaktojnë nivelin e konfidencialitetit dhe aksesueshmërisë përpara se ta ruajnë, përpunojnë ose transferojnë atë. Në përgjithësi, rekomandohet të bëhet kriptimi dhe/ose pseudonimizimi i të dhënave personale përpara transferimit të informacionit drejt burimeve të jashtme ose pajisjeve portative, si laptopë dhe telefona celularë.[40] Aktualisht nuk ka asnjë informacion të disponueshëm mbi modalitetet e ruajtjes së të dhënave nga AKSHI, as nuk ka ndonjë rregullore që përcakton specifikat e PII kur transferohen drejt palëve të tjera të treta.

Kjo është veçanërisht e rëndësishme për rastin e rrjedhjes së të dhënave pasi Raporti i KDIMDP 2020[41] tregon se AKSHI ia kishte ngarkuar një subjekti privat (përpunues) ruajtjen fizike të të dhënave. Sipas raportit, marrëveshja nuk adreson në mënyrë të mjaftueshme rregulloren për mbrojtjen e të dhënave, kërkesat ligjore dhe dispozitat në përputhje me Ligjin për Mbrojtjen e të Dhënave Personale. Operatorët administrues të infrastrukturës kyçe të informacionit si AKSHI dhe Drejtoria e Përgjithshme e Gjendjes Civile i nënshtrohen kontrolleve periodike të kryera nga AKCESK për të garantuar zbatimin e masave minimale të sigurisë.[42] Megjithatë, përpunuesit privatë nuk janë të detyruar të ndjekin masat bazë të sigurisë të vendosura nga AKCESK për infrastrukturën e rëndësishme të informacionit. Ndonëse fragmentimi i politikave është i pashmangshëm në qeverisjen e sigurisë kibernetike, mungesa e llogaridhënies së subjekteve private mund të rregullohet nëpërmjet mekanizmave ndërsektoriale të përmbushjes dhe respektimit të rregullave. Më tej, bashkëpunimi ndërsektorial ndërmjet përfaqësuesve të nivelit qendror dhe institucioneve të pavarura në këtë drejtim mund të përmirësojë mbikëqyrjen e mbrojtjes së të dhënave dhe pajtueshmërinë e përpunuesve privatë të kontraktuar. Është thelbësore të sigurohet, që prej fazës së draftimit, që marrëveshjet me palët e treta përmbajnë edhe qasjen e menaxhimit të rrezikut, duke përcaktuar qartë detyrimet dhe përgjegjësitë e secilës palë. Kapacitetet e operatorëve privatë për përmbushjen e standardeve minimale të sigurisë duhet të vlerësohen duke marrë në konsideratë kapacitetin e institucioneve shtetërore për monitorimin dhe zbatimin e masave efektive të menaxhimit të rrezikut.

Shpesh, kontrollorët dhe përpunuesit përjashtohen nga përgjegjësia për nxjerrjen e të dhënave, nëse vërtetohet se përgjegjësia për shkeljen është e përbashkët (ose bie vetëm mbi) subjektin e të dhënave personale. Për këtë çështje, skandali i nxjerrjes së të dhënave mund të shërbejë si një thirrje zgjimi për të gjithë qytetarët që zgjedhin të pranojnë termat dhe kushtet e faqeve të internetit ku ofrojnë me paramendim të dhëna personale dhe sensitive dhe japin pëlqimin për procedurat e menaxhimit të të dhënave, duke mos qenë në dijeni të rreziqeve.[43] Në përgjithësi, incidenti nxori në pah nevojën për rritjen e edukimit digjital të qytetarëve dhe rritjen e ndërgjegjësimit për shërbime elektronike cilësore.

Në dhjetor të vitit 2021, media raportoi një nxjerrje të re të të dhënave: mes qytetarëve qarkullonin dy databaza të ndryshme që përmbanin informacione personale dhe të dhëna për pagat e 690,000

---

39 *Raporti i Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale në Parlament për vitin 2019.*

40 United States Government Accountability Office (2008) *Ekzistojnë alternativa të privatësisë për të rritur mbrojtjen e informacionit personal të identifikueshëm*.

41 *Raporti i Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale në Parlament për vitin 2019*.

42 Informacion i dhënë nga AKCESK përmes kërkesës për informacion datë 28/7/2022

43 Intervistë me një përfaqësues të shoqërisë civile datë 15/3/2022.

qytetarëve, punonjës të sektorit publik dhe privat. Databazat përbëheshin nga të dhënat e listës së pagave të deklaruara për muajt janar dhe prill 2021 në sistemin e Drejtorisë së Përgjithshme të Tatimeve, të cilat u vërtetuan se kishin dalë nga dy punonjës të brendshëm të Drejtorisë, të cilët më pas u arrestuan.[44] Menjëherë pas skandalit të listës së pagave, doli një listë e tretë me të dhëna të detajuara për targën, modelin e automjetit, ngjyrën, numrin e regjistrimit dhe pronësinë e 530,452 automjeteve. Po zhvillohen hetime administrative për Drejtorinë e Përgjithshme të Tatimeve dhe Drejtorinë e Përgjithshme të Shërbimeve të Transportit Rrugor si dy operatorët e infrastrukturës së informacionit kritik nga ku mendohet se kanë dalë të dhënat.[45]

Nuk është raportuar asnjë incident i krimit kibernetik që të ketë ndodhur si pasojë e nxjerrjes së të dhënave ose në lidhje me to. Megjithatë, incidentet e sipërpërmendura nxjerrin në pah brishtësinë e sigurisë kibernetike dhe infrastrukturës së komunikimit në Shqipëri, duke evidentuar shkelje të rënda të konfidencialitetit dhe rënie të besimit të publikut tek institucionet shtetërore. Ndonëse mungesa e llogaridhënies së institucioneve shtetërore pas skandalit të parë nuk arriti të gjeneronte diskutime konstruktive mbi temën e sigurisë së të dhënave personale në internet, rrjedhjet e mëvonshme të të dhënave e nxitën qeverinë shqiptare të kontraktonte Jones Group International, një kompani me qendër në SHBA, me synimin për të forcuar sigurinë e sistemeve digjitale. Në janar 2022, Ministria për Infrastrukturën dhe Energjinë nënshkroi një Memorandum Mirëkuptimi (MoU) ku i caktoi Jones Group International (JGI) përgjegjësinë për hartimin e një strategjie shumëdimensionale për rritjen e ndërgjegjësimit për privatësinë e të dhënave, me fokus të dy institucionet që menaxhojnë dhe përpunojnë të dhënat, si dhe qytetarët. Sipas Ligjit Nr. 34/2022 për "Përcaktimin e Procedurës së Veçantë për negocimin dhe zbatimin e kontratës me shoqërinë Jones Group International", AKSHI është institucioni përgjegjës që do t'i ofrojë JGI-së hartëzimin e institucioneve të sigurisë kibernetike, fokusin e punës dhe sistemet e përdorura. Projektmarrëveshja do të negociohet nga një komision i përbërë nga përfaqësues të ministrive të infrastrukturës dhe energjisë, mbrojtjes, rendit publik, financave dhe ekonomisë, Prokurorisë së Përgjithshme, AKCESK-ut dhe Drejtorisë së Sigurimit së Informacionit të Klasifikuar. Edhe pse marrëveshja me JGI nuk i është bërë e ditur Komisionerit IDP[46] –dhe ky i fundit as nuk është pjesë e komisionit negociator për projekt-marrëveshjen– në muajt në vijim AKSHI pritet të marrë miratimin me shkrim nga të gjitha agjencitë përkatëse për projektet e propozuara, përpara se të finalizohet marrëveshja.[47] Marrëveshja paraqet një mundësi për të hartuar kuadrin e sigurisë kibernetike në Shqipëri duke ndjekur një "qasje kujdestarie (*stewardship*)[48]" – me angazhim të barabartë të aktorëve publikë dhe jopublikë si OJQ-të, sektori privat dhe qytetarët, për të ndarë përgjegjësinë e respektimit të parimeve të privatësisë.

Aktualisht, përgjegjësia për trajtimin e shkeljeve të privatësisë online që përmbushin kriteret e një vepre penale i takon Policisë së Shtetit. Njësitë e krimit kibernetik të Policisë së Shtetit marrin denoncime nga qytetarë në të gjithë Shqipërinë, ndërsa këta të fundit janë të detyruar të udhëtojnë drejt Tiranës për të bërë ankesat e tyre.[49] Mungesa e burimeve njerëzore dhe vjetërsia e pajisjeve teknike kufizojnë kapacitetet e punonjësve të policisë në trajtimin e ankesave në kohën e duhur dhe për të parandaluar përshkallëzimin e kërcënimeve kibernetike. Nga ana tjetër, kjo ndikon edhe në perceptimin e qytetarëve për efektivitetin e institucionit dhe i dekurajon qytetarët të raportojnë.

---

44 Reporter.al (2022) *Pasiguria e të dhënave personale rrezikon 'qeverisjen dixhitale' të Shqipërisë*.

45 Intervistë me një përfaqësues të zyrës së Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale datë 7/4/2022.

46 Po aty.

47 Ligji nr. 34/2022 për përcaktimin e procedurës së veçantë për negocimin dhe zbatimin e kontratës me shoqërinë Jones Group International për forcimin e sigurisë kibernetike

48 Deibert, Ronald J. (2013) Kodi i Zi: Brenda betejës për hapësirën kibernetike siç referohet në *McClelland dhe Stewart Privatësia dhe Siguria Kibernetike me fokus mbrojtjen e privatësisë në aktivitetet e sigurisë kibernetike*.

49 Intervistë me përfaqësues të Njësisë C për Hetimin e Krimeve Kompjuterike, Policia e Tiranës datë 26/5/2022.

Ministria e Brendshme raporton shifra në rritje të incidenteve kibernetike në tre vitet e fundit, duke treguar rritje të ndërgjegjësimit për sigurinë digjitale. Por, sipas aktivistëve të të drejtave të njeriut, shumë krime kibernetike shpesh nuk raportohen. Kur u pyetën për arsyet e tyre për të mos denoncuar, të intervistuarit shprehën besim të ulët tek institucionet që merren me hetimet. Disa aktivistë të kontaktuar për këtë raport raportuan se u ishin publikuar/shpërndarë fotografitë, videot ose materiale të tjera personale të identifikueshme pa pëlqimin e tyre. Pasi kishte kritikuar publikisht gjuhën diskriminuese dhe seksiste të një imami – një aktiviste feministe – pa emrin, foton dhe llogarinë e saj në Facebook të shpërndarë nga një historian kontrovers, që u përpoq të nxiste publikisht urrejtje kundër saj. Të tjerë aktivistë, në veçanti ata LGBTI+ raportojnë se kanë qenë subjekt i ngacmimeve dhe bullizimit, siç shtjellohet më tej në seksionet e mëposhtme. Vetëm në një nga rastet e evidentuara subjekti i ka denoncuar shkeljet në Policinë e Shtetit. Në rastin në fjalë, një aktivisteje të të drejtave të njeriut iu vodhën fotot dhe materialet e saj nga rrjetet sociale dhe më pas u përdorën për ta ngacmuar, frikësuar dhe kërcënuar. Megjithatë, Policia e Shtetit dështoi në ndjekjen e këtij rasti.

