ITS INSTITUTE FOR TECHNOLOGY AND SOCIETY

Raport Kërkimor

SFIDAT DHE PËRGJEGJËSITË E PËRPUNUESVE TË MËDHENJ TË TË DHËNAVE NË KOSOVË

Nëntor 2024

Përmbajtja

Botuesi: Instituti për Teknologji dhe Shoqëri (ITS)

Autore: Donika Çeta

Redaktorët: Adison Gara dhe Lirim Bllaca

Financuar nga: Projekti HumanRightivism, i zbatuar nga Fondi për Zhvillim të Komunitetit (CDF) dhe mbështetur nga Ambasada e Suedisë në Prishtinë

Prishtinë, 2024

Mbështetur nga:

Institute for Technology and Society
Str. Zenel Salihu no. 28 Prishtina
https://institutets.com/

Lista e shkurtesave

GDPR	General Data Protection Regulation - Rregullorja e Përgjithshme për Mbrojtjen e të Dhënave (BE) 2016/679 e Parlamentit Evropian dhe e Këshillit e datës 27 Prill 2016 për mbrojtjen e personave fizikë në lidhje me përpunimin e të dhënave personale dhe për lëvizjen e lirë të të dhënave, dhe shfuqizimin e Direktivës 95/46 /EC
AIP	Agjencia pwr Informim dhe Privatwsi
LMDHP	Ligji nr. 03/L-172 për Mbrojtjen e të Dhënave Personale
DPO	Data Protection Officer - Zyrtar/e për Mbrojtjen e të Dhënave
DPIA	Data Protection Impact Assessment - Vlerësimi i Ndikimit në Mbrojtjen e të Dhënave
TIK	Teknologjia e Informacionit dhe Komunikimit
IoT	Internet of Things
IHIS	Integrated Health Information System - Sistemi i Integruar Informativ Shëndetësor
BHIS	Basic Health Information System – Sistemi Bazik Informativ Shëndetësor
GG	Government Gateway - Porta e Qeverisë
QKSS	Qendra Kosovare për Studime të Sigurise
SME	Small and Medium-sized Enterprises - Ndërmarrjet e Vogla dhe të Mesme

Përmbledhje ekzekutive

Shtyrë nga digjitalizimi i shpejtë, Kosova po punon drejt krijimit të praktikave të forta për mbrojtjen e të dhënave. Pavarësisht përparimeve të fundit në kuadrin legjislativ, si harmonizimi me Rregulloren e Përgjithshme të BE-së për Mbrojtjen e të Dhënave (GDPR) përmes Ligjit për Mbrojtjen e të Dhënave Personale (LMDHP), Kosova përballet me sfida të mëdha në zbatimin praktik. Këto sfida janë të pranishme edhe tek përpunuesit e mëdhenj të të dhënave, ku pasojat e mundshme të shkeljeve janë më të mëdha. Ky punim vlerëson gjendjen aktuale të mbrojtjes së të dhënave, duke u fokusuar në pajtueshmërinë e sektorëve kryesorë—telekomunikacionit, financave, administratës publike dhe shërbimeve komunale, shëndetësisë dhe arsimit—me LMDHP-në dhe nxjerr në pah sfidat dhe mundësitë për përmirësimin e mbrojtjes së të dhënave në Kosovë.

Punimi identifikon një sërë çështjesh, përfshirë zbatimin jo-konsistent të ligjit për mbrojtjen e të dhënave, boshllëqet në vetëdijen publike dhe kapacitetet e pamjaftueshme të brendshme të organizatave, veçanërisht institucioneve publike. Për më tepër, përpunuesit e mëdhenj të të dhënave, si kompanitë e telekomunikacionit dhe institucionet financiare, përpunojnë sasi të mëdha të të dhënave personale, por pajtueshmëria e tyre me rregulloret e mbrojtjes së të dhënave mbetet e paqëndrueshme. Punimi paraqet raste studimore, përfshirë Kompaninë e Furnizimit me Energji Elektrike të Kosovës (KESCO) dhe Komunën e Gjakovës, për të ilustruar sfidat në mbrojtjen e të dhënave dhe çështjet e zbatimit.

Rezultatet e sondazhit me organizatat e sektorit publik dhe privat tregojnë një dallim në zbatimin e praktikave të mbrojtjes së të dhënave. Ndërsa institucionet më të mëdha po bëjnë përparime në harmonizimin me LMDHP-në, organizatat më të vogla përballen me kufizime të burimeve dhe kapaciteteve, duke çuar në masa të pamjaftueshme mbrojtjeje. Vlen të theksohet se ekziston një nevojë e qartë për trajnim të avancuar të stafit, auditime të rregullta dhe rritjen e ndërgjegjësimit mbi të drejtat për mbrojtjen e të dhënave.

Progresi i Kosovës drejt krijimit të një mjedisi të sigurt për mbrojtjen e të dhënave paraqet mundësi për bashkëpunim mes sektorit publik dhe privat në praktikat më të mira, përmirësimin e pajtueshmërisë dhe ndërtimin e besimit publik në shërbimet digjitale. Duke adresuar sfidat e identifikuara, Kosova mund të përparojë drejt një mjedisi më të sigurt dhe më të ndërgjegjshëm ndaj privatësisë, duke e pozicionuar veten për të përfituar nga integrimi i saj i vazhdueshëm në ekonominë globale digjitale.

Gjetjet Kryesore

Kuadri ligjor i Kosovës për mbrojtjen e të dhënave është i harmonizuar me GDPR-në por zbatimi i tij është i paqëndrueshëm. Burimet e kufizuara, pengesat teknike dhe mungesa e vetëdijes publike pengojnë pajtueshmërinë, veçanërisht ndër përpunuesit e mëdhenj të të dhënave.

Sektorët kryesorë, duke përfshirë telekomunikacionin, financat dhe administratën publike, përballen me sfida unike. Përpunuesit e mëdhenj të të dhënave hasin vështirësi në menaxhimin e pajtueshmërisë për shkak të rritjes së shpejtë të të dhënave dhe kërkesave teknologjike.

Sektori privat tregon pajtueshmëri më të mirë përmes trajnimeve më të shpeshta për mbrojtjen e të dhënave dhe alokimit të burimeve, ndërsa sektori publik shfaq përditësime më të rralla të politikave të privatësisë dhe trajnim të kufizuar të punonjësve.

Rastet studimore, si KESCO dhe Komuna e Gjakovës, ilustrojnë dështimet në mbrojtjen e të dhënave personale, duke rezultuar në gjoba të profilit të lartë dhe duke theksuar nevojën për përmirësimin e pajtueshmërisë.

Shumë organizata nuk arrijnë të përditësojnë rregullisht politikat e mbrojtjes së të dhënave dhe Vlerësimet e Ndikimit mbi Mbrojtjen e të Dhënave (DPIA), duke treguar një qasje reaktive në vend të integrimit të masave të privatësisë në operacionet e tyre.

Gjetjet kryesore & rekomandimet

Gjetjet kryesore:

- Kuadri i mbrojtjes së të dhënave në Kosovë është i harmonizuar me GDPR-në, por zbatimi është i paqëndrueshëm. Burimet e kufizuara, pengesat teknike dhe ndërgjegjësimi i ulët i publikut pengojnë përputhshmërinë, veçanërisht në mesin e përpunuesve të mëdhenj të të dhënave.
- Sektorët kryesorë, përfshirë telekomunikacionin, financat dhe administratën publike, përballen me sfida unike. Përpunuesit e mëdhenj të të dhënave hasin vështirësi në menaxhimin e përputhshmërisë për shkak të rritjes së shpejtë të të dhënave dhe kërkesave teknologjike.
- Sektori privat demonstron përputhshmëri më të mirë përmes trajnimeve më të shpeshta për mbrojtjen e të dhënave dhe alokimit të burimeve, ndërsa sektori publik tregon përditësime më të rralla të politikave të privatësisë dhe trajnim të kufizuar të punonjësve.
- Studimet e rasteve, si KESCO dhe Komuna e Gjakovës, ilustrojnë dështimet në mbrojtjen e të dhënave personale, duke rezultuar në gjoba të profilit të lartë dhe duke nxjerrë në pah nevojën për përmirësimin e përputhshmërisë.
- Shumë organizata nuk përditësojnë rregullisht politikat e mbrojtjes së të dhënave dhe Vlerësimet e Ndikimit të Mbrojtjes së të Dhënave (DPIA), duke treguar një qasje reaktive në vend që të integrojnë masat e privatësisë në operacionet e tyre.

Rekomandimet kryesore:

- Të rriten burimet dhe kapacitetet e Agjencisë për Informim dhe Privatësi (AIP) për të mundësuar inspektime, auditime dhe veprime pasuese më të shpeshta, për të siguruar pajtueshmërinë me mbrojtjen e të dhënave në të gjithë sektorët.
- Të organizohen trajnime të vazhdueshme për mbrojtjen e të dhënave, veçanërisht për punonjësit e sektorit publik, për të ndërtuar një kuptim të fortë të praktikave të mbrojtjes së të dhënave, me fokus të veçantë në harmonizimin e standardeve mes sektorit publik dhe privat.
- Të inkurajohen organizatat që të integrojnë parimet e Privacy by Design (Privatësisë të integruar në Dizajn) në zhvillimin e sistemeve, për të mbrojtur të dhënat në mënyrë proaktive, të plotësuara me DPIA dhe përditësime të rregullta të politikave.

- Të mbahen fushata për të edukuar publikun mbi të drejtat e tyre për mbrojtjen e të dhënave, duke i fuqizuar ata të mbajnë institucionet përgjegjëse dhe duke rritur kërkesën e përgjithshme për pajtueshmëri.
- Të zhvillohen udhëzime të standardizuara për mbrojtjen e të dhënave përmes partneriteteve midis sektorit publik dhe atij privat, për të siguruar pajtueshmëri të qëndrueshme dhe ndërtimin e një kulture të sigurisë së të dhënave në të gjithë sektorët.

Kapitulli I: Hyrje

Në botën e sotme, përpunuesit e mëdhenj, që nënkupton entitete që përpunojnë të dhënat personale për dhe në emër të kontrolluesve të të dhënave, kanë kontroll të konsiderueshëm mbi informacionin personal. Në terminologjinë e mbrojtjes së të dhënave, një kontrollues i të dhënave është një entitet që përcakton qëllimet dhe mënyrat e përpunimit të të dhënave personale, ndërsa një përpunues i të dhënave kryen përpunimin e vërtetë për llogari të kontrolluesit. Përpunuesit e të dhënave trajtojnë informacionin personal në sektorë si telekomunikacioni, financat, shëndetësia, arsimi dhe administrata publike, duke luajtur një rol thelbësor në ruajtjen e privatësisë së të dhënave dhe respektimin e ligjeve për mbrojtjen e të dhënave.

Shumë përpunues përdorin këto të dhëna për të përmirësuar proceset e tyre të biznesit ose për të fituar një avantazh konkurrues, duke kaluar ndoshta kufijtë e ligjit ose duke përfituar nga boshllëqet në ligjet për mbrojtjen e të dhënave. Veçanërisht kur të dhënat përdoren gjerësisht pa mbikëqyrje të mjaftueshme, kjo mund të çojë në shkelje të privatësisë.

Çdo ditë prodhohen të dhëna në mënyrë masive në forma të ndryshme dhe nga burime të ndryshme. Sasia totale e të dhënave të krijuara pritet të rritet në më shumë se 180 zettabajt deri në vitin 2025.[1] Për ta kuptuar më mirë, një film 2-orësh në 4K është rreth 1 gigabajt. Me 180 zettabajt, mund të ruheshin afërsisht 180 trilion filma në 4K. Kjo do të ishte e mjaftueshme që të shihni mbi 1,000,000,000,000 (një trilion) filma.[2] Kompanitë përdorin përparimet teknologjike dhe analizojnë sasinë e madhe të të dhënave nga burime të ndryshme për të fituar një kuptim më të plotë të sjelljes së klientëve.[3]

Në Kosovë, ku digjitalizimi po përparon me shpejtësi, mbrojtja e informacionit personal është një sfidë dhe një mundësi. Përputhshmëria me GDPR-në e BE-së përmes LMDHP-së së Kosovës ishte një hap thelbësor në ruajtjen e privatësisë së qytetarëve. Megjithatë, zbatimi dhe ekzekutimi praktik mbeten të vështirë, dhe përputhshmëria shpesh pengohet nga ndërgjegjësimi i dobët publik, përputhshmëria e ndryshueshme dhe kufizimet e burimeve. Sipas gjetjeve të fundit nga pyetësori ynë, ndonëse shumë organizata e kuptojnë rëndësinë e mbrojtjes së të dhënave, ka boshllëqe të rëndësishme në praktikë. Për shembull, ndonëse shumica e institucioneve publike dhe private kanë politika për privatësinë, ato shpesh përditësojnë këto politika në mënyrë reaktive, dhe jo proaktive. Për më tepër, vetëm 42.9% e institucioneve private dhe 33% e institucioneve publike raportuan kryerjen e DPIA-ve, duke theksuar nevojën për një zbatim më të gjerë dhe të qëndrueshëm të strategjive të menaxhimit të rrezikut.

Për më tepër, sipas rezultateve të pyetësorit, sektorë të ndryshëm ndryshojnë shumë në gatishmërinë e tyre për të trajtuar shkeljet e të dhënave; 71.4% e kompanive private nuk kanë

[1] Amount of data created, consumed, and stored 2010-2020, with forecasts to 2025, published by Petroc Tazlylor, Statista, https://www.statista.com/statistics/871513/worldwide-data-created/

[2] Blog, What's the real story behind the explosive growth of data, https://www.red-gate.com/blog/database-development/whats-the-real-story-behind-the-explosive-growth-of-data

[3] Emerging Trends in Information Management for 2024: Navigating the Future Data, Khan Abdullah, 2024.

një strategji të reagimit ndaj incidenteve, ndërsa 50% e organizatave të sektorit publik janë në të njëjtën situatë. Kjo mospërputhje thekson nevojën thelbësore për një gatishmëri të shtuar, veçanërisht duke pasur parasysh evolucionin e vazhdueshëm të kërcënimeve dixhitale. Përgjigjet e sondazhit treguan gjithashtu mungesën e edukimit të vazhdueshëm për mbrojtjen e të dhënave, veçanërisht në institucionet qeveritare.

Duhet kuptuar fakti se transformimi dixhital po ndryshon jetën tonë të përditshme. Prandaj, është e pamundur të mbivlerësohet rëndësia e një mbrojtjeje të fortë të të dhënave në një kohë kur të dhënat janë kthyer në një burim jetik për të dy, qeveritë dhe korporatat. Menaxhimi i të dhënave të ndjeshme dhe personale është bërë gjithnjë e më i rëndësishëm ndërsa digjitalizimi po përshpejtohet në çdo industri. Kosova është një vend që po i bashkohet shpejt ekonomisë dixhitale globale dhe mbrojtja e të dhënave përbën një mundësi dhe një shqetësim. Përpunuesit e mëdhenj të të dhënave janë thelbësorë për ekonominë, prandaj praktikat e forta të sigurisë së të dhënave janë të nevojshme jo vetëm për përputhshmëri, por edhe për të mbajtur besimin e publikut dhe për të nxitur rritjen afatgjatë. Për më tepër, Qeveria e Kosovës përmes Strategjisë për Qeverisje Elektronike 2023-2027 ka përcaktuar përparësi të qarta drejt dixhitalizimit.[4]

Përtej përputhshmërisë, mbrojtja e të dhënave është thelbësore për ndërtimin e besimit publik në ekonominë dixhitale të Kosovës. Përveç mbrojtjes së privatësisë individuale, një mbrojtje efektive e të dhënave rrit konkurrueshmërinë e vendit në një ekonomi globale që po bëhet gjithnjë e më shumë e varur nga të dhënat. Kjo paraqet njëkohësisht një sfidë dhe një mundësi për Kosovën. Sigurimi i përputhshmërisë mund të hapë rrugën drejt një integrimi të mëtejshëm me Bashkimin Evropian, ndërsa forcimi i masave për mbrojtjen e të dhënave mund të rrisë besimin e qytetarëve dhe t'i inkurajojë ata të përdorin shërbime dixhitale.

Ky studim shqyrton mjedisin aktual të mbrojtjes së të dhënave në Kosovë, me fokus te përpunuesit e mëdhenj të të dhënave. Ai synon të vlerësojë efektivitetin e rregulloreve dhe praktikave aktuale të mbrojtjes së të dhënave, të theksojë sfidat kryesore dhe të tërheqë vëmendjen ndaj fushave që kanë nevojë për zhvillim. Pyetjet kërkimore që drejtojnë këtë studim janë:

- Sa efektive janë ligjet dhe praktikat aktuale të mbrojtjes së të dhënave në Kosovë dhe cilat janë sfidat dhe mundësitë kryesore për përmirësimin e mbrojtjes së të dhënave për të përfituar shoqëria?
- Si i përmbushin përpunuesit e mëdhenj të dhënave kërkesat ligjore dhe rregullative përkatëse?

