KRAF
KOSOVO RESEARCH
AND ANALYSIS FELLOWSHIP

KFOS
Fondacioni i Kosovës për Shoqëri të Hapur
Kosovo Foundation for Open Society
Kosovska Fondacija za Otvoreno Društvo

Balancimi i Sigurisë Kibernetike, Inteligjencës Artificiale dhe të Drejtave të Njeriut: MUNDËSITË DHE SFIDAT NË KOSOVË

IMANE BELLAADEM

Balancimi i Sigurisë Kibernetike, Inteligjencës Artificiale dhe të Drejtave të Njeriut:

MUNDËSITË DHE SFIDAT NË KOSOVË

Titulli:
Balancimi i Sigurisë Kibernetike, Inteligjencës Artificiale dhe të Drejtave të Njeriut:
Mundësitë dhe Sfidat në Kosovë

Autor:
Imane Bellaadem

Kopertina:
Ky ilustrim është gjeneruar nga IA dhe edituar nga Tedel.

Publikuar nga:
Fondacioni i Kosovës për Shoqëri të Hapur

Prishtinë,
Maj 2023

Ky botim është prodhuar si pjesë e Kosovo Research and Analysis Fellowship (KRAF), një iniciativë e Fondacionit të Kosovës për Shoqëri të Hapur.

Balancimi i Sigurisë Kibernetike, Inteligjencës Artificiale dhe të Drejtave të Njeriut: Mundësitë dhe Sfidat në Kosovë

1 Hyrje

Siguria kibernetike, inteligjenca artificiale, *machine learning* (një teknikë e IA që mëson kompjuterët bazuar në përvojë), mediat sociale, interneti janë vetëm disa nga teknologjitë digjitale të disponueshme në ditët e sotme. Me zgjerimin e madh të internetit, së bashku me zhvillimin dhe rritjen e qasjes së pajisjeve digjitale, këto teknologji u bënë në mënyrë të pashmangshme pjesë thelbësore e jetës sonë. Teksa këto teknologji po rriteshin dhe po zhvillonin veçori të reja, ekspertët dhe qeveritë filluan të rrisin zbatueshmërinë në shtresa të ndryshme të infrastrukturës kritike. Pra, në ditët e sotme mund të gjenden administrata publike tërësisht të digjitalizuara ku të gjitha shërbimet mund të ofrohen online, arkivat fizike të zëvendësuara nga baza të digjitalizuara të të dhënave, shkolla që integrojnë mjete digjitale për mësim, e kështu me radhë. Qasja e individëve në internet dhe shumica e aplikacioneve të zakonshme kanë përshpejtuar ndikimin e teknologjive digjitale në jetën e tyre. Të gjithë spektrat e jetës së dikujt mbulohen nga lloje të aplikacioneve ose shërbime të ofruara online. Disa nga aplikacionet më të famshme përfshijnë dallimin e zërit, ndihmën virtuale në shërbimin ndaj klientit dhe makinat e rekomandimeve.[1] Duke qenë se këto teknologji ndihmojnë përdoruesit dhe sigurojnë qasje më të madhe për disa shërbime dhe produkte, janë ngritur shqetësime për privatësinë.

Besueshmëria e infrastrukturës kritike[2]në këto teknologji është prioritet kryesor për shumë qeveri dhe aktorë tjerë kyç ndërkombëtarë. Qeveritë po investojnë kapacitete në mënyrë që t'i zbusin rreziqet që kjo besueshmëri paraqet për qëndrueshmërinë e shtetit. Rëndësia e forcimit të sigurisë kibernetike të shteteve mbetet e qartë dhe është e padiskutueshme, megjithatë, duke përfshirë një qasje me në qendër njeriun, teksa rregullimi i këtyre sferave nuk duhet të neglizhohet. Të drejtat e njeriut dhe qeverisja e mirë janë dy fusha të ndërthurura dhe të ndërvarura. Kur merret parasysh shkalla e përfshirjes

1 IBM Cloud, https://www.ibm.com/topics/artificial-intelligence, qasur më 27 shkurt, 2023
2 BE definon infrastrukturën kritike si 'një aset i sistemit i cili është primar në mirëmbajtjen e funksioneve shoqërore'

së internetit dhe teknologjive digjitale në jetën e një përdoruesi mesatar, bëhet e qartë se siguria kibernetike shërben si një parakusht për garantimin dhe ushtrimin e të drejtave të njeriut. Ky pretendim mbështetet nga përfshirja e të drejtave digjitale si gjenerata e 4-të e të drejtave të njeriut në teorinë akademike[3] dhe nga fakti se shumë instrumente ndërkombëtare kanë zgjeruar zbatueshmërinë e tyre në hapësirat online. Të gjitha të drejtat e mbrojtura të njeriut mund të ushtrohen si në hapësirat online ashtu edhe në ato fizike. Rregulloret ekzistuese janë më shumë të fokusuara në mbrojtjen e të drejtave të njeriut në hapësirën fizike, prandaj është e nevojshme që kjo mbrojtje të shtrihet edhe në hapësirat kibernetike.

Në këtë raport do të shohim nga afër se si siguria kibernetike dhe inteligjenca artificiale (IA) kryqëzohen me lirinë e shprehjes dhe privatësinë në përgjithësi. Për më tepër, do të shqyrtojmë tablon aktuale të sigurisë kibernetike dhe IA-së në Kosovë dhe do të hartojmë sfidat dhe pengesat, si dhe praktikat e mira që janë miratuar në Kosovë. Raporti do të ekzaminojë shkallën në të cilën zbatohet një qasje e bazuar në të drejtat e njeriut ose me në qendër njeriun kur rregullohet siguria kibernetike në Kosovë.

Metodologjia kryesisht mbështetet në hulumtime nga zyra dhe intervista. Hulumtimi nga zyra shqyrton burimet primare (duke filluar nga legjislacioni dhe standardet ndërkombëtare; kuadri kombëtar duke përfshirë legjislacionin në procedura, politika, strategji) dhe burimet dytësore (artikuj akademikë, libra, raporte të organeve qeveritare dhe joqeveritare; artikuj në media).

Gjatë periudhës së hulumtimit nga zyra, dimensione specifike u identifikuan si të rëndësishme për t'u diskutuar me të intervistuarit. Për më tepër, hulumtimi nga zyra tregoi se cilat grupe të palëve të interesuara janë relevante për hulumtimin. Janë realizuar gjithsej shtatë intervista individuale gjysmë të strukturuara, me përfaqësues të shoqërisë civile dhe ekspertë ndërkombëtarë. Një nga mangësitë e hulumtimit është se nuk është intervistuar asnjë institucion shtetëror, për shkak të përgjegjshmërisë së tyre të kufizuar.

Studimi është i ndarë në tre kapituj kryesorë. Kapitulli i parë ofron përkufizime të termave kyç, sigurinë kibernetike dhe IA-në, dhe ofron një pasqyrë të shkurtër të legjislacionit ndërkombëtar. Kapitulli i dytë diskuton ndërthurjen e sigurisë kibernetike dhe IA-së me të drejtat e njeriut, dhe rëndësinë e adoptimit të një qasjeje të bazuar në të drejtat e njeriut. Kapitulli vijues përmbledhë legjislacionin dhe praktikat e sigurisë kibernetike të Kosovës. Studimi përfundon me një sërë rekomandimesh drejtuar palëve të ndryshme të interesit.

1.1. Përkufizimet e sigurisë kibernetike

Ky nënkapitull do të shqyrtojë përkufizimin e sigurisë kibernetike pasi nuk ka një qasje të njëanshme të adoptuar për atë që përfshin siguria kibernetike. Për të kuptuar plotësisht fushën e sigurisë kibernetike, së pari duhet të kuptojmë se cilët janë elementët kritikë të sigurisë kibernetike.

3 Risse,M.Gjenerata e katërt e të drejtave të njeriut: Të drejtat epistemike në botën digjitale,Qendra për të drejtat e njeriut, Shkolla Harvard Kennedy, Universiteti i Harvardit, 2021

Digital Guardian e përkufizon sigurinë kibernetike si “trupin e teknologjive, proceseve dhe praktikave të krijuara për të mbrojtur rrjetet, pajisjet, programet dhe të dhënat nga sulmet, dëmtimet ose qasja e paautorizuar”[4].Nuk ka një përkufizim të njëanshëm të sigurisë kibernetike dhe Agjencia e Bashkimit Evropian për Sigurinë e Rrjetit dhe Informacionit (ENISA) ka vënë në dukje se nuk ka nevojë të ofrohet një përkufizim i zakonshëm, pasi ky është një term në zhvillim dhe praktikisht është e pamundur të përfshihen të gjithë komponentët e sigurisë kibernetike në një përkufizim. Megjithatë, në përpjekje për të standardizuar fushëveprimin e sigurisë kibernetike, ENISA pranon se duhet t’i referohet “sigurisë së hapësirës kibernetike, ku vetë hapësira kibernetike i referohet grupit të lidhjeve dhe marrëdhënieve midis objekteve që janë të qasshme nëpërmjet një rrjeti të përgjithësuar telekomunikacioni, dhe grupit të vetë objekteve ku ato paraqesin ndërfaqe që lejojnë kontrollin e tyre në distancë, qasjen nga distanca në të dhëna

ose pjesëmarrjen e tyre në veprimet e kontrollit brenda asaj hapësire kibernetike”. Koalicioni i Lirisë Online (FOC)[5], partneritet i 36 qeverive në mbarë botën, e përkufizon sigurinë kibernetike si “ruajtjen – nëpërmjet politikave, teknologjisë dhe edukimit – të disponueshmërisë, konfidencialitetit dhe integritetit të informacionit dhe infrastrukturës së tij themelore në mënyrë që të rrisë sigurinë e personave si online dhe offline”.[6]

Siç u cek, këto përkufizime ndjekin strukturën me tre komponentë kyç: çfarë, si dhe kundër çfarë. Si i referohet aktiviteteve, mjeteve, udhëzimeve, politikave, edukimit; çfarë fokusohet në rrjete, sisteme, programe, asete; kundër asaj që thekson sulmin, dëmit, incidentet. Megjithatë, ata pothuajse ose tërësisht e lënë jashtë përfshirjen e aspektit njerëzor të sigurisë kibernetike në përkufizime. Mungesa e përfshirjes së aspektit njerëzor në përkufizime ndikon në aftësinë për t’iu qasur dhe rregulluar domenin kibernetik në mënyrë holistike dhe për të vlerësuar rreziqet që u paraqiten sistemeve dhe përdoruesve në domenin kibernetik.[7]

1.2. Përkufizimi i inteligjencës artificiale

Në vijim të nënkapitullit të mëparshëm, po vazhdojmë me dhënien e përkufizimit të IA. Duke marrë parasysh që IA është një koncept qendror në këtë studim, është shumë e rëndësishme të kuptohet se çfarë është IA dhe cilat elemente të IA-së janë veçanërisht të rëndësishme për këtë studim.

4 Digital Guardian, Çka është siguria kibernetike? Definicioni, praktikat më të mira dhe shembuj, 2022, https://www.digitalguardian.com/blog/what-cyber-security, qasur më 5 maj, 2023
5 Faqja në internet e Koalicionit të Lirisë Online, 2022, https://freedomonlinecoalition.com/members/qasur me 01 mars, 2023
6 Asociacioni për komunikim progresiv, Pse siguria kibernetike është çështje e të drejtave të njeriut, dhe është koha ta trajtojmë si të tillë, 2022, https://www.apc.org/en/news/why-cybersecurity-human-rights-issue-and-it-time-start-treating-it-one qasur më 1 shkurt 2023
7 Cains, M. et al, Përcaktimi i sigurisë kibernetike dhe rrezikut të sigurisë kibernetike brenda një konteksti multidiciplinar duke përdorur nxjerrjet e ekspertëve, Analiza e Rrezikut, një publikim zyrtar i Shoqërisë për analiza rreziku, 2021, Author: Cains, Mariana G : Search (wiley.com), qasur më 15 shkurt 2023

IA është një term që ndërlidhet me vendimmarrjen algoritmike dhe rrallë mund të analizohet vetëm. Të dy veprojnë si terma ombrellë dhe nuk mund të gjendet asnjë vendim uniform.[8] Në të folur, këto terma përdoren në mënyrë të ndërsjellë, megjithatë, është e rëndësishme të vihen re disa dallime thelbësore.

"Inteligjenca Artificiale (IA) i referohet sistemeve që shfaqin sjellje inteligjente duke analizuar mjedisin e tyre dhe duke ndërmarrë veprime – me një farë mase autonomie – për të arritur qëllime specifike. Sistemet e bazuara në IA mund të jenë thjesht të bazuara në softuer, që veprojnë në botën virtuale (p.sh.: asistentët e zërit, softueri i analizës së imazhit, makina të kërkimit, sistemet e njohjes së të folurit dhe fytyrës) ose IA mund të futen në pajisje harduerike (p.sh.: robotë të avancuar, automjete autonome, drone ose aplikacione të Internet of Things).[9]

John McCarthy e përkufizoi IA-në si "shkencë dhe inxhinieri për të bërë makina inteligjente, veçanërisht programe kompjuterike inteligjente. Ajo lidhet me detyrën e ngjashme të përdorimit të kompjuterëve për të kuptuar inteligjencën njerëzore".[10]Organizatat ndërkombëtare si Organizata për Siguri dhe Bashkëpunim në Evropë (OSBE) dhe Këshilli i Evropës kanë dhënë gjithashtu përkufizime për IA-në. Fjalori i Këshillit të Evropës e përkufizon IA-në si "një grup shkencash, teorish dhe teknikash, qëllimi i të cilave është të riprodhojë, me anë të një makinerie, aftësitë njohëse të një qenieje njerëzore për të qenë në gjendje t'i besojë një makinerie detyra komplekse që më parë i ishin deleguar njeriut". Nga ana tjetër, OSBE-ja i referohet IA si "të bazuar në algoritme, të cilat janë grupe udhëzimesh të dizajnuara nga njeriu me procedura të koduara për transformimin e të dhënave hyrëse në një dalje të dëshiruar, bazuar në llogaritjet specifike".

Për më tepër, për të kuptuar plotësisht shtrirjen e algoritmeve, duhet të perceptojmë si pjesë integrale të IA-së dhe vendimmarrjes algoritmike. Algoritmet kanë rolin e njohjes së modeleve për të kryer detyra të caktuara të pavarura nga ndërhyrja njerëzore, duke lehtësuar kështu vendimmarrjen e automatizuar.[11] Përkufizimi i IA-së ka të njëjtat problematika si siguria kibernetike, pasi të dy termat po përparojnë vazhdimisht dhe ekziston nevoja për të rivlerësuar përkufizimet e tyre dhe për t'i zgjeruar ato me komponentë të rinj.

1.3. Përpjekjet për legjislacionin ndërkombëtar

Siguria kibernetike dhe IA janë tema mjaft të reja që ngrihen në komunitetin e së drejtës ndërkombëtare. Prandaj, përpjekjet për të rregulluar janë të pakta dhe të paplota pasi ishte shumë komplekse të parashikohej dhe vlerësohej e ardhmja e këtyre teknologjive. Megjithatë, ekziston një konsensus se ligji ndërkombëtar ekzistues vlen edhe për hapësirat kibernetike.