Ngurrimi për të raportuar shkeljet i atribuohet shpesh edhe frikës së fajësimit të viktimave apo denigrimit publik. Gjatë dy viteve të fundit janë ekspozuar në media disa raste të **shfrytëzimit seksual (sextortion)**[50] të vajzave dhe fëmijëve. Media është kritikuar për shkak të raportimeve joetike të rasteve, shpeshherë duke ekspozuar informacione personale të viktimave.[51] Sa për ilustrim, rasti i një vajze 15-vjeçare, e cila u abuzua seksualisht nga roja i shkollës dhe disa të rinj të tjerë, shkaktoi një reagim masiv publik dhe një valë protestash në të gjithë vendin në vitin 2020.[52]

Emëruesi i përbashkët i të gjitha rasteve të raportuara në media ishte fakti se viktimat ishin vajza të mitura dhe autorët ishin burra. Në shumicën e rasteve, viktima e njihte autorin, qoftë si i njohur, nxënës në të njëjtën shkollë apo ish-partner, gjë që tregon se shfrytëzimi mund të ketë ndodhur pasi viktima është manipuluar ose ka qenë nën presion për të ndarë imazhe me përmbajtje seksuale. Në mënyrë alternative, imazhe intime të shpërndara në konfidencialitet mund të jenë përdorur për shantazh. Media ka raportuar për disa raste kur gratë (veçanërisht të miturat) ishin viktima të **shpërndarjes së paautorizuar të fotove dhe videove intime** që shpërndaheshin me qëllim për t'i poshtëruar dhe për t'i detyruar ato të kryenin marrëdhënie. Duke marrë parasysh jetëgjatësinë e postimeve digjitale, dhuna kibernetike ndaj grave dhe vajzave rrezikon të ketë pasoja të rënda në të drejtën e tyre për privatësi, duke ndikuar në shëndetin dhe mirëqenien e tyre mendore.

Intervistat me aktivistë të të drejtave të njeriut nxorrën në pah nevojën për të trajtuar shqetësimet me bazë gjinore në hapësirën kibernetike në Shqipëri. Siç u ilustrua më lart, gratë janë në shënjestër në mënyrë disproporcionale përmes publikimit dhe shpërndarjes së paautorizuar të fotove dhe videove intime dhe sextortion. Përveç kësaj, edhe **doxing**[53] (doksimi –vjedhja dhe publikimi i të dhënave personale) ndikon në mirëqenien digjitale të aktivisteve. Një aktiviste e Organizatës Politike kujton se pasi iu ndalua pjesëmarrja në një protestë studentore, media online zgjodhi qëllimisht të përdorte fotot e saj të bëra në plazh për të ilustruar një artikull për protestën. *"Mendoj se kjo është bërë me qëllim, duke pasur parasysh se shumica e publikut është shumë konservator dhe të shohësh një vajzë gjysmë të veshur në plazh do të ndikonte në perceptimin e tyre për mua si një person që nuk duhet marrë shumë seriozisht,"* thotë aktivistja, llogaria në Facebook e së cilës u hakerua pas pjesëmarrjes në një tjetër protestë.

Këto raste dëshmojnë urgjencën për të kapërcyer hendekun gjinor digjital në Shqipëri, i cili nuk konsiston

---

50 Sextortion i referohet praktikës së zhvatjes së parave ose kërkimit të favoreve seksuale nga dikush duke e kërcënuar me publikimin e materialeve me përmbajtje seksuale

51 Balkan Insight (2022) *Gratë në median shqiptare: Nga riviktimizimi tek stigmatizimi si imorale.*

52 Exit.al (2020) *Shqiptarët protestojnë kundër dhunës seksuale pas përdhunimit të të miturës.*

53 Doxing i referohet kërkimit dhe publikimit të informacionit privat ose identifikues (për një individ të caktuar në internet), zakonisht me qëllim keqdashës.

thjesht në ofrimin e mundësive të barabarta për akses në internet, por në ndërtimin e një politike të përgjegjshme gjinore që përqafon perspektivën e të gjithë aktorëve.[54] Kjo mund të arrihet duke integruar parimet gjinore në politikëbërjen e sigurisë kibernetike dhe duke zbatuar një qasje shumë-aktoriale që nga faza e formulimit të politikave. Në këtë kontekst, bashkimi i institucioneve të të drejtave të njeriut dhe aktorëve të sigurisë kibernetike ofron një mundësi për të promovuar politika publike më gjithëpërfshirëse dhe për të përmirësuar përfaqësimin e qytetarëve në kuadrin e sigurisë kibernetike, pra duke ndikuar në përvojën egrave, fëmijëve, anëtarëve të komunitetit LGBTQ+, PAK, pakicave etnike dhe grupeve të tjera si përdorues.

Epoka digjitale ka ndryshuar natyrën e kërcënimeve të privatësisë dhe shpeshherë nxjerr në pah një ndërthurje mes shkeljes së privatësisë dhe të drejtave të tjera, si liria e fjalës. Ndërkohë që shkelja e mësipërme evidenton ndikimin që ka raportimi joetik në privatësinë ose imazhin publik të një individi, shkelje të tjera dëshmojnë për mbrojtjen e dobët të privatësisë së qytetarëve, dhe në veçanti të gazetarëve, të dhënat personale të të cilëve mund të sulmohen për qëllime intimidimi ose shantazhimi. E. H., gazetar, raportoi shkelje të të dhënave personale në prill 2022. E.H. kishte zbuluar rastësishtse llogaria e tij në portalin e-Albania ishte aksesuar nga A. B., një noter publik. E njëjta gjë kishte ndodhur me llogarinë e gruas së tij. Noteri kishte gjeneruar një certifikatë familjare dhe një vërtetim të kontributeve shoqërore dhe shëndetësore të bashkëshortes së E.H., të cilat hedhin dritë mbi profesionin, pagën dhe punëdhënësin e saj. Asnjëri prej tyre nuk kishte kërkuar ndonjë shërbim nga noteri dhe as nuk kishte punuar me të më parë. Nëpërmjet një marrëveshjeje institucionale ndërmjet AKSHI-it dhe Dhomës Kombëtare të Noterëve, noterët e regjistruar mund të aksesojnë certifikatat ose informacione të tjera të nevojshme personale të klientëve të tyre nëpërmjet e-Albania.[55] Marrëveshja lehtëson ofrimin e shërbimeve për të gjithë noterët dhe redukton kohën e pritjes dhe dokumentacionin për klientët e tyre. Ndonëse nuk ka ende prova që e lidhin këtë **akses të paautorizuar** në të dhënat personale me aktivitetin profesional të gazetarit E.H., organizatat ndërkombëtare si Safejournalists.net, Komiteti për Mbrojtjen e Gazetarëve dhe Qendra Evropiane për Lirinë e Shtypit dhe Medias u bënë thirrje autoriteteve që të hetojnë rastin duke e konsideruar kërcënim ndaj gazetarisë së lirë. Shkelja e të dhënave u regjistrua edhe në platformën e Këshillit të Evropës “Siguria e gazetarëve” si kërcënim i nivelit të dytë i kategorizuar nën “akte të tjera që kanë një efekt kërcënues mbi lirinë e medias”. Çështja u denoncua tek KDIMDP dhe në Prokurorinë e Tiranës dhe ende pritet një vendim përfundimtar.

Mes implikimeve të tjera të mundshme, çështja ngre shqetësime në lidhje me standardet e sigurisë që aplikojnë noterët dhe masat mbrojtëse që ofron marrëveshja e sipërpërmendur kur aksesohet ose përpunohet informacioni personal. Duke pasur parasysh ndjeshmërinë e të dhënave të tyre, noterët janë të prirur për shkelje të qëllimshme ose të paqëllimshme të të dhënave.[56] Prandaj, për të ulur këto rreziqe, duhet të garantohet zbatimi i ligjit për mbrojtjen e të dhënave. Megjithatë, e-Albania nuk u ofron përdoruesve të saj mundësinë për të dhënë pëlqimin elektronik përpara se një noter të ketë akses në informacionin e tyre. Qytetarët dëshmojnë se as noterët nuk kërkojnë autorizime me shkrim nga klientët e tyre përpara se të kenë akses në të dhënat online të klientëve. Ritmi i shpejtë i digjitalizimit që u mundëson qytetarëve shqiptarë të aksesojnë më shumë se 1200 shërbime në internet duket se ka një ndikim jo të njëtrajtshëm në përpjekjet e vendit për të garantuar privatësinë e të dhënave.

Për të krijuar një hapësirë kibernetike më të sigurt në lidhje me të drejtën e privatësisë, nevojitet të përmirësohet siguria kibernetike e institucioneve kritike, si dhe të investohet në përditësimin e aseteve. Në këtë drejtim është thelbësor parashikimi i mirë i buxhetit, prandaj Agjenda Digjitale e Shqipërisë 2022-2026 dhe plani i saj i veprimit[57] parashikojnë ndër të tjera përmirësimin e sistemeve digjitale për Gjendjen

---

54 WebFoundation (2017). *Reagimi me politikën e përgjegjshme gjinore TIK: çelësi për të lidhur 4 miliardët e ardhshëm*

55 AKSHI (2017) *e-Albania, qytetarët do të kenë nevojë për më pak dokumente kur t’i drejtohen noterëve*

56 Lewis, Michael (2015) *Kriza e Mbrojtjes së Identitetit.*

57 *Regjistri elektronik për njoftimet dhe konsultimet publike.*

Civile Kombëtare dhe sistemin e sigurimeve shoqërore. Sipas draftit të Agjendës Digjitale, deri në vitin 2026 Shqipëria pritet të përdorë të dhënat e mëdha dhe inteligjencën artificiale për qëllime kërkimore shkencore dhe për ofrimin e shërbimeve efikase. Megjithatë, mungesa e llogaridhënies me të cilën institucionet publike menaxhuan rrjedhjen e të dhënave të vitit 2021 ngre shqetësime të mëdha në lidhje me të drejtën e privatësisë në hapësirën kibernetike shqiptare. Procesi i negociatave të marrëveshjes me JGI, nëse bëhet gjithëpërfshirës, paraqet një mundësi për të forcuar bashkëpunimin me institucionet e pavarura mbikëqyrëse dhe garanton që e drejta e privatësisë të merret parasysh ndërkohë që forcohet siguria kombëtare dhe qëndrueshmëria e kuadrit të sigurisë kibernetike në Shqipëri. Së fundi, rritja e transparencës në gjurmimin dhe proceset e PII është gjithashtu e nevojshme për të siguruar që qytetarët të jenë të mirë-informuar për pasojat e shkeljeve të privatësisë në të ardhmen.

2.2. Siguria kibernetike dhe liria e shprehjes

Përpjekjet e qeverisë për të ushtruar kontroll mbi median dhe gazetarët kanë krijuar një mjedis mediatik të pafavorshëm. Krahasuar me vitin 2021, Shqipëria ra me 20 pikë, duke u renditur në vendin 103/180 në *Indeksin e Reporterëve pa Kufij 2022*, i cili thekson rregullimin e medias, krimin e organizuar dhe dhunën politike si faktorë që kërcënojnë integritetin fizik dhe/ose profesional të gazetarëve.[58] Në Shqipëri, sfidat kryesore në lidhje me lirinë e shprehjes online janë të natyrës institucionale dhe etike.

Më parë ka pasur përpjekje të iniciuara nga qeveria për të institucionalizuar kontrollin e mediave online duke prezantuar në vitin 2019 paketën ligjore të quajtur rëndom si "paketa anti-shpifje". Kjo nismë u kundërshtua gjerësisht për shkak të përpjekjeve shqetësuese për censurë që përmbante dhe Komisioni i Venecias rekomandoi rishikimin e nismës.[59] Ndër shqetësimet e tjera, paketa anti-shpifje, nëse miratohet, do t'i jepte AMA-s kompetenca thuajse gjyqësore mbi veprimtarinë e mediave online. Megjithatë, paanshmëria dhe pavarësia e këtij institucioni nuk mund të garantohet, pasi ky institucion drejtohet aktualisht nga bashkëpunëtorë të ngushtë të qeverisë.[60] Mes ndryshimeve drastike ligjore dhe shqetësimeve etike për zbatimin e paketës anti-shpifje, vetë-rregullimi i medias do të ishte një zgjidhje më e volitshme, duke synuar arritjen e një ekuilibri të drejtë mes nevojës për rregullim dhe lirisë nga censura. Në këtë kuadër, në vitin 2020 u krijua Aleanca për Median Etike, e cila bëri bashkë 19 media online që zotohen se do të respektojnë standardet etike të gazetarisë dhe do të përpiqen të mbrojnë lirinë e fjalës. Aleanca shërben si mekanizëm vetërregullues me një bord të pavarur ku qytetarët mund të paraqesin çdo ankesë etike që kanë për këto media.