Ky studim shqyrton mjedisin e mbrojtjes së të dhënave në Kosovë në disa seksione kyçe:

- **Pasqyra e Mbrojtjes së të Dhënave në Kosovë dhe Përpunuesit e të Dhënave:** Ky kapitull ofron një përmbledhje të kuadrit të mbrojtjes së të dhënave në Kosovë dhe mjedisit ligjor në zhvillim, duke theksuar rolet e përpunuesëve dhe kontrolluesve të të dhënave.
- **Përpunuesit e mëdhenj të të Dhënave në Kosovë**: Duke u fokusuar te Përpunuesit kryesorë të të dhënave, ky seksion eksploron rolin e industrive si telekomunikacioni, financat dhe shëndetësia në formësimin e ekosistemit të të dhënave në Kosovë.

[4] eGovernment Strategy Kosovo 2023-2027, https://mpb.rks-gov.net/Uploads/Documents/Pdf/EN/2700/e-Government%20Strategy%20Kosovo%202023-2027.pdf

- **Sfidat e Përpunuesëve të Mëdhenj të të Dhënave:** Ky kapitull identifikon pengesat kryesore me të cilat përballen Përpunuesit e të dhënave, përfshirë kufizimet teknologjike, kompleksitetin rregullativ dhe kapacitetet e kufizuara organizative.
- **Raste Studimi:** Duke shqyrtuar raste konkrete, si KESCO dhe Komuna e Gjakovës, ky seksion ilustron sfidat praktike të përputhshmërisë dhe zbatimit të mbrojtjes së të dhënave në Kosovë.
- **Rezultatet e Pyetësorit**: Ky kapitull paraqet gjetjet nga një pyetësor i shpërndarë në entitete të sektorit publik dhe privat, duke ofruar njohuri kuantitative mbi praktikat e përputhshmërisë dhe boshllëqet.
- **Përfundimet:** Seksioni i fundit sintetizon gjetjet dhe ofron rekomandime për forcimin e kuadrit të mbrojtjes së të dhënave në Kosovë, sigurimin e përputhshmërisë dhe ndërtimin e besimit publik në shërbimet dixhitale.

1.1 Metodologjia

Metodologjia e këtij studimi kombinon qasjet kërkimore cilësore dhe sasiore për të vlerësuar efektivitetin e praktikave të mbrojtjes së të dhënave në Kosovë, veçanërisht te përpunuesit e mëdhenj të të dhënave. Hulumtimi përfshiu një analizë të gjerë të literaturës ekzistuese mbi ligjet e mbrojtjes së të dhënave, si GDPR dhe LMDHP. Ky rishikim ofroi një kontekst historik për mbrojtjen e të dhënave në Kosovë dhe dha njohuri mbi praktikat më të mira ndërkombëtare. Burimet kryesore përfshinin tekste ligjore, raporte qeveritare dhe artikuj akademikë të rëndësishëm, të cilat ndihmuan në ndërtimin e kornizës për analizimin e pajtueshmërisë në Kosovë.

Ky studim u zhvillua rreth pyetjeve kryesore që trajtojnë çështjet qendrore në peizazhin e mbrojtjes së të dhënave në Kosovë, duke u fokusuar veçanërisht te përpunuesit e mëdhenj të të dhënave. Pyetjet përfshijnë: vlerësimin e efektivitetit të ligjeve dhe praktikave aktuale të mbrojtjes së të dhënave, identifikimin e sfidave dhe mundësive kryesore për përmirësimin e mbrojtjes së të dhënave dhe ekzaminimin e pajtueshmërisë së përpunuesve të mëdhenj të të dhënave me LMDHP-në.

Gjithashtu, u zhvilluan dy raste studimore kryesore për të ilustruar sfidat praktike dhe pasojat e zbatimit të mbrojtjes së të dhënave në Kosovë. Rasti i parë u fokusua në KESCO (Kompania e Furnizimit me Energji Elektrike e Kosovës), një përpunues i madh i të dhënave në sektorin e shërbimeve publike, praktikat e së cilës u shqyrtuan nga Agjencia për Informim dhe Privatësi (AIP) pas shkeljeve të mbrojtjes së të dhënave. Rasti i dytë shqyrtoi Komunën e Gjakovës, një entitet i administratës publike që u gjobit për përpunimin e paligjshëm dhe publikimin e të dhënave personale. Ky rast ofroi njohuri mbi sfidat e sektorit publik në menaxhimin e të dhënave të ndjeshme. Këto raste u zgjodhën bazuar në disponueshmërinë e informacionit të detajuar mbi mospajtueshmërinë e tyre dhe veprimet rregullatore të ndërmarra, duke ofruar shembuj realë se si trajtohen çështjet e mbrojtjes së të dhënave në Kosovë.

Ky studim gjithashtu mblodhi informacion përmes një pyetësori të dizajnuar dhe shpërndarë në organizatat publike dhe private të Kosovës për të mbledhur të dhëna mbi praktikat e tyre për mbrojtjen e të dhënave, ndërgjegjësimin mbi kërkesat ligjore dhe sfidat që hasin në pajtueshmërinë me LMDHP-në. Pyetësori u përqendrua në disa fusha kyçe, duke përfshirë: praninë e Zyrtarëve për Mbrojtjen e të Dhënave (DPO), ekzistencën dhe përditësimin e rregullt

të politikave të mbrojtjes së të dhënave, përdorimin e masave teknike mbrojtëse si enkriptimi dhe firewall-et, planet e reagimit ndaj incidenteve për menaxhimin e shkeljeve të të dhënave dhe integrimin e parimeve të Privacy by Design në sistemet e tyre.

Përgjigjet u mblodhën nga disa organizata në sektorë të ndryshëm, duke përfshirë telekomunikacionin, financat, shëndetësinë, arsimin dhe administratën publike. Këto të dhëna ofruan njohuri sasiore mbi nivelin e pajtueshmërisë dhe boshllëqet në praktikat e mbrojtjes së të dhënave në sektorë të ndryshëm.

Gjithashtu, ky studim përfshiu një analizë krahasuese të praktikave të mbrojtjes së të dhënave në Kosovë me vendet e tjera në rajon dhe në Bashkimin Evropian, me fokus të veçantë në sfidat e harmonizimit me standardet e GDPR-së. Ky krahasim nxori në pah fusha ku Kosova ngec në zbatim dhe ku mund të bëhen përmirësime duke mësuar nga shembujt ndërkombëtarë.

Në fund, të dhënat e mbledhura përmes pyetësorit dhe intervistave u analizuan duke përdorur si statistika përshkruese ashtu edhe analiza tematike. Rezultatet e pyetësorit u kategorizuan dhe krahasuan ndër sektorë për të identifikuar modelet në pajtueshmëri, sfidat e zakonshme dhe fushat ku nevojitet mbështetje rregullative. Analiza tematike e intervistave dhe rasteve studimore ofroi njohuri cilësore mbi implikimet reale të kuadrit të mbrojtjes së të dhënave në Kosovë.

Kapitulli II: Pasqyra e Mbrojtjes së të Dhënave në Kosovë dhe Përpunuesit e të Dhënave

1. Përkufizimi, Rëndësia dhe Konteksti Historik

Zbatimi i konceptit modern të mbrojtjes së të dhënave në Evropë filloi në vitin 1990 kur Komisioni Evropian paraqiti një paketë të gjerë propozimesh për mbrojtjen e të dhënave personale, duke shënuar një hap të rëndësishëm drejt miratimit të legjislacionit për mbrojtjen e të dhënave.[5] Kjo përpjekje themeluese vendosi bazat për zhvillimin e vazhdueshëm të mbrojtjes së të dhënave brenda Bashkimit Evropian, e cila ka përparuar përmes një ndërveprimi kompleks të koncepteve ligjore. Terma të tilla si 'privatësia', 'jeta private' dhe 'mbrojtja e të dhënave personale' herë pas here janë trajtuar si të veçanta dhe të izoluara, dhe herë të tjera si identike, duke pasqyruar natyrën e ligjit të BE-së në përcaktimin dhe formimin e të drejtës themelore për mbrojtjen e të dhënave.[6] Zhvillimi i teknologjive dhe shërbimeve gjithnjë e më shumë që po zhvillohen në fushën digjitale sollën gjithashtu disa incidente. Këto incidente të njohura shërbyen si kujtesa për lidhjen me marrjen dhe keqperdorimin e të dhënave.[7] Për shembull, incidenti me shkeljen e të dhënave të Marriott International në vitin 2018, ku rreth 500 milionë të dhëna të mysafirëve u kompromet uan.[8] Prandaj, sigurimi i një balanci mes mbrojtjes së të dhënave dhe përdorimit të të dhënave është i nevojshëm, dhe për ta arritur këtë, duhet të ndërtohet një mekanizëm që inkurajon dhe siguron mbrojtje efektive.[9]

Rregullat e të dhënave të BE-së kanë pasur një ndikim të madh në mbarë botën. Është e vlefshme të përmendet se rreth 67 shtete jashtë BE-së kanë miratuar kuadrin e GDPR-së, nga vendet e Azisë Lindore si Japonia dhe Koreja e Jugut deri tek vendet e Amerikës Latine.[10] Megjithatë, ndërsa teknologjia zhvillohet, rregulloret mund të ndryshojnë gjithashtu dhe, prandaj, nuk mund të supozojmë se rregullat janë në njëshim. Është e vlefshme të përmendet se rregullat e mbrojtjes së të dhënave të GDPR-së janë miratuar gjithashtu në Kosovë përmes Ligjit për Mbrojtjen e të Dhënave Personale.[11]

Në Kosovë, sipas Ligjit për Mbrojtjen e të Dhënave Personale (LMDHP), "mbrojtja e të dhënave" është mbrojtja e të dhënave personale dhe privatësisë së individëve, duke përcaktuar të drejtat, përgjegjësitë dhe parimet për të siguruar që të dhënat personale të përpunohen në mënyrë ligjore dhe të sigurt. Është një të drejtë themelore që mbrohet nga marrëveshjet ndërkombëtare dhe ligjet vendore, duke treguar kuptimin në rritje se privatësia është një komponent i nevojshëm i autonomisë dhe dinjitetit njerëzor. Varësia në rritje nga teknologjia

[5] The Emergence of Personal Data Protection as a Fundamental Right of the EU, Gloria González Fuster Law, Science, Technology and Society (LSTS) Vrije Universiteit Brussel (VUB), 2014.
[6] Ibid, pg. 254.
[7] Balancing Data Protection and Data Utilization: Global Perspectives and Trends, Yishi Wu, April 2024.
[8] Ibid.
[9] Data Rights Law 3.0: The Legislative Prospect, edited by Yuming Lian, Peter Lang Ltd. International Academic Publishers, 2021.
[10] Balancing Data Protection and Data Utilization: Global Perspectives and Trends, Yishi Wu, April 2024.
[11] Law no. 06/L-082 on Protection of Personal Data, https://gzk.rks-gov.net/ActDetail.aspx?ActID=18616

digjitale në Kosovë ka theksuar rëndësinë e mbrojtjes së të dhënave dhe nevojën për rregullore të forta për të siguruar të dhënat personale.

Në mënyrë të verifikueshme, avancimi i sigurimit të informacionit në Kosovë është ndikuar nga lëvizja e saj politike dhe ligjore, veçanërisht brenda periudhës pas shpalljes së pavarësisë, ku janë bërë përpjekje për t'u përshtatur me standardet evropiane. Angazhimi i Kosovës për mbrojtjen e të dhënave është i qartë në sistemin e saj ligjor, i cili është zhvilluar dinamikisht për t'u përballur me sfidat që sjell epoka digjitale.

Asambleja e Kosovës në vitin 2008 miratoi Kushtetutën e Kosovës, e cila njohu të drejtën për privatësinë duke deklaruar se "çdo person gëzon të drejtën e mbrojtjes së të dhënave personale. Mbledhja, ruajtja, qasja, korrigjimi dhe përdorimi i të dhënave personale rregullohen me ligj."[12] Kjo dispozitë kushtetuese paraqet angazhimin e Kosovës për të harmonizuar kuadrin e saj ligjor me masat ndërkombëtare për mbrojtjen e të dhënave, duke garantuar që mbrojtja e të dhënave të jetë një të drejtë kryesore brenda kuadrit ligjor të vendit.

Ligji i parë që avancoi rregullimin e dispozitave të parashikuara në Nenin 36 të Kushtetutës së Republikës së Kosovës ishte Ligji nr. 03/L-172 për Mbrojtjen e të Dhënave Personale. Ky ligj përcaktoi të drejtat, detyrat, standardet dhe masat për të siguruar mbrojtjen e të dhënave në përputhje me Direktivën e BE-së 95/46/EC.[13] Përmes këtij ligji u krijua Agjencia Kombëtare për Mbrojtjen e të Dhënave Personale si agjenci përgjegjëse për mbikëqyrjen e zbatimit të rregullave për mbrojtjen e të dhënave me detyrimin për të raportuar në Kuvendin e Kosovës.[14] Agjencia kishte disa detyra, siç ishin ofrimi i këshillave për organet publike dhe private në çështje të mbrojtjes së të dhënave, vendosja mbi ankesa të subjekteve të të dhënave, kryerja e inspektimeve dhe auditimeve, informimi i publikut për çështje dhe zhvillime në fushën e mbrojtjes së të dhënave, dhe promovimi i të drejtës themelore për mbrojtjen e të dhënave.[15]

Në vitin 2019, u miratua një ligj i ri për mbrojtjen e të dhënave personale. Ligji nr. 06/L-082 për Mbrojtjen e të Dhënave Personale (LMDHP) u miratua pas miratimit të Rregullores (BE) 2016/679 të Parlamentit Evropian dhe të Këshillit të 27 Prillit 2016 për mbrojtjen e personave fizikë në lidhje me përpunimin e të dhënave personale dhe për lëvizjen e lirë të këtyre të dhënave (GDPR).[16]

2. Pasqyra e Rregullores për Mbrojtjen e të Dhënave

Ligji nr. 06/L-082 për Mbrojtjen e të Dhënave Personale në Kosovë (LMDHP) përfaqëson në thelb kuadrin ligjor për mbrojtjen e të dhënave në Kosovë.[17] Ky ligj, i cili u miratua për t'u harmonizuar me Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave të Bashkimit Evropian (GDPR), vendos udhëzime gjithëpërfshirëse në lidhje me mbledhjen, përpunimin, ruajtjen dhe transferimin e të dhënave personale brenda Kosovës. Ligji thekson sigurimin e të drejtave të

[12] Constitution of the Republic of Kosovo, Assembly of the Republic of Kosovo, published: 09.04.2008, art. 36.
[13] Law no. 06/L-082 on Protection of Personal Data, Assembly of the Republic of Kosovo, published on: 31.05.2010.
[14] Ibid Art. 29.
[15] Ibid.
[16] Law no. 06/L-082 on Protection of Personal Data, Assembly of the Republic of Kosovo. Published: 25.02.2019.
[17] Ibid.

privatësisë së individëve, duke promovuar njëkohësisht transparencën dhe llogaridhënien mes kontrolluesve dhe përpunuesve të të dhënave.

LMDHP pasqyron ngushtë GDPR-në, duke treguar angazhimin e Kosovës për të harmonizuar rregulloren e saj për mbrojtjen e të dhënave me ato të Bashkimit Evropian. Raporti i Kosovës për vitin 2019 gjeti se LMDHP i ri përbën një përparim të rëndësishëm në fushën e mbrojtjes së të dhënave.[18]

Të ngjashme me të drejtat e parashikuara në GDPR, LMDHP njeh të drejtën e subjekteve të të dhënave për të pasur qasje, korrigjuar dhe fshirë të dhënat e tyre personale, si dhe të drejtën për portabilitetin e të dhënave dhe të drejtën për t'u kundërvënë përpunimit të të dhënave. Gjithashtu, ai njeh parimin e pëlqimit, që do të thotë se subjekti i të dhënave jep pëlqimin e tij për përpunimin e të dhënave të tij ose saj bazuar në një ose më shumë qëllime të caktuara. LMDHP e definon pëlqimin e subjektit të të dhënave si çdo tregues të dhënë lirisht, të qartë, të informuar dhe të paambigj të dëshirave të subjektit të të dhënave, përmes një deklarate që tregon miratimin për përpunimin e të dhënave personale që lidhen me të.[19]

Për më tepër, LMDHP vendos detyrime për kontrolluesit dhe përpunuesit e të dhënave. Ai kërkon që ata të zbatojnë masa teknike dhe organizative të përshtatshme për të siguruar sigurinë e të dhënave dhe përputhshmërinë me standardet e mbrojtjes së të dhënave.[20] Për më tepër, në lidhje me transferimet ndërkufitare të të dhënave, LMDHP gjithashtu përcakton rregulla dhe kushte për transferimin e të dhënave personale jashtë Kosovës. Ai kërkon që ky lloj transferimi të garantojë një nivel të mjaftueshëm mbrojtjeje të të dhënave, që është i ngjashëm me kërkesat e GDPR-së.[21]

LMDHP krijon AIP-në si autoritetin e pavarur përgjegjës për mbikëqyrjen e zbatimit dhe forcimin e ligjeve për mbrojtjen e të dhënave në Kosovë. AIP ka disa detyra, përfshirë shqyrtimin e ankesave nga individët, kryerjen e hetimeve mbi shkeljet e mundshme, dhënien e mendimeve mbi praktikat më të mira të mbrojtjes së të dhënave, dhe garantimin që sektori publik dhe privat të veprojnë në përputhje me ligjet e mbrojtjes së të dhënave. AIP ka detyrën të zbatojë sanksione për mosrespektimin e ligjit, të propozojë ndryshime administrative dhe të punojë në bashkëpunim me organet ndërkombëtare të mbrojtjes së të dhënave. Ky kuadër ligjor gjithëpërfshirës thekson angazhimin e Kosovës për të garantuar mbrojtjen e të dhënave dhe për t'i përshtatur masat e mbrojtjes së të dhënave me standardet ndërkombëtare, veçanërisht ato të vendosura nga Bashkimi Evropian.[22]

Nga LMDHP rrjedhin disa akte nënligjore, të cilat rregullojnë për shembull procedurat e inspektimit, sistemin e menaxhimit të rasteve të Ministrisë për Komunitete dhe Kthim për mbrojtjen e të dhënave personale, përcaktimin e kritereve dhe procedurave për lëshimin e

[18] Kosovo Country Report, European Commission, 2019, https://neighbourhood-enlargement.ec.europa.eu/document/download/85bb4cd1-fbe1-47b3-8914-7f606f1ede37_en?filename=20190529-kosovo-report.pdf

[19] Law no. 06/L-082 on Protection of Personal Data, Assembly of the Republic of Kosovo, article 3, paragraph 1.17.