8 Zuiderveen Borgesius, F. Diskriminimi, inteligjenca artificiale, dhe algoritmet e vendim-marrjes. Këshilli i Evropës, Drejtorati i Përgjithshëm i Demokracisë, 2018. https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decisionmaking/1680925d73 qasur më 05 mars 2023
9 Ky definicon nga AI HLEG ishte temë e diskutimeve të mëvonshme në grupe. Shih AI HLEG (2019)
10 McCarthy, J. Çka është inteligjenca artificiale?, Universiteti i Stanfordit, 2007
11 Kostić, B. & Sinders, C. IA e përgjegjshme, Këshilli i Evropës, 2022

Rezoluta e Këshillit për të Drejtat e Njeriut e vitit 2012 thekson se ligji ndërkombëtar për të drejtat e njeriut dhe ligji ndërkombëtar humanitar kanë efekt të barabartë si online ashtu edhe offline. Ai gjithashtu thekson nevojën për masa të sigurisë kibernetike për të mbrojtur si përparimet teknologjike ashtu edhe gëzimin e të drejtave të njeriut.[12]Përpjekjet për të rregulluar hapësirën kibernetike janë seriozisht të ndërlikuara për shkak të karakterit të saj transnacional. Shtetet duhet të jenë bashkëpunuese dhe të kenë qëndrime të ngjashme për të pasur një rregullim efikas. Megjithatë, ekziston një marrëveshje e përgjithshme që shtetet duhet të përmbahen nga veprimet e gabuara në hapësirën kibernetike dhe se shtetet kanë juridiksion mbi teknologjinë e informacionit dhe komunikimit.[13]

Përpjekjet e intensifikuara për të miratuar rregullore kanë rezultuar në krijimin e Grupit të Ekspertëve Qeveritar të OKB-së (UN GGE). Ato ishin funksionale midis vitit 2004 dhe diskutonin se si të ruanin sigurinë dhe paqen në hapësirën kibernetike. Në kohën kur GGE e OKB-së pushon së punuari, OKB-ja ka formuar UN Open-Ended Working Groups (OEWG) që nga viti 2020. Fokusi është krijimi i programeve që nuk kufizohen në mandate, ndryshe nga GGE, në fushën e sigurisë kibernetike.[14] Një rezolutë për programin e veprimit për sigurinë kibernetike u miratua në nëntor të vitit 2022, duke siguruar që ky program veprimi të bëhet një mekanizëm i përhershëm pasi përfundimit të OEËG 2021-2025.[15]

Këshilli i Evropës ka prezantuar një nga konventat e para për sigurinë kibernetike. Konventa e Budapestit, e njohur edhe si Konventa e Krimit Kibernetik, ka vendosur standardet për kriminalizimin e krimit kibernetik. Ajo ka parashikuar rritjen e bashkëpunimit midis shteteve për ndjekjen penale të krimit kibernetik dhe shkëmbimin e provave elektronike.[16] BE-ja ka bërë hapa për rregullimin e mëtejshëm të sigurisë kibernetike dhe IA-së. BE-ja ka propozuar Aktin e IA-së në vitin 2021.[17] Kjo është pjesa e parë e rregullores dhe gjatë hartimit të saj ka miratuar një qasje të bazuar në rrezik. Kjo do të çojë në detyrime transparente të bartësve të AI dhe do të rrisë sigurinë dhe të drejtat e njeriut në BE.[18] Prezantimi i Aktit të BE-së për Sigurinë Kibernetike përfshin krijimin e një kuadri certifikimi për produktet, proceset dhe shërbimet e TIK-ut në të gjithë BE-në, i cili është një hap përpara drejt standardizimit në sigurinë kibernetike.[19]

12 Pavlova, P. 'Qasja e bazuar në të drejtat e njeriut ndaj sigurisë kibernetike: Adresimi i rreziqeve të sigurisë së grupeve të synuara', Peace Human Rights Gorvenance, 4(3), 391-418, 2020, PHRG-2020-3-04.pdf (padovauniversitypress.it), qasur më 20 prill, 2023
13 Geneva Internet Platform DigWatch, UN OEWG, UN OEËG in 2023 - DW Observatory (dig.watch), qasur më 29 mars, 2023
14 Zyra e OKB për çështje të çarmatimit, Grupi i ekspertëve qeverisës, Group of Governmental Experts – UNODA qasur më 29 mars, 2023
15 Geneva Internet Platform DigiWatch, UN OEWG, UN OEËG in 2023 - DW Observatory (dig.watch), qasur më 29 mars 2023
16 Konventa e krimeve kibernetike: Edicioni special dedikuar propozuesëve të konventës (1997-2001), Këshilli i Evropës, 2022, 1680a6992e (coe.int)
17 Parlamenti Evropian, Inteligjenca Artificiale, 2023, Artificial intelligence (europa.eu)
18 Propozimi i kornizës rregullatore të BE-së për inteligjencën artificiale,Regulatory framework proposal on artificial intelligence | Shaping Europe's digital future (europa.eu)
19 Komiteti Evropian, Ligji i BE-së per siguri kibernetike, The EU Cybersecurity Act | Shaping Europe's digital future (europa.eu)

Të kuptuarit më mirë i zgjerimit të IA-së dhe rëndësisë së sigurisë kibernetike ka shërbyer si një motivim për të filluar rregullimin. Ndërsa rregulloret e sipërpërmendura shërbejnë si një pikënisje e shkëlqyer, ende është e nevojshme të përcaktohen standardet ndërkombëtare të mbrojtjes së sigurisë kibernetike, të cilat do të shërbenin si bazë për rregullime të mëtejshme. Për më tepër, është e nevojshme të rritet bashkëpunimi ndërkombëtar midis shteteve për të trajtuar në mënyrë efektive kërcënimet e sigurisë kibernetike, por edhe për të zhvilluar një platformë për shkëmbimin e informacionit dhe bashkëpunimin në kërkime.

Do të ishte e dobishme të zhvillohen udhëzime etike të standardizuara për IA-në si një bazë e përbashkët për të siguruar që IA është zhvilluar në mënyrë etike dhe nuk do të dëmtojë individët ose shoqërinë. Së fundi, mund të konkludohet se do të shohim më shumë deklarata dhe rregullore që trajtojnë këto çështje, përveç atyre ekzistuese për shkak të avancimit dhe karakterit të saj global.

2 Siguria kibernetike, IA dhe të drejtat e njeriut

Siguria kibernetike, IA, vendimmarrja algoritmike dhe *machine-learning*janë vetëm disa nga teknologjitë digjitale që po evoluojnë me shpejtësi. Zhvillimi i këtyre teknologjive pasohet nga rritja e përdorimit të tyre në sektorin publik dhe atë privat, por edhe nga individë në jetën e tyre private. Megjithatë, mbetet e paqartë se cilat janë efektet afatgjata të IA-së tek individët dhe shoqëria, ndërsa siguria kibernetike po merr një rol mbrojtës ndaj infrastrukturës kritike, të dhënave dhe aseteve të tjera.

Zhvillimi i IA-së mund të sjellë një gamë të gjerë përfitimesh sociale dhe ekonomike. Fushat që mund të përfitojnë nga përdorimi i IA-së janë të sektorëve me ndikim të lartë dhe përfshijnë ndryshimet klimatike, mjedisin dhe shëndetin, financat, lëvizshmërinë, punët e brendshme dhe bujqësinë. Sidoqoftë, të njëjtat specifika që zhbllokojnë mundësitë e zhvillimit socio-ekonomik paraqesin rreziqe për efekte negative për individët dhe shoqërinë.[20] Disa nga shqetësimet e ngritura janë siguria ndërkombëtare, stabiliteti social dhe politik, prishja e tregjeve të punës, pabarazia ekonomike dhe sociale, etj.

Të gjitha organizatat e mëdha ndërkombëtare identifikuan IA-në si një mundësi kritike të rëndësishme për rritjen dhe ruajtjen e qeverisjes demokratike dhe të drejtave themelore. Është rënë dakord që IA mund të lehtësojë demokracinë pjesëmarrëse, llogaridhënien dhe transparencën. Teknologjitë e bazuara në IA mund të nxisin pluralizmin e medias dhe të ofrojnë mjedis të favorshëm për shoqërinë civile. Nga ana tjetër, përdorimi i këtyre teknologjive mund të ndikojë në sjelljen dhe qëndrimet e qytetarëve, të cilat mund të manipulohen për qëllime të caktuara politike, si ndikimi në proceset zgjedhore, manipulimi i opinionit publik, përhapja e dezinformatave dhe propagandës etj.[21]

20 Komisioni Evropian, Propozimi per rregulloren e Parlamentit Evropian dhe te Këshillit që përcakton rregulla të harmonizuara mbi Inteligjencën Artificiale (Akti i Inteligjencës Artificiale) dhe ndryshimin e akteve legjislative të BE-së COM (2021)206, 2020, 2

21 Asambleja e Këshillit të Evropës, Nevoja për qeverisje demokratike, Rezoluta 2341, 2020, 1

Nënkapitujt e mëposhtëm shqyrtojnë ndërlidhjet midis lirisë së shprehjes dhe lirive të medias dhe të drejtës për privatësi me sigurinë kibernetike dhe IA. Aty ofrohen përkufizime për teknologjitë kryesore digjitale dhe shpjegohen se si ato ndikojnë në lirinë e shprehjes, liritë e medias dhe të drejtën për privatësi. Përkufizimet plotësohen me shembuj ilustrues për tu kuptuar më mirë.

2.1. Liria e shprehjes dhe liritë e medias

Liria e shprehjes dhe liritë e medias konsiderohen si një nga shtyllat kryesore të një demokracie funksionale. Qasja e lirë, e pacensuruar në informacion, përfshirja lirshëm në debate publike janë thelbësore për luftimin e dezinformimit, keqinformimit, avancimit të shkrim-leximit mediatik dhe për të drejtën për t'u informuar për tema me interes publik. Teorikisht, shfaqja e platformave të mediave sociale ka luajtur një rol të rëndësishëm në rritjen e qasjes së informacionit për publikun e gjerë. Në praktikë, shumë sfida dhe pengesa kanë gjetur një mënyrë për t'i penguar këto procese.

Liria e shprehjes mund të ndikohet nga faktorë të shumtë në sferën online. Platformat e mediave sociale, kompanitë private si dhe qeveritë mund të ndikojnë në disponueshmërinë, qasjen dhe vendosjen e informacionit të caktuar në internet.[22] Platformat e mediave sociale ndërtojnë fuqinë mbi gjithëpraninë e tyre në diskursin publik dhe aftësinë për të formësuar fuqinë e opinionit. Fuqia e opinionit mund të përkufizohet si aftësia e medias për të ndikuar në proceset e formimit të opinionit individual dhe publik.[23] Përqendrimi i pushtetit të opinionit në platformat e mediave sociale përfaqëson rrëshqitjen më të madhe për çdo demokraci funksionale. Duke qenë se ato mund të instrumentalizohen lehtësisht si mjete politike për të formësuar diskursin publik në një mënyrë të caktuar, është e nevojshme të shpërndahet përqendrimi i pushtetit të opinionit dhe të sigurohet që platformat e mediave sociale të mbeten një platformë ku të gjithë zërat mund të dëgjohen.[24] Fuqia politike dhe mundësitë jashtëzakonisht fitimprurëse janë faktorët kryesorë në këtë ndërveprim.[25] Për më tepër, moderimi dhe kurimi i përmbajtjes janë mjetet më të fuqishme të IA-së që mund të ndikojnë në lirinë e shprehjes dhe lirinë e medias. Diskutimet rreth këtyre dy termave gjenden në atë që vijon.

Moderimi i përmbajtjes nënkupton që çdo përmbajtje që publikohet kalon përmes një moderimi me tre hapa.[26] Së pari, Kushtet e Shërbimeve të platformave kërkojnë që çdo përmbajtje të vlerësohet me filtra automatikë, për të ekzaminuar nëse përmbajtja plotëson standardet minimale të përcaktuara për t'u publikuar. Hapi i dytë është vendosja e përmbajtjes specifike brenda platformës duke përdorur IA-në

22 Bromell, D. Rregullimi i fjalës së lirë në epokën digjitale: urrejtja, dëmi dhe limitet e cenzurimit, Springer, 2022
23 Neuberger, C. "Meinungsmacht im Internet aus Kommunikationsëissenschaftlicher Perspektive." UFITA 82 (1): 53–68, 2018
24 Helberger, N. Platforma e fuqisë politike: Si e përforëcojnë fuqinë e opinionit përpjektet aktuale për të rregulluar keqinformimin, Digital Journalism, 8:6, 842-854
25 Kostić, B. Kurthet e IA-së dhe diversiteti i mediave: kujdes boshllëqet, Media Diversity Institute, 2021, https://www.media-diversity.org/artificial-intelligence-traps-and-media-diversity-mind-the-loopholes/, qasur më 01 shkurt 2023
26 Bukovska, B. Vëmendja në Inteligjencën Artificiale dhe liria e shprehjes, OSCE, 2020, 3

dhe algoritme. Duke vendosur përmbajtje, ne i referohemi renditjes, optimizimit dhe rekomandimit të përmbajtjes bazuar në kritere të caktuara. Ky hap është vendimtar për dukshmërinë e përmbajtjes, pasi proceset e automatizuara "vendosin" se kujt dhe në çfarë mase do t'i ekspozohet një përmbajtje e caktuar, p.sh.: nëse përmbajtja juaj vendoset në faqen e dytë të kërkimit të Google, kjo do të ndikojë në informacionin që dëshironi të transmetoni, pasi vetëm 6% e klikimeve në uebsajt vijnë nga faqja e dytë e kërkimit në Google.[27] Hapi i fundit ka të bëjë me përmbajtjen kur ajo tashmë është publikuar. Ato përbëhen kryesisht nga mekanizmi raportues i secilës platformë. Këta mekanizma u mundësojnë përdoruesve të raportojnë, shenjëzojnë ose bllokojnë përmbajtjen, gjë që rezulton në një vlerësim të kombinuar të inteligjencës artificiale dhe njerëzore për mosmarrëveshjen. Përmbajtja mund të fshihet, përdoruesit mund të sanksionohen ose bllokohen.[28]

Domethënë, dy hapat e fundit janë më të rëndësishmit për lirinë e shprehjes dhe liritë e medias, pasi vendosin nëse një përmbajtje do të publikohet, kujt do t'i shfaqet dhe nëse do të hiqet dhe censurohet. Kjo është veçanërisht e rëndësishme në kohë të ndjeshme politikisht, siç janë fushatat parazgjedhore apo fushatat për legjislacionin. Nëpërmjet punës me organet e medias, një përfaqësues i shoqërisë civile thekson se ekziston një model i heqjes së përmbajtjes satirike nga mediat sociale pasi ato u cilësuan si problematike.[29] Kjo tregon mungesën e të kuptuarit të kontekseve politike, socio-ekonomike dhe gjuhësore të këtyre teknologjive, por ka fuqinë të kufizojë zërin e medias dhe të vlerësojë atë që duhet hequr.[30] Një shembull tjetër i gjallë është kur në maj 2018, Facebook pezulloi profilin e gazetarit boshnjak Dragan Bursać për një periudhë prej 24 orësh, sepse ai postoi një imazh të një kampi burgimi për boshnjakët në Serbi gjatë luftës në Bosnje dhe Hercegovinë. Sipas raportimeve të mediave lokale, Facebook konsideroi se postimi i Bursać-it shkelte "standardet e komunitetit"[31], pasi fotografia kishte përmbajtje eksplicite. Specifikisht, Bursać konsiderohet një gazetar i pavarur nga Bosnja dhe Hercegovina, që kundërshton tentativat e qeverisë të glorifikojnë dhe mohojnë krimet e luftës në BeH. Pra, pezullimi i profilit të tij në Facebook mund të përdoret si argument për të diskreditуar punën e tij nga politikanë apo palë tjera, për punën e të cilëve Bursać është kritik. Kjo gjithashtu ndezi një diskutim se pse është e papërshtatshme të postohet lidhur me kampet e paraburgimit në Serbi dhe nga kush vlerësohet si e papërshtatshme nëse pretendimet janë të vërteta. Për shkak të transparencës së kufizuar të sistemeve të automatizuara të përdorura, kjo mbetet një çështje për kërkime të mëtejshme. Nga ana tjetër, sistemet e automatizuara nuk arrijnë të heqin përmbajtjen e dëmshme, pavarësisht se përditësohen rregullisht dhe nuk janë gjithmonë në gjendje të dallojnë përmbajtjen e dëmshme dhe të

