Geneva Centre for Security Sector Governance

Foreign, Commonwealth & Development Office

Institute for Democracy and Mediation
Instituti për Demokraci dhe Ndërmjetësim

Përmbledhje e gjetjeve të studimit

Tejkalimi i hendekut mes sigurisë kibernetike dhe të drejtave të njeriut

Megi Reçi dhe **Sara Kelmendi**

Instituti për Demokraci dhe Ndërmjetësim

Metodologjia

Shqyrtimi i literaturës

Kuadri ligjor dhe strategjik; vendime të gjykatave vendase; vendime të institucioneve të pavararua; studime dhe raporte; kërkesa për informacion etj.

Pyetësori anonim

U plotësua elektronikisht në mënyrë anonime nga 19 aktivistë, gazetarë dhe përfaqësues të OSHC-ve. Kishte qëllim hartëzimin e rasteve të shkeljeve dhe reagimin institucional.

15 intervista të thelluara

Me ekspertë të të drejtave të njeriut, aktivistë, gazetarë, juristë, përfaqësues të institucione të sigurisë kibernetike, përfaqësues të institucioneve të pavarura, përfaqësues të organizatave të shoqërisë civile etj.

4 takime validuese

Përfshinë aktorë të ndryshëm publikë dhe jo publikë. Kishin qëllim konsultimin/validimin e gjetjeve paraprake dhe rekomandimeve kryesore para publikimit të studimit.

Kuadri ligjor, institucional dhe politik për sigurinë kibernetike

MANGËSI DHE SFIDA

- Legjislacioni penal nuk mbulon përndjekjen (stalking) në internet.
- Legjislacioni penal nuk mbulon plotësisht krimet e motivuara nga urrejtja/diskriminimi, por është i kufizuar tek motivet e racizmit dhe ksenofobisë.
- Legjislacioni anti-diskriminim nuk mbulon rastet e vendimmarrjes automatike diskriminuese.
- Mungesa e rregullimeve ligjore të plota në lidhje me median online dhe nevoja për të balancuar rregullimin potencial me mbrojtjen nga censura.
- Mungesa e rregullimeve ligjore për mbrojtjen e lirisë së tubimit në internet.

Kuadri ligjor, institucional dhe politik për sigurinë kibernetike

MANGËSI DHE SFIDA

Aktorë të natyrave të ndryshme janë të përfshirë në çështjet e sigurisë kibernetike. (institucione të qeverisjes qëndrore dhe instituticione të pavarura.)

Këto agjenci janë të natyrës më shumë teknike se sa politikëbërëse.

Institucione të reja po krijohen - Qendra Kombëtare e Operacioneve të Sigurisë Kibernetike dhe Qendra e Ekselencës për Sigurinë Kibernetike.

Vështirësitë në koordinim dhe mosndarja e qartë e detyrave mund të zbehin kufinjtë e përgjegjësisë, llogaridhënies dhe kontrollit.

Dokumenteve strategjikë të sigurisë kibernetike u mungon qasja e të drejtave të njeriut, ndërsa në dokumentet strategjikë për mbrotjen e të drejtave të njeriut mungon dimension i sigurisë.

Konsultimet e këtyre dokumenteve nuk janë ndërsektoriale dhe mjaftueshëm gjithëpërfshirëse.

SFIDA TË TJERA TË IDENTIFIKUARA

MUNGESA E TË DHËNAVE TË DISAGREGUARA

për krimet e motivuara nga urrejtja dhe diskriminimi në nivel kombëtar.

NUMRI I ULËT I RAPORTIMEVE DHE PANDËSHKUESHMËRIA

për shkeljet e të drejtave të njeriut në internet.

BURIMET NJERËZORE DHE KAPACITETET TEKNIKE TË KUFIZUARA

të agjencive ligjzbatuese dhe institucioneve të pavarura të të drejtave të njeriut.

MUNGESA E PËRGJITHSHME E NDËRGJEGJËSIMIT PUBLIK NË LIDHJE ME KËTO ÇESHTJE

Kuadri gjithëpërfshirës ligjor dhe institucional dhe vëmendja e politikave që i kushtohet mbrojtjes së fëmijëve në internet.