[20] Ibid.

[21] Ibid, Chapter XI.

[22] Ibid, Artc. 92.

certifikatës për përpunimin e të dhënave personale, përpunimin e të dhënave personale të marra nga përdorimi i dronëve dhe shumë të tjera.[23]

Deri më tani, nuk ka pasur një vlerësim ex-post të LMDHP. Megjithatë, është e qartë se numri i rasteve të sjella para AIP-së është rritur. Sipas Raportit Vjetor të AIP-së të botuar në vitin 2024 për vitin 2023[24], ata morën 121 ankesa. Në vitin 2022, ata morën 145 ankesa dhe për gjashtë muajt e vitit 2021, AIP mori 45 ankesa.[25] Ky trend mund të tregojë se më shumë qytetarë janë të gatshëm të ushtrojnë të drejtat e tyre sipas LMDHP, çka mund të reflektojë një rritje të besimit në mekanizmat për trajtimin e çështjeve të mbrojtjes së të dhënave. Për më tepër, këto raporte zbulojnë një rritje të numrit të inspektimeve të kryera, duke sugjeruar një mbikëqyrje më të fuqishme nga ana e AIP-së.

Nga informacioni i mbledhur përmes pyetësorit, mund të theksohet se shumë kompani, veçanërisht ndërmarrjet më të mëdha dhe institucionet publike, kanë bërë përpjekje të rëndësishme për të përshtatur praktikat e tyre me kërkesat e LMDHP-së. Nga ana tjetër, ndërmarrjet më të vogla dhe organizatat me burime të kufizuara shpesh hasin vështirësi për të përmbushur këto kërkesa. Ndikimi i GDPR-së është më i dukshëm në përpjekjet e pajtueshmërisë të organizatave që merren me përpunimin ndërkufitar të të dhënave ose që kanë për qëllim të ndërtojnë besim me partnerët ndërkombëtarë.

Pavarësisht këtyre përpjekjeve, një numër i konsiderueshëm organizatash, veçanërisht në sektorin privat, mbeten të pavetëdijshëm ose të pasiguruar për të përmbushur plotësisht kërkesat për mbrojtjen e të dhënave. Zonat më të zakonshme të mos-pajtueshmërisë përfshijnë masa të pamjaftueshme të sigurisë së të dhënave, metoda të pamjaftueshme për marrjen dhe menaxhimin e pëlqimit, dhe mungesën e dokumentacionit dhe regjistrimeve të aktiviteteve të përpunimit. Për më tepër, emërimi i Oficerëve të Mbrojtjes së Të Dhënave (DPO) nuk është gjithmonë i pranishëm, veçanërisht në organizatat që janë të pasiguruara nëse ato bien brenda kufijve që kërkojnë një përfaqësues të tillë.[26]

Që nga viti 2021, kemi qenë dëshmitarë të ndryshimeve pozitive. Raporti gjysmëvjetor i AIP-s tregoi se në periudhën e raportimit Janar – Qershor 2021, Agjencia mori 63 ankesa nga institucione publike dhe private dhe 15 u transferuan nga viti 2023. Nga totali i 78 ankesave, 53 raste janë përfunduar ndërsa 25 të tjera janë ende në proces.[27] Sipas statistikave të publikuara, natyra e ankesave të dorëzuara lidhet kryesisht me mbikëqyrjen me kamera, pasuar nga marketingu i drejtpërdrejtë, botimi i paautorizuar i të dhënave personale, keqpërdorimi i të dhënave dhe kështu me radhë.[28]

Gjithashtu, është e rëndësishme të theksohet se AIP ka krijuar masa mbrojtëse për të mbështetur zbatimin efektiv të Ligjit për Mbrojtjen e të Dhënave Personale, duke ofruar udhëzime dhe

[23] Bylaws that derive from Law on Protection of Personal Data, https://gzk.rks-gov.net/ActDetail.aspx?ActID=18616&langid=2.
[24] Annual Working Report, Information and Privacy Agency, 2024, https://aip.rks-gov.net/download/raport-vjetor-i-performances-per-vitin-2023/?wpdmdl=6119&refresh=66c89a203ca4f1724422688
[25] Annual Working Report, Information and Privacy Agency, 2023, https://aip.rks-gov.net/download/raport-vjetor-i-punes-per-vitin-2022/?wpdmdl=6122&refresh=66ee19fa5a96d1726880250
[26] Information gathered from the questionnaire.
[27] Bi-annual Report 2024 of the Information and Privacy Agency, July 2024, https://aip.rks-gov.net/download/raporti-gjashtemujor-aip-2024/?wpdmdl=6222&refresh=66c89a2037fad1724422688
[28] Ibid, page 3.

burime për të ndihmuar organizatat dhe individët të respektojnë standardet e mbrojtjes së të dhënave.[29] Këto masa përfshijnë ofrimin e udhëzimeve të plota për menaxhimin e të dhënave, kryerjen e inspektimeve të rregullta për të siguruar përputhshmërinë dhe ofrimin e burimeve arsimore për të rritur ndërgjegjësimin për të drejtat e privatësisë së të dhënave. Duke zbatuar këto masa mbrojtëse, AIP luan një rol kyç në promovimin e një kulture përgjegjësie dhe llogaridhënieje në përpunimin e të dhënave në sektorët publik dhe privat.

3. Sfidat dhe Boshllëqet në Mekanizmat e Zbatimit të Ligjit

Zbatimi i ligjeve për mbrojtjen e të dhënave në Kosovë paraqet shumë sfida teknike, politike, organizative dhe ligjore. Së pari, AIP është e autorizuar për të mbikëqyrur përputhshmërinë, por ajo has kufizime në terma të burimeve dhe kapacitetit. Kjo pengon aftësinë e saj për të kryer inspektime të thella, rishikime dhe veprime pasuese. Një nga sfidat kryesore ligjore që ka hasur AIP është procedurat e vonuara të rekrutimit, të cilat kanë rezultuar në mbingarkimin e stafit ekzistues, duke shtyrë kështu implementimin e disa proceseve. Për më tepër, nevoja për rregullore të qarta për mbledhjen e gjobave të vendosura ndaj institucioneve publike ka kufizuar AIP-në që të mbështetet në procedurat e zbatimit, duke çuar në kosto shtesë për buxhetin e Kosovës.[30]

Ndërkohë që AIP ka autoritetin për të vendosur gjoba dhe masa të tjera ndëshkuese, zbatimi i vërtetë i këtyre masave herë pas here përballet me vonesa procedurale, për shkak të kompleksitetit të rasteve, dhe ndonjëherë mungesës së bashkëpunimit nga organizatat. Një nga mangësitë kryesore në zbatimin e ligjit është niveli mjaft i ulët i ndërgjegjësimit publik në lidhje me të drejtat e mbrojtjes së të dhënave. Ky mungesë ndërgjegjësimi ka çuar në një numër më të vogël ankesash të paraqitura nga individët të cilët kanë pësuar dëm nga shkelja e të drejtave të tyre, duke ulur kështu presionin e përgjithshëm mbi organizatat për të përmbushur kërkesat e ligjit. Për më tepër, natyra e avancuar e teknologjive digjitale paraqet një sfidë të vazhdueshme për sistemin administrativ, pasi lindin forma të reja të përpunimit të të dhënave që nuk trajtohen plotësisht nga ligjet dhe rregulloret ekzistuese.

Një tjetër sfidë kritike është mungesa e një sistemi të fortë për bashkëpunimin ndërkufitar në çështjet e mbrojtjes së të dhënave. Duke pasur parasysh aspiratat e Kosovës për integrim më të ngushtë me Bashkimin Evropian, ekziston një nevojë urgjente për të përmirësuar mekanizmat e bashkëpunimit ndërkombëtar, veçanërisht në rastet që përfshijnë organizata shumëkombëshe ose flukse të të dhënave ndërkufitare.

Për të përparuar në përputhshmërinë dhe zbatimin e ligjit, është thelbësore të forcohen kapacitetet institucionale të AIP-së, të përmirësohen fushatat e ndërgjegjësimit publik dhe të sigurohet që organizatat të kenë rregulla të qarta dhe mbështetje për të përmbushur obligimet e tyre për mbrojtjen e të dhënave. Po ashtu, përditësimi i kuadrit ligjor për të trajtuar teknologjitë në zhvillim dhe nxitja e pjesëmarrjes ndërkombëtare do të jenë hapa thelbësorë për të garantuar mbrojtje të fortë të të dhënave në Kosovë.

[29] List of Safeguards available in the website of the AIP, https://aip.rks-gov.net/mbrojtja-e-te-dhenave-personale/mbrojtja-e-te-dhenave-personale/

[30] Annual Report of the AIP for 2023, https://aip.rks-gov.net/download/raport-vjetor-i-performances-per-vitin-2023/?wpdmdl=6119&refresh=66c89a203ca4f1724422688

4. Përpunuesit e Mëdhenj e të Dhënave

Sipas GDPR, termini ‘Përpunues’ definohet si ‘një person fizik ose juridik, autoritet publik, agjenci ose një organ tjetër që përpunon të dhënat personale në emër të kontrolluesit”.[31] *Big Data,* siç është përcaktuar në Strategjinë Digjitale të BE-së, i referohet një sasie të madhe të dhënash që prodhohen shumë shpejt nga një numër i lartë burimesh të ndryshme."[32] Prandaj, ne do të kombinojmë këto përkufizime dhe do të përdorim një përkufizim funksional për këtë raport, i cili e përcakton termin Përpunues të Mëdhenj të të Dhënave (Big Data Processors)si entitete publike ose private që përpunojnë sasi të mëdha të dhënash që prodhohen shumë shpejt nga burime të ndryshme.

Sot, po bëjmë dëshmitarë të një kalimi në një mjedis biznesi të bazuar në të dhëna. Kompanitë po shfrytëzojnë Big Data dhe analizat për t'u ndihmuar në marrjen e vendimeve për kompanitë e tyre. Për shembull, ato përdorin burime të jashtme të të dhënave për të ofruar kontekst dhe pasqyrime shtesë, siç janë mediat sociale, raportet e hulumtimit të tregut dhe të dhënat e qeverisë.[33]

Këta përpunues shpesh përballen me disa sfida në përpunimin e të dhënave për shkak të volumit dhe llojshmërisë së tyre. Menaxhimi dhe ruajtja e datasetëve të mëdha dhe të pa strukturuara paraqesin probleme të rëndësishme për Përpunuesit e Mëdhenj. Këto datasetë përfshijnë të dhëna transaksionale, ushqime nga mediat sociale, të dhëna sensorike nga pajisjet IoT dhe më shumë. Për shembull, për të ofruar eksperienca të personalizuara, bizneset si Capital One dhe Amazon përpunojnë sasira të mëdha të të dhënave të klientëve në industrinë e shitjeve me pakicë dhe financave. Për të ofruar marketing të personalizuar dhe sugjerime për produkte, ato analizojnë tendencat që gjenden në të dhënat transaksionale, ndërveprimet me konsumatorët dhe historitë e blerjeve.[34]

Për të mbetur në përputhje me GDPR-në, Përpunuesit e mëdhenj të të dhënave duhet të sigurojnë që të jenë vendosur masa të përshtatshme sigurie për të parandaluar aksesin e paautorizuar, shkeljet ose keqpërdorimin e të dhënave. Sasia e madhe e informacionit personal dhe të ndjeshëm të përpunuar mund të përbëjë një shqetësim për privatësinë. Për shembull, institucionet mjekësore si Memorial Sloan Kettering Cancer (MSKCC) menaxhojnë një sasi të madhe të dhënash shumë të ndjeshme dhe përdorin analiza të Big Data për të personalizuar trajtimet për kancerin.[35] Prandaj, institucione të tilla duhet të jenë shumë të kujdesshëm, pasi shkeljet e këtij informacioni të ndjeshëm mund të çojnë në pasoja të mëdha.

Një çështje tjetër për përpunuesit është marrja dhe menaxhimi i pëlqimit nga individët të cilëve po përpunohen të dhënat. Pasi është shumë e vështirë të shpjegohet metodat e mbledhjes së të dhënave, individët priren të pajtohen pa e kuptuar me përpunimin e të dhënave të tyre nga shërbime të palëve të treta. Për shembull, platformat e mediave sociale, si Facebook, kanë qenë nën hetim për çështje që lidhen me pëlqimin dhe transparencën, veçanërisht në rastin e

[31] GDPR, art. 3

[32] Digital Strategy: Shaping Europe’s digital future, 2024, https://digital-strategy.ec.europa.eu/en

[33] Strategies for Leveraging Big Data and Analytics for Business Development: A Comprehensive Review Across Sectors, N. Adaobi Ochuba, et. Al., published: 9 March 2024.

[34] Ibid.

[35] Designing Data Spaces: The Ecosystem Approach to Competitive Advantage, edited by Boris Otto, et al., Springer International Publishing AG, 2022.

skandalit të Cambridge Analytica, ku të dhënat e miliona përdoruesve u mblodhën pa pëlqimin e tyre të qartë..[36] Në këtë rast, Cambridge Analytica ishte një kompani britanike konsulente politike, e cila përmes një kuizi mblodhi të dhëna nga profilet e miliona përdoruesve të Facebook. Mendohet se kjo ndodhi për shkak të masave të pamjaftueshme mbrojtëse kundër firmave që merren me nxjerrjen e të dhënave dhe mbikëqyrjes së pamjaftueshme nga Facebook.[37]

Një çështje tjetër sfiduese është se Përpunuesit e mëdhenj të të dhënave që operojnë ndërkombëtarisht duhet të përmbushin rregullat e GDPR-së, përfshirë kufizimet për transferimet ndërkombëtare të të dhënave. Menaxhimi i operacioneve globale, ndërkohë që respektohen ligjet rajonale për mbrojtjen e të dhënave, sjell kompleksitet shtesë. Në rastin e kompanive shumëkombëshe (p.sh., Amazon), ato duhet të përmbushin ligje të ndryshme për mbrojtjen e të dhënave, siç janë GDPR dhe Ligji i Privatësisë së Konsumatorëve të Kalifornisë (CCPA), të cilat kërkojnë mbikëqyrje dhe përditësim të vazhdueshëm të praktikave të tyre të përpunimit të të dhënave.[38]

[36] Strategies for Leveraging Big Data and Analytics for Business Development: A Comprehensive Review Across Sectors, N. Adaobi Ochuba, et. Al., published: 9 March 2024.
[37] Facebook – Cambridge Analytica data harvesting: What you need to know, Ikhlaq ur Rehman, University of Nebraska – Lincoln, 2019.
[38] Designing Data Spaces: The Ecosystem Approach to Competitive Advantage, edited by Boris Otto, et al., Springer International Publishing AG, 2022.

Kapitulli III: Përpunuesit e Mëdhenj në Kosovë

1. Përpunuesit e mëdhenj dhe mbrojtja e të dhënave

Përpunuesit e mëdhenj luajnë një rol të rëndësishëm në përpunimin dhe menaxhimin e të dhënave personale të qytetarëve të Kosovës, veçanërisht duke marrë parasysh nivelin e lartë të digjitalizimit në Kosovë. Këto entitete operojnë në sektore të ndryshëm, si telekomunikacionet, financat dhe shëndetësia, dhe janë në gjendje të përpunojnë sasi të mëdha informacioni, disa prej të cilave janë të ndjeshme. Prandaj, është thelbësore të vlerësohet nëse këta Përpunues të Mëdhenj veprojnë në përputhje me Ligjin për Mbrojtjen e të Dhënave Personale (LMDHP).

Nëpër botë, kemi qenë dëshmitarë të shkeljeve të mëdha të të dhënave që ekspozuan dobësitë brenda disa nga përpunuesve më të mëdhenj të të dhënave. Shembuj si rasti i përmendur i skandalit Facebook-Cambridge Analytica, si dhe shkelja e të dhënave financiare nga Equifax dhe shkeljet masive të llogarive të përdoruesve nga Yahoo, kanë treguar ndikimin e thellë që keqpërdorimi i të dhënave mund të ketë tek individët dhe besimi i publikut. Këto shkelje theksojnë sfidat globale në mbrojtjen e të dhënave dhe theksojnë nevojën për përputhshmëri të plotë me kuadrot ligjore.