27 Forbes, Vlerat e rangimit të rezultateve të kërkimeve, 2017, The Value Of Search Results Rankings (forbes.com)
28 Kostić B, Sinders C, Inteligjenca Artificiale e përgjegjshme, Këshilli i Evropës, 2022, 15
29 Intervistë me Ena Bavčić, 01 mars 2023
30 Ibid.
31 Jeremić et al, Facebook, Tëitter duke luftuar kundër shkeljeve të përmbajtjes në Ballkan, BIRN, 2021, Facebook, Twitter Struggling in Fight against Balkan Content Violations | Balkan Insight, qasur më 15 mars 2023

urrejtjes.[32]Është gjetur se pothuajse 50% e përmbajtjes së raportuar me origjinë nga Ballkani Perëndimor që është raportuar, është ende e disponueshme në internet.[33]

Moderimi i përmbajtjes është i lidhur ngushtë me kurimin e përmbajtjes dhe ato plotësojnë njëra-tjetrën në mënyrë që moderimi kundërshton përmbajtjen e dëmshme, ndërsa kurimi fokusohet në vendndodhjen e përmbajtjes. Prandaj, **kurimi i përmbajtjes** i referohet kryesisht sistemit të rekomandimeve të vendosur nga secila platformë. Algoritmet kërkojnë të optimizojnë atë që përdoruesit shohin në profilet e tyre duke identifikuar dhe vlerësuar modelet në sjelljen digjitale, duke rezultuar kështu në një *feed* të personalizuar. Në një përpjekje për të maksimizuar fitimin, platformat kërkojnë të tërheqin përdoruesit që të kalojnë më shumë kohë në mediat sociale duke personalizuar burimin e tyre, bazuar në ndërveprimet e tyre, vendndodhjet, historikun e kërkimit etj.[34] Ky njihet gjithashtu si fenomeni i filtrave të internetit.[35] Kjo është arsyeja kryesore pse askush nuk e sheh të njëjtin burim kryesor në një platformë të mediave sociale. Krijimi i një jehonë në hapësirat online duke mos pasur një luhatje të burimeve të ndryshme të informacionit dhe duke filtruar dhe bllokuar përmbajtjen është një tokë pjellore për ndarjen e keqinformatave dhe dezinformatave, dhe mbështetja e tepërt e mediave në platformat e mediave sociale është një faktor kontribuues në këtë fenomen.[36]Ndërsa kurimi i përmbajtjes nuk e pengon një individ të shprehet lirshëm, ai mund të pengojë të drejtën e tij për të kërkuar, marrë dhe përhapur informacion dhe ide përmes çdo media dhe pavarësisht nga kufijtë.[37] Ai shërben vetëm për të përforcuar njëanshmërinë e përdoruesit dhe për të kufizuar ekspozimin ndaj pikëpamjeve të kundërta. Për shembull, në prill 2020, Twitter fshiu më shumë se 20,000 llogari të rreme të lidhura me qeveritë saudite, serbe dhe egjiptiane dhe u vlerësuan si "përpjekje e synuar për të minuar diskutimin publik". Një total prej 8,558 llogarish ishin të lidhura me Partinë Progresive Serbe (SNS) të Aleksandar Vuçiqit, me mbi 43 milionë postime në Twitter që promovonin lajme në favor të administratës së Vuçiqit dhe sulmonin liderët politikë të opozitës.[38] Kjo ndodhi vetëm dy muaj para zgjedhjeve parlamentare të Serbisë[39], me qëllim të formësimit të opinionit të elektoratit të SNS-së.

Një studim ka testuar konfirmimin e njëanshëm si një mjet keqinformimi në lidhje me ndryshimet klimatike. Ai tregoi se konfirmimi i njëanshëm i arritur kur merr informacion në përputhje me pikëpamjet para-ekzistuese është veçanërisht i fortë tek mohuesit e ndryshimeve klimatike. Ky

32 Bukovska, B. Vëmendja në Inteligjencën Artificiale dhe liria e shprehjes, OSCE, 2020, 56
33 Jeremić et al, Facebook, Tëitter duke luftuar kundër shkeljeve të përmbajtjes në Ballkan, BIRN, 2021, Facebook, Twitter Struggling in Fight against Balkan Content Violations | Balkan Insight, qasur më 15 mars 2023
34 Pirkova, E. et al, Vëmendja në Inteligjencën Artificiale dhe liria e shprehjes – Një manual politikash, OSCE, 2021, 66
35 Kostić B, Sinders C, Inteligjenca Artificiale e përgjegjshme, Këshilli i Evropës, 2022, 16
36 Leslie D et al. Inteligjenca Artificiale, të drejtat e njeriut, demokracia, dhe sundimi i ligjit: Së pari. Këshilli i Evropës, 2021
37 Deklarata univerzale e të drejtave të njeriut, 1948
38 The Guardian, Tëitter fshinë 20,000 llogari të rreme që lidheshin me qeverinë Saudite, Serbe dhe Egjiptiane, 2020, Izbori u Srbiji 2020: Šta sve mogu naprednjaci sa dvotrećinskom većinom u skupštini - BBC News na srpskom, qasur me 20 mars 2023
39 BBC, Izbori u Srbiji 2020: Šta sve mogu naprednjaci sa dvotrećinskom većinom u skupštini, 2020, Izbori u Srbiji 2020: Šta sve mogu naprednjaci sa dvotrećinskom većinom u skupštini - BBC News na srpskom, qasur më 20 mars 2023

pozicion vetëm sa përforcoi pikëpamjet e tyre para-ekzistuese dhe rriti polarizimin mbi ndryshimin e klimës.[40]

Teksa analizojmë sigurinë kibernetike dhe efektin e saj në lirinë e shprehjes dhe medias, duhet të theksojmë sulmet kibernetike që synojnë mediat dhe gazetarët, ku sulmet kibernetike përdoren si mjet frikësimi për të ndikuar sesi objektivi i tyre funksionon apo jo.[41] Pasoja e një sulmi kibernetik është më e gjerë se një sulm i thjeshtë ndaj një sistemi ose një rrjeti, por zakonisht ka edhe një konotacion politik. Qëllimi kryesor është "të ndryshojë sjelljen e tyre duke bërë kërcënime për të mohuar, degraduar ose ndërprerë rrjetet, ose ndikuar në disponueshmërinë ose integritetin e të dhënave të ruajtura në to".[42] Kjo rëndon lirinë e tyre për të punuar pa frikën e persekutimit, hakmarrjes dhe vrasjes digjitale. Efekti psikologjik i sulmeve kibernetike nuk duhet neglizhuar. Perceptimi i rrezikut tek grupet ose individët e targetuar ndryshon, megjithatë, mund të pritet që të detektohet një ndryshim në sjellje. Duke pasur parasysh se sulmet kibernetike zakonisht shtrihen tek anëtarët e familjeve të gazetarëve, ata mund të jenë më ngurrues për të mbuluar një temë nëse parashikojnë një sulm kibernetik si reagim. Kjo do të thotë që një sulm kibernetik nuk duhet domosdoshmërisht të ndodhë, por mjafton që objektivi të jetë i vetëdijshëm për atë mundësi për të arritur rezultatin e dëshiruar.[43]Nëse ky mjedis ushqehet në një periudhë më të gjatë kohore, profesioni i medias shoqërohet me një gamë të gjerë anësh negative, të cilat mund të çojnë në uljen e interesit për gazetarinë si karrierë.

Si përfundim, një nga pasojat kryesore që mund të kenë sulmet kibernetike dhe mungesa e masave efikase të sigurisë kibernetike lidhet me vetë-censurën mes profesionistëve të medias. Kjo mund të përkeqësojë rëndë pluralizmin dhe diversitetin mediatik. Ndërsa IA ka një ndikim më të madh në të drejtën për tu informuar pa ndërhyrje, IA mund të identifikohet gjithashtu si një faktor kontribues në një mjedis armiqësor ndaj lirisë së shprehjes dhe lirive të medias.

2.2. E drejta për privatësi

E drejta për privatësi i referohet mbrojtjes së të dhënave personale dhe respektimit të konfidencialitetit të korrespondencës dhe komunikimeve të dikujt.[44] Ajo gjithashtu përfshin të drejtën për të qenë të lirë nga mbikëqyrja dhe përgjimi i komunikimeve tona, përpunimi i paautorizuar i të dhënave, përmbajtja pornografike dhe të tjera.[45] Tre palët kryesore në sigurimin e kësaj të drejte janë qytetarët, qeveritë dhe aktorët e biznesit. Shqetësimet për sigurinë e të dhënave janë shfaqur duke rritur qasjen në internet dhe duke kuptuar vlerën e të

40 Zhou, Y, & Shen, L. Paragjykimi i konfirmimit dhe vazhdimësia e keqinformimit mbi ndryshimet klimatike. Hulumtim mbi komunikimin, 49(4), 500-523, 2022, https://doi.org/10.1177/00936502211028049, qasur më 07 prill 2023
41 Bur Burton, J. Sulmet kibernetike dhe liria e shprehjes: Shtrëngimi, frikësimi dhe pushtimi virtual, Studimet Evropiane të gazetarisë Baltike, Universiteti i Teknologjisë i Talinit, Vol. 9, No. 3 (28), 117-132
42 Burton, J. Sulmet kibernetike dhe liria e shprehjes: Shtrëngimi, frikësimi dhe pushtimi virtual, Studimet Evropiane të gazetarisë Baltike, Universiteti i Teknologjisë i Talinit, Vol. 9, No. 3 (28), 117-132
43 Ibid.
44 Privatësia dhe mbrojtja e të dhënave, Këshilli i Evropës, Council of Europe Data Protection website - Data Protection (coe.int), qasur më 10 mars 2023
45 Leslie D et al. Inteligjenca Artificiale, të drejtat e njeriut, demokracia, dhe sundimi i ligjit: Së pari. Këshilli i Evropës, 2021

dhënave për shtetet dhe kompanitë private. Të ardhurat e kompanive dhe ushtrimi i kontrollit të shtetit mbi qytetarët bazohen në të dhëna.[46]

Implikimet që siguria kibernetike, IA dhe teknologji të tjera të ngjashme digjitale kanë në lirinë e shprehjes janë të ndërthurura me të drejtën për privatësi dhe të drejta të tjera themelore të njeriut. Siç u shpjegua, sulmet kibernetike mund të perceptohen dyfish: si sulm ndaj infrastrukturës kritike të shteteve dhe si sulm ndaj një individi. Teksa një sulm kibernetik në infrastrukturën kritike mohon qasjen në shërbime, u mundëson qeverive në disa përpjekje, ai është gjithashtu i prirur të çojë në rrjedhje masive të të dhënave personale, për të gjurmuar dhe për të vëzhguar grupet ose individët e synuar.[47] Disa qeveri përdorin sigurinë kibernetike për të vendosur një shkallë më të lartë kontrolli mbi internetin dhe për të kufizuar më tej të drejtat.[48] Aftësia e aktorëve publikë dhe privatë për të pasur qasje në historinë digjitale, informacionin personal, vendndodhjen, lëvizjet e dikujt ngre shumë shqetësime për privatësinë. Teknologjitë e njohjes së fytyrës, vëzhgimi në sfera të ndryshme publike dhe private, së bashku me mundësinë e gjurmimit dhe ruajtjes së këtyre të dhënave kanë të bëjnë me mbrojtjen e të dhënave personale. Kjo mund të jetë veçanërisht shqetësuese në vendet me tendenca kufizuese, ku qeveritë mund të ndërhyjnë lehtësisht në autonominë dhe sigurinë e dikujt.[49]Kur Amnesty International raportoi se një anëtar i stafit të tyre dhe një aktivist për të drejtat e njeriut nga Arabia Saudite ishin shënjestër e një fushate të fuqizuar nga NSO.[50] Ky program spiunazhi do të mundësonte qasje të plotë në pajisjen e personit të synuar, duke përfshirë mbledhjen e të dhënave dhe gjurmimin e objektivit[51], gjë që mund të rrezikonte jetën dhe punën e tyre.

Përveç sulmeve kibernetike, ka edhe teknologji të tjera digjitale të ndihmuara nga IA që mund të ndërhyjnë në të drejtën e privatësisë. Në vazhdim, në këtë nënkapitull, do të ofrojmë definicione dhe shembuj ilustrues për disa prej këtyre teknologjive, në veçanti: vëzhgimi (masiv, privat dhe privat-shtetëror) dhe teknologjitë e njohjes së fytyrës.

Privacy International shpjegon se "vëzhgimi masiv përfshin fitimin, përpunimin, gjenerimin, analizën, përdorimin, ruajtjen ose depozitimin e informacionit për numër të madh të njerëzve, pa marrë parasysh nëse dyshohen për keqbërje".[52] Vëzhgimi masiv bazohet në hipotezën se të gjitha të dhënat e mbledhura mund të jenë të dobishme për të luftuar një kërcënim

46 Prezantimi i të drejtave digjitale, Share Foundation, 2021
47 Freedom on the Net 2022, Kundër një rishikimi autoritar të internetit, Freedom House 2023
48 Human Rights Watch, Është koha ta trajtojme sigurinë kibernetike si çështje e të drejtave të njeriut: Të mëdhenjtë e kibernetikës SHBA dhe Rusia ishin të heshtur në të drejta, 2020, https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue, qasur më 5 mars 2023
49 Special Rapporteur në promovimin dhe mbrojtjen e të drejtës së lirisë së mendimit dhe shprehjes, mbikëqyrja dhe të drejtat e njeriut, A'/HRC/41/35, 2019, 7
50 Fushata e fuqizuar nga NSO është një platformë komerciale e sofistikuar spiunimi dhe eksploatimi e shitur nga një shitës izraelit
51 Amnesty International, Amnesty International në mesin e objektivave të fushatës së fuqizuar nga NSO, 2018, https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/,qasur më 07 prill 2023
52 Vëzhgimi në masë, Privacy International, https://privacyinternational.org/learn/mass-surveillance, qasur më 20 mars 2023

hipotetik.[53] Monitorimi sistemik i jetëve të njerëzve ofron të dhëna të pakufizuara për qeveritë dhe kompanitë private, të cilat më pas mund të përdoren për qëllime të ndryshme.[54] OSBE ka raportuar se kjo teknologji është përdorur për të penguar punën dhe hulumtimet e gazetarëve, janë identifikuar mbrojtës të të drejtave të njeriut që kanë marr pjesë në protesta, janë ndjekur dhe lokalizuar aktivistë me pikëpamje kundër dhe sinjalizuesit.[55] Rusia dhe Kina janë të njohura për zhvillimin e teknologjive më të avancuara të vëzhgimit, megjithatë vëzhgimi përdoret gjerësisht në gjithë botën. Mënyra se si përdoret ndryshon dhe përcakton qëllimet e vëzhgimit. *Citizens Lab*ka raportuar se vetëm duke supozuar se dikush mund të jetë subjekt i vëzhgimit masiv do të çonte në vetë-cenzurë.[56] Vetë-censurimi mund të interpretohet analogisht si përjashtim nga çdo veprim që në raste të tjera do të ndiqej. Për shembull, Rusia po përdor teknologjitë e vëzhgimit masiv për të ndjekur protestuesit opozitarë deri në shtëpitë e tyre dhe për t'i arrestuar.[57] Shtetet e Bashkuara gjithashtu kanë përdorur metoda të vëzhgimit për të ndjekur demonstruesit e lëvizjes *Black Lives Matter*.[58] Motivimi pas këtij vëzhgimi është për të kufizuar aktivitetet e grupeve të targetuara dhe jo për të lehtësuar identifikimin e kriminelëve, ashtu siç thuhet zakonisht.