I vetmi dokument strategjik për çështjet e sigurisë kibernetike me qasje të të drejtave të njeriut ishte Plani i Veprimit për një internet më të sigurtë për fëmijët në Shqipëri 2018-2020.

Kuadri ligjor, institucional dhe politik për sigurinë kibernetike

PRAKTIKA TË MIRA

Siguria kibernetike dhe ndalimi i diskriminimit

GJETJET KRYESORE

Format më të përhapura të diskriminimit të identifikuara në hapësirën kibernetike: gjuha e urrejtjes dhe ngacmimi (shqetësimi).

Grupet më të targetuara: gratë, fëmijët, minoritetet (Romët, Egjiptianët, LGBTI+, PAK), Mbrojtësit e të Drejtave të Njeriut (veçanërisht aktivistet gra dhe LGBTI+).

Praktika institucionale e Komisionerit për Mbrojtjen nga Diskriminimi ka adresuar raste të:

- Gjuhës së urrejtjes ndaj Romëve, Egjiptianëve, LGBTI+, PAK;
- Vendimmarrjes automatike diskriminuese.

Në rastet e idetifikuara diskriminimi ka ardhur nga:

- Politikanë dhe figura të tjera publike
- Media online dhe komentet që kanë pasuar publikimet e tyre
- Institucionet publike

- Mungon praktika gjyqësore për rastet e diskriminimit në hapësirën kibernetike.
- Institucionet ligjzbatuese janë më pak reaguese/të ndjeshme ndaj rasteve të diskriminimit, në krahasim me institucionet e pavarura të të drejtave të njeriut.
- Numri i ulët i raportimeve dhe mungesa e besimit tek institucionet ligjzbatuese nga ana e grupeve të diskriminuara, për shkak të pandëshkueshmërisë.
- Mungesa e ndërgjegjësimit dhe debatit publik në lidhje me format më komplekse të diskriminimit si p.sh. vendimmarrja automatike diskriminuese, paragjykimet algoritmike, diskriminimi i shumëfishtë.
- Mungesa e të dhënave statistikore të disagreguara në lidhje me krimet e urrejtjes, krimet seksuale që kryhen në hapësirën kibernetike, nuk lejon kryerjen e analizave të plota që informojnë politikat dhe masat që duhen ndërmarrë.
- Mungesë e të dhënave në lidhje me grupet që nuk kanë akses në internet, u mungojnë njohuritë dixhitale apo kanë nevojë për shërbime të përshtatura, nuk lejon kryerjen e vlerësimeve të riskut për të drejtat e njeriut në kuadër të dixhitalizimit të shërbimeve publike.

Siguria kibernetike dhe ndalimi i diskriminimit

MANGËSI DHE SFIDA

- Përfshirja ndërsektoriale në Aleancën Kundër Gjuhës së Urrejtjes;
- Studimet dhe monitorimet e kryera në lidhje me përdorimin e gjuhës së urrejtjes në internet;
- Përfshirja e OSHC-ve në raportimin/referimin e rasteve të ngacmimeve të të miturve në internet;
- Masat e parashikuara në lidhjet me krimet e urrejtjes dhe gjuhën e urrejtjes në Planin Kombëtar të Veprimit për Barazinë, Përfshirjen dhe Pjesëmarrjen e Romëve dhe Egjiptianëve 2021-2025.

Siguria kibernetike dhe ndalimi i diskriminimit

PRAKTIKA TË MIRA

Siguria kibernetike dhe liria e tubimit paqësor

GJETJET KRYESORE

Mungon rregullimi dhe debati publik në lidhje me mbrojtjen e lirisë së tubimit në internet.

Janë identifikuar disa forma të cënimit, intimidimit ose dekurajimit të aktivistëve që lidhen me ushtrimin e lirisë së tubimit në internet.

Nuk ka patur raste të kufizimit apo bllokimit të internetit para, gjatë, ose pas organizimit të një proteste.