Në Kosovë, këto shqetësime po bëhen gjithnjë e më të rëndësishme për shkak të integrimit të thellë të vendit në ekonominë globale digjitale. Sipas Agjendës Digjitale të Kosovës 2030, Kosova është një shoqëri informacioni që po punon drejt zhvillimit të teknologjive dhe shërbimeve të reja.[39] Objektivat kryesore që dalin nga kjo Agjendë janë:

- Atlas i plotë i digjitalizuar i Infrastrukturës së Broadband-it të Fiksuar;
- Lidhje Gigabit në dispozicion për të gjitha Institucionet Publike;
- Mbulim i avancuar i 5G në nivel kombëtar; 80% e Kompanive Kosovare që përdorin Cloud/AI/Big Data;
- 100% e Shërbimeve Kyçe Publike në dispozicion Online;
- 90% e Qytetarëve të Kosovës që përdorin Identifikimin Digjital;
- 100% e Regjistrave Mjekësorë të disponueshëm në formë digjitale Online; dhe kështu me radhë.

Duke kuptuar se fokusi i Qeverisë së Kosovës është të avancojë dhe të punojë drejt këtyre objektivave, ky studim do të kufizojë gamën e kërkimit të tij. Për më tepër, pasi që institucionet financiare të mëdha, kompanitë e telekomunikacionit dhe organizatat e sektorit publik përpunojnë sasi të mëdha të të dhënave personale dhe transaksionale çdo ditë, ky studim do të fokusohet vetëm në këto fusha. Për më shumë, duke pasur parasysh rolin e tyre në formësimin e mjedisit të të dhënave në Kosovë, bëhet e domosdoshme të shqyrtohen praktikat e tyre dhe të sigurohet që ato janë në përputhje me LMDHP-në dhe kërkesat për mbrojtjen e të dhënave në përputhje me GDPR-në.

Shumë përpunues të njohur të të dhënave ndikojnë ndjeshëm në peizazhin digjital të Kosovës, secili luan një rol kyç në mbledhjen, organizimin dhe menaxhimin e të dhënave personale në

[39] Kosovo Digital Agenda 2030: Strategic orientation for Kosovo transformation into a successful digital country, Government of Kosovo, 2023.

sektorë të ndryshëm. Aktorët kryesorë përfshijnë bizneset e mëdha të shitjes me pakicë, institucionet financiare, shërbimet publike dhe kompanitë e telekomunikacionit. Këto entitete janë qendrore për funksionimin e infrastrukturës digjitale të Kosovës, duke përpunuar sasi të mëdha informacioni personal dhe të ndjeshëm çdo ditë. Duke pasur parasysh ndikimin e tyre, është thelbësore të vlerësohen praktikat e tyre të mbrojtjes së të dhënave për të siguruar që ato plotësojnë standardet e vendosura nga LMDHP-ja dhe janë në përputhje me kërkesat e GDPR-së, duke siguruar kështu mbrojtjen e privatësisë së qytetarëve në ekonominë digjitale në zhvillim të Kosovës.

2. Kompanië e Telekomunikacionit

Sipas Udhëzuesit Komercial të Vendit nga Administrata e Tregtisë Ndërkombëtare, Telekomi i Kosovës (Vala) mban një pjesë të konsiderueshme të tregut të telekomunikacioneve, rreth 50%. Gjithashtu, IPKO, një tjetër lojtar kryesor, konkurron në segmentet e telefonisë mobile dhe broadband. Këto dy kompani janë operatorët kryesorë dhe së bashku dominuojnë shumicën e tregut.[40]

Në Kosovë, kompanitë e telekomunikacioneve si Telekomi (Vala) dhe IPKO luajnë një rol të rëndësishëm në ekosistemin digjital. Si ofrues kryesorë të shërbimeve mobile dhe broadband, ato përpunojnë sasi të mëdha të të dhënave personale çdo ditë, duke përfshirë identifikimin e përdoruesve, të dhënat e trafikut dhe të dhënat e vendndodhjes. Me objektivat e Qeverisë të përcaktuara në Agjendën Digjitale të Kosovës 2030, pritet që kompanitë e telekomunikacioneve të mbështesin qëllime kyçe, si ofrimi i mbulimit të avancuar kombëtar 5G, arritja e lidhjes gigabit për institucionet publike dhe mundësimi i identifikimit digjital të plotë. Roli i këtyre kompanive si përpunues të mëdhenj të të dhënave i bën ato lojtarë të rëndësishëm në mbrojtjen e të dhënave personale dhe ruajtjen e të drejtave të privatësisë së qytetarëve.

Kompanitë e telekomunikacioneve në mbarë botën përballen me mundësi unike për të përmirësuar perspektivat e tyre në treg për shkak të avancimeve teknologjike. Këto kompani përpunojnë sasi të mëdha të të dhënave personale dhe transaksionale, prandaj, sfidat që lidhen me mbrojtjen e të dhënave dhe përputhshmërinë janë të pashmangshme. Studimet e fundit tregojnë se Analitika e Big Data-s – procesi i shqyrtimit të grupeve të mëdha dhe komplekse të të dhënave, të njohura si "big data", për të zbuluar modele, tendenca, korrelacione dhe kuptime që mund të ndihmojnë në marrjen e vendimeve biznesore – ka transformuar sektorin e telekomunikacioneve, duke mundësuar këto kompani të kenë një avantazh konkurrues, veçanërisht në identifikimin e efikasiteteve, alokimin optimal të burimeve dhe përmirësimin e proceseve.[41] Kjo i ndihmon kompanitë që përdorin Analitikën e Big Data-s të dalin në pah në një treg shumë konkurrues, duke ofruar shërbime të personalizuara sipas nevojave të konsumatorëve. Analitika e Big Data-s mundëson që kompanitë e telekomunikacioneve të analizojnë sasi të mëdha të të dhënave të konsumatorëve në kohë reale, duke përmirësuar kënaqësinë e konsumatorëve.

[40] International Trade Administration, Kosovo – Country Commercial Guide, https://www.trade.gov/country-commercial-guides/kosovo-telecommunications

[41] Impact of Big Data Analytics on Telecom Companies' Competitive Advantage, A. Alshawawreh, et.al., 2024.

Po ashtu, në Kosovë, kompani si Telekomi (Vala), Ipko dhe Telcos janë ndër përpunuesit më të mëdhenj të të dhënave, duke përpunuar sasi të mëdha të të dhënave personale. Përmes analitikës së avancuar të të dhënave, ato mund të parashikojnë më mirë sjelljen e konsumatorëve, të optimizojnë ofertat e shërbimeve dhe të adresojnë ankesat e konsumatorëve në kohë.

Përveç këtyre avantazheve, avancimi i përmendur ngre shqetësime për privatësinë. Kompanitë e telekomunikacioneve në Kosovë duhet të sigurojnë që masat për mbrojtjen e të dhënave të jenë në përputhje me Ligjin për Mbrojtjen e të Dhënave Personale (LMDHP). Sigurimi i përputhshmërisë me ligjin lokal dhe adresimi i rritjes së rreziqeve të shkeljeve të të dhënave, veçanërisht me dataset të mëdha, është thelbësor për këto organizata për të ruajtur besimin e konsumatorëve.

Për një krahasim, mund të analizohet Vodafone, një nga ofruesit më të mëdhenj të telekomunikacionit në BE. Vodafone duhet të përputhet me Rregulloren e Përgjithshme për Mbrojtjen e të Dhënave (GDPR). Vodafone deklaron se është e rëndësishme të respektohet dhe mbrohet e drejta për privatësinë në mënyrë që të ruhet e drejta e konsumatorit. Vodafone siguron përputhshmërinë me GDPR duke zbatuar politika për mbrojtjen e të dhënave, përfshirë emërimin e Oficerëve për Mbrojtjen e të Dhënave (DPO) në të gjitha degët e saj evropiane, duke zbatuar parimin e Privacy by Design dhe duke mundësuar përdoruesve të kontrollojnë të dhënat e tyre personale përmes sistemeve të menaxhimit të pëlqimeve.[42] Vodafone gjithashtu ndërmerr hapa për të anonimizuar dhe koduar të dhënat, duke minimizuar rrezikun e shkeljeve. Për më tepër, Vodafone publikojnë raporte vjetore dhe deklarata për privatësinë për të informuar klientët e saj në lidhje me përputhshmërinë me GDPR.[43]

Nga ana tjetër, IPKO Telecommunications LLC, një nga ofruesit më të mëdhenj të shërbimeve të telekomunikacionit në Kosovë, ka një seksion në faqen e saj të internetit që informon publikun në lidhje me përputhshmërinë e saj me Ligjin aktual për Mbrojtjen e të Dhënave Personale. Ajo informon publikun se përpunimi i të dhënave personale të përdoruesve të shërbimeve të saj të komunikimeve elektronike bëhet në përputhje me LMDHP-në.[44] Politika e Privatësisë e IPKO-s përcakton se kompania mbledh dhe përdor të dhënat personale mbi disa baza ligjore, siç janë pëlqimi, kërkesat ligjore, detyrimet kontraktuale dhe interesat legjitime. Informacioni mbi identifikimin e një personi, të dhënat e komunikimit dhe të dhënat që lidhen me përdorimin e shërbimeve të IPKO-s—siç janë të dhënat e vendndodhjes dhe trafikut—janë ndër të dhënat që përpunohen.[45]

Për më tepër, Politika e Privatësisë e IPKO-s thekson disa hapa që ata ndërmarrin për të garantuar privatësinë e të dhënave, duke përfshirë vendosjen e procedurave për mbrojtjen e të dhënave kur trajtohen të dhënat personale, përcaktimin nëse përpunimi i të dhënave është i nevojshëm dhe mundësinë për përdoruesit që të revokojnë pëlqimin e tyre në çdo moment. Gjithashtu, në faqen e tyre të internetit, ka informacion dhe një adresë emaili për të kontaktuar

[42] Privacy Centre, Vodafone, https://www.vodafone.com/about-vodafone/how-we-operate/consumer-privacy-and-cyber-security/privacy-centre
[43] Vodafone, Annual Report 2024, https://reports.investors.vodafone.com/view/197179846/47/#zoom=true
[44] IPKO Telecommunications LLC website, data protection section, https://www.ipko.com/en/private/data-protection/
[45] Ibid.

Ofiçerin për Mbrojtjen e të Dhënave të IPKO-s, për çështje që lidhen me mbrojtjen e të dhënave.[46]

3. Institucionet Financiare

Institucionet financiare përpunojnë një sasi të madhe të dhënash shumë të ndjeshme. Ndërsa bankat dhe ofruesit e tjerë të shërbimeve financiare trajtojnë sasi të mëdha të të dhënave personale, transaksionale dhe financiare çdo ditë, ato luajnë një rol të rëndësishëm në ekonominë digjitale. Integrimi i analizës së të dhënave të mëdha dhe inteligjencës artificiale (AI) ka transformuar ndjeshëm sektorin financiar, duke i ofruar institucioneve mjete për të optimizuar shërbimet e tyre, menaxhuar rreziqet dhe përmirësuar përvojat e konsumatorëve. Institucionet financiare, duke shfrytëzuar këtë aset, mund të kuptojnë më mirë tregjet, klientët, produktet, rregullat dhe konkurentët, gjë që do t'u mundësojë të konkurrojnë më mirë.[47] Kjo ka treguar efikasitet edhe në fusha të ndryshme si zbulimi i mashtrimeve, vlerësimi i kredive dhe përputhshmëria me rregulloret. Për shembull, teknologjitë e inteligjencës artificiale dhe të dhënat e mëdha luajnë një rol thelbësor në ndihmën e institucioneve financiare për automatizimin e zbulimit të mashtrimeve duke identifikuar modelet dhe anomali në kohë reale, duke parandaluar transaksionet e paautorizuara dhe duke mbrojtur të dhënat e konsumatorëve.[48]

Megjithatë, këto përparësi vijnë së bashku me përgjegjësi të mëdha në lidhje me privatësinë dhe sigurinë e të dhënave. Institucionet financiare janë të detyruara të mbrojnë të dhënat e ndjeshme nga shkeljet dhe keqpërdorimi, duke zbatuar rregullat për mbrojtjen e të dhënave.[49]

Një shembull i një institucioni financiar në BE është Deutsche Bank. Si një nga bankat më të mëdha në Europë, Deutsche Bank ka zbatuar masa për t'u pajtuar me Rregulloren e Përgjithshme për Mbrojtjen e të Dhënave (GDPR).[50] Këto masa përfshijnë emërimin e një Oficeri për Mbrojtjen e të Dhënave (DPO), i cili është përgjegjës për mbikëqyrjen e pajtueshmërisë dhe vepron si një lidhës midis bankës dhe autoriteteve rregullatore. Informacioni në lidhje me DPO mund të gjendet në faqen e tyre të internetit.[51] Nga informacioni i ofruar nga Deutsche Bank, kuptohet se banka ndiqka parimet e GDPR-së, siç janë minimizimi i të dhënave, duke mbledhur vetëm të dhënat e nevojshme për qëllime të caktuara, dhe kufizimi i qëllimit, duke siguruar që të dhënat përdoren vetëm për qëllimin e synuar.

Për më tepër, Deutsche Bank ofron politika të qarta për privatësinë që përshkruajnë të drejtat e klientëve, duke përfshirë të drejtën për të aksesuar, korrigjuar, fshirë ose transferuar të dhënat

[46] Ibid.

[47] New Horizons for a Data-Driven Economy : A Roadmap for Usage and Exploitation of Big Data in Europe, edited by José María Cavanillas, et al., Springer International Publishing AG, 2016.

[48] Ibid.

[49] A Comprehensive Study on Integration of Big Data and AI in Financial Industry and AI in Financial Industry and its Effect on Present and Future Opportunities, S. Ahmadi, International Journal of Current Science Research and Review, 2024, 07 (01), pp.66-74. ff10.47191/ijcsrr/V7-i1-07ff. ffhal-04456267ff

[50] Deutsche Bank website, Privacy Notice, https://www.db.com/legal-resources/privacy-notice?language_id=1&kid=cookies.redirect-en.shortcut#show-content-of-cookies

[51] Data Protection Information under the EU General Data Protection Regulation for "natural persons", May 2018, https://www.deutsche-bank.de/dam/deutschebank/de/shared/pdf/GDPR_Datenschutzhinweis_f%C3%BCr%20Interessenten_EN.PDF.

e tyre. Për të parandaluar shkeljet e të dhënave, banka përdor masa të forta të sigurisë kibernetike, siç janë enkriptimi dhe auditimet e rregullta. Punonjësit trajnohen për kërkesat e GDPR-së për të siguruar pajtueshmërinë në të gjitha nivelet e organizatës. Këto përpjekje ndihmojnë Deutsche Bank të ruajë transparencën, të mbrojë të dhënat e klientëve dhe të shmangë mundësitë për ndëshkime nën GDPR.

Në Kosovë, numri i institucioneve financiare të licencuara dhe të regjistruara në Bankën Qendrore të Republikës së Kosovës është 154. Ky numër përfshin banka të licencuara, institucione mikro-financiare, institucione financiare jo-banking, kompani sigurimesh, brokerë sigurimesh, brokerë të pavarur dhe fonde pensionesh.[52] Në përgjithësi, institucionet financiare në Kosovë, veçanërisht Bankat, kanë mekanizmat më të avancuar për përputhshmërinë me mbrojtjen e të dhënave dhe kërkesat e tjera të aplikueshme.

Raiffeisen Bank Kosovo dhe Banka Ekonomike janë dy shembuj të bankave dhe ofruesve të shërbimeve financiare që luajnë një rol të rëndësishëm në përpunimin e të dhënave financiare të ndjeshme. Për shkak të ndjeshmërisë së të dhënave që këto organizata trajtojnë, ato janë subjekt i kufizimeve të rrepta lidhur me sigurinë e të dhënave dhe privatësinë. Aktivitetet e tyre janë një kontribues i rëndësishëm në ekonominë digjitale të Kosovës, pasi përdorin teknologji të avancuar të përpunimit të të dhënave për të bërë transaksione të sigurta dhe për të lehtësuar administrimin financiar.

Si banka lokale e Kosovës, Banka Ekonomike informon publikun për mbrojtjen e të dhënave duke postuar rregulla të qarta në faqen e saj të internetit. Klientët këshillohen nga banka që të dërgojnë kërkesa me shkrim në një email të caktuar ose të vizitojnë zyrat e tyre nëse kanë ndonjë shqetësim lidhur me mënyrën se si përpunohen të dhënat e tyre personale nëpërmjet faqes së internetit ose nëse duan të ushtrojnë të drejtat e tyre për mbrojtjen e të dhënave.[53] Po ashtu, Banka Ekonomike përmend se, për t'u përputhur me kërkesat, njoftimi i saj për privatësinë mund të ndryshohet rregullisht.[54]

Raiffeisen Bank në Kosovë ka një pjesë të tregut të huave prej 20 përqind deri në fund të qershorit 2023 dhe është banka më e madhe në Kosovë.[55] Për shkak të madhësisë dhe ndikimit të tij në peizazhin financiar, Raiffeisen Bank thekson ruajtjen e një infrastrukture të fuqishme për mbrojtjen e të dhënave personale. Politikat e saj për privatësinë përshkruajnë parimet e mbrojtjes së të dhënave dhe informojnë klientët për të drejtat e tyre për të aksesuar, rregulluar ose fshirë informacionin e tyre personal. Në përputhje me LMDHP-në, Raiffeisen Bank angazhohet për sigurimin e të dhënave, duke zbatuar masa mbrojtëse si kodimin, minimizimin e të dhënave dhe kufizimin e qëllimit për të mbrojtur informacionin e klientëve.