Teknologjitë e njohjes së fytyrës janë faktori kyç që lejon vëzhgimin masiv të jetë edhe më shqetësues. Njohja e fytyrave është mjet që bazohet në *machine-learning* për të gjetur përputhje identiteti përmes imazheve statike dhe videove të fytyrave të njerëzve.[59] Një shqetësim tjetër është se njohja e fytyrave mund të përkeqësojë diskriminimin dhe të mundësojë profilizimin, pasi që synon të profilizojë individët në bazë të karakteristikave të ndryshme si etnia, gjinia, raca, kombësia e të tjera.[60] Kjo mund të çojë në diskriminim dhe arrestime të paligjshme, kufizime të të drejtës për lëvizje dhe të drejtës për integritet personal.[61] Duke pasur parasysh se IA nuk është neutral dhe i lirë nga paragjykimet, por është një mjet i trajnuar me të dhëna, ajo mund të shfrytëzohet lehtësisht për identifikimin e grupeve të targetuara në bazë të karakteristikave të caktuara.[62] Teknologjitë e njohjes së fytyrës

53 Ibid.
54 Sekalala, S. et al, Analiza e impaktit të të drejtave të njeriut në rritjen e vrojtimit dixhital të shëndetit public përgjatë krizës me COVID-19, Health and Human Rights Journal, Volumi 22/2, dhjetor 2020, 7 / 20, https://www.hhrjournal.org/2020/12/analyzing-the-human-rights-impact-of-increased-digital-public-health-surveillance-during-the-covid-19-crisis/, qasur më 01 mars 2023
55 Pirkova, E. et al, Vëmendja në Inteligjencën Artificiale dhe liria e shprehjes – Një manual politikash, OSCE, 2021, 64
56 Knockel, J. et al, Ne bisedojmë, ata shikojnë se si përdoruesit ndërkombëtarë ndërtojnë pa dashje aparatin e censurimit kinez të WeChat, CitizensLab, 2020, https://citizenlab.ca/2020/05/we-chat-they-watch/, qasur më 18 shkurt 2023
57 The Washington Post, Gjendja e vëzhkimit të Rusisë ende nuk është në nivelin e Kinës. Por Putin është duke punuar në atë drejtim, 2021, Russia is growing its surveillance state but not everyone is monitored equally - The Washington Post, qasur më 01 prill 2023
58 ICNL, Protestimi në epokën e vëzhgimit qeveritar, 2023, Protesting in an Age of Government Surveillance - ICNL, qasur më 25 mars 2023
59 Human Rights Watch, Rregullat për realitetin e ri të vëzhgimit, 2019, https://www.hrw.org/news/2019/11/18/rules-new-surveillance-reality, qasur më15 mars 2023.
60 Special Rapporteur në promovimin dhe mbrojtjen e të drejtës së lirisë së mendimit dhe shprehjes, mbikëqyrja dhe të drejtat e njeriut, A'/HRC/41/35, 2019, 7
61 Human Rights Watch, Rregullat për realitetin e ri të vëzhgimit, 2019, https://www.hrw.org/news/2019/11/18/rules-new-surveillance-reality, qasur më15 mars 2023.
62 Zuiderveen Borgesius, F. Diskriminimi, inteligjenca artificiale, dhe algoritmet vendim-marrëse. Këshilli i Evropës, Drejtoria per Demokracinë e Përgjithshme, 2018. https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decisionmaking/1680925d73, qasur me 15 mars 2023

kanë një nivel të lartë saktësie, megjithatë, kjo nuk aplikohet në të njëjtën mënyrë për të gjitha demografitë.[63]Ka më shumë gjasa që modelet e paracaktuara të lidhen me kuptimet e përbashkëta të shumicës[64] dhe më shumë false pozitive ndodhin tek njerëzit me ngjyrë, gratë, fëmijët dhe të moshuarit.[65]Afro-amerikanët kanë më shumë gjasa të identifikohen gabimisht në SHBA, ndërsa IA e zhvilluar në Azi ka gjasë të identifikojë më saktësisht njerëzit aziatikë se sa të bardhët.[66] Në vitin 2018, Policia e Gjirit të Wales-it publikoi të dhëna sipas të cilave rreth 92% e përputhjeve të fytyrave të kryera gjatë finales së Ligës së Kampionëve në vitin 2017 ishin pozitive të rreme, duke përbërë një shifër prej 2,297 nga 2,470[67], e cila mbështet pretendimin se teknologjitë e njohjes së fytyrës nuk mund të përdoren gjithmonë për identifikimin e kriminelëve, pasi shpesh nuk arrijnë ta bëjnë këtë me sukses.

Së fundi, organet kineze të rendit kanë përdorur teknologjinë e njohjes së fytyrës me qëllim të mbështetjes së "njohjes së fytyrës për të identifikuar atributet e ujgurëve/jo-ujgurëve".[68] Prandaj, është e rëndësishme të projektohen me kujdes teknologjitë e njohjes së fytyrës duke marrë parasysh të gjitha përfitimet dhe disavantazhet që mund të sjellë.

Përveç kësaj, gjithnjë e më shumë hasim vëzhgim privat dhe partneritete midis sektorit privat dhe shtetit. Sektori privat vepron si shitës dhe ofrues shërbimi për shumë qeveri, për shkak të stimujve, ekspertizës dhe burimeve të tyre.[69] Sigurimi i qeverive me të dhëna të marra nga pajisjet dhe rrjetet e përdoruesve është gjithashtu subjekt diskutimi mes ekspertëve të të drejtave të njeriut. Agjencitë e rendit kanë kërkuar gjithnjë e më shumë të dhëna nga platformat e mediave sociale. Raportet e *Apple* për transparencës tregojnë se në periudhën nga korriku 2021 deri në dhjetor 2021, ata ofruan të dhëna në 85% të rasteve të kërkuara.[70]

Shqetësimet lidhur me privatësinë shfaqen në shumë fusha tjera, si proceset e rekrutimit, kujdesi shëndetësor, shërbimi ndaj klientëve, mjetet e përkthimit, pajisjet shtëpiake, lodrat dhe të ngjashme. Kjo fushë digjitale që përfshin shumë aspekte është nënregulluar dhe interesat e shumë palëve influencojnë politikë-bërësit. Së fundi, mbledhja e të dhënave personale, përpunimi dhe ripërdorimi i këtyre të dhënave duhet të bëhet në përputhje me legjislacionin përkatës dhe duke mbështetur vlerat themelore demokratike, ku çdo kufizim i të drejtave të njeriut duhet të jetë i nevojshëm dhe në proporcion me qëllimin.

63 Najibi, A, Diskrimini racor në teknologjinë e njohjes së fytyrës, Universiteti i Harvardit, Racial Discrimination in Face Recognition Technology - Science in the News (harvard.edu), 2020, 07 prill 2023
64 Human Rights Watch, Rregullat për realitetin e ri të vëzhgimit, 2019, https://www.hrw.org/news/2019/11/18/rules-new-surveillance-reality, qasur më15 mars 2023.
65 Forbes, Njohja e fytyrës shkelë të drejtat e njeriut, vendosë gjykata, 2020, Facial Recognition Violates Human Rights, Court Rules (forbes.com), qasur më 01 prill 2023
66 The Atlantic, Programi i njohjes së fytyrës mund të ketë një problem paragjykimi racor, 2016, Facial-Recognition Software Might Have a Racial Bias Problem - The Atlantic, qasur më 01 prill 2023
67 Endgadget, Programi i policisë për njohje të fytyrës keqidentifikon 2,300 njerëz si kriminiel potencial, 2018, Police face recognition misidentified 2,300 as potential criminals | Engadget, qasur më 01 prill 2023
68 The New York Times, Një muaj, 500,000 skanime fytyrash: Si po e përdorë Kina IA për profilizim të një minoriteti, 2019, One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority - The New York Times (nytimes.com), qasur më 01 prill 2023
69 Special Rapporteur në promovimin dhe mbrojtjen e të drejtës së lirisë së mendimit dhe shprehjes, mbikëqyrja dhe të drejtat e njeriut, A'/HRC/41/35, 2019
70 Apple Inc. Kërkesat nga llogaritë, https://www.apple.com/legal/transparency/account.html, qasur më 01 mars 2023

2.3. Qasja bazuar në të drejtat e njeriut ndaj sigurisë kibernetike dhe AI

OKB-ja përkufizon qasjen bazuar në të drejtat e njeriut (HRBA) si një kornizë konceptuale që bazohet normativisht në standardet ndërkombëtare të të drejtave të njeriut dhe është drejtuar në mënyrë operacionale për të promovuar dhe mbrojtur të drejtat e njeriut.[71] Ajo synon të analizojë se si diskutohen të drejtat e njeriut brenda kontekstit të sigurisë kibernetike dhe si të ndryshohet fokusi nga siguria kombëtare në sigurinë njerëzore. Shoqata për Komunikime Progresive përkufizon një qasje të bazuar në të drejtat e njeriut ndaj sigurisë kibernetike si *"vënia e njerëzve në qendër dhe sigurimi i besimit dhe sigurisë në rrjete dhe pajisje që përforcojnë- në vend që të kërcënojnë- sigurinë njerëzore. Një qasje e tillë është sistematike, që do të thotë se trajton së bashku aspektet teknologjike, sociale dhe ligjore dhe nuk bën dallime ndërmjet interesave të sigurisë kombëtare dhe sigurisë së internetit global"*.[72]

Siguria kombëtare është vënë në qendër të narrativës së sigurisë kibernetike.[73] Siguria mund të trajtohet në mënyrë pozitive dhe në mënyrë negative. Aspekti negativ i sigurisë ka të bëjë me mungesën e kërcënimeve ndaj të drejtave themelore të njeriut, ndërsa kuptimi pozitiv i referohet masave dhe qasjeve që mbrojnë dhe u mundësojnë individëve ushtrimin e lirë dhe të sigurt të të drejtave të tyre. Fatkeqësisht, aspekti pozitiv i sigurisë duket se nuk njihet shumë në diskutimet e sotme mbi sigurinë kibernetike. Qeveritë tradicionalisht e kanë parë sigurinë nga një pikëpamje negative, dhe në këtë kuptim, siguria kibernetike lidhet kryesisht me parandalimin e dëmeve.[74] Kuptimi parësor i sigurisë kibernetike është i përqendruar tek interesat shtetërore, territori dhe infrastruktura, më shumë se tek individët.[75] Kjo pikëpamje vjen për arsye pragmatike, pasi siguria e këtyre komponentëve është parakushti për të përmbushur të drejtat e njeriut[76], dhe për faktin se shtetet i ofrojnë siguri qytetarëve të tyre.[77] Elementi njerëzor konsiderohet si pjesë e spektrit të kërcënimit, më shumë se sa subjekt i sigurisë. Kjo, së bashku me konceptin negativ të sigurisë, ka çuar në politika të krijuara për të mbrojtur infrastrukturat kritike dhe jo për të lehtësuar aftësinë e njerëzve për të pasur qasje në mjete dhe burime të hapësirës kibernetike.[78] Nga perspektiva e sigurisë kibernetike, siguria

71 Grupi i zhvillimit të qëndrueshëm në OKB, UNSDG | Human Rights-Based Approach, më 25 mars 2023
72 Asociacioni për komunikim progresiv, APC policy explainer: A human rights-based approach to cybersecurity | Association for Progressive Communications, qasur më 01 shkurt 2023
73 Liaropoulos, A. Një qasje njerëzore në qendër të sigurisë kibernetike: Sigurimi i njeriut në epokën e kiberfobisë, Journal of Information Warfare, 14, 4, 2015, (PDF) A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia, Journal of Information Warfare, 14, 4 (2015). (researchgate.net), qasur më 20 mars 2023
74 Ibid.
75 Pavlova, P. "Qasja e bazuar në të drejtat e njeriut ndaj sigurisë kibernetike: Adresimi i rreziqeve të sigurisë të grupeve të synuara", Peace Human Rights Governance, 4(3), 391-478, 2020, PHRG-2020-3-04.pdf (padovauniversitypress.it), qasur më 20 mars 2023
76 Ibid.
77 Liaropoulos, A. Një qasje e sigurisë kibernetike me në qendër njeriun: Sigurimi i njeriut në epokën e kiberfobisë, Journal of Information Warfare, 14, 4, 2015 (PDF) A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia, Journal of Information Warfare, 14, 4 (2015). (researchgate.net), qasur më 20 mars 2023
78 Kovacs, A, Haëtin, D. (2013) 'Siguria kibernetike, vëzhgimi kibernetik dhe të drejtat e njeriut në internet', Global Partners Digital, Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf (gp-digital.org), qasur më 05 mars 2023

nuk referohet vetëm te mbajtja e njerëzve të sigurt në internet, por duhet të ketë një rol lehtësues në fuqizimin e njerëzve për të gëzuar të drejtat e tyre, përderisa respektojnë të drejtat e tjera të njeriut.[79]

Përveç kësaj, qasja e bazuar në të drejtat e njeriut kërkon një vlerësim të hollësishëm të masave të ndërmarra të sigurisë kibernetike dhe ndikimin e tyre në të dyja; mbrojtjen e hapësirës kibernetike dhe të të drejtave të njeriut. Në këtë kuptim, çdo kufizim duhet të jetë proporcional, i nevojshëm dhe me qëllim legjitim.[80] Një praktikë kibernetike që mbron njerëzit nga një dëm i caktuar, por në të njëjtën kohë shkel të drejtat e tyre njerëzore përtej nivelit të proporcionalitetit dhe të domosdoshëm, pa një qëllim legjitim, nuk mund të vlerësohet si masë e arsyeshme. Ky rregull aplikohet për kufizimet në hapësirën kibernetike dhe atë jashtë saj.

Hapësira kibernetike është një fushë transnacionale që përpiqet të balancojë përfshirjen e aksionarëve ndërkombëtarë dhe privat, shteteve në njërën anë dhe nga ana tjetër shtresave të ndryshme të interesit. Ky domain është i ndryshëm nga çdo tjetër, prandaj mbrojtja e të drejtave të njeriut brenda kësaj hapësire kibernetike është sfidë e vështirë.[81] Adoptimi qasjes së bazuar në të drejtat e njeriut rrit nivelin e kuptimit se si ndërthuren të drejtat e njeriut dhe siguria dhe se si pozicionet e tyre janë të lidhura. Duke kuptuar pozicionin që njerëzit kanë në hapësirën kibernetike dhe vlerësimin e rëndësisë së sigurisë kibernetike, është e mundur të identifikohen praktikat dhe politikat që janë njësoj të dobishme për të dyja palët. Gjithashtu, definimi i infrastrukturës kritike duhet të interpretohet në mënyrë që të fokusohet edhe në qytetarët. Së fundi, domosdoshmëria dhe shtrirja e kufizimit të të drejtave të njeriut për të zbutur rreziqet e sigurisë duhet të udhëhiqen nga parime që vënë në prioritet sigurinë kombëtare si mjet për të krijuar një mjedis të sigurt për qytetarët.