Duke qenë se objekti i projektligjeve kundër shpifjes ishte tepër i gjerë, ato përbënin kërcënim jo vetëm për median online, por edhe për blogerët si individë dhe përdoruesit e rrjeteve sociale. Pavarësisht se paketa kundër shpifjes nuk u miratua, ka pasur incidente të shumta ku përdoruesit e rrjeteve sociale janë hetuar si pasojë e përmbajtjeve online që kishin publikuar në profilet e tyre personale. Pas një statusi publik në profilin e tij në Facebook, ku u bën thirrje qytetarëve të mblidhen në protestë, një aktivist politik u procedua arbitrarisht si organizator i protestës. Në mënyrë të ngjashme, janë ndjekur penalisht aktivistë të tjerë pasi reaguan kundër kushteve të këqija të punës së minatorëve dhe kritikuan Albchrome-in, kompaninë kryesore minerare në Shqipëri, për keq-menaxhim. Vdekjet e më shumë se tetë minatorëve[61] nxitën shumë qytetarë, përfshirë edhe aktivistë të Organizatës Politike (OP), një grupim i majtë, të bëjnë thirrje për kushte më të mira pune për minatorët në mbështetje të Sindikatës së Minatorëve të Bashkuar

58 Reporterë pa Kufij (2021) *Indeksi i Lirisë së Shtypit, Shqipëria.*

59 *Opinioni nr. 980/2022 i Komisionit të Venecias*.

60 Qendra Evropiane për Lirinë e Shtypit dhe Medias (2021) *Deklaratë për shtyp*.

61 Exit.al (2020) *Dy minatorë të plagosur në minierën e Albkromit mes protestave të vazhdueshme.*

të Bulqizës. Aktivistët e OP bënë thirrje të ngjashme në profilet e tyre të medias sociale dhe më vonë u ndoqën penalisht nga policia bazuar vetëm në përmbajtjen e Facebook që këta përdorues kishin krijuar ose shpërndarë nga faqe të tjera publike. Duke qenë të lidhur me grupin e majtë, akuzat sugjerojnë se aktivistët janë bërë objekt i **përgjimit elektronik** dhe për rrjedhojë shënjestrohen për qëndrimet e tyre politike.

Kur përballet me një fatkeqësi natyrore, vëmendja e qeverisë zhvendoset për t'i dhënë përparësi ndihmës humanitare për të siguruar të drejtat dhe nevojat bazë të popullatës së dëmtuar, që lidhen me sigurinë fizike, si dhe me nevojat e mbrojtjes ekonomike dhe sociale. Në raste të tilla, është e rëndësishme të monitorohen afër edhe të drejtat e tjera civile dhe politike, si liria e fjalës. Për shembull, regjimet autokratike në përgjithësi përpiqen të shtypin kundërshtarët e mundshëm politikë duke u kufizuar atyre lirinë e fjalës dhe tubimit.[62] Në Shqipëri, tërmeti i nëntorit 2019 që shkaktoi 51 viktima dhe ndikimi i pandemisë Covid-19 nxorën në pah faktorë shqetësues që kontribuuan në përkeqësimin e lirisë së shprehjes dhe lirisë së medias në vend.

Pas tërmetit shkatërrues, aktivistja 26-vjeçare, Xh. A., **u procedua penalisht** për shpërndarjen e disa postimeve në profilin e saj personal në Facebook. Ajo iu bënte apel qytetarëve durrsakë që të largoheshin nga vendburimet e gazit të Porto Romanos dhe kishte shpërndarë një artikull të një portali italian lajmesh që pretendonte se depozitat e gazit ishin dëmtuar nga tërmeti dhe përbënin rrezik për popullatën. Xh. A. kishte dëgjuar më parë nga zyrtarë të përmendnin dëmin dhe kishte kërkuar informacione nga autoritetet shtetërore për të konfirmuar informacionin, por nuk kishte marrë asnjë përgjigje.[63] Ajo qëndroi dy ditë e arrestuar, nën akuzën se kishte shkaktuar panik dhe u kishte bërë thirrje qytetarëve të largoheshin nga qyteti, edhe pse statusi i saj kishte marrë vetëm 26 reagime. Pas ndjekjes penale që zgjati 11 muaj, Xh. A. u shpall e pafajshme nga Gjykata e Rrethit Gjyqësor Durrës. Çështja e Xh.A. u bë precedent i rëndësishëm për vendimet e mëvonshme, duke siguruar që askush të mos dënohet për mendimet ose opinionet e tij.[64]

Portalet online dhe kanalet e informacionit janë vënë shpesh nën presion nga autoritetet, në kuadër të luftës kundër lajmeve të rreme. Një portal i njohur online, joqalbania.com, i njohur për përdorimin e gjuhës kritike dhe satirës kundër qeverisë, **u mbyll** nga AKEP me akuzat për shkaktimin e panikut në lidhje me tërmetin e vitit 2019. Këshilli Shqiptar i Medias (KSHM) reagoi kundër bllokimit[65], duke denoncuar kryeministrin se ka shfrytëzuar rastin për të bllokuar faqen pa arsye legjitime. Në të njëjtën kohë, 5 gazetarë dhe 3 administratorë të mediave online u proceduan penalisht për përhapje të lajmeve të rreme që shkaktuan panik. Këto arrestime ngritën shqetësime për mekanizmat e përdorur për të filtruar përmbajtjet që mund të etiketohen si lajme të rreme dhe kompetencat përkatëse të Policisë së Shtetit për identifikimin dhe trajtimin e lajmeve të rreme. Duke iu referuar rastit, KSHM mendon se përgjegjësia për të filtruar përmbajtjen ose për të monitoruar zbatimin e standardeve etike duhet të jetë e organeve të pavarura.[66]

Ngjarjet që ndodhën pas skandalit të rrjedhjes së të dhënave të prillit 2021 (përmendur me sipër), nxorën në pah ndër të tjera çështje që lidhen me lirinë e shtypit dhe mbrojtjen e burimeve të informacionit të gazetarëve. Përveç qarkullimit ndërmjet platformave të koduara të komunikimit në internet, databaza që përmbante të dhënat personale dhe preferencat e pretenduara politike të 910 mijë qytetarëve u publikua fillimisht nga një media online, Lapsi.al. Prokuroria e Posaçme Kundër Korrupsionit dhe Krimit të

62 Lin, Thung-Hong, 2015. *Qeverisja e fatkeqësive natyrore: Kapaciteti shtetëror, demokracia dhe cenueshmëria e njerëzve.*

63 Balkan Insight (2020) *Lufta e Shqipërisë kundër 'Nxitësve të frikës' i lë në ankth aktivistët e të drejtave.*

64 Po aty.

65 Këshilli Shqiptar i Medias (2019) *Deklaratë: Raporti shqetësues i qeverisë me mediat.*

66 Reporter.al (2020) *'Shpërndarje paniku': Policia përndoqi gazetarët pas tërmetit dhe COVID-19.*

Organizuar (SPAK), gjatë hetimeve të saj, urdhëroi **sekuestrimin e pajisjeve** të Lapsi.al pasi ky i fundit refuzoi t'i jepte SPAK-ut burimin që qëndronte pas databazës me qëllim mbrojtjen e burimit të gazetarit. Burime të tilla gëzojnë mbrojtje sipas ligjit në Shqipëri dhe kjo masë e prokurorisë u konsiderua gjerësisht si një precedent kërcënues për lirinë e fjalës. Përfshirja e subjektit më të lartë kundër korrupsionit dhe krimit të organizuar në këtë çështje u perceptua nga shumë ekspertë si një masë joproporcionale dhe një përpjekje për të intimiduar gazetarët për të zbuluar burimin që ka nxjerrë databazën nga Partia Socialiste. Drejtuesit e portalit online i paraqitën një kërkesë urgjente Gjykatës Evropiane të të Drejtave të Njeriut, e cila vendosi në favor të Lapsi.al dhe urdhëroi SPAK të ndalonte sekuestrimin e pajisjeve të gazetarëve. Gjykatat shqiptare e lanë në fuqi këtë vendim, duke krijuar një precedent të rëndësishëm për mbrojtjen e burimeve të gazetarëve. Duhet theksuar se GJEDNJ ndërhyn në këtë mënyrë vetëm në raste ekstreme,[67] dhe kjo është hera e dytë në historinë e kësaj gjykate që zbatohet një procedurë e tillë për të trajtuar shkeljen e lirisë së shprehjes.[68]

Rastet e sipërpërmendura dëshmojnë mbi kufizimet e lirisë në dhënien e informacionit dhe ideve në hapësirën kibernetike shqiptare. Siç ilustrohet nga rastet e aktivistëve politikë, të cilët u ndoqën penalisht në mënyrë arbitrare për postime në mediat e tyre sociale, vërehen dallime të konsiderueshme në qasjen institucionale ndaj lirisë për publikimin e opinioneve. Përkundrazi, fushatat e shpifjeve (*që trajtohen më poshtë*) që venë në shënjestër gazetarët dhe aktivistët mbeten pa u trajtuar nga Policia e Shtetit. Për më tepër, mbyllja kontroversiale e faqes së internetit JOQ dhe përpjekja për të frikësuar gazetarët e Lapsi.al për të treguar burimet e tyre, tregojnë një prirje për të reaguar nxitimxhi, duke tkurrur mjedisin mediatik ndaj pikëpamjeve të kundërta.

Qasja e qeverisë ndaj informacionit publik gjatë pandemisë Covid-19 e zbehu edhe më tej dallimin mes informacionit zyrtar dhe propagandës politike. Mediat sociale të kryeministrit dhe transmetuesi personal online ERTV u bënë burimi kryesor i informacionit për përditësimet mbi vendimet e rëndësishme të qeverisë. Gjatë izolimit kombëtar për shkak të pandemisë, konferencat për shtyp ishin të ndaluara për gazetarët, prandaj centralizimi i informacionit ishte i dukshëm, veçanërisht për personat PAK dhe ata pa akses në internet. Edhe grupeve të tjera të interesit, si gazetarët dhe OSHC-të, u duhej të mbështeteshin në mediat sociale për të marrë informacion mbi ndryshimet e fundit ligjore, të cilat në disa raste u publikuan në mediat sociale përpara se të pasqyroheshin në Fletoren Zyrtare.[69] Tranzicioni i qeverisjes në median sociale solli kritika nga Avokati i Popullit dhe grupimet joqeveritare si Qendra Evropiane për Lirinë e Medias dhe Shtypit, Safejournalists.net, etj. Përveç kësaj, themelimi i një Agjencie të re për Median dhe Informimin (AMI), shpallur në shtator 2021[70] ngriti shqetësime të tjera për centralizimin e mëtejshëm të publikimit të informacionit. AMI pritet të monitorojë median online si dhe të menaxhojë marrëdhëniet dhe komunikimin e ministrive me median, gjë që mund të rezultojë në shkelje të mundshme të së drejtës për informim.[71]

Në janar 2021, për shkak të një seri **sulmesh të shpërndara të mohimit të shërbimit (DDoS)** faqja e internetit e Federatës Shqiptare të Futbollit (FShF) dhe e disa mediave online dolën jashtë funksioni. Ato raportuan ndërprerje të shërbimit ose serverëve dhe aspekteve të tjera lidhur me praninë e tyre në internet.[72] Sulmet kibernetike ndodhën menjëherë pasi mediat[73] publikuan një audio regjistrim të

---

67 Rregulli 39 i Rregullores së Gjykatës së GJEDNJ-së për Masat e Përkohshme.

68 Intervistë me një avokat për të drejtat e njeriut, datë 14/4/2022.

69 OBC Transeuropa (2020) *Shqipëria: Informimi publik bëhet viktimë e COVID-19.*

70 *Vendim i Këshillit të Ministrave, datë 18/9/2020*

71 Res Publica (2021) *Qeveria "rregullon" informimin publik, pa përfillur Komisionerin që ligji i ka varur në qafë "celësat" e të drejtës së informimit*

72 Qendra Evropiane për Lirinë e Shtypit dhe Medias (2022) *Sulme kibernetike kundër mediave të ndryshme pas publikimit të skandalit të dyshuar zgjedhor*.