Institucionet financiare të tjera në Kosovë, megjithëse ndryshojnë në madhësi dhe përhapje, gjithashtu janë të lidhura me detyrimet për mbrojtjen e të dhënave sipas LMDHP-së. Këto

---

[52] Financial Licensed and registered Institutions, Central Bank of the Republic of Kosovo, https://bqk-kos.org/wp-content/uploads/2024/08/Lista-e-institucioneve-financiare_12.02.2024-005.pdf.

[53] Banka Ekonomike website, https://bekonomike.com/sq/Mbrojtja-e-t%C3%AB-dh%C3%ABnave-personale-%7C-P%C3%ABrdorimi-i-Cookies

[54] Ibid.

[55] European Bank for Reconstruction and Development (EBRD), 2024 https://www.ebrd.com/news/2024/ebrd-teams-up-with-raiffeisen-to-boost-msme-lending-in-kosovo.html#:~:text=Raiffeisen%20Bank%20is%20the%20largest,than%20900%20employees%20across%20Kosovo.

institucione duhet të krijojnë mekanizma mbrojtjeje të të dhënave, të emërojnë DPO (Oficerë për Mbrojtjen e Të Dhënave) dhe të kryejnë audite të rregullta për të siguruar përputhshmërinë me standardet kombëtare dhe ato të përshtatshme me BE-në. Ndërkohë që sektori financiar i Kosovës integrohet më thellë në ekonominë digjitale globale, përpjekjet e vazhdueshme për forcimin e praktikave të mbrojtjes së të dhënave do të jenë të domosdoshme për të ruajtur përputhshmërinë, mbrojtur informacionin e klientëve dhe për të nxitur besimin e publikut në shërbimet financiare digjitale.

4. Administrata Publike

Administrata publike në Kosovë luan një rol të rëndësishëm në përpunimin dhe menaxhimin e një sasie të konsiderueshme të dhënash personale. Është jashtëzakonisht e rëndësishme që institucionet publike të sigurojnë mbrojtjen e të dhënave për të ruajtur besimin e publikut dhe për të shmangur dëmin për qytetarët. Këto institucione përfshijnë ministra, agjenci, organe rregullatore dhe entitete të qeverisjes lokale, të cilat shpesh menaxhojnë informacione të ndjeshme si shëndeti i qytetarëve, të dhënat financiare, çështjet ligjore dhe shërbimet sociale. Për të siguruar që të dhënat që ato përpunojnë dhe kanë qasje në to janë të sigurta, LMDHP-ja është e aplikueshme edhe për institucionet publike.

Strategjia e eGovernment e Kosovës 2023-2027 përparon nevojën për një qasje më të bashkërenduar, duke u fokusuar në koordinimin e eGovernment, sigurinë kibernetike dhe zhvillimin e aftësive digjitale. Strategjia inkurajon inovacionin, në mënyrë që të arrijë qëllimin për ta bërë Kosovën një vend të digjitalizuar modern me një ekonomi digjitale të avancuar dhe administratë publike efikase deri në vitin 2030.[56] Në vitin 2023, Qeveria e Kosovës miratoi Agjendën Digjitale 2030, ku prioritetet kryesore strategjike janë zhvillimi i infrastrukturës TIK, zhvillimi i përmbajtjes dhe shërbimeve elektronike dhe përkrahja e përdorimit të tyre, dhe rritja e kapaciteteve të banorëve të Kosovës për të përdorur TIK.[57] Kjo do të thotë se Qeveria po punon drejt digjitalizimit. Në Kosovë, lansimi i Portalit eKosova mundësoi që qytetarët e Kosovës të interaktojnë me Administratën Publike në mënyrë digjitale. Në këtë platformë, ofrohen shërbime për qytetarët dhe bizneset, duke përfshirë shërbime për statusin civil, arsim, tatime, polici, shëndetësi dhe shumë të tjera.[58]

Përdorimi i platformës ka përjetuar një rritje të konsiderueshme gjatë viteve. Platforma eKosova konsiderohet si një nga reformat kyçe në Administratën Publike të Kosovës, ku sot ofrohen 155 shërbime online në 22 kategori nga ky portal.[59]

Megjithatë, një sfidë e mbetur është se menaxhimi teknik i platformës eKosova, së bashku me shërbimet e tjera të qeverisë elektronike, varet shumë nga partnerët e jashtëm. Ky varshmëri nga partnerët jashtë për funksionet teknike kyçe—si infrastruktura e sistemeve, siguria kibernetike dhe mirëmbajtja e vazhdueshme—kufizon kontrollin direkt të Kosovës mbi këto

[56] eGovernment Strategy Kosovo 2023-2027, https://mpb.rks-gov.net/Uploads/Documents/Pdf/EN/2700/e-Government%20Strategy%20Kosovo%202023-2027.pdf

[57] Kosovo Digital Agenda 2030: Strategic orientation for Kosovo transformation into a successful digital country, Government of Kosovo, 2023.

[58] eKosova Platform, https://ekosova.rks-gov.net/Services

[59] Kosovo 2024 Digital Public Administration Factsheet: Main developments in digital public administrations and interoperability, https://joinup.ec.europa.eu/sites/default/files/inline-files/NIFO_2024%20Supporting%20Document_Kosovo_vFinal_rev.pdf

platforma. Kjo varshmëri mund të ndikojë në qëndrueshmërinë afatgjatë, sigurinë dhe përshtatshmërinë e eKosova dhe shërbimeve të tjera digjitale të qeverisë.[60]

Përdorimi në rritje i Teknologjisë së Informacionit dhe Komunikimit (TIK) në administratën publike gjithashtu paraqet rreziqe, veçanërisht në sigurimin e të dhënave private të qytetarëve. Sipas një studimi mbi digjitalizimin, përdorimi i TIK-ut në administratën publike të Kosovës ka mundësuar ofrimin më të shpejtë dhe më transparent të shërbimeve, por gjithashtu ka ngritur shqetësime mbi shkeljet e të dhënave dhe përshtatshmërinë e mbrojtjeve ligjore.[61]

Agjencia për Regjistrimin Civil është një nga agjencitë më të mëdha që përpunon të dhëna personale. Në janar 2024, u miratua Ligji nr. 08/L-240 për Agjencinë e Regjistrimit Civil, i cili krijoi Agjencinë për Regjistrimin Civil dhe përcaktoi detyrat dhe përgjegjësitë e saj në nivelin qendror dhe lokal.[62] Agjencia ka një sasi të madhe të dhënash personale. Megjithatë, aksesimi është i kufizuar vetëm për funksionarët e autorizuar brenda Agjencisë për Regjistrimin Civil. Që nga viti 2018, Agjencia ka përdorur Platformën e Interoperabilitetit të Kosovës, e cila bazohet në Portën e Qeverisë (GG) të Microsoft. Numri i transaksioneve të procesuar përmes kësaj platforme ka qenë në rritje dhe në vitin 2023 kaloi 16 milionë, duke shënuar një rritje prej 26 për qind krahasuar me vitin e kaluar. [63]

5. Shërbimet Publike

Shërbimet publike, si Prishtina Parking dhe Korporata Energjetike e Kosovës (KEK), luajnë një rol të rëndësishëm në ekonominë digjitale të Kosovës, duke menaxhuar sasi të mëdha të të dhënave personale dhe operacionale. Këto kompani mbështeten në sistemet TIK për të optimizuar ofrimin e shërbimeve, për të monitoruar përdorimin e burimeve dhe për të lehtësuar ndërveprimet me klientët. Po ashtu, si institucionet qeveritare, kompanitë e shërbimeve publike duhet të respektojnë ligjet për mbrojtjen e të dhënave për të mbrojtur informacionin personal nga aksesimi i paautorizuar ose shkeljet e mundshme.

Me rritjen e shërbimeve publike digjitale, kompanitë e shërbimeve publike gjithashtu po integrojnë modele të qeverisjes elektronike për të përmirësuar proceset dhe shërbimin ndaj klientëve. Për shembull, Prishtina Parking ka adoptuar sisteme digjitale për menaxhimin e shërbimeve të parkimit, duke e bërë mbrojtjen e të dhënave një shqetësim kyç pasi ato trajtojnë informacion të ndjeshëm mbi automjetet dhe pagesat. Ligji për Organet e Shoqërisë së Informacionit në Kosovë përcakton udhëzime të qarta për përdorimin e TIK-ut për menaxhimin e të dhënave, duke siguruar që shërbimet publike të respektojnë rregulloret kombëtare për mbrojtjen e të dhënave.

Kushtet e përgjithshme të sektorit lidhur me mbrojtjen e të dhënave në Kosovë zbulojnë një përzierje forcash dhe fusha që kërkojnë përmirësim. Ndërsa shumë kompani, si KESCO, kanë ndërmarrë hapa për të publikuar politika për privatësinë në faqet e tyre të internetit, shpesh ka mangësi në transparencë dhe aksesueshmëri për klientët që kërkojnë informacione më të

[60] eGovernment Strategy Kosovo 2023-2027, https://mpb.rks-gov.net/Uploads/Documents/Pdf/EN/2700/e-Government%20Strategy%20Kosovo%202023-2027.pdf

[61] Digitalization of Administration and Legal Basis in Kosovo, K.Dërmaku, A.Emini, 2024.

[62] Law no.08/L-240 on Civil Registration Agency, https://gzk.rks-gov.net/ActDetail.aspx?ActID=85153

[63] Kosovo 2024 Digital Public Administration Factsheet: Main developments in digital public administrations and interoperability, https://joinup.ec.europa.eu/sites/default/files/inline-files/NIFO_2024%20Supporting%20Document_Kosovo_vFinal_rev.pdf

detajuara. Për shembull, Politika e Privatësisë së KESCO-s është e qasshme online dhe përshkruan angazhimin e kompanisë për mbrojtjen e të dhënave; megjithatë, ajo ka mungesë udhëzimesh të qarta se si klientët mund të adresojnë shqetësimet për mbrojtjen e të dhënave ose të raportojnë shkeljet e mundshme.[64]

Ky hendek nuk është i veçantë për KESCO-n. Në sektorë të ndryshëm, praktikat e mbrojtjes së të dhënave shpesh nuk plotësojnë plotësisht nevojat e klientëve për transparencë dhe përgjegjësi. Pak kompani ofrojnë informacione specifike kontaktimi për përgjegjësit e mbrojtjes së të dhënave (DPO) ose një pikë kontakti të drejtpërdrejtë për pyetje lidhur me privatësinë. Për më tepër, ndërsa politikat mund të përshkruajnë parime të përgjithshme të mbrojtjes së të dhënave, detaje të veprueshme—si procedurat për menaxhimin e shkeljeve të të dhënave ose trajtimin e kërkesave të klientëve për ushtrimin e të drejtave të tyre për të dhënat—shpesh mungojnë.

Për të forcuar praktikat e mbrojtjes së të dhënave nëpër sektore, do të kërkohet që kompanitë jo vetëm të respektojnë kërkesat rregullatore si LMDHP-ja, por gjithashtu të adoptojnë një qasje proaktive në bëjnë proceset e tyre të menaxhimit të të dhënave transparente. Kanale të qarta komunikimi, kontakte të dedikuara për mbrojtjen e të dhënave dhe politika të detajuara të privatësisë mund të ndihmojnë në ndërtimin e besimit publik dhe të sigurojnë përputhshmërinë me standardet lokale dhe ato të harmonizuara me BE-në.

6. Sektori shëndetësor

Sektori shëndetësor në Kosovë përfshin një rrjet të gjerë institucionesh publike dhe private që merren me sasi të mëdha të të dhënave të ndjeshme shëndetësore. Sipas Agjencisë së Statistikave të Kosovës, në vend janë 2,095 institucione shëndetësore private të licencuara, përfshirë 29 spitale dhe 2,066 institucione të tjera shëndetësore si ambulanca, poliklinika dhe laboratorë.[65] Pavarësisht se Kosova ka bërë hapa për të përmirësuar mbrojtjen e të dhënave në sektorin e shëndetësisë, shumë institucione ende përballen me sfida në implementimin e masave të plota të sigurisë për shkak të resurseve të kufizuara dhe mbështetjes teknike.

Kosova është në proces të zhvillimit të një Sistemi të Integruar të Informacionit Shëndetësor (SIIS), i cili konsiderohet shumë i rëndësishëm për të ofruar dhe përmirësuar cilësinë e kujdesit shëndetësor. Ky informacion mund të përdoret gjithashtu nga politikanët për të kontribuar në këto përmirësime.

Aktualisht, është në funksion një Sistemi Bazik i Informacionit Shëndetësor (SBIS), dhe funksionaliteti i tij ka shpërthyer kohët e fundit përtej thjesht regjistrimit të pacientëve, duke përfshirë edhe ndjekjen e historikut mjekësor të pacientëve. SBIS komunikon me disa nga sistemet ekzistuese (si ePrescription, Sistemi i Fluksit të Informacionit Shëndetësor, Sistemi i Menaxhimit të Stokut Farmaceutik, Sistemi i Mbikëqyrjes dhe Sistemi i Parashikimit të Hershëm).[66] Furnizuesit e shërbimeve shëndetësore menaxhojnë të dhëna të ndjeshme të pacientëve, siç janë historiku mjekësor, diagnozat dhe trajtimet, gjë që e bën sektorin veçanërisht të ndjeshëm ndaj shkeljeve të të dhënave. Sipas studimeve ndërkombëtare, nëse

[64] Privacy Policy, KESCO, 2020, https://www.kesco-energy.com/?pageId=74&language=2&isPreview=True

[65] Health Statistics 2022, Kosovo Agency of Statistics, https://ask.rks-gov.net/Releases/Details/7265

[66] Kosovo 2024 Digital Public Administration Factsheet: Main developments in digital public administrations and interoperability, https://joinup.ec.europa.eu/sites/default/files/inline-files/NIFO_2024%20Supporting%20Document_Kosovo_vFinal_rev.pdf

ndodhin shkelje të të dhënave personale shëndetësore, ato mund të kenë pasoja të rënda, duke përfshirë vjedhjen e identitetit dhe mashtrimin me sigurime. Një shembull i njohur i kësaj është shkelja e të dhënave në masë në një sigurues shëndetësor të bazuar në SHBA, ku u vodhën 78.8 milionë regjistrime pacientësh, duke theksuar seriozitetin e ngjarjeve të tilla. [67] Kjo shkelje çoi në vjedhjen e identitetit në masë, ku informacionet personale dhe mjekësore të vjedhura u përdorën për të marrë shërbime mjekësore në mënyrë mashtruese dhe për të bërë kërkesa për sigurime, duke ndikuar në stabilitetin financiar të pacientëve dhe në aksesin e tyre në shërbime shëndetësore. Ngjarje të tilla theksojnë nevojën kritike për ofruesit e shërbimeve shëndetësore që të zbatojnë masa të forta sigurie. Në Kosovë, kjo thekson rëndësinë që institucionet shëndetësore të adoptojnë masa të rrepta për të mbrojtur të dhënat e pacientëve nga qasja e paautorizuar dhe keqpërdorimi, duke ruajtur kështu privatësinë e pacientëve dhe besimin në sistemin shëndetësor.

Në Kosovë, mbrojtja e të dhënave dhe privatësia në sektorin shëndetësor janë në kuadër të Ligjit për Mbrojtjen e të Dhënave Personale (LMDHP), i cili kërkon që ofruesit e shërbimeve shëndetësore të zbatojnë masa teknike dhe organizative për të mbrojtur të dhënat. Me rritjen e sistemeve digjitale të shëndetësisë, këto institucione duhet gjithashtu të investojnë në teknologji të avancuara për mbrojtjen e të dhënave, siç janë enkriptimi dhe metodat e sigurta të autentifikimit, dhe të ofrojnë trajnime të rregullta për stafin lidhur me protokollet e privatësisë. Kjo është veçanërisht e rëndësishme pasi përdorimi në rritje i telemjekësisë dhe shërbimeve të kujdesit për pacientët në distancë sjell rreziqe të reja.

Përvoja globale e sektorit shëndetësor ofron një mësim të vlefshëm për Kosovën. Është vërtetuar se organizatat shëndetësore janë më të ndjeshme ndaj shkeljeve të të dhënave krahasuar me sektorët e tjerë, për shkak të faktorëve si numri i madh i individëve që kanë qasje në të dhënat e pacientëve, përfshirë klinicistët, stafin administrativ dhe ofruesit e shërbimeve të jashtme.[68] Për të forcuar mbrojtjen e të dhënave, organizatat shëndetësore në Kosovë duhet të zbatojnë masa specifike të sigurisë kibernetike, siç janë kryerja e auditimeve të rregullta të sigurisë, zhvillimi i planeve për reagimin ndaj incidenteve dhe trajnimi i stafit për të njohur kërcënimet e mundshme të sigurisë. Duke ndërmarrë këto hapa proaktivë, ata mund të mbrojnë më mirë informacionet e pacientëve, të ruajnë përputhshmërinë dhe të krijojnë besim të qëndrueshëm brenda sistemit shëndetësor.