79 Ibid.
80 Ibid.
81 Liaropoulos, A. Një qasje e sigurisë kibernetike me në qendër njeriun: Sigurimi i njeriut në epokën e kiberfobisë, Journal of Information Ëarfare, 14, 4, 2015 (PDF) A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia. Journal of Information Warfare, 14, 4 (2015). (researchgate.net), qasur më 20 mars 2023

3 Kosova: Përmbledhje e politikave dhe praktikave

Rajoni i Ballkanit Perëndimor ka bërë përparim të konsiderueshëm në përmirësimin e sigurisë kibernetike në vitet e fundit. Shumica e vendeve në rajon kanë krijuar strategji dhe institucione për të luftuar kërcënimet kibernetike, dhe janë ndërmarrë masa të rëndësishme ligjore për të rregulluar dhe mbrojtur sigurinë kibernetike. Megjithatë, ende ka vend për përmirësim në forcimin e kapaciteteve kibernetike kombëtare dhe rajonale, promovimin e bashkëpunimit ndërkufitar dhe ndarjes së informacionit, dhe ngritjen e ndërgjegjësimit te qytetarët dhe bizneset.[82] Teksa përshpejtohet transformimi digjital, siguria kibernetike po bëhet gjithnjë e më e rëndësishme për stabilitetin, prosperitetin dhe sigurinë e rajonit të Ballkanit Perëndimor.

Që nga shpallja e pavarësisë nga Serbia në vitin 2008, Kosova ka bërë hapa të rëndësishëm në zhvillimin e ekonomisë dhe infrastrukturës së saj. Megjithatë, vendi ende përballet me shumë sfida, duke përfshirë mungesën e qasjes në teknologji dhe burimet e kufizuara për të investuar në sigurinë kibernetike dhe IA-në. Përpjekjet për të zhvilluar dhe rregulluar këto fusha janë të lidhura me bashkëpunimin me Perëndimin, bazuar në modelet dhe praktikat më të mira në BE dhe NATO. Gjithashtu, është e rëndësishme të theksohet se sfidat më të mëdha të Kosovës janë ende të lidhura me statusin e saj të kontestuar. Në Kosovën e pas luftës ka pasur prani të madhe të aktorëve ndërkombëtarë, siç është Misioni i Administratës së Përkohshme të Kombeve të Bashkuara në Kosovë (UNMIK), i cili ka udhëhequr vendin në zhvillimin e institucioneve, ekonomisë dhe duke lehtësuar paqen dhe sigurinë.[83] Që nga pavarësia e saj, është shfaqur debati rreth të drejtës për vetëvendosje. Ky debat rrjedh nga fakti që Serbia e konsideron Kosovën si pjesë integrale të territorit serb, dhe në këtë mënyrë konteston statusin e saj si vend i pavarur. Kosova ka fituar mbështetje nga

82 Korniza rregullatore në fushën e të drejtave digjitale, analizë krahasuese: Shqipëria, Bosjna dhe Hercegovina, Kosova, Mali i Zi, Maqedonia e Veriut, Serbia, 2021, Digital-rights-legal-analysis_EN-1.pdf (sharefoundation.info), qasur më 25 mars 2023

83 Misioni në Kosovë i OKB-së, Mandate | UNMIK (unmissions.org), qasur më 07 prill 2023

vende të rëndësishme ndërkombëtare dhe evropiane, megjithatë deri më sot, pesë shtete anëtare të BE-së nuk e kanë njohur pavarësinë e saj.[84] Për më tepër, Kosova nuk është anëtare e OKB-së pasi Rusia[85] dhe Kina[86] nuk janë të gatshme ta njohin atë për shkak të lidhjeve të tyre të ngushta me Serbinë. Prandaj, statusi i Kosovës në organizatat ndërkombëtare si NATO, BE dhe Këshillin e Evropës është i diskutueshëm, pasi nuk ka një marrëveshje të përbashkët mbi statusin e Kosovës si shtet.

Si shumë vende të botës dhe rajonit të Ballkanit Perëndimor, Kosova nuk bën përjashtim kur bëhet fjalë për sulmet kibernetike. Pavarësisht se ka ndërmarrë hapa kritikë,[87] Kosova i është nënshtruar shumë sulmeve kibernetike që nga viti 2018. Sulmi i fundit kibernetik ishte në shtator të vitit 2022 i cili kishte në shënjestër Telekomin e Kosovës.[88] Përveç kësaj, Banka Ekonomike, Komisioni i Pavarur për Media i Kosovës, HIB Petrol, Ministria e Ekonomisë, Komisioni Qendror i Zgjedhjeve të Kosovës janë vetëm disa nga viktimat e sulmeve kibernetike në Kosovë. Objektivat e sulmeve kanë qenë të shumta dhe disa prej tyre kanë pasur pasoja për publikun në përgjithësi[89], ndërsa disa prej tyre kanë vënë në pah cenueshmërinë e sistemit.

Marrëdhëniet ndërkombëtare të Kosovës në fushën e sigurisë kibernetike bazohen kryesisht në marrëveshje për bashkëpunim bilateral. Deri tani, marrëveshjet bilaterale që përfshijnë aspekte kibernetike janë të pakta dhe kufizohen në bashkëpunim policor. Kosova ka nënshkruar marrëveshje me Shqipërinë, Bullgarinë, Italinë, Malin e Zi, Zvicrën dhe Turqinë. Bashkëpunimi me Shqipërinë është i avancuar përmes nënshkrimit të një Marrëveshjeje për Bashkëpunim në Teknologji të Informacionit dhe Komunikimit (TIK) dhe një Memorandumi të Mirëkuptimit për bashkëpunim mes dy CERT-ave kombëtare.[90]

Duke pasur parasysh përdorimin e gjerë të internetit, platformave të mediave sociale dhe përpjekjet e shtuara të digjitalizimit, rreziku i sulmeve kibernetike dhe të formave të tjera të shkeljes së të drejtave të njeriut është në rritje. Portali DataRe raporton se Kosova ka një përhapje të internetit prej 96.6% dhe 1.6 milion përdorues interneti në janar 2023. 56.1% e popullsisë totale ishin përdorues aktivë të mediave sociale ndërsa 58.1% e bazës së përdoruesve të internetit të Kosovës përdornin të paktën një platformë të mediave sociale. Kepios vuri re një rritje prej 0.2% të përdoruesve të internetit në vitet 2022 dhe 2023.[91]

84 Al Jazeera, Cilat shtete e njohin shtetësinë e Kosovës?, 2023, Which countries recognise Kosovo's statehood? | Infographic News | Al Jazeera, qasur më 07 prill 2023
85 Qëndrim i shkruar i Federatës Ruse në Gjykatën Ndërkombëtare të Drejtësisë, 2009, 15628.pdf (icj-cij.org), qasur më 07 prill 2023
86 Qëndrim i shkruar i Republikës Popullore të Kinës në Gjykatën Ndërkombëtare të Drejtësisë në çështjen e Kosovës, 2009, 15611.pdf (icj-cij.org), qasur më 07 prill 2023
87 Kosova ka ndërmarrë hapa kritikë në sigurinë kibernetike, thotë vlerësimi i ri i modelit të maturimit të kapaciteteve të sigurisë kibernetike, Banka Botërore, 2020, Kosovo Has Undertaken Critical Steps in Cybersecurity, Says New Cybersecurity Capacity Maturity Model Assessment (worldbank.org), qasur më 20 mars 2023
88 BIRN, Kosova do të themelojë Agjencinë për Siguri Kibernetike pas sulmeve të fundit, 2022, Kosovo to Establish Agency for Cyber Security Amid Recent Attacks | Balkan Insight, qasur më 15 mars 2023
89 Sulmi kibernetik në Bankën Ekonomike të Kosovës, Raporti mbi ekosistemin në sigurinë kibernetike, Ballkani Perëndimor: Kërcënimet kibernetike në rritje, PëC, 2022, 30, PwC-Cybersecurity-Ecosystem-Report-WB.pdf (isac-fund.org), qasur më 20 mars 2023
90 Raporti mbi ekosistemin në sigurinë kibernetike, Ballkani Perëndimor: Kërcënimet kibernetike në rritje, PëC, 2022, 30, PwC-Cybersecurity-Ecosystem-Report-WB.pdf (isac-fund.org), qasur më 20 mars 2023
91 Portali DataRe, Digital 2023: Kosova, 2023, Digital 2023: Kosovo — DataReportal – Global Digital Insights, qasur më 20 mars 2023

Dy nënkapitujt e ardhshëm do të analizojnë legjislacionin ekzistues dhe zbatimin e tij në Kosovë. Një vëmendje e veçantë do t'i kushtohet legjislacionit të sapo miratuar, i cili përfaqëson ombrellën e legjislacionit. Kjo do të pasohet nga një analizë e praktikave ekzistuese dhe se si legjislacioni përkthehet në zbatim në Kosovë.

3.1. Legjislacioni

Kosova ka vazhduar të miratojë disa ligje të rëndësishme për të rregulluar efikasitetin e sigurisë kibernetike. Në vitin 2022, ligjvënësit e Kosovës kanë intensifikuar përpjekjet e tyre për të tejkaluar boshllëkun që ka ekzistuar në strukturën ligjore kibernetike. Është parashikuar të miratohet një paketë që përbëhet nga një ligj, një strategji kombëtare dhe një plan veprimi. Disa institucione dhe njësite të reja pritet të themelohen në fushën e sigurisë kibernetike në Kosovë. Fokusi i këtij nënkapitulli është Ligji mbi Sigurinë Kibernetike dhe Strategjia Kombëtare për Sigurinë Kibernetike, pasi janë ligjshmëritë më të reja.

Strategjia Kombëtare për Sigurinë Kibernetike është parashikuar të caktojë objektivat strategjike brenda periudhës kohore 2023-2027. Ekziston një dispozitë kushtuar balancimit të sigurisë dhe të drejtave të njeriut, kryesisht privatësisë, qasjes së lirë në informacion dhe të drejtave të tjera themelore. Ai pranon se rritja e sigurisë kibernetike mund të jetë e dobishme për ushtrimin e të drejtave të njeriut në hapësirën kibernetike. Megjithatë, kjo nuk është përcaktuar si objektiv specifik i Strategjisë. Strategjia dhe Plani i Veprimit janë në dispozicion vetëm si propozime dhe do të miratohen në vitin 2023.[92]

Ligji mbi Sigurinë Kibernetike është miratuar në fillim të vitit 2023, pasi ka qenë në pritje për disa vjet. Agjencia Kombëtare për Sigurinë Kibernetike dhe Këshilli Kombëtar për Sigurinë Kibernetike do të themelohen si institucionet kryesore për zbatimin dhe monitorimin e sigurisë kibernetike në Kosovë. Kjo Agjenci është themeluar në kuadër të Ministrisë së Punëve të Brendshme të Kosovës, ndërsa Këshilli do të jetë organ i pavarur këshillues për Qeverinë, palë të tjera të interesuara publike dhe private. Pas miratimit, mbetet të shihet si Ligji do të përmirësojë peisazhin kibernetik në Kosovë. Qendra shtetërore e Trajnimit për Sigurinë Kibernetike brenda Ministrisë së Mbrojtjes do të organizojë trajnime të specializuara dhe programe certifikimi për personelin angazhuar në fushën e sigurisë kibernetike. Një përfaqësues i shoqërisë civile sqaron se Kosova ka zgjedhur të adoptojë një nga modelet ekzistuese, pasi kjo është praktikë e suksesshme në shumë vende evropiane.[93]

Ekspertët në fushën e sigurisë kibernetike vlerësojnë se ky ligj ishte i nevojshëm, por efektiviteti i tij varet nga mënyra si do të interpretohen dispozita të caktuara. Një shqetësim tjetër në lidhje me zbatimin e tij është mungesa e kapaciteteve, që gjithashtu shtrihet edhe te ligjet që janë miratuar para këtij ligji. Një ekspert i sigurisë kibernetike vuri re se ky Ligj parashikon një plan realist

92 Draft strategjia për sigurinë kibernetike në Kosovë 2023-2027, verzioni i propozuar _0.1 2022-12-30, 2022, Anglsht-DRAFT-Strategjia-per-siguri-kibernetike_V2.0_06032023.DOCX (live.com)
93 Intervistë me Leonora Hasani, 16 mars 2023

dhe do të rrisë koordinimin dhe harmonizimin, megjithatë kapacitetet janë të kufizuara.[94] Ligji ka forcuar detyrimin e operatorëve të shërbimeve themelore për të raportuar një incident kibernetik në Agjencinë Kombëtare për Sigurinë Kibernetike. Ai parashtron kërkesat që incidenti kibernetik të kualifikohet se ka një "ndikim të rëndësishëm të sistemit ose vazhdimësinë e shërbimit". Ai gjithashtu përcakton kohëzgjatjen dhe gjobat e përcaktuara nëse nuk respektohet. Përveç kësaj, ai detyron institucionin të informojë personat që preken nga incidenti kibernetik, dhe nëse personat janë të disponueshëm, institucioni duhet të njoftojë publikun.[95]

Pyetja kryesore është se si do të përcaktohet infrastruktura kritike në kuadrin e sigurisë kibernetike. Pasi që Ligji për Infrastrukturën Kritike e ka përcaktuar infrastrukturën kritike në një mënyrë të gjerë dhe përfshin monumentet kombëtare si një nga segmentet e saj; kritika kryesore ndaj Ligjit për Sigurinë Kibernetike, nga eksperti për sigurinë dhe një përfaqësues i një *Think Tank*, është se nuk ofron një prioritizim të shtresave të infrastrukturës kritike.[96]

Ligji për Mbrojtjen e të Dhënave Personale është në përputhje me Direktivën 95/46/EC të Komisionit të Bashkimit Evropian mbi Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave. Ai përcakton mbrojtjen ligjore, përgjegjësitë institucionale për monitorimin e ligjshmërisë së trajtimit të të dhënave dhe qasjen në dokumente publike, si dhe sanksionet lidhur me mbrojtjen e të dhënave personale dhe privatësinë e individëve.[97] Para kësaj, Kosova kishte miratuar ligje të tjera që kanë të bëjnë me sigurinë kibernetike, megjithatë, është bërë progres i kufizuar.[98] Aktet ligjore kyçe përfshijnë: Ligjin për Parandalimin dhe Luftën kundër Krimit Kibernetik, Ligjin për Shërbimet e Shoqërisë Informatike, Ligjin për Komunikimet Elektronike, Ligjin për Përgjimin e Komunikimeve Elektronike, Ligjin për Infrastrukturën Kritike.[99]

Ky nënkapitull ka ofruar një analizë paraprake të Ligjit të ri për Sigurinë Kibernetike dhe të Strategjisë Kombëtare për Sigurinë Kibernetike. Shumica e konkluzioneve janë bërë në bazë të intervistave të realizuara me përfaqësues të shoqërisë civile dhe ekspertë të sigurisë kibernetike. Duke qenë se është ende herët për të parashikuar rezultatet e sakta që do të japë ky legjislacion, mund të konkludojmë se qeveria e Kosovës ka bërë një hap shumë të rëndësishëm drejt mbrojtjes më të mirë të sigurisë kibernetike.