73 RTV Ora, Lapsi.al, Dosja.al, Syri.net, Maska.al, Gijotina.al, Faktor.al dhe SportEkspress u prekën nga këto sulme kibernetike.

kryebashkiakut të Tiranës, E. V., i cili kërcënonte dhe fliste keq për kreun e FShF-së A. D. dhe tentonte të ndërhynte në zgjedhjet e ardhshme brenda FShF-së. Me sa duket, sulmet synonin t'i nxirrnin jashtë funksioni faqet e internetit për të parandaluar shpërndarjen e audio përgjimit. Mes të tjerash, në atë që kryebashkiaku e cilësoi si "bisedë mes çunash", ai tregon në mënyrë flagrante kapjen politike të SPAK-ut, teksa akuzonte kreun e FShF-së për korrupsion.[74] Kur u pyet për përvojën e tij në trajtimin e sulmeve kibernetike, një përfaqësues i një media online, e cila u bë pre e sulmit DDoS me qëllim fshirjen e arkivit online, tregoi se procesi i identifikimit të autorit është i ndërlikuar dhe i kushtueshëm. Sipas tyre, në këto situata, mediat online i përqendrojnë të gjitha energjitë e tyre në rikthimin e të dhënave dhe minimizimin e dëmit, në vend që të denoncojnë autorin, i cili në rastin e tyre mbeti i paidentifikuar.

Në lidhje me ngacmimet dhe shpifjet online kundër gazetarëve, gjatë viteve të fundit ka pasur probleme të shumta. Gazetaret femra duket se janë veçanërisht në shënjestër, ndërkohë që një nga rastet më të fundit përfshin A. T., një gazetare që mori kërcënime me vdekje përmes Facebook. Edhe pse A. T. kishte kryer vetë punën hetimore dhe kishte gjetur informacione që mund të identifikonin autorin, nga Policia e Shtetit nuk u ndërmor asnjë veprim.[75] Më herët, një tjetër gazetare, S. M. ishte subjekt i diskreditimit, kërcënimeve dhe bullizmit në internet pasi kishte kritikuar një mjek në llogarinë e saj në Facebook.

Gjatë përcaktimit të mjedisit të mediave sociale në Shqipëri, u raportuan raste të Sjelljes së Koordinuar Joautentike (CIB) ku llogaritë e mediave dhe të MDNJ-ve iu nënshtruan raporteve të koordinuara që synonin mbylljen e llogarive të tyre. Raportet e koordinuara erdhën pas publikimit të shkrimeve redaksionale ose videove investigative ose të debatueshme. Në një rast, subjekti pretendoi se më shumë se 50 njerëz po komentonin në një video dhe po nxisnin njëri-tjetrin të raportonin llogaritë e autorit në mediat sociale. Këto sjellje online nuk janë të reja për Shqipërinë dhe sipas një denoncuesi në Facebook, në vend funksionojnë disa rrjete faqesh dhe profilesh false të angazhuara në përpjekje për të shtrembëruar debatin politik.[76]

Rëndësia e trajtimit të CIB theksohet edhe nga një përfaqësues i Këshillit Shqiptar të Medias. Gjatë një interviste, ai tha: *"Problemi është se ato [mediat online] përdorin një platformë me të cilën Shqipëria nuk ka asnjë kontakt. [...] I gjithë ndërveprimi bazohet në algoritmet e Facebook dhe kjo prodhon një marrëdhënie të njëanshme. Facebook bllokon ndarjen e përmbajtjes herë pas here ose e ndalon të gjithë faqen – dhe disa nga arsyet që ata citojnë për këtë kanë të bëjnë me artikullin që nuk është në përputhje me rregulloren e Facebook."* Eksperti i medias thotë se afati kohor për bllokimin ndryshon nga ndalim një ose tre-ditor për të përdorur platformën deri në një javë – dhe ndalim deri në 10 muaj. Megjithatë, eksperti argumenton se mungesa e ndërveprimit të medias me administratën e Facebook-ut i pengon mediat shqiptare që t'i zgjidhin këto çështje menjëherë. Gazetarët shqiptarë që janë përpjekur të apelojnë ndalimin, e përshkruajnë procesin si jotransparent dhe kohëzgjatja e shqyrtimit nuk është e përcaktuar. Aktualisht është e paqartë nëse Facebook ka një mekanizëm kontrolli që filtron përmbajtjen në gjuhën shqipe, mungesa e të cilit tregon se ndalimi i përmbajtjes mbështetet vetëm në algoritmet dhe politikat e platformës, të cilat kanë një ndikim negativ në mënyrë disproporcionale në mediat kritike. Një studim pilot i kryer nga Këshilli Shqiptar i Medias mbi portalet që shpërndajnë artikujt e tyre përmes Facebook, sugjeronte se platforma e mediave sociale tenton të censurojë raportet investigative dhe shkrimet redaksionale, duke cituar në shumicën e rasteve standardet etike.[77]

Gjetjet nga intervistat me gazetarë dhe MDNJ konfirmojnë se raportimet e koordinuara të përmbajtjeve

---

74 Exit.al (2022) *Armand Duka fiton mandatin e gjashtë si President i Federatës Shqiptare të Futbollit.*

75 Balkan Insight (2022) *Gratë si mbajtëse të përgjegjësisë.*

76 Exit.al (2021) *Sinjalizuesja e Facebook Sophie Zhang: "Ajo që gjeta në Shqipëri ishte kaq e rëndë… Ndjeva sikur kisha gjak në duart e mia"*.

77 Këshilli Shqiptar i Medias (2022) *Studim pilot mbi problematikën e rregullimit etik të mediave shqiptare nga platforma e Facebook.*

online për tema politike, mjedisore, ekonomike ose LGBTQ+ janë shpesh të suksesshme. Platforma e mediave sociale bllokon përmbajtjen ndërsa përdoruesit mbeten duke spekuluar rreth motiveve. Të intervistuarit sugjerojnë se shpeshherë koordinimi ndodh përmes kanaleve të ndryshme të komunikimit, duke ia bërë të vështirë Facebook-ut të ndërhyjë.

Përmbajtjet veçanërisht kritike për punën e qeverisë, ose që përmendin oligarkët, raportohet të jenë fshirë nga Acromax Media GmbH, kompani e menaxhimit të të drejtave digjitale në Gjermani. Artikujt e publikuar në faqet e internetit që kanë kontratë me Acromax mund të hiqen pa njoftuar paraprakisht autorin.[78] Shqetësimet për censurën politike u rritën në vitin 2019 kur pronari shqiptar i kompanisë pretendoi se Acromax po bashkëpunonte me PS-në me qëllim raportimin në Facebook të lajmeve të rreme për anëtarët e partisë. Raportet nga gazetarët tregonin se nga interneti po hiqeshin sistematikisht përmbajtje të caktuara kritike ndaj qeverisë apo kryetarit të Bashkisë së Tiranës. Acromax aktualisht operon në bazë të marrëveshjeve për të drejtën e autorit me disa transmetues digjitalë shqiptarë, dhe i mundëson kompanisë të censurojë përmbajtjen e prodhuar nga këto grupe mediatike në emër të tyre.[79] Për shembull, nëse një gazetar dëshiron t'i referohet në një artikull një deklarate të dhënë nga një zyrtar qeveritar gjatë një interviste, ai nuk mund ta bëjë këtë. Acromax mund të pengojë gazetarin të citojë zyrtarin në një artikull, edhe pse gazetari mund ta ketë kryer vetë intervistën.[80] Megjithatë, vëzhgimet tregojnë se kompania zbaton një standard të dyfishtë kur bëhet fjalë për përmbajtjet që promovojnë ose lavdërojnë punën e qeverisë, e cila, nëse shpërndahet, rrallëherë fshihet nga Acromax.

Gjatë dy viteve të fundit, Shqipëria ka qenë dëshmitare e një sërë shkeljesh të lirisë së shprehjes, duke përfshirë mbikëqyrjen elektronike, ndjekjet penale, sjelljet e koordinuara joautentike dhe forma të tjera censurimi dhe frikësimi. Rastet e mbylljeve të porositura të uebsajteve, sulmet kibernetike të targetuara, ngacmimet në internet të gazetarëve dhe ngushtimi i hapësirës për lirinë për të marrë dhe për të dhënë informacion, dëshmojnë më tej rënien e lirisë së medias. Me rritjen e formave online për censurimin që mbytin kritikën dhe promovojnë propagandën qeveritare, gazetaria e pavarur përballet me sfida në rritje. Kështu, tërheqja nga qasja e "rregullimit shtetëror të medias", ndërkohë që promovohet vetë-rregullimi dhe raportimi etik, dhe rritet transparenca qeveritare, mund t'i sjellë peizazhit mediatik në Shqipëri ndryshimin pozitiv që i mungon.