Nuk ka patur raste të bllokimit të komunikimeve elektronike para, gjatë, ose pas organizimit të një proteste.

Siguria kibernetike dhe liria e tubimit paqësor

MANGËSI DHE SFIDA

Format e identifikuara të cënimit, intimidimit ose dekurajimit të ushtrimit të lirisë së tubimit në internet:

- Targetimi i aktivistëve të angazhuar në organizim protestash nëpërmjet fushatave të përbaltjes;
- Raportime të koordinuara të profileve të aktivistëve në rrjete sociale;
- Monitorimi i aktivitetit të aktivistëve në rrjete sociale;
- Referimi në mënyrë arbitrare i statuseve të bëra në *Facebook* në momentin e ngritjes së akuzës penale mbi aktivistët, duke i identifikuara ata si organizatorë;
- Shkelje të të drejtës për t'u mos vetëinkriminuar duke u kërkuar aktivistëve akses në profilet dhe komunikimet e tyre private, gjatë marrjes në pyetje në lidhje me një protestë;
- Sulme kibernetike mbi media të pavarura gjatë raportimit të protestave.

Siguria kibernetike dhe liria e tubimit paqësor

PRAKTIKA TË MIRA

- Rritja e përdorimit të rrjeteve sociale dhe internetit në përgjithësi për të koordinuar, organizuar, mobilizuar protesta përgjatë viteve të fundit. (kulmoi gjatë pandemisë)
- Roli pozitiv i mediave të pavarura që aplikojnë modelin e gazetarisë qytetare, në raportimin e protestave në kohë reale.
- Ndërgjegjësimi i disa grupeve të aktivistëve në lidhje me përdorimin e platformave më të sigurta të komunikimit ndërmjet tyre për qëllime koordinimi.

Siguria kibernetike dhe e drejta e privatësisë

ÇËSHTJET KRYESORE

Rrjedhjet e të dhënave në 2021 nxorrën në pah copëzimin e qeverisjes së sigurisë kibernetike në Shqipëri dhe mungesën e zbatimit të standardeve për mbrojtjen e të dhënave personale.

Hetime sipërfaqësore nga ana e institucioneve kryesore dhe mungesë e llogaridhënies.

Ruajtja e infrastrukturës fizike të e-Albania i është ngarkuar një përpunuesi privat, duke e përjashtuar atë nga përgjegjësia për të zbatuar ligjet e mbrojtjes së të dhënave.

Marrëveshjet me palët e treta duhet të përfshijnë qasjen e menaxhimit të rrezikut, duke përcaktuar qartë detyrimet dhe përgjegjësitë e secilës palë dhe duke marrë në konsideratë kapacitetin e institucioneve shtetërore për monitorimin dhe zbatimin e masave efektive të menaxhimit të rrezikut.

Siguria kibernetike dhe e drejta e privatësisë

GJETJET KRYESORE

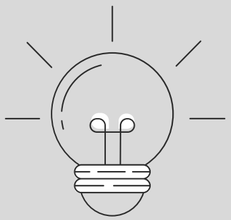
Marrëveshja me JGI paraqet një mundësi për të hartuar kuadrin e sigurisë kibernetike në Shqipëri duke angazhuar në mënyrë të barabartë aktorë publikë dhe jopublikë si OJQ-të, sektorin privat dhe qytetarët, për të ndarë përgjegjësinë e respektimit të parimeve të privatësisë.

Mungesë e mekanizmave bashkëkohorë për raportimin e kërcënimeve të sigurisë.

Mungesa e burimeve njerëzore dhe pajisjet teknike të vjetëruara reduktojnë efikasitetin e Njësisë së Krimit Kibernetik.

Shkeljet e të drejtës së privatësisë Online kanë cënuar një sërë aktivistësh politikë dhe të të drejtave të njeriut *(doxing)*, gazetarë *(akses i paautorizuar i të dhënave)*, ndërkohë që shumë gra dhe vajza kanë rënë pre e shfrytëzimeve seksuale *(revenge porn, sextortion)*.