Duke mësuar nga praktikat ndërkombëtare, si ato të zbatuara në Bashkimin Evropian nën Rregulloren e Përgjithshme për Mbrojtjen e të Dhënave (GDPR), sektori shëndetësor i Kosovës mund të përmirësojë strategjitë e tij për mbrojtjen e të dhënave. Për shembull, implementimi i Privacy by Design—i cili përfshin mbrojtjen e të dhënave në zhvillimin e sistemeve të reja—mund të ndihmojë në parandalimin e shkeljeve. Gjithashtu, mbajtja e transparencës me pacientët rreth mënyrës se si mblidhen, përpunohen dhe ruajnë të dhënat e tyre është thelbësore për të ndërtuar besim.[69]

[67] Ibid.
[68] Ibid.
[69] Ibid.

7. Sektori i Arsimit

Sektori i arsimit në Kosovë trajton informacione personale të ndjeshme, përfshirë regjistrat e studentëve, pjesëmarrjen, informacionin shëndetësor dhe historinë disiplinore. Ai luan një rol tjetër të rëndësishëm në mbledhjen dhe përpunimin e të dhënave personale, veçanërisht me rritjen e përdorimit të platformave dixhitale të mësimit dhe sistemeve të menaxhimit të studentëve. Institucionet arsimore, nga universitetet deri te shkollat fillore, mbledhin një sasi të madhe të dhënash personale mbi studentët, stafin mësimor dhe administrativ, duke përfshirë informacione të ndjeshme siç janë regjistrat akademikë, informacionet shëndetësore dhe të dhënat financiare lidhur me shkollimin dhe bursat. Këto institucione gjithashtu janë të detyruara ligjërisht të respektojnë Ligjin për Mbrojtjen e të Dhënave Personale (LMDHP).

Me rritjen e platformave të mësimit elektronik dhe mësimit në distancë si pasojë e pandemisë COVID-19, sasia e të dhënave personale që përpunohen është rritur ndjeshëm, duke sjellë sfida të reja për mbrojtjen e të dhënave në sektorin arsimor. Shkollat dhe universitetet duhet të adoptojnë masa të forta të sigurisë kibernetike për të mbrojtur kundër shkeljeve të të dhënave që mund të ekspozojnë informacionin e studentëve. Për shembull, shumë institucione po kalojnë në sisteme të bazuara në re për menaxhimin e regjistrave të studentëve, të cilat kërkojnë enkriptim të fortë dhe protokolle të sigurisë për aksesin për të parandaluar aksesin e paautorizuar.

Këto të dhëna janë të nevojshme për menaxhimin e programeve akademike dhe ofrimin e shërbimeve të cilësisë së arsimit, por mbrojtja e tyre është thelbësore për të siguruar privatësinë e studentëve. Megjithatë, rezultatet nga pyetësorët e përgjithshëm tregojnë nivele të ndryshme të përputhshmërisë dhe ndërgjegjësimit rreth kërkesave për mbrojtjen e të dhënave, duke sugjeruar se institucionet arsimore në Kosovë mund të hasin gjithashtu sfida në implementimin e praktikave të qëndrueshme të mbrojtjes së të dhënave.

Globalisht, shkeljet në sektorin arsimor kanë qenë në rritje. Studime të fundit ndërkombëtare kanë treguar se institucionet arsimore po targetohen gjithnjë e më shumë nga sulmet kibernetike, shpesh për shkak të të dhënave të ndjeshme personale dhe financiare që ato ruajnë.[70] Në shumë raste, shkeljet e të dhënave rezultojnë nga dobësitë në sistemet e teknologjisë së informacionit të vjetruara, trajnimi i pamjaftueshëm i stafit mbi mbrojtjen e të dhënave, ose metodat e pasigurta të komunikimit siç janë email-et pa enkriptim. Këto çështje krijojnë mundësi për akses të paautorizuar dhe mund të dëmtojnë rëndë sigurinë e të dhënave të ndjeshme të studentëve dhe stafit.[71]

Për të siguruar përputhshmërinë me rregulloret lokale dhe standardet globale, institucionet arsimore në Kosovë duhet të përqendrohen në minimizimin e të dhënave—duhet të mblidhen vetëm të dhënat e nevojshme për qëllime arsimore—dhe të zbatojnë parimet e Privacy by Design, ku mbrojtja e të dhënave integrohet në zhvillimin dhe implementimin e mjeteve të reja digjitale. Për më tepër, shkollat dhe universitetet duhet të ofrojnë trajnime të rregullta për stafin mbi protokollet e privatësisë dhe sigurisë së të dhënave, duke siguruar që të gjithë ata që merren me përpunimin e të dhënave personale të jenë të vetëdijshëm për rreziqet dhe rëndësinë e përmbushjes së ligjeve mbi mbrojtjen e të dhënave.

[70] A systematic analysis of failures in protecting personal health data: A scoping review, J. Pool, et. Al., 2023.
[71] Ibid.

Një gjetje kyçe nga anketimi ishte adoptoni i kufizuar i Vlerësimeve të Pasojave mbi Privatësinë të të Dhënave (DPIA), që është gjithashtu relevant për institucionet arsimore. DPIA-t janë thelbësore për vlerësimin e rreziqeve para se të futen sisteme të reja përpunimi të të dhënash, siç janë sistemet për menaxhimin e informacionit të studentëve. Implementimi i DPIA-ve do të ndihmojë në identifikimin e mundësive për mbrojtjen e mëtejshme të të dhënave dhe sigurinë e sistemeve digjitale që përdoren nga institucionet arsimore. Përdorimi i kufizuar i Vlerësimeve të Pasojave mbi Privatësinë të të Dhënave (DPIA) mund të tregojë një nevojë për ndërgjegjësim më të madh dhe burime të shtuar në sektorin arsimor për të vlerësuar rreziqet e të dhënave në mënyrë gjithëpërfshirëse.

Për më tepër, përgjigjet nga anketa theksuan se shumë organizata në Kosovë nuk kanë një plan të formuar për përgjigjen ndaj incidenteve. Ky hendek është veçanërisht i rëndësishëm për sektorin arsimor, ku shkeljet e të dhënave të studentëve mund të kenë pasoja të rënda, duke përfshirë aksesin e paautorizuar në rekordet akademike ose keqpërdorimin e informacionit personal. Zhvillimi i protokolleve për përgjigjen ndaj incidenteve dhe trajnimi i stafit për këto procedura mund të përmirësojë ndjeshëm mbrojtjen e të dhënave në shkolla dhe universitete.

Gjetjet theksojnë rëndësinë e investimeve të synuara në teknologji të avancuara për mbrojtjen e të dhënave dhe masa organizative brenda sektorit arsimor. Ndërkohë që transformimi digjital i Kosovës vazhdon, krijimi i protokolleve për privatësinë dhe sigurimi i komunikimit të hapur rreth praktikave të përpunimit të të dhënave janë hapa kyç për mbrojtjen e informacionit të studentëve.

Kapitulli IV: Sfidat e Përpunuesve të Mëdhenj

1. Çështjet rregullatore dhe të pajtueshmërisë

Entitetet në Kosovë përballen me sfida në zbatimin e ligjeve për mbrojtjen e të dhënave për shkak të arsyeve të ndryshme. Një nga vështirësitë kryesore është natyra komplekse dhe në rritje e rregulloreve për mbrojtjen e të dhënave. Ndërsa ligjet e Kosovës për mbrojtjen e të dhënave janë përgjithësisht të përshtatura me GDPR-në, shumë organizata kanë vështirësi për të kuptuar dhe zbatuar plotësisht këto rregulla. Kjo është veçanërisht e vërtetë për bizneset të vogla dhe të mesme (BVM-të), të cilat shpesh nuk kanë mjetet ose aftësitë për të siguruar përputhshmëri të plotë.

Megjithatë, këto sfida janë të pranishme edhe në vendet e BE-së, dhe madje edhe bizneset e mëdha përballen me vështirësi në përputhjen me GDPR-në. Një shembull i tillë është Vodafone, një nga kompanitë udhëhuese të telekomunikacionit në Evropë, e cila u gjobit me mbi 12 milionë euro nga Autoriteti i Mbrojtjes së të Dhënave të Italisë (DPA) në vitin 2020 për shkeljen e rregullave të GDPR-së. Gjobita u vendos për praktikat agresive të telemarketingut që injoronin pëlqimin e konsumatorëve, duke përfshirë telefonata për individë që kishin refuzuar shprehimisht.[72]

Për më tepër, gjatë hetimit, DPA zbuloi se ishte përdorur numra telefoni të falsifikuar për të realizuar thirrje marketingu. DPA urdhëroi Vodafone që të implementojë sisteme dhe të provojë se përpunimi për telemarketing do të kryhet në përputhje me kërkesat e pëlqimit.[73] Si rezultat, kompania nuk e përpunoi të dhënat në përputhje me ligjin, dhe pas vlerësimit, u gjet se subjekti i të dhënave mund të identifikohej përsëri përmes mënyrave të arsyeshme. Këto sfida nuk janë të kufizuara vetëm në kompanitë e telekomunikacionit dhe në sektorin e shëndetësisë; ato shtrihen në shumë sektorë, përfshirë arsimin dhe financat. Rasti i Vodafone thekson nevojën për që organizatat të monitorojnë vazhdimisht aktivitetet e tyre të përpunimit të të dhënave, të zbatojnë strategji të forta për përputhshmëri dhe të sigurojnë që pëlqimi i klientëve të respektohet siç duhet në të gjitha operacionet e tyre.

Një rast tjetër të fundit është vendimi i Autoritetit Mbikëqyrës të Francës më 5 shtator 2024 për të shqiptuar një gjobë prej 800,000 Eurosh ndaj CEGEDIM SANTÉ. Hetimet filluan në vitin 2021 dhe zbuluan se kjo kompani kishte përpunuar të dhëna shëndetësore që nuk ishin anonimizuar pa autorizim. Ata i kishin transmetuar tek klientët e tyre për të realizuar studime dhe për të prodhuar statistika në sektorin e shëndetësisë. Këto raste ilustrojnë se edhe kompanitë e konsoliduara kanë vështirësi në përputhjen e plotë me rregulloret strikte të përcaktuara nga GDPR, veçanërisht në fusha që lidhen me mbledhjen e të dhënave, menaxhimin e pëlqimit dhe transparencën.

Kosova, me Ligjin e saj për Mbrojtjen e të Dhënave Personale (LMDHP), përballet me sfida të ngjashme, pasi përpunuesit lokalë të të dhënave përpiqen të përshtatin praktikat e tyre me

[72] Aggressive telemarketing practices: Vodafone fined over 12 million Euro by Italian DPA, November 2020, https://www.edpb.europa.eu/news/national-news/2020/aggressive-telemarketing-practices-vodafone-fined-over-12-million-euro_en

[73] Ibid.

rregulloret kombëtare dhe standardet ndërkombëtare. Kjo përputhje bëhet edhe më komplekse kur merren parasysh kufizimet e burimeve, boshllëqet teknologjike dhe peizazhet e ndryshueshme rregullatore në rajon.

2. Sfidat Teknologjike

Sfidat teknologjike paraqesin një pengesë tjetër të rëndësishme për mbrojtjen efikase të të dhënave në Kosovë. Kërcënimet në fushën e sigurisë kibernetike, siç janë hakimi, phishing dhe sulmet ransomware, janë një shqetësim i vazhdueshëm për organizatat që trajtojnë sasi të mëdha të dhënash personale. Shumë organizata, veçanërisht ato në sektorin publik, varen nga infrastrukturat teknologjike të vjetra ose të pasigurta, duke e bërë masat e tyre të sigurisë kibernetike pothuajse të pasigurta. Përveç kësaj, ritmi i shpejtë i zhvillimit të teknologjisë do të thotë se organizatat duhet të përditësojnë vazhdimisht sistemet e tyre për t'u përshtatur me kërcënimet moderne, një detyrë që mund të jetë e shtrenjtë dhe kërkon shumë burime.

Qendra Kosovare për Studime të Sigurisë (KCSS) raporton se Kosova ka përjetuar një rritje të dukshme të sulmeve kibernetike, duke përfshirë malware, inxhinieri sociale dhe ransomware, me fokus veçanërisht te institucionet publike si Telekomi i Kosovës dhe e-Kosova.[74] Këto sulme keqpërdorin sistemet teknologjike të vjetra dhe të pasigurta që janë në përdorim, të cilat janë të zakonshme në shumë organizata, veçanërisht brenda sektorit publik.

Për më tepër, megjithë përmirësimet e fundit, infrastruktura e sigurisë kibernetike e Kosovës ende mbetet pas asaj të rajoneve më të zhvilluara. Këto rreziqe përkeqësohen nga mungesa e punonjësve të kualifikuar IT dhe aksesit të kufizuar në zgjidhje moderne të sigurisë kibernetike, duke e bërë të vështirë për bizneset të menaxhojnë dhe mbrojnë siç duhet të dhënat e tyre. Përpjekjet e rajonit për të përmirësuar mbrojtjen e të dhënave bëhen edhe më të vështira nga nevoja e vazhdueshme për të përditësuar procedurat dhe sistemet për të mbetur para kërcënimeve në zhvillim.[75]

3. Ndërgjegjësimi

Një shqetësim kyç në Kosovë është gjithashtu kuptimi i pamjaftueshëm i të drejtave dhe detyrimeve lidhur me privatësinë e të dhënave. Mungesa e ndërgjegjësimit për rëndësinë e mbrojtjes së të dhënave mes shumë individëve dhe organizatave mund të çojë në menaxhimin e pakujdesshëm të të dhënave personale dhe masa të pamjaftueshme sigurie. Ky problem është veçanërisht i dukshëm te ndërmarrjet e vogla dhe të mesme (SME) dhe organizatat shtetërore, ku siguria e të dhënave mund të mos i jepet prioriteti i duhur ose të integrohet plotësisht në operacionet e përditshme.[76]

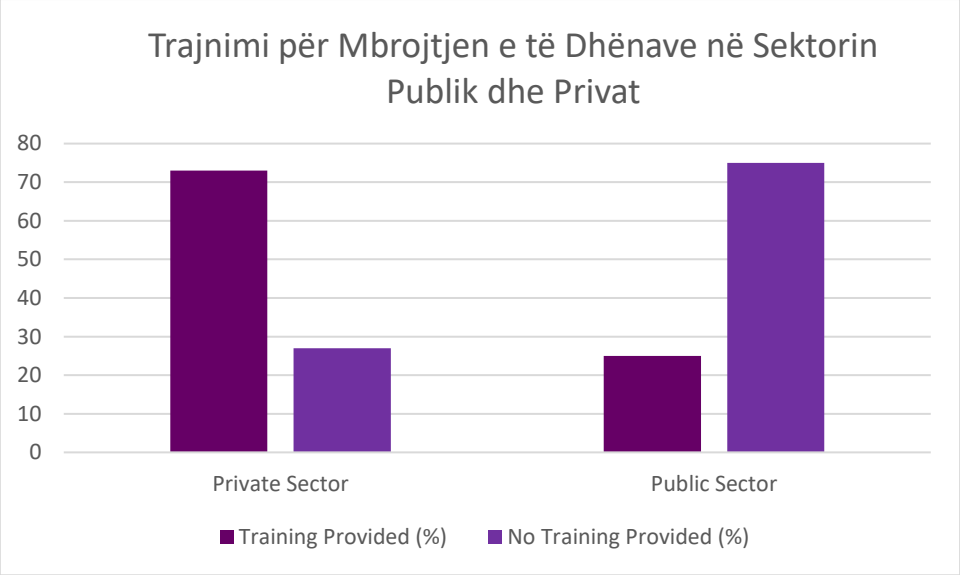
Për më tepër, mësimdhënia e palëve të interesuara mbi ligjet e privatësisë së të dhënave dhe praktikat e rekomanduara është mjaft e vështirë. Edhe pse disa organizata kanë implementuar fushata ndërgjegjësimi dhe kanë trajnuar punonjësit e tyre, këto përpjekje shpesh janë të pamjaftueshme. Për shkak të mungesës së programeve gjithëpërfshirëse dhe efektive të

[74] ROAD TO RESILIENCE: Governance and Capacity Building in Kosovo's Cyber Defense and Critical Infrastructure, KCSS, March 2024, https://qkss.org/images/uploads/files/Road_to_Resilience.pdf.
[75] Ibid.
[76] Country Situation Report: Digital Rights in Kosovo, Open Data Kosovo, 2022.

mësimdhënies, shumë individë ende nuk janë të vetëdijshëm për të drejtat e tyre në mbrojtjen e të dhënave.