2.3 Siguria kibernetike dhe ndalimi i diskriminimit

Hapësira kibernetike përfaqëson një sferë të re ku lulëzojnë shkeljet e të drejtave të njeriut dhe grupe të caktuara targetohen në mënyrë të veçantë. Shkeljet që ndodhin në këtë mjedis disi të paqeverisur shpesh mbeten të pandëshkuara, ndërkohë që institucionet dështojnë t'i përgjigjen realitetit të ri dhe të garantojnë të njëjtat të drejta online dhe offline. Ndër format më të zakonshme të diskriminimit të identifikuara në mjedisin digjital në Shqipëri janë gjuha e urrejtjes dhe ngacmimi (shqetësimi). Sipas një sondazhi kombëtar[81] rreth 58% e qytetarëve shqiptarë mendojnë se gjuha e urrejtjes është shumë e përhapur në vend, ndërsa nga ana e qytetarëve që i përkasin grupeve të margjinalizuara - 9 nga 10 mendojnë se gjuha e urrejtjes është shumë e përhapur. 64% mendojnë se media sociale është mjedisi ku gjuha e urrejtjes është më e përhapur. Të dhëna të tjera tregojnë se në shënjestër të këtyre shkeljeve më

78 Intervistë me një gazetar datë 3/2/2022.

79 Qendra për Studimin e Demokracisë (2020) *Tkurrja e hapësirës për lirinë e medias në Evropën Juglindore në mes të pandemisë Covid-19 dhe emergjencës shtetërore: një përmbledhje krahasimore.*

80 Netzpolitik (2020) *Një kompani gjermane është përgjegjëse për fshirjen e videove kritike për qeverinë shqiptare.*

81 Komisioneri për Mbrojtjen nga Diskriminimi (2021) *Përtej përkufizimeve, një thirrje për veprim kundër gjuhës së urrejtjes në Shqipëri*.

së shumti janë gratë,[82] fëmijët[83] dhe minoritetet, si romët, egjiptianët[84] dhe personat LGBTI+.[85] Gjithashtu vihet re se ata që mbrojnë të drejtat e këtyre grupeve, si MDNj-të, bëhen edhe vetë shënjestër e sulmeve dhe përbaltjes online.[86]

Vitet e fundit, Avokati i Popullit dhe KMD i kanë nënvizuar këto probleme në raportet e tyre vjetore, si dhe në vendimmarrjen apo deklaratat e tyre publike. Trajtimi i gjuhës së urrejtjes është me rëndësi të madhe pasi, ndër pasoja të tjera, gjuha e urrejtjes mund të çojë edhe në krime të urrejtjes.[87] Pavarësisht rëndësisë, mungon një sistem i përgjithshëm gjithëpërfshirës i mbledhjes së të dhënave që do të bënte të mundur një vlerësim të plotë të situatës në nivel kombëtar. Kjo konfirmohet edhe nga Komisioni Evropian kundër Racizmit dhe Intolerancës (ECRI) dhe OSBE/ODIHR, sipas të cilëve, Shqipëria nuk ka raportuar sistematikisht shifra për krimet e urrejtjes të regjistruara nga policia.[88] Për ilustrim, Raporti Vjetor i Prokurorit të Përgjithshëm për Gjendjen e Kriminalitetit për vitin 2020 konstaton se gjatë vitit 2020 janë ndjekur penalisht 6 raste të nxitjes së urrejtjes dhe është dënuar një person, por nuk tregon nëse ato kanë ndodhur online apo offline dhe se cilat grupe ishin në shënjestër.[89] Po ashtu, sipas të njëjtit raport, gjatë vitit 2020 nuk është regjistruar asnjë denoncim për kërcënime me motive raciste ose ksenofobike ose raste të shpërndarjes së përmbajtjeve raciste ose ksenofobike përmes sistemeve informatike.

Për sa i përket ngacmimeve seksuale, në vitin 2020 janë ndjekur penalisht 58 raste dhe janë dënuar 18 persona. Edhe në këtë rast, raporti nuk tregon nëse ngacmimi ka ndodhur në internet apo jo. Të dhëna të tilla të kufizuara nuk lejojnë që të bëhet një analizë gjithëpërfshirëse për të identifikuar fushat ku mund të ndërhyhet për të trajtuar gjuhën e urrejtjes, ngacmimin ose forma të tjera të diskriminimit ose veprave penale të motivuara nga diskriminimi që ndodhin në hapësirën kibernetike. Vetë raporti njeh mangësitë në sistemin e mbledhjes së të dhënave, duke vënë në dukje nevojën e përpunimit të të dhënave për motivet e krimeve, si dhe nevojën për një sistem funksional të automatizuar në nivel kombëtar. Nga ana tjetër, ai thekson se përmirësimi i sistemit të mbledhjes së të dhënave kërkon një qasje të koordinuar dhe të harmonizuar që shkon përtej nevojave të brendshme të çdo institucioni të përfshirë. Sipas të njëjtit raport, në vitin 2020, u krijua një regjistër i dedikuar për mbledhjen dhe përpunimin e të dhënave në lidhje me dhunën ndaj grave dhe fëmijëve, krimet e motivuara nga urrejtja dhe dhunën në familje. Megjithatë, urdhri i Prokurorit të Përgjithshëm,[90] që rregullon funksionimin e këtij regjistri dhe mënyrën e mbledhjes dhe përpunimit të të dhënave statistikore, mbulon vetëm krimet ndaj të miturve.

Me gjithë mangësitë e shumta në trajtimin e çështjeve të lartpërmendura, janë identifikuar disa praktika të mira mbi të cilat mund të ndërtohet më tej. Në 2019, u krijua Aleanca Kundër Gjuhës së Urrejtjes,[91] nëpërmjet një memorandumi bashkëpunimi të nënshkruar nga Avokati i Popullit, KMD, AMA dhe Këshilli Shqiptar i Medias - një organizatë e pavarur gazetarësh që promovon vetë-rregullimin e medias. Kjo aleancë synon të përfshijë aktorët kryesorë në parandalimin e gjuhës së urrejtjes, të koordinojë dhe bashkojë përpjekjet për të ndërgjegjësuar dhe luftuar kundër këtij fenomeni. Një tjetër shembull pozitiv i përpjekjeve të koordinuara ndërmjet OSHC-ve, institucioneve publike dhe industrisë së internetit dhe

82 Reporter.al (2020) *Gjuha e urrejtjes në media targeton gratë dhe komunitetet e margjinalizuara*

83 ISIGURT.AL (2022) *Dhuna dhe ngacmimet seksuale të fëmijëve në internet vazhdojnë në shifra të larta*

84 Komisioni Evropian kundër Racizmit dhe Intolerancës (2020) *Raporti i ECRI për Shqipërinë (cili i gjashtë i monitorimit)*.

85 Komisioneri për Mbrojtjen nga Diskriminimi (2021) *Përtej përkufizimeve, një thirrje për veprim kundër gjuhës së urrejtjes në Shqipëri.*

86 Civil Rights Defenders (2020) *Mbrojtësit e të Drejtave të Njeriut në Ballkanin Perëndimor.*

87 Intervistë me një përfaqësues të zyrës së Komisionerit për Mbrojtjen nga Diskriminimi datë 14/4/2022.

88 Komisioni Evropian kundër Racizmit dhe Intolerancës (2020) *Raporti i ECRI për Shqipërinë (cili i gjashtë i monitorimit).*

89 *Raporti i Prokurorit të Përgjithshëm për Gjendjen e Kriminalitetit në 2020*.

90 Urdhri nr. 124/2020 i Prokurorit të Përgjithshëm.

91 Raporti vjetor i Avokatit të Popullit për 2020.

komunikimit është krijimi i linjës telefonike kombëtare shqiptare për sigurinë në internet[92] nga CRCA Albania, e cila është një platformë ku mund të raportohen rastet e ngacmimit të fëmijëve dhe gjuhës dhe krimeve të urrejtjes për t'iu referuar më pas autoriteteve përkatëse. Së fundi, miratimi i Udhëzimit të Përgjithshëm të Prokurorit të Përgjithshëm[93] për hetimin penal të dhunës ndaj grave, dhunës në familje dhe dhunës me motive urrejtjeje, ishte një tjetër hap pozitiv i ndërmarrë në vitin 2020. Ky udhëzim synon të unifikojë praktikën institucionale në këtë drejtim dhe të sigurojë efikasitet në ndjekjen penale të këtyre krimeve. Udhëzimi adreson aspekte të përndjekjes online, përdorimin e mediave sociale për krimet e urrejtjes si dhe ofron një listë të gjatë të motiveve diskriminuese që mund të çojnë në krime të urrejtjes, duke shkuar përtej Kodit Penal, i cili nuk e bën të njëjtën gjë.

Edhe pse shkeljet e të drejtave të njeriut në lidhje me gjuhën e urrejtjes dhe ngacmimet që ndodhin në hapësirën kibernetike duket se rrallëherë arrijnë të depërtojnë në sistemin shqiptar të drejtësisë penale, situata është më inkurajuese kur bëhet fjalë për reagimin e institucioneve të pavarura të të drejtave të njeriut. Gjatë viteve të fundit janë trajtuar disa raste të diskriminimit në hapësirën kibernetike, kryesisht nëpërmjet ankesave të paraqitura nga OSHC-të, por në disa raste edhe të iniciuara nga KMD-ja (*ex officio*). Disa vendime të marra nga KMD-ja ofrojnë analizë të thelluar të rasteve të gjuhës së urrejtjes si formë diskriminimi, si dhe ndërlidhjen e saj me lirinë e shprehjes dhe kufijtë e kësaj të fundit. KMD në vendimet e tij i referohet standardeve ndërkombëtare të të drejtave të njeriut dhe të drejtës kibernetike, Rekomandimit Nr. 15 të ECRI-t për luftën kundër gjuhës së urrejtjes si dhe praktikës gjyqësore të GJEDNJ-së dhe Gjykatës Evropiane të Drejtësisë. Nga ana tjetër, praktika gjyqësore e gjykatave shqiptare në këtë drejtim është pothuajse inekzistente.

Për sa i përket **diskriminimit racor**, në një rast të identifikuar, portali online (joq.al) përdori gjuhë diskriminuese dhe stereotipizuese ndaj komunitetit rom dhe egjiptian në një postim në Facebook dhe një OSHC paraqiti ankesë tek KMD. KMD-ja e gjeti portalin në diskriminim të drejtpërdrejtë ndaj romëve dhe egjiptianëve, në formën e shqetësimit dhe u kërkoi atyre të ndalonin së publikuari materiale me përmbajtje diskriminuese.[94] Ky rast është me interes për shkak të dimensioneve të shumta që adreson. Së pari, gjatë hetimit administrativ, KMD u tregua shumë proaktiv dhe pas disa përpjekjeve të pasuksesshme për të lokalizuar dhe komunikuar me administratorët e portalit, kontaktoi drejtpërdrejt me Facebook (kompaninë) dhe kërkoi heqjen e postimit në fjalë. Kjo vë në dukje sfidat në lidhje me identifikimin e pronarëve/administratorëve të mediave online për të garantuar llogaridhënie, sepse siç është adresuar në seksionet e mësipërme, këto nuk janë të regjistruar. Zbatimi i vendimeve të KMD-së në raste të tilla varet nga vullneti i administratorëve të mediave apo platformave të rrjeteve sociale për të hequr materialin me përmbajtje diskriminuese, përndryshe nuk mund të zbatohet.[95] Më tej, vendimi i analizuar më sipër referon Konventën për Krimin në Fushën e Kibernetikës dhe protokollin shtesë të saj, si dhe shtjellon ndikimin që mund të kishte ky portal online për shkak të audiencës dhe popullaritetit të tij të madh, në përhapjen e qëndrimeve agresive, negative dhe diskriminuese ndaj romëve dhe egjiptianëve.

KMD-ja ka trajtuar gjithashtu disa raste të **diskriminimit ndaj komunitetit LGBTI+** që kanë ndodhur në hapësirën kibernetike. Me marrjen e një ankesë të paraqitur nga OSHC-të, KMD-ja gjeti se gjuha e përdorur në një postim në Facebook nga një parti politike (Aleanca Kuq e Zi) ishte diskriminuese, në formën e gjuhës së urrejtjes kundër komunitetit LGBTI+.[96] Postimi bënte thirrje publike për protestë kundër legalizimit të martesave mes të njëjtit seks dhe kundër paradës së krenarisë. Postimi mori shumë komente me përmbajtje urrejtje të cilat bënin thirrje për dhunë dhe vdekje ndaj personave LGBTI+. Sipas vendimit të KMD, postimi në Facebook dhe komentet nxitën urrejtje të bazuar në orientimin seksual dhe

92 *www.isigurt.al* Aksesuar për herë të fundit më datë 13/06/2022.