- Me rritjen e formave online për censurimin që shtypin kritikën dhe promovojnë propagandën qeveritare, gazetaria e pavarur përballet me sfida në rritje, të cilat janë të një natyre institucionale dhe etike.



Praktikë e mirë: Themelimi i Aleancës për Median Etike e cila mund të mundësojë zmbrapsjen nga qasja e “rregullimit shtetëror të medias”, ndërkohë që promovon vetë-rregullimin dhe raportimin etik.

Siguria kibernetike dhe liria e shprehjes

PËRPJEKJET E QEVERISË PËR TË CENTRALIZUAR INFORMACIONIN PËFSHIJNË:

- Paketa Anti-shpifje e propozuar në 2019 e cila synonte të institucionalizonte kontrollin e medias online
- Agjencia për Media dhe Informacion e cila pritet të monitorojë median online si dhe të menaxhojë marrëdhëniet dhe komunikimin mes ministrive dhe medias
- Qeverisja përmes medias sociale, që zëvendësoi përkohësisht median tradicionale dhe median e pavarur online gjatë izolimit për shkak të pandemisë
- Censurimi politik, që mundësohet prej një kompanie të menaxhimit të të drejtave digjitale.

Siguria kibernetike dhe liria e shprehjes

ÇËSHTJET KRYESORE

PËRSA I PËRKET LIRISË SË SHTYPIT ONLINE, SHKELJET MË TË RËNDA KANË QENË:

- Mbyllja e një website (JOQ Albania) nën akuzën e shkaktimit të panikut
- Konfiskimi i pajisjeve dhe intimidim i gazetarëve për të zbuluar burimet e tyre të informacionit (Lapsi.al)
- Fushata shpifjeje online kundra gazetarëve (gratë gazetare janë veçanërisht të targetuara)
- Sulme Distributed Denial-of-Service (DDoS) drejtuar mediave që janë kritike ndaj qeverisë ose fshirje e artikujve (Acromax)

Siguria kibernetike dhe liria e shprehjes

ÇËSHTJET KRYESORE

PËRSA I PËRKET LIRISË PËR TË SHPËRNDARË INFORMACION DHE IDE ONLINE, STUDIMI THEKSOI:

- Raste aktivistësh të cilët kanë qenë pre e survejimit elektronik, e raportimeve të koordinuara ose janë proceduar penalisht për shkak të postimeve kritike ndaj qeverisë.

- Gjatë izolimit për shkak të pandemisë, konferencat për shtyp ishin të paaksesueshme për gazetarët, duke i bërë kështu grupet si PAK dhe qytetarët me akses të limituar në internet më të cënueshëm ndaj keqinformimit online apo duke ua kufizuar më tej hapësirat e informimit.

Siguria kibernetike dhe liria e shprehjes

ÇËSHTJET KRYESORE

Rekomandime për aktorët publikë

(Qeveria, Parlamenti dhe institucionet ligjzbatuese)

Mbi kuadrin ligjor:

·Duhet ndryshuar Kodi Penal në lidhje me krimet me motive diskriminimi ose urrejtje për të siguruar mbrotje në hapësirën kibernetike.

·Duhet ndryshuar Kodi Penal për të trajtuar rastet e përndjekjes online.

·Duhet miratuar legjislacioni anti-SLAPP për të forcuar garancinë ligjore për mbrojtjen e lirisë së shprehjes duke trajtuar kontekstin online dhe offline.

·Duhet ndryshuar Ligji për Mbrojtjen nga Diskriminimi për të adresuar në mënyrën e duhur format e diskriminimit që ndodhin në hapësirën kibernetike dhe vendimmarrjen automatike diskriminuese.

·Duhet ndryshuar Ligji për Tubimet për të ofruar garancitë e nevojshme për tubimet online.

·Duhen bërë ndryshimet e nevojshme në legjislacionin mbi mediat dhe atë mbi komunikimet elektronike për të dhënë një përkufizim të unifikuar ligjor të përmbajtjes së dëmshme dhe të paligjshme dhe për të përcaktuar me ligj autoritetet që mund të kërkojnë fshirjen e përmbajtjeve të tilla në internet.