Mungesa e ndërgjegjësimit dhe trajnimet e paplotësuara për oficerët e mbrojtjes së të dhënave është një problem kryesor që treguan rezultatet e anketës sonë. Këta oficerë e kanë të vështirë të zbatojnë me sukses rregullat dhe procedurat e kërkuara për të mbrojtur të dhënat brenda bizneseve të tyre nëse nuk janë trajnuar siç duhet. Hendeku në trajnim ka ndikim të drejtpërdrejtë në aftësinë e tyre për të siguruar përputhshmërinë me ligjet e mbrojtjes së të dhënave dhe për të ruajtur integritetin e informacionit personal.[77]

Në studimin tonë, zbuluam një hendek të madh në trajnimin për mbrojtjen e të dhënave mes sektorit publik dhe atij privat. Nga ata që morën pjesë në anketë nga sektori privat, 73% thanë se organizatat e tyre ofrojnë rregullisht trajnim për mbrojtjen e të dhënave për stafin. Në krahasim, 75% e përgjigjësve nga sektori publik thanë se institucionet e tyre nuk ofrojnë këtë lloj trajnimi. Ky dallim thekson nevojën për të theksuar më shumë edukimin për mbrojtjen e të dhënave, veçanërisht në organizatat publike, ku mungesa e trajnimit mund të pengojë zbatimin efektiv të masave të sigurisë së të dhënave.[78]



5. Pyetjet kryesore për vlerësimin e pajtueshmërisë me mbrojtjen e të dhënave në Kosovë

Ndërsa Kosova forcon kuadrin e saj ligjor për mbrojtjen e të dhënave sipas Ligjit për Mbrojtjen e të Dhënave Personale (LMDHP), është thelbësore që organizatat të vlerësojnë përputhshmërinë e tyre me këto standarde. Studimi ynë është ndërtuar rreth pyetjeve kyçe që

[77] Information gathered from questionnaire on data protection in Kosovo.
[78] Information gathered from questionnaire on data protection in Kosovo.

jo vetëm udhëhoqen përputhshmërinë, por gjithashtu shërbejnë si një burim i vlefshëm për entitetet që synojnë të përmirësojnë praktikat e tyre të mbrojtjes së të dhënave. Këto pyetje ofrojnë një qasje të strukturuar që ndihmon organizatat të identifikojnë zona specifike për përmirësim dhe mund të mbështesë vlerësimet e ardhshme ndërkohë që ligjet dhe rreziqet për mbrojtjen e të dhënave vazhdojnë të evoluojnë.

Më poshtë janë pesë pyetje kyçe të dizajnuara për të vlerësuar se sa mirë organizatat përputhen me standardet e LMDHP-së. Përgjigjja e këtyre pyetjeve mund të mundësojë entitetet të mbrojnë të dhënat personale më efektivisht, të reduktojnë rrezikun e shkeljeve dhe të sigurojnë përputhshmërinë me standardet lokale dhe ndërkombëtare për mbrojtjen e të dhënave:

1. **A keni një Oficer për Mbrojtjen e të Dhënave (DPO)?**

Emërimi i një DPO është një kërkesë thelbësore sipas ligjeve për mbrojtjen e të dhënave si GDPR dhe LMDHP. DPO është përgjegjës për mbikëqyrjen e strategjive për mbrojtjen e të dhënave dhe për sigurimin që organizata të përmbushë kërkesat ligjore. Ky rol është kyç për menaxhimin e rreziqeve të sigurisë së të dhënave dhe vepron si një pikë kontakti për autoritetet rregullatore. Në mungesë të një DPO, organizatat mund të përballen me boshllëqe të mëdha në monitorimin e përputhshmërisë dhe menaxhimin e rreziqeve.

2. **A ka organizata juaj një politikë të shkruar dhe të përditësuar rregullisht për mbrojtjen e të dhënave?**

Një politikë e formuluar dhe e shkruar për mbrojtjen e të dhënave është themeli i përputhshmërisë. Ajo përcakton qasjen e organizatës ndaj mbrojtjes së të dhënave, duke përshkruar protokollet për grumbullimin, përpunimin, ruajtjen dhe sigurinë e të dhënave. Përditësimet e rregullta të kësaj politike sigurojnë që organizata të adaptohet me ndryshimet në rregullore, teknologji ose llojin e të dhënave që përpunohen. Pa një politikë ose me një politikë të vjetër, organizatat janë më të ekspozuara ndaj shkeljeve të rregulloreve dhe gjobave.

3. **Çfarë masash sigurie, siç janë enkriptimi dhe muret mbrojtëse (firewalls), janë vendosur për të mbrojtur të dhënat?**

Në një epokë digjitale ku shkeljet e të dhënave janë gjithnjë e më të zakonshme, masat e forta teknike si enkriptimi, muret mbrojtëse dhe sistemet e kontrollit të aksesit janë të domosdoshme. Këto teknologji mbrojnë të dhënat personale nga qasja e paautorizuar, vjedhja ose humbja. Organizatat që nuk kanë masa të mjaftueshme sigurie jo vetëm që rrezikojnë humbjen e besimit të konsumatorëve, por gjithashtu mund të përballen me gjoba të mëdha sipas LMDHP dhe GDPR për dështim në mbrojtjen e të dhënave të ndjeshme.

4. **A keni një plan përgjigjeje për menaxhimin e shkeljeve të të dhënave?**

Shkeljet e të dhënave nuk janë një çështje "nëse", por "kur". Një plan i plotë i përgjigjes për incidentet lejon organizatat të zvogëlojnë dëmin e shkaktuar nga një shkelje. Plani duhet të përfshijë hapa për njoftimin e individëve të prekur, raportimin e shkeljes te autoritetet dhe riparimin e shkakut të shkeljes. Pa një plan, organizatat mund të kenë vështirësi për t'u përgjigjur në mënyrë efikase, duke rezultuar në gjoba më të mëdha dhe dëmtim të reputacionit.

5. **A është Privacy by Design e integruar në sistemet dhe proceset tuaja?**

Privacy by Design i referohet integrimit të konsideratave për privatësinë në zhvillimin e sistemeve, proceseve dhe produkteve që nga fillimi. Duke përfshirë privatësinë në dizajnin

themelor, organizatat mbrojnë të dhënat proaktivisht, në vend që të trajtojnë çështjet pas shfaqjes së tyre. Ky qasje jo vetëm që siguron përputhshmëri me LMDHP, por gjithashtu përputhet me praktikat më të mira globale, siç janë ato të përshkruara në GDPR.

Këto pyetje jo vetëm që shërbejnë si kornizë për vlerësimin e pajtueshmërisë me LMDHP-në, por gjithashtu ndihmojnë subjektet të identifikojnë fushat ku mund të bëhen përmirësime. Duke adresuar këto aspekte kyçe, organizatat mund të mbrojnë më mirë të dhënat personale, të zvogëlojnë rrezikun e shkeljeve dhe të sigurojnë që ato të mbeten në përputhje me standardet lokale dhe ndërkombëtare të mbrojtjes së të dhënave. **Pyetja kryesore**	**Opsionet e pajtueshmërisë**	**Vlerësimi i përputhshmërisë (nga i ulët në të lartë)**	**Masat e rekomanduara**
1. A keni një Zyrtar për Mbrojtje të të Dhënave (DPO) të caktuar?	1. Jo, nuk kemi	E Ulët	Emërimi një DPO; raportoni tek menaxhmenti; kryeni rishikime të rregullta
	2. DPO me kohë të pjesshme me shtrirje të kufizuar	E mesme	Caktoni DPO me kohë të plotë me mbikëqyrje të plotë të aktiviteteve të mbrojtjes së të dhënave
	3. DPO me kohë të plotë, të trajnuar	E Lartë	Kryeni trajnime të rregullta të DPO-së; caktoni DPO-në si pikë kontakti me autoritetet
	1. Asnjë politikë formale	E Ulët	Zhvilloni një politikë gjithëpërfshirëse për mbrojtjen e të dhënave; siguroni

2. A ekziston një politikë e shkruar për mbrojtjen e të dhënave?			miratimin e menaxhmentit
	2. Politika ekziston por është e vjetëruar	E mesme	Rishikoni dhe përditëoni rregullisht politikën (çdo vit ose kur rregulloret ndryshojnë)
	3. Politika e përditësuar rregullisht	E Lartë	Publikoni politikën e brenda dhe të jashtë; përfshijeni në trajnimin e punonjësve
3. Çfarë masash sigurie ekzistojnë?	1. Mbrojtje elementare (fjalëkalimet)	E Ulët	Zbatoni enkriptimin, firewalls dhe autentikimin me shumë faktorë (Multi Factor Authentication - MFA)
	2. Elementare + Enkriptim apo firewall	E mesme	Miratoni protokolle të avancuara të enkriptimit, përditësime të rregullta të softuerit
	3. Masa gjithëpërfshirëse të sigurisë	E Lartë	Kryeni auditime të sigurisë; përdorni maskimin e të dhënave për të dhëna të ndjeshme
	1. Asnjë plan reagimi ndaj incidentit	E Ulët	Zhvilloni një plan reagimi ndaj incidentit, përshkruani hapat e reagimit dhe caktoni role

4. A ekziston një plan reagimi ndaj incidentit?	2. Reagime joformale, ad-hoc	E mesme	Formalizoni përgjigjen ndaj incidentit duke përfshirë përditësimet e rregullta dhe caktimet e roleve
	3. Plan gjithëpërfshirës, i testuar	E Lartë	Testoni rregullisht planin; trajnoni punonjësit për protokollet e reagimit
5. A zbatohet Privacy by Design?	1. Nuk ka masa të Privacy by Design	E Ulët	Integroni konsideratat e privatësisë në zhvillimin e sistemeve; kryeni DPIA
	2. Masa të kufizuara nga të Privacy by Design	E mesme	Aplikoni Privacy by Design në projekte të reja; rishikoni rregullisht strategjitë e projektimit
	3. Privacy by Design e integruar plotësisht	E Lartë	Rishikoni dhe përditësoni rregullisht parimet Privacy by Design; kryeni trajnime

Kapitulli V: Raste Studimi

1. Rasti Studimit 1: KESCO

Kompania e Furnizimit me Energi Elektrike në Kosovë (KESCO) funksionon si furnizuesi universal i energjisë elektrike në Kosovë, duke siguruar furnizimin me energji elektrike për konsumatorët në gjithë vendin. Ky rol përfshin jo vetëm furnizimin me energji për amvisëritë dhe bizneset, por edhe menaxhimin e shërbimeve që mbështesin shpërndarjen e energjisë, faturimin dhe marrëdhëniet me konsumatorët.[79] KESCO përpunon sasi të mëdha të të dhënave personale, duke përfshirë informacionin mbi faturimin dhe identitetet e klientëve, si një përpunues i madh i të dhënave. Respektimi i standardeve të mbrojtjes së të dhënave është thelbësor, duke pasur parasysh natyrën e ndjeshme të informacionit të përfshirë.

Siç është përmendur më parë, KESCO ka publikuar Politikën e Privatësisë në faqen e saj të internetit.[80] Kjo Politikë Privatësie ka të bëjë kryesisht me faqen e internetit dhe shpjegon se si do të përdoren të dhënat e klientëve. Ajo shpjegon se si përdorimi i të dhënave do të rrisë efikasitetin dhe do të ofrojë shërbim dhe kujdes më të mirë për klientët. Ndër të tjera, në Politikat e Privatësisë thuhet: “Siguria e të dhënave tuaja është e rëndësishme për ne, por kujtoni se asnjë metodë e transmetimit përmes Internetit, ose metodë e ruajtjes elektronike nuk është 100% e sigurt. Ndërsa ne mundohemi të përdorim mjete komercialisht të pranueshme për të mbrojtur të dhënat dhe informacionin tuaj personal, nuk mund ta garantojmë sigurinë e saj absolute."[81]

Agjencia për Informacionin dhe Privatësinë (AIP) e Kosovës ka filluar hetimin ndaj KESCO-s në vitin 2024 për shkelje të Ligjit për Mbrojtjen e të Dhënave Personale. Rezultatet e inspektimit treguan se KESCO nuk kishte vendosur masa të mjaftueshme sigurie për të dhënat personale, çka mund të kishte rrezikuar shkeljet e të dhënave dhe qasjen e paligjshme. Ligji për Mbrojtjen e të Dhënave Personale, i cili imponon mbrojtje strikte për përpunimin dhe ruajtjen e të dhënave personale, kishte shumë dispozita të rëndësishme që u shkelën nga këto gabime.

Pas këtyre përfundimeve, KESCO u gjobit me njërën nga gjobat më të mëdha për shkelje të privatësisë së të dhënave në Kosovë—20,000 EUR—nga AIP.[82] Ky vendim u mor pas disa ankesave të marra nga AIP. Këto ankesa, të dorëzuara nga subjektet e të dhënave, pretendonin se KESCO kishte dorëzuar faturat e energjisë elektrike hapur, pa letra mbrojtëse, në kuti postare gjysmë të ekspozuara pranë dyerve në korridore të përbashkëta dhe hyrje shtëpish, duke i bërë ato lehtësisht të aksesueshme për palë të treta.[83] AIP i dha KESCO-s një afat prej katër muajsh për të përmirësuar këtë praktikë dhe për të vepruar në përputhje me ligjin. Megjithatë, KESCO nuk arriti të mbrojë të dhënat e klientëve të saj dhe për këtë arsye, AIP mori vendimin

[79] Kosovo Electricity Supply Company, KESCO, https://www.kesco-energy.com/eng/about-us/about-us/

[80] Privacy Policy of KESCO, https://www.kesco-energy.com/shq/legjislacioni/rregullat-dhe-procedurat/politikat-e-privatesise/

[81] Ibid.

[82] Decision of AIP, no. 182/2024, date 16 August 2024, https://aip.rks-gov.net/download/vendim_nr_182_-ndaj-kompanise-kosovare-per-furnizim-me-energji-elektrike-sh/?wpdmdl=6374&refresh=66cd969e170761724749470

[83] Ibid.

e përshkruar më parë. Ky rast shërbeu si një shembull kujdesi për përpunuesit e tjerë të mëdhenj të të dhënave në vend dhe theksoi rëndësinë e respektimit të rregullave të mbrojtjes së të dhënave.

Në gusht 2024, KESCO e informoi publikun se kishte filluar shpërndarjen e faturave të energjisë elektrike në letra mbrojtëse për mbi 700,000 klientë në gjithë Kosovën. Ky ndryshim erdhi pas një projekti pilot dhe u zbatuan në përgjigje të një vendimi nga Agjencia për Informacionin dhe Privatësinë për të përmirësuar mbrojtjen e të dhënave personale. Për më tepër, ata e informuan publikun se kompania përballej me sfida, duke përfshirë mungesën e kutive postare dhe identifikuesve të adresave në zonat rurale, që ngadalësuan procesin.[84]

Rasti i KESCO-s shërben si një kujtesë për vështirësitë që kanë bizneset e mëdha në ruajtjen e përputhshmërisë me ligjet e mbrojtjes së të dhënave. Ai gjithashtu thekson rëndësinë e organizatave rregullatore si AIP në ruajtjen e këtyre rregullave dhe mbrojtjen e informacionit privat të individëve nga shfrytëzimi. Ky ngjarje ka stimuluar ndoshta KESCO-n dhe bizneset e tjera në Kosovë që të rishikojnë politikat e tyre të mbrojtjes së të dhënave dhe të sigurohen që ato janë plotësisht në përputhje me ligjin.

2. Rast Studimi 2: Komuna e Gjakovës

Në vitin 2024, Komuna e Gjakovës u gjobit me 20 mijë euro nga Agjencia për Informim dhe Privatësi (AIP) për përpunim të paligjshëm dhe zbulim publik të të dhënave personale. Komuna kishte publikuar në faqen e saj zyrtare lista që përmbanin informacione delikate si emrat, vitet e lindjes, numrat e identifikimit personal, diagnozat mjekësore dhe të dhënat bankare të individëve që kishin aplikuar për subvencione të kujdesit shëndetësor. Ky zbulim ka shkelur dispozita të shumta të Ligjit për Mbrojtjen e të Dhënave Personale, veçanërisht në lidhje me përpunimin e papërshtatshëm të të dhënave sensitive pa bazën e duhur ligjore apo pëlqimin.[85]

Incidenti filloi kur AIP, duke vepruar sipas një raporti të marrë në qershor 2024, hetoi dhe zbuloi se Gjakova kishte ekspozuar pa dashje të dhënat personale të përfituesve dhe jopërfituesve në faqen e saj të internetit. Ky informacion, i aksesueshëm për publikun, përfshinte të dhëna të ndjeshme mjekësore, numra personal identifikimi dhe detaje kontakti. Pavarësisht se u kontaktua nga gazetarët për shkeljen, përgjigja fillestare e bashkisë ishte e pamjaftueshme, duke pretenduar se gabimi ishte për shkak të mbikëqyrjes njerëzore gjatë publikimit.