93 Udhëzim i Përgjithshëm nr. 17/2020 i Prokurorit të Përgjithshëm

94 Vendim nr. 135, 13/6/2018 i Komisionerit për Mbrojtjen nga Diskriminimi.

95 Intervistë me një përfaqësues të zyrës së Komisionerit për Mbrojtjen nga Diskriminimi datë 14/4/2022.

96 Vendim nr. 125, 01/08/2014 i Komisionerit për Mbrojtjen nga Diskriminimi.

identitetin gjinor. Edhe pse partia politike e fshiu postimin, KPD vendosi masë administrative (gjobë) ndaj saj dhe u kërkoi të kërkonin falje publike. Ky vendim i KMD u kundërshtua më pas në Gjykatën Administrative të Shkallës së Parë në Tiranë, e cila la në fuqi vendimin e KMD-së.[97] Si vendimi i KMD-së ashtu edhe ai i gjykatës, janë ndër të parët e kësaj natyre, pasi janë dhënë vetëm pak vite pas miratimit të Ligjit për Mbrojtjen nga Diskriminimi dhe mund të konsiderohen si një pikë referimi për mbrojtjen e LGBTI+ nga gjuha e urrejtjes online. Në një rast tjetër të ngjashëm[98] KMD-ja kërkoi që një politikan të kërkonte falje publike dhe të tërhiqej nga deklaratat e bëra në facebook të cilat denigronin dhe përbuznin personat LGBTI+.

Diskriminimi në bazë të aftësisë së kufizuar është një tjetër formë e identifikuar e diskriminimit. Gjatë një reality show në televizionin Top Channel u përdor gjuhë stigmatizuese ndaj personave me sindromën Doën dhe transmetimi u shpërnda edhe në kanalet e tij në rrjetet sociale. KMD-ja me nismën e tij konstatoi se gjuha e përdorur ishte diskriminuese për shkak të aftësisë së kufizuar në formën e shqetësimit dhe kërkoi që kanali televiziv të kërkonte falje publike.[99] Njësoj si për rastet e tjera të trajtuara, ky rast sjell në vëmendje ndikimin e mediave audiovizive në hapësirën kibernetike dhe përdorimin e legjislacionit kundër diskriminimit për trajtimin e gjuhës së urrejtjes që ndodh në kanalet televizive, kanalet e tyre të mediave sociale dhe komentet që vijojnë. Megjithatë, sigurimi i llogaridhënies së për këto të fundit mbetet një sfidë pasi mediat online nuk janë të regjistruara dhe menaxhimi i komenteve nuk është i rregulluar.

Më tej, personat me aftësi të kufizuar mund të ekspozohen ndaj diskriminimit të tërthortë nëse nuk u ofrohen **shërbime publike të aksesueshme/përshtatura online**. Nga maji i vitit 2022, të gjitha shërbimet publike filluan të ofrohen online, ndërkohë që mungojnë vlerësimet mbi ndikimin që ky vendim mund të ketë për grupe të caktuara. Kjo mund të bëjë që personat me aftësi të kufizuar ose ata që nuk kanë njohuri digjitale të përjetojnë një trajtim të padrejtë. Grupe të tilla shpesh përballen edhe me rritjen e barrës financiare, pasi mbështeten gjithnjë e më shumë tek bizneset private për të marrë ndihmë me aplikime online për shërbime. Digjitalizimi i shërbimeve, pa garantuar akomodim dhe përshtatje të arsyeshme, mund të rezultojë në shkelje të Ligjit për Mbrojtjen nga Diskriminimi dhe Ligjit për Përfshirjen dhe Aksesueshmërinë e Personave me Aftësi të Kufizuara. Nga ana tjetër, ndërkohë që rreth 88.3% e familjeve shqiptare kanë **akses në shërbimin e internetit**,[100] nuk ka të dhëna për grupet që nuk kanë akses në internet dhe si rrjedhojë mund të diskriminohen nga vendime të tilla, duke mos qenë në gjendje të përfitojnë nga shërbimet publike online. Këto mangësi janë bërë gjithnjë e më evidente që nga fillimi i pandemisë Covid-19 kur shumë institucione filluan të punojnë online dhe duhet të adresohen menjëherë në kuadër të dixhitalizimit të shërbimeve publike.[101]

Ngacmimi (shqetësimi) seksual u rendit si një nga format e diskriminimit në Ligjin për Mbrojtjen nga Diskriminimi në vitin 2020, ndërsa kur përmbushen kriteret e përcaktuara në Kodin Penal, ngacmimi seksual mund të klasifikohet edhe si vepër penale. Meqenëse ndryshimi ligjor i sipërpërmendur është bërë vitet e fundit, numri i rasteve të ngacmimeve seksuale (kibernetike) të shqyrtuara nga KMD është i kufizuar. Gjithashtu, kapacitetet e kufizuara teknike të KMD-së pamundësojnë që institucioni të kryejë hetime të plota administrative në rastet kur ngacmimet seksuale ndodhin online. Për ilustrim, në një rast ngacmimi seksual në vendin e punës, provat kryesore të administruara nga KMD ishin mesazhet e shkëmbyera në aplikacionin WhatsApp. Në pamundësi për të verifikuar vërtetësinë e tyre, KMD pezulloi hetimin administrativ. Ndërkohë, krahas ankesës në KMD ishte bërë edhe një kallëzim penal për këtë çështje (proceset nuk pengojnë njëri-tjetrin) dhe Prokuroria kishte kërkuar verifikimin e mesazheve në kuadër të hetimit penal. Vetëm kur siguroi aktin e ekspertimit të hartuar në kuadër të hetimit penal që vërtetonte vërtetësinë e mesazheve të WhatsApp-it, KMD-ja mundi të rifillonte hetimin administrativ duke

97 Vendim nr. 3127, 09/06/2015 i Gjykatës Administrative të Shkallës së Parë Tiranë.

98 Vendim nr. 81, 10/08/2020 i Komisionerit për Mbrojtjen nga Diskriminimi.

99 Vendim nr. 155, 30/10/2020 i Komisionerit për Mbrojtjen nga Diskriminimi.

100 Instituti i Statistikave (2021) *Përdorimi i Teknologjisë së Informacionit dhe Komunikimit në Familje, 2021*

101 Intervistë me një përfaqësues të zyrës së Komisionerit për Mbrojtjen nga Diskriminimi datë 14/4/2022.

gjetur se paditësja ishte diskriminuar për shkak të gjinisë në formën e ngacmimit seksual.[102]

Gjuha e urrejtjes me bazë gjinore është një tjetër formë diskriminimi në rritje në Shqipëri. Një monitorim i vitit 2020 për mediat online[103] nxori në pah se 70% e rasteve të gjuhës së urrejtjes kanë si subjekt gratë. Të njëjtat të dhëna tregojnë se gjatë dy viteve të fundit, rastet e gjuhës së urrejtjes seksiste dhe me bazë gjinore janë dyfishuar. Për më tepër, studimet tregojnë se gratë janë veçanërisht të shënjestruara kur angazhohen në aktivizëm apo në aktivitete publike. Një raport mbi MDNJ-të në Shqipëri zbulon se **Gratë Mbrojtëse të të Drejtave të Njeriut (GMDNJ)** janë grupi i dytë më të rrezikuara i MDNJ-ve, pas aktivistëve LGBTI+.[104] Në shënjestër duket se janë veçanërisht MDNJ-të që punojnë me viktima të trafikimit të qenieve njerëzore ose dhunës në familje, aktivistet feministe ose LBT+ dhe gazetaret.[105] Ato bëhen subjekt i ngacmimeve të vazhdueshme jo vetëm për shkak të gjinisë, por edhe për shkak të punës që bëjnë, ndaj dhe motivet, në këtë rast, janë **ndërsektoriale**. Pavarësisht rëndësisë, duke qenë se diskriminimi ndërsektorial dhe diskriminimi i shumëfishtë janë përfshirë rishtazi në legjislacionin shqiptar kundër diskriminimit, praktika institucionale dhe ndërgjegjësimi i publikut në këtë drejtim janë ende të kufizuara. GMDNJ -të e kontaktuara për këtë raport raportuan përjetimin e rasteve të ngacmimit seksual në mediat sociale, duke përfshirë marrjen e komenteve mizogjene e me përmbajtje urrejtje, bulizimin, përbaltjen dhe talljen nëpërmjet shpërndarjes së fotove dhe informacione të tyre private, marrjen e kërcënimeve për përdhunim si dhe diskriminim për shkak të gjinisë dhe aktivizimit të tyre politik apo feminist. Shumica e tyre (me një përjashtim) nuk i kishin kallëzuar (raportuar) këto shkelje, kryesisht për shkak të mosbesimit se autoritetet do të përgjigjeshin ose do të ofronin ndonjë zgjidhje efektive. Vetëm një aktiviste, e cila zgjodhi të mbetej anonime, kishte denoncuar në polici një rast ngacmimi kibernetik, por policia nuk kishte marrë asnjë masë. Mungesa e reagimit nga Policia dhe Prokuroria për rastet e ngacmimeve kibernetike me bazë gjinore evidentohet edhe në një raport të DCAF, ku për rastin e zgjedhur nga Shqipëria tregohet se pavarësisht disa incidenteve të raportuara, nuk ishte marrë asnjë masë nga autoritetet.[106] Në këtë rast, njësia e krimit kibernetik pranë Policisë së Shtetit kishte luajtur më tepër rol këshillues se ligjzbatues pa arritur të ofronte mbrojtje efektive për aktivisten dhe gazetaren e kërcënuar.[107] Ndërkohë, Prokuroria nuk kishte nisur hetim penal për shkak se nuk i kishte cilësuar veprimet si "kërcënim".[108] Këto institucione duhen fuqizuar pasi shpesh kanë burime njerëzore të pamjaftueshme dhe mungesë të infrastrukturës teknike dhe trajnimit, gjë që e bën të vështirë reagimin e duhur ndaj denoncimeve që marrin.[109]

Sipas raportit të Civil Rights Defenders,[110] krahas GMDNJ-ve, kategoria më e shënjestruar e MDNJ-ve në Shqipëri janë **aktivistët LGBTI+** dhe ata që punojnë për të drejtat e punëtorëve të seksit. Ata kanë më shumë gjasa se të tjerët të përballen me kërcënime anonime, ndërkohë që gjuha e urrejtjes në internet kundër këtyre aktivistëve është mjaft e zakonshme. K.P, aktivist dhe themelues i një organizate LGBTI+, u largua nga Shqipëria dhe iu dha azil në një shtet tjetër, pasi mori dhjetëra kërcënime me vdekje dhe mesazhe denigruese në rrjetet sociale.[111] Xh.K, një tjetër aktiviste e njohur LGBTI+, u bë target i gjuhës së urrejtjes dhe kërcënimeve në internet pasi u shfaq në një televizionet kombëtare duke folur në favor të të drejtave prindërore për personat LGBTI+.[112] Një aktivist transgjinor, i cili dëshironte të mbetej anonim, tha

---

102 Vendim nr. 259, 29/12/2021 i Komisionerit për Mbrojtjen nga Diskriminimi.

103 Citizens Channel (2020) *Monitorim: Rreth 70% e gjuhës së urrejtjes dhe diskriminimit në median online prek vajzat dhe gratë*

104 Civil Rights Defenders (2020) *Mbrojtësit e të Drejtave të Njeriut në Ballkanin Perëndimor.*

105 Po aty.

106 DCAF (2021) *Dhuna kibernetike ndaj grave dhe vajzave në Ballkanin Perëndimor: Raste Studimore të Përzgjedhura dhe një Qasje e Qeverisjes së Sigurisë Kibernetike.*

107 Intervistë me një ekspert për të drejtat e njeriut datë 3/2/2022.

108 DCAF (2021) *Dhuna kibernetike ndaj grave dhe vajzave në Ballkanin Perëndimor: Raste Studimore të Përzgjedhura dhe një Qasje e Qeverisjes së Sigurisë Kibernetike.*