Rekomandime për aktorët publikë

(Qeveria, Parlamenti dhe institucionet ligjzbatuese)

Mbi kuadrin politik:

·Duhet zbatuar një qasje ndërsektoriale për politikëbërjen në fushën e sigurisë kibernetike dhe të drejtave të njeriut në mënyrë që dokumentet e sigurisë kibernetike të konsiderojnë aspektet e të drejtave të njeriut dhe dokumentet strategjike të të drejtave të njeriut të trajtojnë dimensionin e sigurisë kibernetike.

·Duhet të zhvillohen procese konsultimi gjithëpërfshirëse mes institucioneve të sigurisë kibernetike, institucioneve të pavarura të të drejtave të njeriut dhe aktorëve jopublikë, kur hartohen dokumenta strategjikë.

·Duhet të kryhen vlerësime të riskut të të drejtave të njeriut për të mitiguar risqet e diskriminimit dhe për të siguruar vendimmarrje të bazuar në prova sa i përket dixhitalizimit të shërbimeve publike.

·Duhet të krijohet një sistem i unifikuar dhe gjithëpërfshirës i mbledhjes së të dhënave për krimet me motive diskriminimi/urrejtje, duke trajtuar kontekstin online dhe offline.

Rekomandime për aktorët publikë

(Qeveria, Parlamenti dhe institucionet ligjzbatuese)

Mbi kuadrin politik:

·Duhet zbatuar një qasje mbikëqyrje dhe kontrolli që lejon ndarjen e përgjegjësisë së aktorëve publikë dhe privatë në mbrojtjen e privatësisë në hapësirën kibernetike dhe formësimin e një politikëbërje gjithëpërfshirëse.

·Duhet të merren masa urgjente për të forcuar garancitë e mbrojtjes së të dhënave personale dhe përputhshmërinë e marrëveshjeve ndërinstitucionale dhe atyre me subjektet private.

·Duhet të rritet transparenca në lidhje me modalitetet e ruajtjes së të dhënave mbi informacionin personal të identifikueshëm dhe transferimit të tij tek palët e treta.

·Duhet të merren masa të përshtatshme për t'u mundësuar autoriteteve publike të zgjerojnë monitorimin e zbatimit të masave minimale të sigurisë për çdo palë nënkontraktore të operatorëve që administrojnë infrastrukturën kritike të informacionit, për të rritur përgjegjshmërinë e sektorit privat.

Rekomandime për aktorët publikë

(Qeveria, Parlamenti dhe institucionet ligjzbatuese)

Mbi kapacitetet dhe bashkëpunimin institucional:

·Duhet të përmirësohet bashkëpunimi ndërmjet institucioneve të sigurisë kibernetike dhe institucioneve të pavarura të të drejtave të njeriut në shkëmbimin e informacionit dhe ekspertizës, në rastet e shkeljeve të të drejtave të njeriut në hapësirën kibernetike.

·Duhet të shtohen përpjekjet për koordinimin ndërmjet institucioneve të sigurisë kibernetike, për të mundësuar mbikëqyrje dhe llogaridhënie adekuate si për çështjet teknike ashtu edhe për ato politike.

·Duhet të rriten kapacitetet e oficerëve të policisë, gjyqtarëve dhe prokurorëve në lidhje me standardet ndërkombëtare për garantimin e të drejtave të njeriut në hapësirën kibernetike.

·Policia e Shtetit dhe Prokuroria duhet të pajisen me burime të mjaftueshme njerëzore dhe teknike për të trajtuar krimin kibernetik si në nivel qendror ashtu edhe në atë vendor.

Rekomandime për aktorët publikë

(Qeveria, Parlamenti dhe institucionet ligjzbatuese)

Mbi kapacitetet dhe bashkëpunimin institucional:

·Institucionet e pavarura të të drejtave të njeriut duhet të pajisen me burime të përshtatshme njerëzore dhe teknike për të kryer hetime të plota administrative për shkeljet e të drejtave të njeriut në hapësirën kibernetike.