3.2. Sfidat aktuale

Kjo pjesë fokusohet në çështjet kryesore të ngritura nga ekspertët në fushën e sigurisë kibernetike dhe IA-së në Kosovë. Në thelb, kjo pjesë nënvizon praktikat që përkeqësojnë të drejtën për privatësi dhe lirinë e shprehjes, si dhe sfidat me të cilat ballafaqohet Kosova për

94 Intervistë me Arianit Dobroshi, 15 mars 2023
95 Ligji për sigurinë kibernetike, 2023
96 Intervistë me Mentor Vrajolli, 16 mars 2023
97 Siguria kibernetike dhe të drejtat e njeriut në Ballkanin Perëndimor: Harta e qeverisjes che aktorëve, DCAF- Geneva Centre for Security Sector Governance, 2022, CybersecurityHumanRightsWesternBalkans_EN_March2023.pdf (dcaf.ch), qasur më 18 shirt 2023
98 Intervistë me Mentor Vrajolli, 16 mars 2023
99 Strategjitë kombëtare të sigurisë kibernetike në ekonomitë e Ballkanit Perëndimor: Kosova, DCAF- Geneva Centre for Security Sector Governance, 2021, NationalCybersecurityStrategiesWB_2021.pdf (dcaf.ch), qasur më 20 mars 2023

shkak të statusit të saj pjesërisht të njohur. Gjetjet bazohen kryesisht në intervistat e kryera me aktorë të ndryshëm si burime primare.

3.2.1. Sfidat në fushën e sigurisë kibernetike

Statusi i kontestuar i shtetësisë pasqyron pozicionin e Kosovës në hapësirën kibernetike, si pasojë, Kosova nuk njihet në hapësirën kibernetike dhe nuk e ka domenin e saj. Aktualisht, domenet më të përdorur janë .ks dhe .rks, por trafiku i internetit zakonisht realizohet nëpërmjet serverëve në Shqipëri dhe Serbi.[100] Publiku i gjerë nuk di se cilin server ka përdorur dhe nuk mund të dijë nëse rrjedha e informacionit është penguar.[101] Pasi që Kosova nuk ka një pikë qendrore hyrëse në trafikun e internetit, do të ishte shumë e vështirë për qeverinë që të zbatonte politika të cilat do të kufizonin rrjedhën e informacionit në internet.[102]Në anën tjetër, një ekspert i sigurisë kibernetike në Kosovë shpjegon se mungesa e posedimit të një domeni bën të mundur që media të vendosura jashtë vendit të kenë faqe interneti dhe të përfaqësojnë median e Kosovës dhe të prodhojnë përmbajtje nën domenin e Kosovës.[103] Kjo gjithashtu vlen edhe për pajisjet të cilat janë të vendosura fizikisht në Kosovë që regjistrohen në Shqipëri ose Serbi. Ky fakt ka ndikim në trajtimin e raporteve mbi incidente, pasi raportet mbi incidentet që kanë të bëjnë me adresat në Kosovë më shumë janë të administrueshme në Shqipëri dhe Serbi, sesa në Kosovë. Duke pasur parasysh bashkëpunimin me Shqipërinë, ata zakonisht i përcjellin raportet mbi incidentet në Kosovë, ndërsa me Serbinë një bashkëpunim i tillë realizohet vetëm me raste.[104] Kjo bën që sistemi të jetë i prirur për përhapjen e dezinformimit dhe keqinformimit, pasi kjo gjendje e zonës së gri komplikon rregullimin e saj.

Mungesa e njohjes së Kosovës është e lidhur ngushtë me ushtrimin e të drejtave digjitale, veçanërisht të të drejtës për të jetuar në harresë, pasi themeli i kësaj të drejte është vendosur në legjislacionin e BE-së. Të drejta për të jetuar në harresë jep individëve të drejtën të kërkojnë nga motorët e kërkimit të fshijnë të dhënat e tyre personale.[105] Megjithëse Kosova ka prezantuar dhe miratuar ligjshmëri të përputhshme, kjo të drejtë vështirë se mund të zbatohet pa qasje në gjykatat ndërkombëtare.[106]

Ligji për Sigurinë Kibernetike është procesuar shumë shpejt, pasi ka pasur interes për të treguar se është bërë progres serioz në procesin e anëtarësimit në BE. Disa komponentë kryesorë janë lënë jashtë në këtë proces. Ligji mbi Infrastrukturën Kritike duhet të jetë ligj mbrojtës dhe të gjitha ligjet e tjera duke përfshirë Ligjin mbi Sigurinë Kibernetike, duhet të përgatiten në përputhje me Ligjin mbi Infrastrukturën Kritike. Zbatimi i ligjit do

100 Intervistë me Mentor Vrajolli, 16 mars 2023
101 Ibid.
102 Intervistë me Arianit Dobroshi, 15 mars 2023
103 Intervistë me Mentor Hoxhaj, 16 mars 2023
104 Rishikimi I kapaciteteve të sigurisë kibernetike në Republikën e Kosovës 2020, 2020, cybersecuritycapacityassessmentfortherepublicofkosovo2019pdf (ox.ac.uk), qasur më 20 mars 2023
105 Gjithcka që duhet të dini për "të drejtën për t'u harruar", GDPR EU, Everything you need to know about the "Right to be forgotten" - GDPR.eu, qasur më 25 mars 2023
106 Intervistë me Mentor Hoxhaj, 16mars 2023

të tregojë kundërshtitë midis këtyre dy akteve ligjore.[107] Një nga dobësitë është se grupi punues kryesisht ka përfshirë përfaqësues nga institucionet publike, nga industria dhe ekspertë të huaj.[108]

Themelimi i Agjencisë Kombëtare të Sigurisë Kibernetike është e kontestuar nga ekspertët e fushës së sigurisë kibernetike, pasi ekzistojnë shumë institucione që kanë një nivel të caktuar të kompetencave në këtë fushë.[109] Një nga opsionet e propozuara ishte zgjerimi i juridiksionit të CERT-it kombëtar dhe emërimi i tij si institucioni qendror që do koordinonte të gjitha aktivitetet lidhur me kibernetikën. KOS-CERT aktualisht ka vetëm dy persona të punësuar, prandaj efikasiteti i tyre është shumë i kufizuar.[110] Nga ana tjetër, Agjencia do të adresojë çështjen e fragmentimit të kompetencave ndërmjet institucioneve të ndryshme dhe do të përpiqet të harmonizojë të gjitha ligjet dhe politikat në fuqi.[111]Së fundi, efikasiteti i Agjencisë varet vetëm nga burimet njerëzore dhe financiare që do t'u caktohen. Qasja në të dhëna, monitorimi i tyre dhe përfshirja e Ministrisë së Brendshme dhe Ministrisë së Mbrojtjes në aspektet civile të administratës publike, duhet të jenë të kufizuara.[112]

Ligji për Sigurinë Kibernetike nuk ka përfshirë *ex officio* PPP (Partneritetin Privat-Publik), ndërsa Këshillat zakonisht shkëputen nga praktika dhe mund të mos kenë njohuritë e duhura.[113] Prandaj, ka shqetësim se Këshilli Kombëtar për Sigurinë Kibernetike nuk do t'i japë prioritet partneritetit privat-publik (PPP).[114] Kompanitë private dhe ekspertët individualë kanë dijen dhe aftësitë për të përmirësuar sigurinë kibernetike në Kosovë. Institucioneve u mungojnë këto kapacitete dhe kjo mund të zbutet duke krijuar PPP në Kosovë me fokus përfshirjen e ekspertëve vendas në vend të atyre të huajve.[115] Modeli i përdorimit të ekspertizës së huaj në vend të asaj vendase është përkthyer në grupin e punës për Ligjin për Sigurinë Kibernetike dhe Strategjinë Kibernetike.[116]

Pavarësisht mangësive dhe sfidave potenciale që mund të ndodhin, qeveria e Kosovës ka treguar vullnet politik serioz për të përmirësuar mbrojtjen në hapësirën kibernetike, duke trajtuar sigurinë kibernetike institucionalisht dhe sistemikisht. Pasja e një pjese të legjislacionit dhe institucioneve të fokusuar tërësisht në sigurinë kibernetike do ta përmirësojë këtë fushë dhe harmonizimi dhe pengesat e tjera do të zbuten në përputhje me rrethanat.

3.2.2. Privatësia dhe sfidat e tjera

Ky nënkapitull do të trajtojë privatësinë dhe sfidat e tjera të lidhura me teknologjitë digjitale që nuk mund të trajtohen nga siguria kibernetike. Privatësia në nënkapitull do të

107 Intervistë me Mentor Vrajolli, 16 mars 2023
108 Intervistë me Arianit Dobroshi, 15mars 2023
109 Ibid.
110 Ibid.
111 Intervistë me Erblind Morina, 15mars 2023
112 Intervistë me Arianit Dobroshi, 15mars 2023
113 Intervistë me Mentor Vrajolli, 16mars 2023
114 Ibid.
115 Intervistë me Erblind Morina, 15mars 2023
116 Intervistë me Arianit Dobroshi, 15mars 2023

analizohet përmes lenteve të mbikëqyrjes masive, rrjedhjeve të të dhënave dhe shkeljeve tjera të privatësisë të kryera nga institucionet publike dhe shkeljeve tjera të targetuara të të dhënave në Kosovë. Gjetjet bazohen kryesisht në intervista të bëra me palë të ndryshme të interest si burime primare.

Sa i përket mbikëqyrjes, është vënë re se shumë kamera CCTV që mbikëqyrin hapësirat publike janë instaluar në Kosovë. Ligji parashikon që çdo zonë publike e mbikëqyrur duhet të ketë një shenjë që tregon se hapësira është nën mbikëqyrje. Një nga ekspertët kibernetikë, me bazë në Prishtinë, ka vërejtur se një nënkalim i frekuentuar në Prishtinë është nën mbikëqyrje, por autoritetet nuk kanë vendosur ndonjë shenjë. Është kuptuar se kamera është në pronësi dhe kontroll të policisë, por pavarësisht njoftimit të autoriteteve kompetente, shenja nuk është vendosur deri më sot.[117]

Një formë tjetër e shkeljes së privatësisë është publikimi i fotove në media sociale për qëllime të vendndodhjes. Konkretisht, ka pasur raste kur policia ka publikuar fotografi të shkelësve, zakonisht në Facebook. Kjo është vërtetuar si metodë që policia përdor për të lokalizuar shkelësit e ligjit.[118] Është vënë re se këto janë raste që lidhen me shkelje të lehta. Ky është një rast i qartë shkeljeje i privatësisë së të dhënave nga autoritetet. Për më tepër, kjo praktikë është përhapur në disa media, të njohura për shpërndarjen e informacioneve personale lidhur me zhvillimet e fundit në Kosovë. Nuk dihet nëse AKI ka reaguar pasi ata vazhdojnë me të njëjtin praktikë.[119]

Duke marrë parasysh se Kosova po përdor në mënyrë të kufizuar disa metoda të mbikëqyrjes dhe që po mbështetet në mediat sociale për qëllime identifikimi e cila korrespondon me fushën e rregullimit të IA-së, deri më tani vendi nuk ka mbajtur qëndrim lidhur me IA-në[120]. Megjithatë, është ngritur një bashkëpunim me platforma të mediave sociale dhe Kodi i shtetit të Kosovës është shtuar në Facebook.[121] Një vlerësim i kryer në vitin 2020 tregoi se Kosova është në një fazë fillestare në fushën e mediave dhe mediave sociale. Ky vlerësim thekson se diskutimi lidhur me sigurinë kibernetike dhe përshtatjen e saj në këtë fushë është i kufizuar dhe duhet të përmirësohet.[122] Së fundi, edukimi dhe ngritja e ndërgjegjësimit për rëndësinë e sigurisë kibernetike dhe IA-së është në Kosovë është në nivel të ulët. Megjithatë, Fondacioni SHARE nuk ka raportuar ndonjë shkelje lidhur me bllokimin dhe filtrimin e përmbajtjes.[123] Në këtë mënyrë, qytetarët do të inkurajohen të raportojnë të gjitha shkeljet dhe vështirësitë që ndodhin në internet dhe të shtyjnë autoritetet të jenë më të përgjegjshme dhe transparente.

Duke kaluar te siguria kibernetike dhe efektet e saj në privatësi, është theksuar nga një ekspert kosovar i sigurisë kibernetike se raporti i shkeljes së të dhënave dhe raportet gjithëpërfshirëse të incidenteve të të dhënave janë dy elemente që duhet të përsëriten në periudhën në vijim.

117 Intervistë me Arianit Dobroshi, 15 mars 2023
118 Intervistë me Mentor Vrajolli, 16mars 2023
119 Ibid.
120 Intervistë me Arianit Dobroshi, 15 mars 2023
121 Intervistë me Mentor Hoxhaj, 16mars 2023
122 Rishikimi I kapaciteteve të sigurisë kibernetike në Republikën e Kosovës 2020, 2020, cybersecuritycapacityassessmentfortherepublicofkosovo2019pdf (ox.ac.uk), qasur më 20 mars 2023
123 Baza e të dhënave e SHARE Foundation, SHARE Monitoring (bird.tools), qasur më 29 mars 2023

Pavarësisht se janë të përcaktuara me ligj, këto raporte rrallë shkruhen dhe bëhen publike. Raporti për shkeljen e të dhënave përmban detajet e shkeljes së ndodhur dhe paraqet pasojat e kësaj shkeljeje për qytetarët e zakonshëm, ndërsa ky i fundit do të ofronte analiza më të thella mbi tendencat, modelet dhe pritshmërinë.[124] Një ekspert vuri në dukje se ka pasur shkelje të të dhënave në institucionet publike të cilat nuk janë komunikuar apo nuk është njoftuar publiku,[125] me arsyetimi se *front-end* ishte subjekt i sulmit, përderisa *back-end* mbeti i sigurt.[126] Për më tepër, zbulimi i përgjegjshëm duhet të parashikohet nga Ligji i ri për Sigurinë Kibernetike[127]. Zbulimi i përgjegjshëm nënkupton që kur zbulohet një gabim brenda një sistemi ose rrjeti, ai duhet të raportohet menjëherë te institucioni kompetent. Personi do të njoftohej dhe defekti do të mund të rregullohej në kohën e duhur. Legjislacioni aktual nuk e parashikon këtë mundësi.[128] Së fundmi, një vlerësim i kapaciteteve të sigurisë kibernetike i kryer në vitin 2020 e vlerësoi këtë fushë si formuese, që korrespondon me një notë mesatare në metodologjinë e vlerësimit.