109 Intervistë me përfaqësues të Njësisë C për Hetimin e Krimeve Kompjuterike, Policia e Tiranës, datë 26/5/2022.

110 Civil Rights Defenders (2020) *Mbrojtësit e të Drejtave të Njeriut në Ballkanin Perëndimor.*

111 Dritare.net (2017) *Kërcënohet me jetë, ikën nga Shqipëria Kristi Pinderi.*

112 Komiteti Norvegjez i Helsinkit (2021) *Shqipëri: Të hetohen kërcënimet ndaj Xheni Karajt.*

se u përball me gjuhë urrejtje dhe kërcënime në platformat e mediave sociale kur doli hapur si transgjinor ose në rastet kur publikonte materiale mbi të drejtat e LGBTI+. Deri më sot, nuk është mbajtur përgjegjës asnjë autor për ndonjë nga shkeljet e përmendura më sipër.[113] Ashtu si GMDNJ-të, aktivistët LGBTI+ rrallë i raportojnë kërcënimet që marrin në internet, për shkak të besimit që mbizotëron mes tyre se kërcënimet homofobike online nuk merren seriozisht nga Policia dhe Prokuroria. Ata argumentojnë se teksa pandëshkueshmëria është në shifra të larta edhe kur bëhet fjalë për krime (fizike) të urrejtjes me natyrë homofobike, ndjeshmëria e autoriteteve ndaj sulmeve të tilla kibernetike është pothuajse inekzistente. Asnjë nga rastet që është denoncuar prej tyre nuk është ndjekur penalisht, pasi autoritetet ose nuk kanë arritur të identifikojnë individët që fshiheshin pas profileve të rreme, ose provat nuk janë konsideruan të mjaftueshme që kërcënimi i raportuar të plotësonte kriteret për tu cilësuar si vepër penale.[114]

Për sa i përket **vendimmarrjes automatike diskriminuese**, referuar ndryshe si **paragjykim algoritmik**, në përgjithësi mungojnë praktikat institucionale, rregullimi ligjor dhe ndërgjegjësimi publik. Në këtë drejtim, u identifikua një rast, i cili kishte të bënte me skualifikimin e padrejtë të disa familjeve që kishin aplikuar për ndihmë financiare nga shteti nëpërmjet një sistemi elektronik pilot të prezantuar nga qeveria në vitin 2014.[115] Sistemi i automatizuar vlerësonte kërkesat e qytetarëve për ndihmë financiare sipas 52 variablave dhe sipas KMD-së, dukej se favorizonte familjet me numër më të madh anëtarësh, duke lënë jashtë shpesh herë gratë kryefamiljare, të moshuarit që jetonin vetëm, familjet rome dhe egjiptiane etj., edhe kur këta i plotësonin kriteret ligjore. KMD-ja konstatoi diskriminim dhe rekomandoi përmirësimin e sistemit elektronik të automatizuar për të mos lejuar trajtim të diferencuar dhe skualifikime të padrejta të qytetarëve që plotësonin kriteret ligjore për të përfituar ndihmën financiare.[116]

Si përfundim, nevojiten më shumë përpjekje për trajtimin efektiv të rasteve të diskriminimit që ndodhin në hapësirën kibernetike, për rritjen e besimit dhe ndërgjegjësimit, si dhe për të adresuar pandëshkueshmërinë që mbizotëron, veçanërisht në sistemin e drejtësisë penale. Për më tepër, duhet të krijohet një sistem gjithëpërfshirës i mbledhjes së të dhënave për incidentet e urrejtjes në nivel kombëtar. Të dhëna të tilla do të mundësonin identifikimin e fushave të ndërhyrjes për trajtimin e gjuhës së urrejtjes, ngacmimit ose formave të tjera të diskriminimit dhe veprave penale që ndodhin në hapësirën kibernetike. Së fundi, kuadri ligjor përkatës duhet të përditësohet dhe institucionet duhet të pajisen me njohuri dhe infrastrukturë që i lejon t'i përgjigjen sfidave të reja të të drejtave të njeriut në hapësirën kibernetike, në mënyrë që të ofrojnë të njëjtën mbrojtje online dhe offline.

2.4 Siguria kibernetike dhe liria e tubimit paqësor

Interneti dhe hapësira kibernetike janë vendet kryesore bashkëkohore ku njerëzit ndërveprojnë dhe marrin pjesë në çështjet publike. Gjatë dekadës së fundit, këto janë bërë gjithnjë e më të rëndësishme për ushtrimin e lirisë së tubimit paqësor, duke shërbyer si hapësirë dhe si mjet. Ndikimi i madh i mjeteve të tilla në Shqipëri dhe në rang global u ndje veçanërisht gjatë periudhave të gjata të karantinimit për shkak të pandemisë Covid-19, kur MDNj-të, OSHC-të dhe qytetarët e përdorën intensivisht internetin për të planifikuar, organizuar, promovuar, regjistruar dhe marrë pjesë në tubime dhe ngjarje publike. Aktualisht nuk ka asnjë debat publik në Shqipëri mbi tubimet online ose rregullimin e tyre dhe në përgjithësi mungon ndërgjegjësimi në lidhje me sfidat e paraqitura ndaj ushtrimit të lirisë së tubimit në hapësirën kibernetike. Megjithatë, grupe të ndryshme si lëvizja feministe,[117] grupet mjedisore,[118] të rinjtë dhe

113 Intervistë me një aktivist LGBTI+ datë 29/3/2022.

114 Po aty.

115 Intervistë me ish-Komisioneren për Mbrojtjen nga Diskriminimi datë 6/5/2022.

116 Vendim nr. 185, datë 24/12/2015 i Komisionerit për Mbrojtjen nga Diskriminimi.

117 Reporter.al (2020) *Shquarja e valës së re të lëvizjes feministe në Shqipëri.*

118 Media Centar Sarajevo (2016) Komunikimi i protestave të qytetarëve që kërkojnë llogaridhënie publike: Raste studimore nga Shqipëria, Bosnja dhe Hercegovina dhe Maqedonia

studentët,[119] lëvizja LGBTI+,[120] po i përdorin gjithnjë e më shumë platformat e mediave sociale, kryesisht Facebook, për të organizuar dhe koordinuar protesta dhe evente dhe për të kontaktuar me publikun. Kjo arriti kulmin gjatë izolimit në periudhën e pandemisë Covid-19 kur në Shqipëria u mbajt parada e krenarisë në internet,[121] ndërsa një pjesë e mirë e protestave të organizuara gjatë viteve të fundit janë iniciuar dhe shpërndarë përmes mediave sociale. Qeveria nuk ka vendosur ndonjë kufizim mbi përdorimin e mediave sociale dhe organizatorët/pjesëmarrësit në tubime mund ta përdorin internetin para, gjatë dhe pas organizimit të tubimit. Deri më sot, nuk është regjistruar asnjë rast i bllokimit të aksesit në komunikim-in online.[122]

Disa nga kërcënimet më të zakonshme të identifikuara në lidhje me ushtrimin e lirisë së tubimit në internet kanë të bëjnë me targetimin e **MDNJ-ve të përfshirë në organizimin e protestave**, përmes fushatave të shpifjes dhe përbaltjes, kërcënimeve, si dhe sulmeve DDoS në llogaritë e tyre personale në rrjete sociale. Një aktivist transgjinor që zgjodhi të mbetet anonim u ngacmua në mediat sociale duke marrë mbi 500 komente urrejtjeje pasi publikoi një postim që ftonte njerëzit t'i bashkoheshin paradës së krenarisë në Tiranë. Përmes raportimeve të organizuara, autorët arritën t'i bllokojnë llogarinë për gati një muaj. Aktivistët e Organizatës Politike, një organizatë e majtë, janë përballur me ngacmime dhe përbaltje të ngjashme në internet për shkak të përfshirjes së tyre në protestat e studentëve të vitit 2019 si dhe aktivitetit të tyre publik në mbështetje të të drejtave të minatorëve. Ata besojnë se sulmet vinin nga aktorë të lidhur me qeverinë dhe biznesmenë vendas. Disa aktivistëve të së njëjtës organizatë, treguan që persona të paidentifikuar u përpoqën të hynin në llogaritë e tyre personale në rrjete sociale pas një demonstrate që kishin organizuar kundër kryeministrit. Taktika të tilla të ngacmimit dhe raportimit të koordinuar kundër aktivistëve janë mjaft të zakonshme dhe synojnë të ndikojnë në mënyrë strategjike debatin në mediat sociale, me qëllimi çorientimin e opinionit publik dhe dekurajimin e veprimeve të aktivistëve.[123] Për të minimizuar rreziqe të tilla, disa aktivistë treguan se kanë filluar të përdorin platforma më të sigurta online për qëllime të koordinimit të brendshëm.

Për sa i përket **mbikëqyrjes së tubimeve**, perceptimi i aktivistëve është se aktiviteti i tyre në mediat sociale në lidhje me organizimin e protestave apo kritikën ndaj politikave qeveritare monitorohet nga autoritetet, partitë politike apo aktorë të tjerë që veprojnë në emër të tyre.[124] Këto perceptime vijnë si pasojë e disa masave që ka marrë qeveria lidhur me survejimin. Së pari, krijimi i AMI-t, institucioni i përmendur më sipër, i cili ndër të tjera, do të kryejë monitorimin e mediave sociale për të evidentuar perceptimin dhe qëndrimet e publikut ndaj veprimtarisë së institucioneve të administratës publike, shihet si një mekanizëm i mundshëm mbikëqyrjeje.[125] Po ashtu, në një email të rrjedhur tregohej se në vitin 2014 qeveria shqiptare mendonte të blinte softuer nga The Hacking Team, i njohur për hakerim të gazetarëve, politikanëve dhe aktivistëve në emër të qeverive globale.[126] Në vijim të këtyre perceptimeve, një aktiviste për të drejtat e romëve dhe egjiptianëve tha se nuk postonte për protesta në mediat sociale, nga frika se survejohej, veçanërisht gjatë pandemisë Covid-19, kur u vendos ndalimi i çdo lloj tubimi, si dhe një gjobë prej 40 mijë euro për ata që e shkelin këtë rregull. Aktivistë të tjerë që kërkuan të mbeten anonimë deklaruan se kur janë marrë në pyetje nga Prokuroria në lidhje me pjesëmarrjen në një protestë, iu është kërkuar të zbulojnë emrat e administratorëve të faqeve të mediave sociale që përdoren për aktivizëm, dhe t'u lejonin të kishin akses në llogaritë e tyre personale apo në telefon, gjë që e kishin refuzuar. Në raste

119 Po aty.

120 Pro LGBT (2020) *Shqipëria mban paradën e parë online: Nuk ka drejtësi për personat LGBTI nëse nuk ka demokraci për të gjithë të tjerët.*

121 Po aty.

122 Partnerë Shqipëri (2017) *Monitorimi i lirisë së tubimit: Raporti i Shqipërisë 2016-2017.*

123 Civil Rights Defenders (2020) *Mbrojtësit e të Drejtave të Njeriut në Ballkanin Perëndimor.*

124 Intervistë me një ekspert për të drejtat e njeriut datë 3/2/2022.

125 Intervistë me një avokat për të drejtat e njeriut datë 14/4/2022.

126 Exit.al (2021) *Qeveria Shqiptare ka konsideruar blerjen e grupit të hakerave nga konkurrenti i NSO Group në 2014.*

të ngjashme, gjatë marrjes në pyetje, kur ata nuk i kishin telefonat me vete, oficerët e policisë u kishin kërkuar të hynin në llogaritë e tyre personale të mediave sociale nga kompjuterët e zyrës së tyre. Praktika të tilla, kur personi i pyetur nuk ka statusin e të akuzuarit, janë në kundërshtim me Kodin e Procedurës Penale dhe mund të cenojnë të drejtën për mosinkriminim të vetes.[127] Veç kësaj, aktivistët kishin patur raste kur policia i ishte referuar postimeve në rrjetet sociale për të identifikuar në mënyrë arbitrare organizatorin e një proteste të caktuar dhe për ta ndjekur penalisht. Praktika të tilla mund të kenë efekt shqetësues tek MDNJ dhe pjesëmarrësit e tjerë në tubim, duke dekurajuar kështu përdorimin e mediave sociale për tubime.[128]