·Oficerët e policisë dhe prokurorët e krimit kibernetik duhet të trajnohen mbi Udhëzimin e Përgjithshëm të Prokurorit të Përgjithshëm mbi hetimin efektiv penal të dhunës ndaj grave, dhunës në familje dhe dhunës me motive urrejtjeje. Duhet të ndërmerren masa për forcimin e besimit midis këtyre autoriteteve dhe grupeve që targetohen shpesh në internet.

·Duhet të bëhet funksional dhe i aksesueshëm për qytetarët mekanizmi i raportimit online i Policisë së Shtetit për krimin kibernetik për të mundësuar denoncimin në kohë të shkeljeve.

Rekomandime për aktorët jo-publikë

(OSHC-të, akademia, media, donatorët ndërkombëtarë)

Mbi ndërgjegjësimin dhe llogaridhënien:

·Duhet të monitorohen në mënyrë aktive shkeljet e të drejtave të njeriut që ndodhin në hapësirën kibernetike për të mundësuar hulumtime dhe vlerësime të plota mbi situatën, të cilat aktualisht janë të pamjaftueshme.

·Duhet të inkurajohet kontributi aktiv i aktorëve jopublikë në proceset e konsultimit për ndryshimet ligjore dhe dokumentet e politikave strategjike në lidhje me sigurinë kibernetike dhe të drejtat e njeriut.

·Duhet të rritet ndërgjegjësimi i publikut për format e diskriminimit që ndodhin në hapësirën kibernetike në mënyrë që të inkurajohet raportimi i rasteve dhe të ndërtohen praktika institucionale në këtë drejtim.

·Duhet të rritet ndërgjegjësimi i publikut për kërcënimet ndaj privatësisë në hapësirën kibernetike, për të inkurajuar qytetarët të identifikojnë dhe raportojnë çdo shkelje.

Rekomandime për aktorët jo-publikë

(OSHC-të, akademia, media, donatorët ndërkombëtarë)

Mbi kapacitetet dhe mbështetjen e OSHC-ve dhe medias:

·Duhet të promovohet dhe mbështetet një qasje vetërregulluese e medias online, në përputhje me praktikat më të mira, për të siguruar proporcionalitet ndërmjet llogaridhënies për shkeljet dhe lirisë nga censura.

·Duhet të rriten kapacitetet e gazetarëve dhe mediave online në lidhje me raportimin etik dhe çështjet e të drejtave të njeriut.

·Duhet të rriten kapacitetet e OSHC-ve dhe aktivistëve në lidhje me sfidat e paraqitura ndaj ushtrimit të lirisë së tubimit në hapësirën kibernetike.

·Duhet të shtohet trajnimi dhe mbështetja teknike për sigurinë dixhitale për gazetarët dhe aktivistët.

·Duhet të mbështeten shërbimet ligjore për gazetarët dhe aktivistët që përballen me kërcënime kibernetike.

Kjo përmbledhje paraqet gjetjet kryesore të studimit **"Tejkalimi i hendekut mes sigurisë kibernetike dhe të drejtave të njeriut"**. Ky studim është kryer gjatë periudhës dhjetor 2021-maj 2022, në kuadër të projektit të Qendrës së Gjenevës për Qeverisjen e Sektorit të Sigurisë (DCAF) "Qeverisja e mirë e sigurisë kibernetike në Ballkanin Perëndimor", mbështetur nga Zyra e Jashtme e Komonuelthit dhe Zhvillimit e Mbretërisë së Bashkuar (FCDO). Ky studim është publikuar fillimisht në shtator të 2022 nga DCAF, si pjesë e një botimi rajonal mbi gjashtë shtetet e Ballkanit Perëndimor. Studimi i plotë gjendet në www.idmalbania.org.

Pikëpamjet dhe përfundimet e shprehura në këtë studim janë të autorëve dhe Institutit për Demokraci dhe Ndërmjetësim (IDM) dhe nuk reflektojnë domosdoshmërisht pikëpamjet e DCAF dhe FCDO.