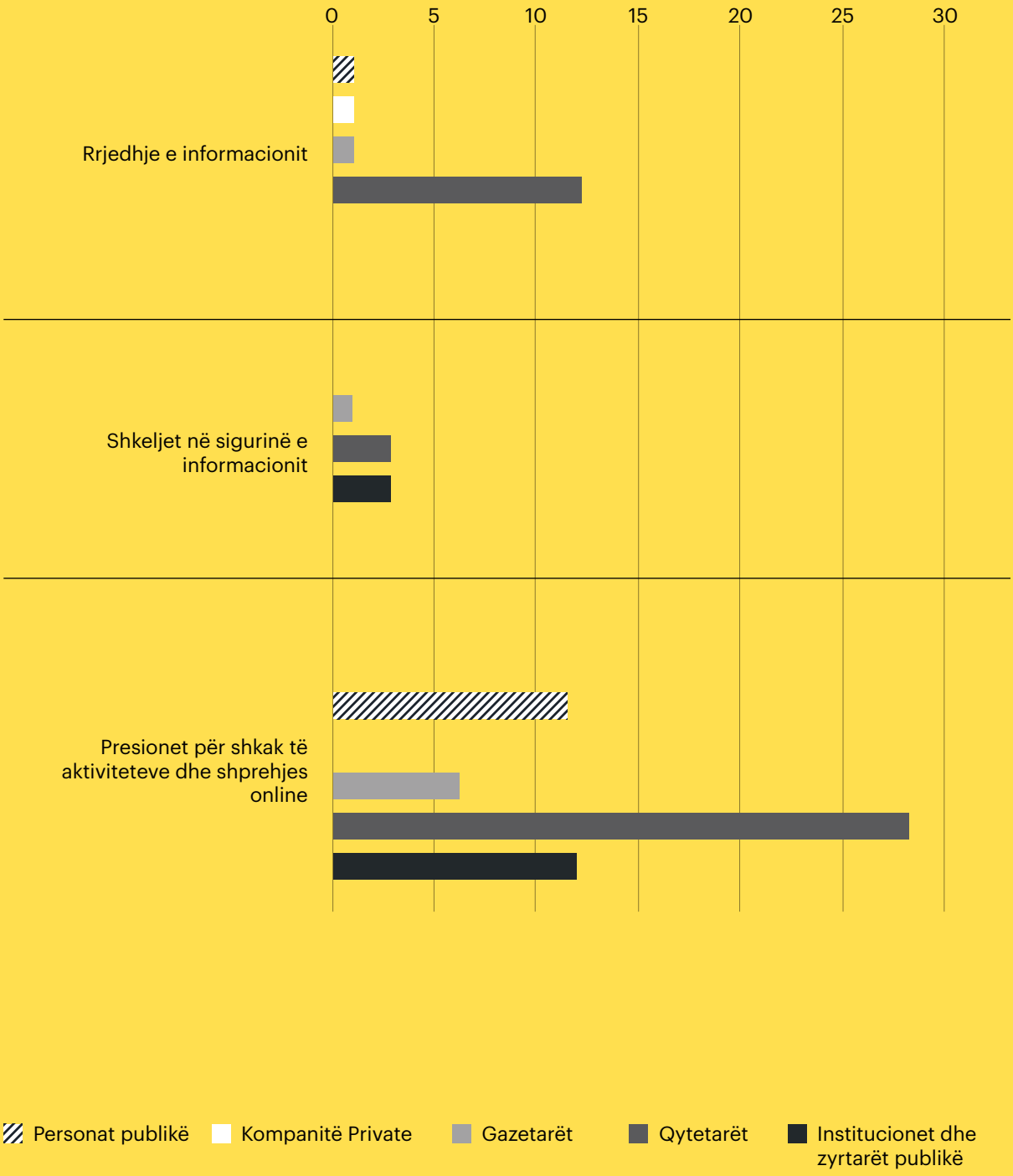
Disa raste të rrjedhjes së të dhënave të institucioneve publike janë vërejtur në Kosovë. BIRN ka raportuar për një rrjedhje të të dhënave personale nga uebfaqja e Komisionit Qendror të Zgjedhjeve[129], një peticion kundër Asociacionit të Komunave Serbe që përmbante të dhëna personale të pambikëqyrura[130], të dhëna personale të kompromentuara gjatë një sulmi kibernetik ndaj Telekomit të Kosovës.[131] Reagimi i Komisionerit të Agjencisë për Informim dhe Privatësi, AIP, është vlerësuar si i kufizuar. Marrë parasysh emërimin rishtazi të Komisionerit, pritet që puna e tyre të intensifikohet dhe të jetë më proaktive.

Share Foundation monitoron shkeljet e të drejtave digjitale në të gjitha vendet e Ballkanit Perëndimor, përfshirë Kosovën. Baza e të dhënave mbulon shkeljet e ndodhura nga marsi 2020 deri te më e fundit në korrik 2022. Grafiku i mëposhtëm tregon palët e prekura në të gjitha rastet e regjistruara.[132]

Në përfundim, të dhënat e paraqitura tregojnë se qytetarët janë më të prekurit kur bëhet fjalë për shkeljet online. Në 117 nga 178 raste, Fondacioni Share ka shenjëzuar vetëm qytetarët si të prekur, ndërsa zyrtarët publikë dhe institucionet shtetërore si të prekur në 52 raste. Sulmuesit ishin mediat online në 106 raste. Këto shifra mbështesin pretendimin se çështjet ligjore dhe politikat e sigurisë kibernetike duhet të jenë të orientuara drejt qytetarëve, pasi tregohet se ata janë kategoria më e prirë për të prekur nga sulmet kibernetike dhe shkeljet e të dhënave. Ky sistem i tërë kibernetik është i ndërlidhur dhe gjithë këto elemente duhet të jenë në një nivel të kënaqshëm që Kosova të ketë një strukture funksionale të sigurisë kibernetike dhe zbatueshmëri që vepron në dobi të sigurisë kombëtare dhe sigurisë individuale.

124 Intervistë me Mentor Hoxhaj, 16 mars 2023
125 Intervistë me Mentor Hoxhaj, 16 mars 2023
126 Intervistë me Mentor Vrajolli, 16 mars 2023
127 Intervistë me Mentor Hoxhaj, 16 mars 2023
128 Ibid.
129 BIRN, në Kosovo the Shqipëri, të dhënat personale janë të disponueshme, 2022, In Kosovo and Albania, Personal Data Up for Grabs | Balkan Insight, qasur më 15 mars 2023
130 Intervistë me Arianit Dobroshi, 15 mars 2023
131 BIRN, Kosova do të themelojë Agjencinë për Siguri Kibernetike pas sulmeve të fundit, 2022, Kosovo to Establish Agency for Cyber Security Amid Recent Attacks | Balkan Insight, qasur më 15 mars 2023
132 Baza e të dhënave e SHARE Foundation, SHARE Monitoring (bird.tools), qasur më 29 mars 2023

Figura 1: Palët e prekura në rastet e monitoruara në Kosovë



4. Përfundimet

Dikush mund të thotë se nuk zgjidhje ideale, por vetëm praktika të mira që mund të zbusin pasojat për shkak të kompleksitetit të çështjeve të paraqitura.[133] Meqenëse po shfaqen teknologji të reja dhe po avancohen ato ekzistuese, nuk ka kthim prapa nga ajo që është arritur në kuptimin teknologjik, por duhet të mësojmë t'i zbusim sfidat ekzistuese. Këto duhet të vlerësohen dhe të ri-vlerësohen vazhdimisht për shkak të natyrës progresive të tyre. Në njërën anë, këto procese përfshijnë shumë aksionarë dhe interesa, të cilat janë të lidhura dhe potencialisht të kundërta. Në anën tjetër, interneti është një platformë globale që është e qasshme në nivel botëror dhe duhet të merren parasysh shumë kontekste të ndryshme historike, politike, sociale, gjuhësore e të tjera. Ky fragmentim dhe kompleksitet gjithashtu shfaqet edhe në përpjekjen për krijimin e rregulloreve ligjore ndërkombëtare. Shtetet kanë për detyrë të mbrojnë, respektojnë dhe promovojnë të drejtat e njeriut dhe vetëm shtetet mund të mbajnë përgjegjësi për shkeljet e të drejtave të njeriut, prandaj përgjegjësia për të mbrojtur dhe mundësuar mbrojtjen e të drejtave të njeriut në hapësirat online bie mbi shtetet. Në përgjithësi, ngritja e bashkëpunimit mes shteteve dhe ndërmjetësve të internetit duhet të bëhet në një mënyrë që obligon ligjërisht ndërmjetësit e internetit të raportojnë mbi mënyrat e operimit, por shtetet gjithashtu duhet të vendosin kërkesa minimale për transparencë dhe bashkëpunim.

Nismat e ndërmarra tashmë, si në nivel ndërkombëtar ashtu edhe në nivel kombëtar, njohën rolin që po luajnë platformat e mediave sociale, si lehtësues por edhe kufizues, duke iu ndarë atyre rolin e udhëheqësit të lirisë së shprehjes në internet. Këto nisma synojnë të rrisin përgjegjshmërinë dhe transparencën e platformave.[134] Deri më tani, rregullat që udhëheqin algoritmet vendimmarrës nuk janë mjaftueshëm transparente dhe as shtetet as përdoruesit nuk janë të vetëdijshëm për kriteret që aplikohen në situata të caktuara dhe pse. Është e nevojshme që dokumentacioni që përdoret për moderimin dhe kurimin e përmbajtjes, të vihet në dispozicion dhe të jetë i qasshëm për shtetet. Përdoruesit duhet të njoftohen se përmbajtja e disponueshme për ta ka qenë subjekt i moderimit dhe kurimit të përmbajtjes, duke përfshirë një mundësi për të mos pranuar marrjen e vendimeve të automatizuara.[135]

Gjetjet e hulumtimit treguan se Kosova po bën përparim të qëndrueshëm në termat e strukturave ligjore dhe politikave. Pavarësisht progresit të konsiderueshëm,

133 Intervistë me Bojana Kostić, 07 mars 2023
134 Helberger, N. Helberger, N. Platforma e fuqisë politike: Si e përforëcojnë fuqinë e opinionit përpjektet aktuale për të rregulluar keqinformimin, Digital Journalism, 8:6, 842-854
135 Bukovska, B. Vëmendja në Inteligjencën Artificiale dhe liria e shprehjes, OSCE, 2020, 40

niveli i suksesit të Ligjit të ri për Sigurinë Kibernetike varet nga harmonizimi i tij me Ligjin për Infrastrukturën Kritike dhe ligjet e tjera që tashmë janë në fuqi. Pakoja e re e përbërë nga Ligji për Sigurinë Kibernetike, Strategjia Kibernetike dhe Plani i Veprimit do të avancojë institucionet dhe kapacitetet kibernetike në Kosovë. Ajo ka aftësinë për të centralizuar këtë çështje dhe për të përmirësuar efikasitetin e saj. Gjithashtu u theksua se institucionet e Kosovës kanë mungesë të kapaciteteve për të trajtuar çështjet e sigurisë kibernetike. Kjo çështje pritet të adresohet me krijimin e Qendrës Kombëtare për Trajnime. Kosova nuk ka mungesë të ekspertëve kibernetikë në sektorin privat, megjithatë bashkëpunimi mes sektorit privat dhe publik është i kufizuar. Çështja e PPP duhet të jepet prioritet dhe përfshirja e ekspertëve lokalë duhet të rritet, kështu që mbështetja e Kosovës në ekspertiza të huaja do të zvogëlohet. Gjetjet e kërkimit tregojnë se viktimat kryesore të sulmeve kibernetike në që kanë të bëjnë me privatësinë janë qytetarët e zakonshëm dhe ka hapësirë për përmirësimin e përgjegjshmërisë dhe transparencës së institucioneve publike në rastet kur ndodh një sulm kibernetik. Së fundi, sfidat me të cilat përballet Kosova janë të ngjashme me ato që hasen në vendet e tjera të Ballkanit Perëndimor, por edhe në të gjithë botën. Edhe pse Kosova ka një kornizë ligjore, ka qenë subjekt disa sulmeve kibernetike të cilat po ashtu kanë ndodhur edhe në shtetet tjera të Ballkanit Perëndimor. Përveç mungesës së domenit, Kosova është në pozitë të ngjashme me vendet e tjera të rajonit sa i përket rreziqeve dhe sfidave që lidhen me sigurinë kibernetike. Bashkëpunimi ndërmjet shteteve në rajon duhet të rritet për të rritur efikasitetin në luftimin e këtyre rreziqeve.

Si përfundim, siguria kibernetike, IA dhe të drejtat e njeriut janë dy koncepte të ndërlidhura që kërkojnë shqyrtim dhe balancim të kujdesshëm. Masat e sigurisë kibernetike janë të nevojshme për t'u mbrojtur nga kërcënimet kibernetike, ato nuk duhet të zbatohen në kurriz të të drejtave themelore të njeriut, si liria e shprehjes dhe privatësia. Zhvillimi dhe zbatimi i IA-së duhet të bëhet në mënyrë etike që respekton të drejtat themelore. Kjo përfshin sigurimin e një procesi vendimmarrës të drejtë dhe transparent, shmangien e paragjykimeve dhe diskriminimit, mbrojtjen e privatësisë dhe të dhënave personale, si dhe ruajtjen e llogaridhënies dhe përgjegjësisë. Bashkëpunimi i qëndrueshëm mes qeverive, kompanive private dhe përdoruesve është i nevojshëm për të krijuar një infrastrukturë digjitale që është e sigurt, e mbrojtur dhe respektuese ndaj të drejtave të njeriut. Është e rëndësishme të theksohet se teknologjitë digjitale ekzistojnë për të lehtësuar nevojat tona dhe jo për të kufizuar të drejtat e njeriut, dhe të dyja mund të realizohen në të njëjtën kohë me politikat dhe praktikat e duhura.

5. Rekomandimet

Qeveria e Kosovës:

- të sigurojë harmonizimin e Ligjit për Sigurinë Kibernetike me Ligjin për Infrastrukturën Kritike the ligje tjera të rëndësishme në Kosovë;
- të miratojë Strategjinë e re Kombëtare për Sigurinë Kibernetike dhe Planin e Veprimit që ofron udhëzime politikash për institucionet e sigurisë kibernetike, me theks të veçantë në zbatimin e një qasjeje të bazuar në të drejtat e njeriut;
- të zhvillojë dhe zbatojë plane për reagim ndaj incidenteve që të përgjigjet ndaj çdo incidenti të sigurisë kibernetike dhe të prezantojë sanksione të përshtatshme;
- të përmirësojë infrastrukturën digjitale në Kosovë, duke përfshirë pozicionin e saj në hapësirën kibernetike, duke prezantuar programe të avancuara për të procesuar dhe ruajtur të dhënat dhe të formojë serverët e vet cloud;
- përvetësimi i një kulture të sigurisë kibernetike që fillon nga koka e një organizate dhe vazhdon tek të gjithë punëtorët mund të ndihmojë në parandalimin e sulmeve kibernetike;
- investimi në programe trajnuese dhe edukative për profesionistë të sigurisë kibernetike, që mund të lehtësojë tutje themelimin e PPP;
- puna me shtete tjera për të përmirësuar bashkëpunimin ndërkombëtar për siguri kibernetike dhe IA, duke ndarë inteligjencën kërcënuese, njohuritë dhe praktikat më të mira;
- nisma për ndërgjegjësim dhe programe edukuese që kanë për target bizneset dhe individët duhet të bëhen për të promovuar ndërgjegjësimin e rreziqeve të sigurisë kibernetike, praktikave më të mira dhe sjelljes së përgjegjshme online;
- promovimi i IA-së në edukim, me synim rritjen e ndërgjegjes për zbatimin e IA-së

Sektori privat:

- mbështet themelimin e PPP-së përmes krijimit të një rrjeti vullnetar shkëmbyes;
- ndërlidhja e përfaqësuesve akademikë dhe jo qeveritarë për të rritur kapacitetet e tyre në sigurinë kibernetike dhe IA-në;

Akademia dhe sektori jo qeveritar:

- të rritet edukimi rreth sigurisë kibernetike IA-së në të gjitha nivelet në mënyrë që të promovohet ndërgjegjësimi;
- të përvetësojë i bashkëpunimit me të dyja, sektorin privat dhe atë public, duke synuar të adoptojë një qasje gjithëpërfshirëse ndaj sigurisë kibernetike dhe IA-së;
- të forcojë aftësitë për të mbikëqyrur institucionet publike në fushën e sigurisë kibernetike dhe IA-së

6. Bibliografia

Shkrimet akademike

Bromell D, Rregullimi i fjalës së lirë në një epokë digjitale: urrejtja, dëmtimi dhe kufijtë e censurës. Springer, 2022