Një tjetër element i rëndësishëm në lidhje me ushtrimin e lirisë së tubimit online është **roli i medias** në dokumentimin dhe komunikimin e aktiviteteve/protestave që zhvillohen. Mediat sociale përdoren gjerësisht për të shpërndarë informacion në kohë reale mbi aktivitetet ndërkohë që ato zhvillohen, pa kaluar ndonjë proces formal redaktimi. Një qasje e tillë gjithëpërfshirëse ndaj raportimit mund të ndihmojë në rritjen e ndërgjegjësimit për protesta, për t'u kërkuar llogari autoriteteve për veprimet e tyre gjatë protestës, por gjithashtu mund të ndihmojë në mobilizimin e njerëzve të tjerë për t'iu bashkuar aktivitetit.[129] Raportimi transparent, i pacensuruar dhe i paanshëm, për vende si Shqipëria bëhet edhe më i rëndësishëm, pasi mjedisi i medias kryesore dominohet nga propaganda pro-qeveritare dhe gazetarët janë vazhdimisht nën presion. Në këto rrethana, publiku shpeshherë i drejtohet mediave online, si burim më i besueshëm informacioni. Prandaj, për shkak të rolit të rëndësishëm që luajnë dhe ndikimit të madh publik që mund të kenë, mediat e pavarura online kur raportojnë për tubimet mund të bëhen edhe vetë shënjestër. Në dhjetor të 2020, në të gjithë vendin u organizuan protesta masive si reagim ndaj vrasjes së një të riu, K.R, nga një oficer policie, teksa po kthehej në këmbë për në shtëpi pas orarit të izolimit (gjatë pandemisë). Faqja e internetit e Citizens Channel, një media e pavarur online që promovon gazetarinë qytetare të përshkruar më sipër, po transmetonte drejtpërdrejt dhe po raportonte intensivisht për këto protesta për disa ditë me radhë, duke përfshirë raportimin për dhunën dhe abuzimin e policisë, kur pati një sulm DDoS dhe u mbyll për disa ditë. Sulmi synonte të fshinte të gjithë përmbajtjen ekzistuese nga faqja e tyre e internetit. Edhe pse burimi i sulmit mbetet ende i paidentifikuar, disa ekspertë e panë si sulm në lidhje me raportimin që Citizens Channel po bënte mbi protestat.[130]

Si përfundim, revolucioni digjital duket se po i ndryshon edhe tubimet, mënyrën e organizimit dhe mbajtjes së tyre, por edhe mënyrën se si ato mbikëqyren dhe shtypen. Kjo kërkon rritje të ndërgjegjësimit për sfidat e reja që shfaqen, dhe reagim të përgatitur nga të gjithë aktorët përkatës për t'i adresuar ato, si dhe një legjislacion më mundësues dhe bashkëkohor që shkon përtej mjeteve klasike të garantimit të ushtrimit të lirisë së tubimit.

127 Intervistë me një avokat për të drejtat e njeriut datë 14/4/2022.

128 Po aty.

129 European Center for Nonprofit Law (2020). Mbrojtja e tubimeve në internet.

130 Intervistë me një ekspert për të drejtat e njeriut datë 3/2/2022.

REKOMANDIME

Për aktorët publikë (Qeveria, Parlamenti dhe autoritetet ligjzbatuese)

Mbi kuadrin ligjor:

- Duhet ndryshuar Kodi Penal në lidhje me krimet me motive diskriminimi ose urrejtje për të siguruar mbrojtje në hapësirën kibernetike.
- Duhet ndryshuar Kodi Penal për të trajtuar rastet e përndjekjes online.
- Duhet miratuar legjislacioni anti-SLAPP për të forcuar garancinë ligjore për mbrojtjen e lirisë së shprehjes duke trajtuar kontekstin online dhe offline.
- Duhet ndryshuar Ligji për Mbrojtjen nga Diskriminimi për të adresuar në mënyrën e duhur format e diskriminimit që ndodhin në hapësirën kibernetike dhe vendimmarrjen automatike diskriminuese.
- Duhet ndryshuar Ligji për Tubimet për të ofruar garancitë e nevojshme për mbrojtjen e tubimeve online.
- Duhen bërë ndryshimet e nevojshme në legjislacionin mbi mediat dhe atë mbi komunikimet elektronike për të dhënë një përkufizim të unifikuar ligjor të përmbajtjes së dëmshme dhe të paligjshme dhe për të përcaktuar me ligj autoritetet që mund të kërkojnë fshirjen e përmbajtjeve të tilla në internet.

Mbi kuadrin politik:

- Duhet zbatuar një qasje ndërsektoriale për politikëbërjen në fushën e sigurisë kibernetike dhe të drejtave të njeriut në mënyrë që dokumentet e sigurisë kibernetike të konsiderojnë aspektet e të drejtave të njeriut dhe dokumentet strategjike të të drejtave të njeriut të trajtojnë dimensionin e sigurisë kibernetike.
- Duhet të zhvillohen procese konsultimi gjithëpërfshirëse mes institucioneve të sigurisë kibernetike, institucioneve të pavarura të të drejtave të njeriut dhe aktorëve jopublikë, kur hartohen dokumenta strategjikë.
- Duhet të kryhen vlerësime të riskut të të drejtave të njeriut për të mitiguar risqet e diskriminimit dhe për të siguruar vendimmarrje të bazuar në të dhëna sa i përket digjitalizimit të shërbimeve publike.
- Duhet të krijohet një sistem i unifikuar dhe gjithëpërfshirës i mbledhjes së të dhënave për krimet me motive diskriminimi/urrejtje, duke trajtuar kontekstin online dhe offline.
- Duhet zbatuar një qasje mbikëqyrje dhe kontrolli që lejon ndarjen e përgjegjësisë së aktorëve publikë dhe privatë në mbrojtjen e privatësisë në hapësirën kibernetike dhe formësimin e një politikëbërje gjithëpërfshirëse.
- Duhet të merren masa urgjente për të forcuar garancitë e mbrojtjes së të dhënave personale dhe përputhshmërinë e marrëveshjeve ndërinstitucionale dhe atyre me subjektet private.
- Duhet të rritet transparenca në lidhje me modalitetet e ruajtjes së të dhënave mbi informacionin personal të identifikueshëm dhe transferimit të tij tek palët e treta.
- Duhet të merren masa të përshtatshme për t'u mundësuar autoriteteve publike të zgjerojnë monitorimin e zbatimit të masave minimale të sigurisë për çdo palë nënkontraktore të operatorëve që administrojnë infrastrukturën kritike të informacionit, për të rritur përgjegjshmërinë e sektorit privat

Mbi kapacitetet dhe bashkëpunimin institucional:

- Duhet të përmirësohet bashkëpunimi ndërmjet institucioneve të sigurisë kibernetike dhe institucioneve të pavarura të të drejtave të njeriut në shkëmbimin e informacionit dhe ekspertizës, në rastet e shkeljeve të të drejtave të njeriut në hapësirën kibernetike.
- Duhet të shtohen përpjekjet për koordinimin ndërmjet institucioneve të sigurisë kibernetike, për të mundësuar mbikëqyrje dhe llogaridhënie adekuate si për çështjet teknike ashtu edhe për ato politike.
- Duhet të rriten kapacitetet e oficerëve të policisë, gjyqtarëve dhe prokurorëve në lidhje me standardet ndërkombëtare për garantimin e të drejtave të njeriut në hapësirën kibernetike.
- Policia e Shtetit dhe Prokuroria duhet të pajisen me burime të mjaftueshme njerëzore dhe teknike për të trajtuar krimin kibernetik si në nivel qendror ashtu edhe në atë vendor.
- Institucionet e pavarura të të drejtave të njeriut duhet të pajisen me burime të përshtatshme njerëzore dhe teknike për të kryer hetime të plota administrative për shkeljet e të drejtave të njeriut në hapësirën kibernetike.
- Oficerët e policisë dhe prokurorët e krimit kibernetik duhet të trajnohen mbi Udhëzimin e Përgjithshëm të Prokurorit të Përgjithshëm mbi hetimin efektiv penal të dhunës ndaj grave, dhunës në familje dhe dhunës me motive urrejtjeje. Duhet të ndërmerren masa për forcimin e besimit midis këtyre autoriteteve dhe grupeve që targetohen shpesh në internet.
- Duhet të bëhet funksional dhe i aksesueshëm për qytetarët mekanizmi i raportimit online i Policisë së Shtetit për krimin kibernetik për të mundësuar denoncimin në kohë të shkeljeve.

Për aktorët jo-publikë (OSHC-të, akademia, media, donatorët ndërkombëtarë)

Mbi ndërgjegjësimin dhe llogaridhënien:

- Duhet të monitorohen në mënyrë aktive shkeljet e të drejtave të njeriut që ndodhin në hapësirën kibernetike për të mundësuar hulumtime dhe vlerësime të plota mbi situatën, të cilat aktualisht janë të pamjaftueshme.
- Duhet të inkurajohet kontributi aktiv i aktorëve jopublikë në proceset e konsultimit për ndryshimet ligjore dhe dokumentet strategjike në lidhje me sigurinë kibernetike dhe të drejtat e njeriut.
- Duhet të rritet ndërgjegjësimi i publikut për format e diskriminimit që ndodhin në hapësirën kibernetike në mënyrë që të inkurajohet raportimi i rasteve dhe të konsolidohen praktika institucionale në këtë drejtim.
- Duhet të rritet ndërgjegjësimi i publikut për kërcënimet ndaj privatësisë në hapësirën kibernetike, për të inkurajuar qytetarët të identifikojnë dhe raportojnë çdo shkelje.

Mbi kapacitetet dhe mbështetjen e OSHC-ve dhe medias:

- Duhet të promovohet dhe mbështetet një qasje vetërregulluese e medias online, në përputhje me praktikat më të mira, për të siguruar proporcionalitet ndërmjet llogaridhënies për shkeljet dhe lirisë nga censura.
- Duhet të rriten kapacitetet e gazetarëve dhe mediave online në lidhje me raportimin etik dhe çështjet e të drejtave të njeriut.
- Duhet të rriten kapacitetet e OSHC-ve dhe aktivistëve në lidhje me sfidat e paraqitura ndaj ushtrimit të lirisë së tubimit në hapësirën kibernetike.
- Duhet të shtohet trajnimi dhe mbështetja teknike për sigurinë digjitale për gazetarët dhe aktivistët.
- Duhet të mbështeten shërbimet ligjore për gazetarët dhe aktivistët që përballen me kërcënime kibernetike.

DCAF Geneva Centre for Security Sector Governance

Institute for Democracy and Mediation
Instituti për Demokraci dhe Ndërmjetësim

DCAF-Geneva Centre for Security Sector Governance

Maison de la Paix, Chemin Eugène-Rigot 2E

CH-1202, Geneva, Switzerland

Tel: +41 22 730 94 00

Email: info@dcaf.ch

Website: www.dcaf.ch

Twitter @DCAF_Geneva

Instituti për Demokraci dhe Ndërmjetësim (IDM)

Rr. Shenasi Dishnica, Nd. 35, H. 1,

1017, Tirana, Shqipëri

Tel: +355 4 240 0241

Email: info@idmalbania.org

Website: www.idmalbania.org

Facebook: facebook.com/IDMAlbania/

Twitter @IDM_Albania