Pas një inspektimi të detajuar, AIP arriti në përfundimin se veprimet e bashkisë përbënin një rrezik të konsiderueshëm për privatësinë dhe sigurinë e individëve, veçanërisht në një epokë të dixhitalizimit në rritje. AIP theksoi se një ekspozim i tillë i të dhënave të lidhura me shëndetin mund të ndikojë rëndë dinjitetin dhe privatësinë e individëve të përfshirë. Komuna u kritikua gjithashtu për dështimin në emërimin e një zyrtari për mbrojtjen e të dhënave, një kërkesë ligjore që do të kishte ndihmuar në parandalimin e çështjeve të tilla.[86]

---

[84] KESCO is distributing electricity bills in envelopes for over 700,000 customers, 28 August 2024, https://www.kesco-energy.com/shq/artikujt-e-fundit/kesco-po-shperndan-faturat-e-rrymes-ne-zarfe-521/

[85] Decision no.105/2024, date 14 June 2024, https://aip.rks-gov.net/download/vendim-nr-105-komuna-gjakoves/?wpdmdl=5672&refresh=66ff0f0adb97b1727991562

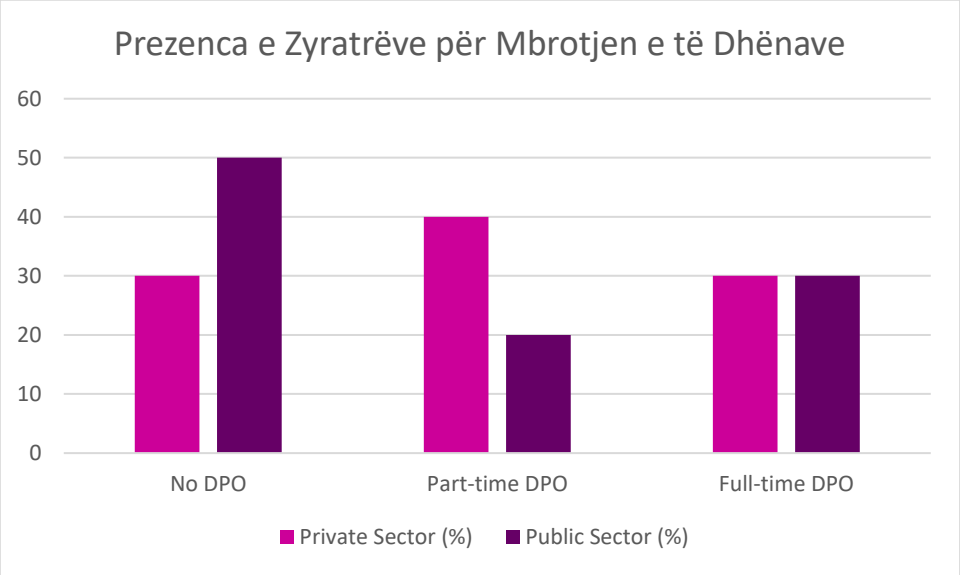
[86] Ibid.

Megjithatë, faqja e internetit e Komunës së Gjakovës nuk ofron ndonjë informacion të qartë në lidhje me emërimin e Zyrtarit për Mbrojtjen e të Dhënave (DPO). Pavarësisht kërkesës në bazë të ligjeve për mbrojtjen e të dhënave për institucionet publike që të kenë një zyrtar të caktuar përgjegjës për sigurimin e pajtueshmërisë me rregulloret për mbrojtjen e të dhënave, asnjë detaj kontakti ose informacion specifik për një OPAK nuk mund të gjendet në faqe.

Rasti nënvizon rëndësinë kritike të ruajtjes së të dhënave personale dhe të ndjeshme, veçanërisht brenda institucioneve publike. Gjoba dhe shqyrtimi i mëvonshëm theksojnë domosdoshmërinë e respektimit të ligjeve për mbrojtjen e të dhënave për të mbrojtur privatësinë e individëve si në sektorin publik ashtu edhe në atë privat.

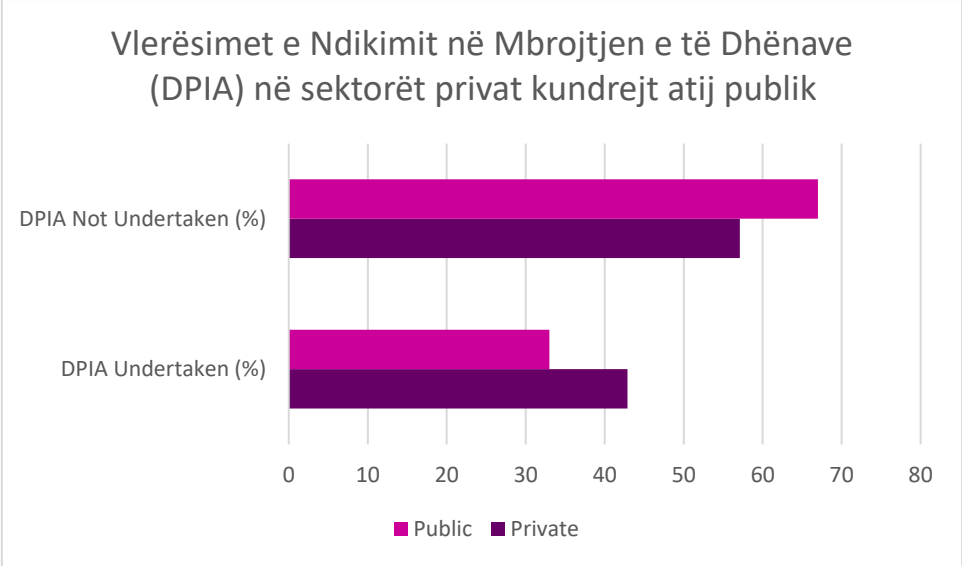
Kapitulli VI: Vështrime nga Anketa e Pajtueshmërisë për Mbrojtjen e të Dhënave

Kuptimi i të anketuarve për mbrojtjen e të dhënave rezultoi të ishte përgjithësisht i fortë, siç tregohet nga shumica e të anketuarve që i dhanë njohuritë e tyre notën 4 nga 5. Në sektorin publik, ku shumica miratoi emërimin e një Zyrtari për Mbrojtjen e të Dhënave (DPO), kjo tendencë ishte veçanërisht e rëndësishme. Ndërkohë që OPAK raportoheshin edhe nga sektori privat, të dhënat tregojnë një mospërputhje më të madhe në përputhshmëri sesa në sektorin publik.



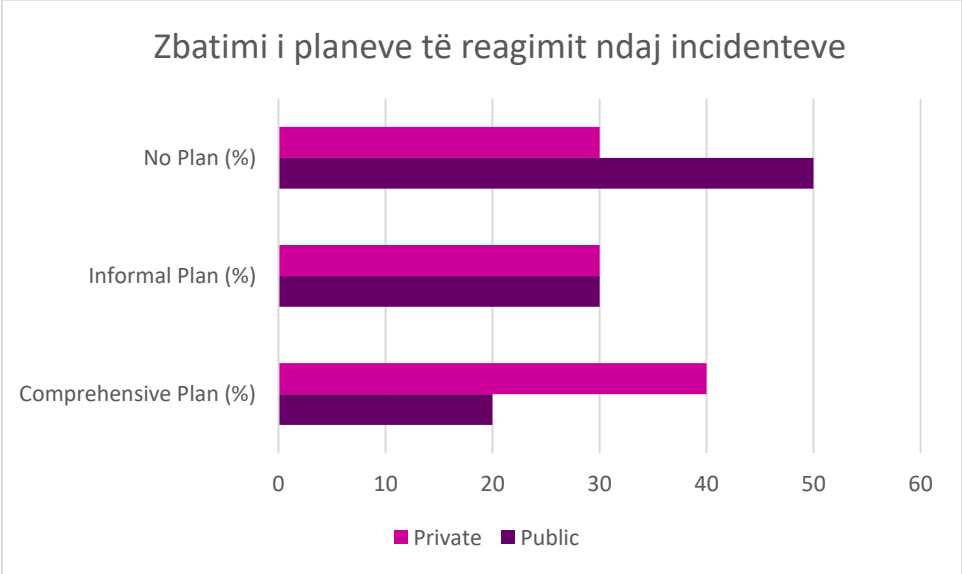
Shumica e institucioneve qeveritare dhe private u përgjigjën pozitivisht kur u pyetën nëse kanë hartuar rregullat e privatësisë. Megjithatë, përgjigja më tipike nga të gjithë sektorët në lidhje me përditësimin e këtyre rregullave ishte se ato bëhen "sipas nevojës", duke sugjeruar një strategji reaktive në krahasim me një strategji proaktive.

Vetëm 42.9% e të anketuarve të sektorit tregtar dhe 33% e të anketuarve të sektorit publik raportuan se kishin ndërmarrë DPIA, të cilat janë thelbësore përpara miratimit të operacioneve të reja të përpunimit. Kjo tregon për një nevojë të qartë për zhvillim, veçanërisht në dritën e rreziqeve të mundshme që lidhen me teknologjinë në zhvillim.



Të dy sektorët raportuan se menaxhonin të dhënat personale, financiare dhe shëndetësore për sa i përket kategorive të të dhënave të mbledhura dhe të përpunuara; megjithatë, të dhënat e marketingut ishin më të zakonshme në sektorin privat. Teknologjitë si maskimi i të dhënave, sistemet e kontrollit të aksesit dhe muret e zjarrit përdoren shpesh për të menaxhuar dhe mbrojtur këto të dhëna.

Ka pasur boshllëqe të konsiderueshme në gatishmërinë e sektorit tregtar për shkelje të të dhënave; 71.4% e të anketuarve thanë se u mungonte një plan reagimi ndaj incidenteve, ndërsa 50% e të anketuarve në sektorin publik thanë se kishin. Kjo pabarazi nxjerr në pah nevojën urgjente që sektori privat të bëhet më i përgatitur.



Vështirësitë dallonin në të gjitha industritë. Sfidat kryesore në sektorin publik ishin mungesa e njohurive dhe trajnimit, burimet e pamjaftueshme dhe kufizimet teknike. Sektori privat identifikoi mungesën e njohurive dhe rregulloret e rënduara, përveç kufizimeve teknologjike, si problemet e tij kryesore.

Sektori qeveritar pretendoi trajnime më pak të shpeshta, duke treguar një mospërputhje në arsimin e vazhdueshëm, ndërsa sektori komercial zakonisht u përgjigj pozitivisht kur u pyet

nëse ata shpesh marrin trajnime për mbrojtjen e të dhënave. Sektori publik kishte mendime të ndryshme për efikasitetin e rregullave aktuale, ndërsa sektori privat dha përgjigje që varionin nga neutrale deri në mesatarisht efektive kur u pyet për efikasitetin e masave aktuale të zbatimit të ligjit.

Fushatat e ndërgjegjësimit publik të dy sektorëve ishin të ngjashme në atë që ata mbështeteshin kryesisht në rregullat e privatësisë së faqeve të tyre të internetit. Por kur u pyetën për synimet për të zbatuar teknologjinë e re për të rritur sigurinë e të dhënave, një shumicë e konsiderueshme në të dy sektorët – 85% në privat dhe 75% në publik – thanë se nuk kishin synime të tilla.

Është interesante të theksohet se asnjë industri nuk raportoi ndonjë shkelje të të dhënave në vitin e kaluar. Kjo mund të jetë për shkak të procedurave efektive të zbulimit të incidentit ose masave të rrepta të sigurisë së të dhënave. Duket se ka mungesë konsistence në verifikimin e respektimit të rregullave për mbrojtjen e të dhënave, veçanërisht në sektorin publik ku shumë prej tyre kanë deklaruar se nuk bëhen kontrolle të pajtueshmërisë. Praktikat në sektorin privat ishin disi më të mira dhe disa organizata kryen monitorime rutinë.

Kërkesat nga klientët për akses, modifikim ose fshirje të të dhënave të tyre shpesh trajtohen nga departamentet e shërbimit ndaj klientit në sektorin privat. Nga ana tjetër, sektori publik shpesh u përgjigjet këtyre pyetjeve përmes emaileve me shkrim, ndërkohë që disa organizata pretendonin se nuk i kishin marrë kurrë ato.

Një fushë tjetër ku institucionet qeveritare ndryshojnë nga sektori privat është ndarja e të dhënave. E para zakonisht raportoi se nuk ndante të dhëna personale me palët e tjera, ndërsa e dyta e bën këtë në rrethana të caktuara.

Së fundi, sondazhi përvijoi pengesat dhe shanset kryesore për rritjen e sigurisë së të dhënave. Sektori privat ka disa pengesa, të tilla si mungesa e personelit të kualifikuar, trajnimi dhe burimet e pamjaftueshme, dhe vështirësia për të mbajtur hapin me peizazhin ligjor që po zhvillohet shpejt. Çështjet kryesore me të cilat përballej sektori publik ishin nxjerrja e rregulloreve të brendshme, zbatimi me rigorozitet i ligjit dhe tejkalimi i kufizimeve teknologjike. Lidhur me mundësitë, të dyja industritë njohin vlerën e kryerjes së investimeve teknologjike, përmirësimit të trajnimit të punonjësve dhe krijimit të politikave të plota të korporatës për të përmirësuar procedurat e sigurisë së të dhënave.[87]

[87] Informacioni i mbledhur nga pyetësori për mbrojtjen e të dhënave në Kosovë.

Kapitulli VII: Përfundimet

Korniza e mbrojtjes së të dhënave në Kosovë ka bërë përparime të dukshme përmes përshtatjes me GDPR-në dhe krijimit të LMDHP-së. Megjithatë, studimi ynë thekson mangësitë e rëndësishme midis përparimeve ligjore dhe zbatimit praktik. Rekomandimet e mëposhtme synojnë të adresojnë këto sfida dhe të mbështesin Kosovën në krijimin e një peizazhi digjital të sigurt dhe të ndërgjegjshëm për privatësinë:

1. **Forcimi i Burimeve dhe Kapaciteteve të AIP-së**: Për të mundësuar inspektime, auditime dhe ndjekje të rregullt, AIP ka nevojë për burime të përmirësuara dhe personel të kualifikuar. Forcimi i kapaciteteve të AIP-së do të mundësojë mbikëqyrje më të thelluar dhe mbështetje më të mirë për organizatat në kuptimin dhe përmbushjen e kërkesave të përputhshmërisë.
2. **Organizimi i Trajnimeve të Rregullta për Mbrojtjen e të Dhënave në të Gjitha Sektorët:** Gjetjet tona tregojnë një pasiguri në trajnimin për mbrojtjen e të dhënave ndërmjet sektorëve publik dhe privat, me një mungesë të dukshme të edukatës së vazhdueshme në institucionet publike. Programet e trajnimit të rregullta, të përshtatura për secilin sektor, janë të domosdoshme për të krijuar një kulturë mbrojtjeje të të dhënave, duke siguruar që punonjësit në të gjitha sektorët të kuptojnë dhe zbatojnë praktikat më të mira në menaxhimin e të dhënave.
3. **Detyrimi i Kryerjes Rregullisht të Vlerësimeve të Ndikimit në Mbrojtjen e të Dhënave (Data Protection Impact Assessment-DPIA) dhe Përditësimeve të Politikave:** Shumë institucione ende nuk kanë implementuar masa proaktive për mbrojtjen e të dhënave, si rishikimet e politikave dhe DPIA. Zbatimi i këtyre kërkesave, veçanërisht në organizatat që përpunojnë shumë të dhëna ose të dhëna ndjeshme, mund të përmirësojë menaxhimin e rrezikut dhe përputhshmërinë, duke zvogëluar mundësitë për shkelje.
4. **Adoptimi i Parimeve "Privacy by Design" dhe "Privacy by Default" (Privatësia si Parazgjedhje):** Integrimi i masave të mbrojtjes së të dhënave në fazat e para të dizajnit të sistemeve digjitale mund të rrisë sigurinë e të dhënave dhe përputhshmërinë. Ky qasje duhet të inkurajohet në të gjitha sektorët, veçanërisht në organizatat që kalojnë në transformim digjital, për të siguruar që privatësia të jetë e inkorporuar në proceset operacionale.
5. **Zhvillimi dhe Zbatimi i Udhëzimeve të Standardizuara për Mbrojtjen e të Dhënave**: Një përpjekje bashkëpunuese midis sektorëve publik dhe privat për të krijuar praktika uniforme për mbrojtjen e të dhënave mund të promovojë përputhshmëri të qëndrueshme. Udhëzimet standardizuara do të ndihmonin në përputhjen e praktikave ndërmjet sektorëve dhe adresimin e pasaktësive të gjetura në anketën tonë.
6. **Lansimi i Fushatave të Ndërgjegjësimit Publik për Të Drejtat e Mbrojtjes së të Dhënave:** Fuqizimi i qytetarëve për të kuptuar dhe ushtruar të drejtat e tyre për mbrojtjen e të dhënave është thelbësor për llogaridhënie. Fushatat e ndërgjegjësimit dhe udhëzimet e qasshme mund të inkurajojnë individët që të kërkojnë praktika më të mira për të dhënat personale, duke forcuar kështu përputhshmërinë dhe besimin në shërbimet digjitale.
7. **Inkurajimi i Zhvillimit të Planëve të Reagimit ndaj Incidenteve:** Duke pasur parasysh mungesën e planeve formale të reagimit ndaj incidenteve në shumë

organizata, veçanërisht në sektorin privat, është thelbësore të inkurajohet krijimi i procedurave të strukturuara për menaxhimin e shkeljeve të të dhënave. Një plan efikas i reagimit ndaj incidenteve ndihmon organizatat të reagojnë shpejt, duke zvogëluar dëmet dhe duke rritur besimin e klientëve.

Duke zbatuar këto rekomandime, Kosova mund të adresojë sfidat praktike të identifikuara në këtë studim dhe të përparojë në zhvillimin e peizazhit të saj për mbrojtjen e të dhënave. Ky qasje jo vetëm që përputhet me standardet ndërkombëtare, por gjithashtu promovon një kulturë të orientuar nga privatësia, duke pozicionuar Kosovën për të përfituar nga integrimi i saj në rritje në ekonominë digjitale globale.

ITS INSTITUTE FOR TECHNOLOGY AND SOCIETY