Cains, M. et al, Përcaktimi i sigurisë kibernetike dhe rrezikut të sigurisë kibernetike brenda një konteksti multi-disciplinar duke përdorur nxjerrjet e ekspertëve, Analiza e Rrezikut, një publikim zyrtar i Shoqërisë për analiza rreziku, 2021, Author: Cains, Mariana G : Search (wiley.com), qasur më 15 shkurt 2023

Burton, J. Sulmet kibernetike dhe liria e shprehjes: Shtrëngimi, frikësimi dhe pushtimi virtual, Studimet Evropiane të gazetarisë Baltike, Universiteti i Teknologjisë i Talinit, Vol. 9, No. 3 (28), 117-132

McCarthy, J. Çka është inteligjenca artificiale?, Universiteti i Stanfordit, 2007

Liaropoulos, A. Një qasje njerëzore në qendër të sigurisë kibernetike: Sigurimi i njeriut në epokën e kiberfobisë, Journal of Information Warfare, 14, 4, 2015, (PDF) A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia, Journal of Information Warfare, 14, 4 (2015). (researchgate.net), qasur më 20 mars 2023

Risse,M. Gjenerata e katërt e të drejtave të njeriut: Të drejtat epistemike në botën digjitale, Qendra për të drejtat e njeriut, Shkolla Harvard Kennedy, Universiteti i Harvardit, 2021

Helberger, N. Platforma e fuqisë politike: Si e përforcojnë fuqinë e opinionit përpjekjet aktuale për të rregulluar keqinformimin, Digital Journalism, 8:6, 842-854

Neuberger, C.. “Meinungsmacht im Internet aus Kommunikationsëissenschaftlicher Perspektive.” *UFITA* 82 (1): 53–68, 2018

Pavlova, P. ‘Qasja e bazuar në të drejtat e njeriut ndaj sigurisë kibernetike: Adresimi i rreziqeve të sigurisë së grupeve të synuara’, Peace Human Rights Gorvenance, 4(3), 391-418, 2020, PHRG-2020-3-04.pdf (padovauniversitypress.it), qasur më 20 prill, 2023

Sekalala, S. et al, Analiza e impaktit të të drejtave të njeriut në rritjen e vrojtimit digjital të shëndetit publik përgjatë krizës me COVID-19, Health and Human Rights Journal, Volumi 22/2, dhjetor 2020, 7 / 20, https://www.hhrjournal.org/2020/12/analyzing-the-human-rights-impact-of-increased-digital-public-health-surveillance-during-the-covid-19-crisis/, qasur më 01 mars 2023

Zhou, Y, & Shen, L. Paragjykimi i konfirmimit dhe vazhdimësia e keqinformimit mbi ndryshimet klimatike. Hulumtim mbi komunikimin, 49(4), 500-523, 2022, https://doi.org/10.1177/00936502211028049, qasur më 07 prill 2023

Legjislacioni

Draft strategjia për sigurinë kibernetike në Kosovë 2023-2027, versioni i propozuar _0.1 2022-12-30, 2022, Anglsht-DRAFT-Strategjia-per-siguri-kibernetike_V2.0_06032023.DOCX (live.com)

Ligji për sigurinë kibernetike, 2023

Deklarata universale për të drejtat e njeriut, 1984

Propozimi i kornizës rregullatore të BE-së për inteligjencën artificiale, Regulatory framework proposal on artificial intelligence | Shaping Europe's digital future (europa.eu)

Komiteti Evropian, Ligji i BE-së për siguri kibernetike, The EU Cybersecurity Act | Shaping Europe's digital future (europa.eu)

Special Rapporteur në promovimin dhe mbrojtjen e të drejtës së lirisë së mendimit dhe shprehjes, mbikëqyrja dhe të drejtat e njeriut, A'/HRC/41/35, 2019, 7

Asambleja e Këshillit të Evropës, Nevoja për qeverisje demokratike, Rezoluta 2341, 2020, 1

Konventa e krimeve kibernetike: Edicioni special dedikuar propozuesve të konventës (1997-2001), Këshilli i Evropës, 2022, 1680a6992e (coe.int)

Parlamenti Evropian, Inteligjenca Artificiale, 2023, Artificial intelligence (europa.eu)

Komisioni Evropian, Propozimi për rregulloren e Parlamentit Evropian dhe te Këshillit që përcakton rregulla të harmonizuara mbi Inteligjencën Artificiale (Akti i Inteligjencës Artificiale) dhe ndryshimin e akteve legjislative të BE-së COM (2021)206, 2020

Qëndrim i shkruar i Federatës Ruse në Gjykatën Ndërkombëtare të Drejtësisë, 2009, 15628.pdf (icj-cij.org), qasur më 07 prill 2023

Qëndrim i shkruar i Republikës Popullore të Kinës në Gjykatën Ndërkombëtare të Drejtësisë në çështjen e Kosovës, 2009, 15611.pdf (icj-cij.org), qasur më 07 prill 2023

Artikuj lajmesh

Al Jazeera, Cilat shtete e njohin shtetësinë e Kosovës?, 2023, Which countries recognise Kosovo's statehood? | Infographic News | Al Jazeera, qasur më 07 prill 2023

BBC, Izbori u Srbiji 2020: Šta sve mogu naprednjaci sa dvotrećinskom većinom u skupštini [What can progressive do ëith a tëo-third majority in the Assembly], 2020, Izbori u Srbiji 2020: Šta sve mogu naprednjaci sa dvotrećinskom većinom u skupštini - BBC Neës na srpskom, qasur më20 mars 2023

BIRN, në Kosovë the Shqipëri, të dhënat personale janë të disponueshme, 2022, In Kosovo and Albania, Personal Data Up for Grabs | Balkan Insight, qasur më 15 mars 2023

BIRN, Kosova do të themelojë Agjencinë për Siguri Kibernetike pas sulmeve të fundit, 2022, Kosovo to Establish Agency for Cyber Security Amid Recent Attacks | Balkan Insight, qasur më 15 mars 2023

Endgadget, Programi i policisë për njohje të fytyrës keqidentifikon 2,300 njerëz si kriminiel potencial, 2018, Police face recognition misidentified 2,300 as potential criminals | Engadget, qasur më 01 prill 2023

Forbes, Njohja e fytyrës shkelë të drejtat e njeriut, vendosë gjykata, 2020, Facial Recognition Violates Human Rights, Court Rules (forbes.com), qasur më 01 prill 2023

Forbes, Vlerat e rangimit të rezultateve të kërkimeve, 2017, The Value Of Search Results Rankings (forbes.com)

Jeremić et al, Facebook, Twitter duke luftuar kundër shkeljeve të përmbajtjes në Ballkan, BIRN, 2021, Facebook, Twitter Struggling in Fight against Balkan Content Violations | Balkan Insight, qasur më 15 mars 2023

The Atlantic, Programi i njohjes së fytyrës mund të ketë një problem paragjykimi racor, 2016, Facial-Recognition Softëare Might Have a Racial Bias Problem - The Atlantic, qasur më 01 prill 2023

The Guardian, Twitter fshinë 20,000 llogari të rreme që lidheshin me qeverinë Saudite, Serbe dhe Egjiptiane, 2020, Izbori u Srbiji 2020: Šta sve mogu naprednjaci sa dvotrećinskom većinom u skupštini - BBC Neës na srpskom, qasur me 20 mars 2023

The New York Times, Një muaj, 500,000 skanime fytyrash: Si po e përdorë Kina IA për profilizim të një minoriteti, 2019, One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority - The New York Times (nytimes.com), qasur më 01 prill 2023

Raporte

Knockel, J. et al, Ne bisedojmë, ata shikojnë se si përdoruesit ndërkombëtarë ndërtojnë pa dashje aparatin e censurimit kinez të WeChat, CitizensLab, 2020, https://citizenlab.ca/2020/05/we-chat-they-watch/, qasur më 18 shkurt 2023

Najibi, A, Diskrimini racor në teknologjinë e njohjes së fytyrës, Universiteti i Harvardit, Racial Discrimination in Face Recognition Technology - Science in the News (harvard.edu), 2020, 07 prill 2023

Amnesty International, Amnesty International në mesin e objektivave të fushatës së fuqizuar nga NSO, 2018, https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/,qasur më 07 prill 2023

Human Rights Watch, Rregullat për realitetin e ri të vëzhgimit, 2019, https://www.hrë.org/news/2019/11/18/rules-new-surveillance-reality, qasur më15 mars 2023.

Asociacioni për komunikim progresiv, Pse siguria kibernetike është çështje e të drejtave të njeriut, dhe është koha ta trajtojmë si të tillë, 2022, https://www.apc.org/en/news/why-cybersecurity-human-rights-issue-and-it-time-start-treating-it-one qasur më 1 shkurt 2023

Asociacioni për komunikim progresiv, APC policy explainer: A human rights-based approach to cybersecurity | Association for Progressive Communications, qasur më 01 shkurt 2023

Bukovska, B. Vëmendja në Inteligjencën Artificiale dhe liria e shprehjes, OSCE, 2020

Kostić, B. Kurthet e IA-së dhe diversiteti i mediave: kujdes boshllëqet, Media Diversity Institute, 2021, https://www.media-diversity.org/artificial-intelligence-traps-and-media-diversity-mind-the-loopholes/, qasur më 01 shkurt 2023

Sulmi kibernetik në Bankën Ekonomike të Kosovës, Raporti mbi ekosistemin në sigurinë kibernetike, Ballkani Perëndimor: Kërcënimet kibernetike në rritje, PwC, 2022, 30, PwC-Cybersecurity-Ecosystem-Report-WB.pdf (isac-fund.org), qasur më 20 mars 2023

Raporti mbi ekosistemin në sigurinë kibernetike, Ballkani Perëndimor: Kërcënimet kibernetike në rritje, PwC, 2022, 30, PwC-Cybersecurity-Ecosystem-Report-WB.pdf (isac-fund.org), qasur më 20 mars 2023

Siguria kibernetike dhe të drejtat e njeriut në Ballkanin Perëndimor: Harta e qeverisjes che aktorëve, DCAF-Geneva Centre for Security Sector Governance, 2022, CybersecurityHumanRightsËesternBalkans_EN_March2023.pdf (dcaf.ch), qasur më 18 shkurt 2023

Rishikimi i kapaciteteve të sigurisë kibernetike në Republikën e Kosovës 2020, 2020, cybersecuritycapacityassessmentfortherepublicofkosovo2019pdf (ox.ac.uk), qasur më 20 mars 2023

Portali DataRe, Digital 2023: Kosova, 2023, Digital 2023: Kosovo — DataReportal – Global Digital Insights, qasur më 20 mars 2023

Human Rights Watch, Është koha ta trajtojmë sigurinë kibernetike si çështje e të drejtave të njeriut: Të mëdhenjtë e kibernetikës SHBA dhe Rusia ishin të heshtur në të drejta, 2020, https://www.hrw.org/neës/2020/05/26/its-time-treat-cybersecurity-human-rights-issue, qasur më 5 mars 2023

Digital Guardian, Çka është siguria kibernetike? Definicioni, praktikat më të mira dhe shembuj, 2022, https://www.digitalguardian.com/blog/what-cyber-security, qasur më 5 maj, 2023

Gjithçka që duhet të dini për "të drejtën për t'u harruar", GDPR EU, Everything you need to know about the "Right to be forgotten" - GDPR.eu, qasur më 25 mars 2023

Freedom on the Net 2022, Kundër një rishikimi autoritar të internetit, Freedom House 2023

ICNL, Protestimi në epokën e vëzhgimit qeveritar, 2023, Protesting in an Age of Government Surveillance - ICNL, qasur më 25 mars 2023

Prezantimi i të drejtave digjitale, Share Foundation, 2021

Kosova ka ndërmarrë hapa kritikë në sigurinë kibernetike, thotë vlerësimi i ri i modelit të maturimit të kapaciteteve të sigurisë kibernetike, Banka Botërore, 2020, Kosovo Has Undertaken Critical Steps in Cybersecurity, Says New Cybersecurity Capacity Maturity Model Assessment (ëorldbank.org), qasur më 20 mars 2023

Kostić B, Sinders C, Inteligjenca Artificiale e përgjegjshme, Këshilli i Evropës, 2022, 15

Kovacs, A, Hawtin, D. (2013) 'Siguria kibernetike, vëzhgimi kibernetik dhe të drejtat e njeriut në internet', Global Partners Digital, Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf (gp-digital.org), qasur më 05 mars 2023

Leslie D et al. Inteligjenca Artificiale, të drejtat e njeriut, demokracia, dhe sundimi i ligjit: Së pari. Këshilli i Evropës, 2021

Strategjitë kombëtare të sigurisë kibernetike në ekonomitë e Ballkanit Perëndimor: Kosova, DCAF- Geneva Centre for Security Sector Governance, 2021, NationalCybersecurityStrategiesWB_2021.pdf (dcaf.ch), qasur më 20 mars 2023

Pirkova, E. et al, Vëmendja në Inteligjencën Artificiale dhe liria e shprehjes – Një manual politikash, OSCE, 2021

Korniza rregullatore në fushën e të drejtave digjitale, analizë krahasuese: Shqipëria, Bosjna dhe Hercegovina, Kosova, Mali i Zi, Maqedonia e Veriut, Serbia, 2021, Digital-rights-legal-analysis_EN-1.pdf (sharefoundation.info), qasur më 25 mars 2023

Grupi i zhvillimit të qëndrueshëm në OKB, UNSDG | Human Rights-Based Approach, më 25 mars 2023

Whitepaper në Inteligjencës Artificiale – Një qasje evropiane ndaj përsosmërisë dhe besimit, COM(2020) 65 final

Zuiderveen Borgesius, F. Diskriminimi, inteligjenca artificiale, dhe algoritmet e vendim-marrjes. Këshilli i Evropës, Drejtorati i Përgjithshëm i Demokracisë, 2018. https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decisionmaking/1680925d73 qasur më 05 mars 2023

Website

Apple Inc. Kërkesat nga llogaritë, https://www.apple.com/legal/transparency/account.html, qasur më 01 mars 2023

Faqja në internet e Koalicionit të Lirisë Online, 2022, https://freedomonlinecoalition.com/members/qasur me 01 mars, 2023

Geneva Internet Platform DigWatch, UN OEËG, UN OEWG in 2023 - DW Observatory (dig.watch), qasur më 29 mars, 2023

IBM Cloud, https://www.ibm.com/topics/artificial-intelligence, qasur më 27 shkurt, 2023

Vëzhgimi në masë, Privacy International, https://privacyinternational.org/learn/mass-surveillance, qasur më 20 mars 2023

Privatësia dhe mbrojtja e të dhënave, Këshilli i Evropës, Council of Europe Data Protection website - Data Protection (coe.int), qasur më 10 mars 2023

Baza e të dhënave e SHARE Foundation, SHARE Monitoring (bird.tools), qasur më 29 mars 2023

Zyra e OKB për çështje të çarmatimit, Grupi i ekspertëve qeverisës, Group of Governmental Experts – UNODA qasur më 29 mars, 2023

Misioni në Kosovë i OKB-së, Mandate | UNMIK (unmissions.org), qasur më 07 prill 2023

Rreth autorit

Imane Bellaadem is human rights defender and activist from BiH. She completed her BA in Law and a MA in human rights and democracy at the University of Sarajevo. Currently, Imane is working on issues concerning civil and political rights in the region, environment for human rights defenders and freedom of expression. Her interests are civil rights, minorities, and environmental human rights.