B FILM MONTENEGRO

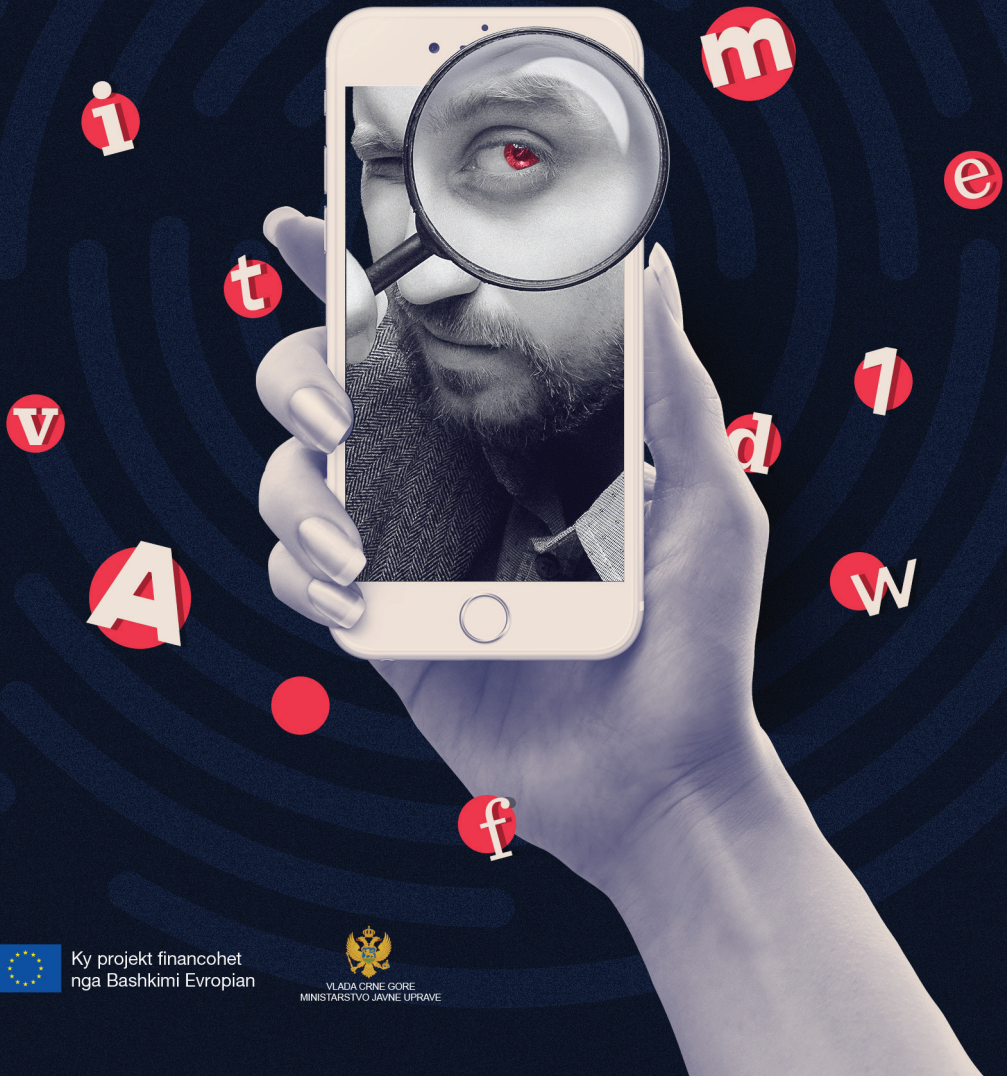
Centar za građansko obrazovanje
Centre for Civic Education

SHARE FOUNDATION

IPFP

MANUAL PËR GAZETARINË E EPOKËS DIGJITALE:

mbrojtja teknike dhe ligjore



Ky projekt financohet nga Bashkimi Evropian

VLADA CRNE GORE
MINISTARSTVO JAVNE UPRAVE

MANUAL PËR GAZETARINË E EPOKËS DIGJITALE:
mbrojtja teknike dhe ligjore

Botues:
Qendra për Arsim Qytetar (QAQ)

Redaktorët:
Andrej Petrovski
Gjorgje Krivokapiq

Autorët/et:
Jelena Adamoviq
Anka Kovaçeviq
Nevena Krivokapiq Martinoviq
Filip Milosheviq
Bojan Perkov
Kristina Qendiq

Redaktimi i tekstit:
Milica Jovanoviq

Dizajni dhe produksioni:
Qendra për Arsim Qytetar (QAQ)

Përkthimi në gjuhën shqipe:
Amina Nikoviq

Qarkullimi:
30 kopje

Manuali është pjesë e projektit „Mbështetje mediave lokale - tregime të dorës së parë! Mbështetje gazetarisë hulumtuese dhe shkrim-leximit mediatik në nivelin lokal në Malin e Zi“ të cilin e realizojnë B-film Montenegro, Qendra për Arsim Qytetar (QAQ), Fondacioni SHARE dhe Instituti për shkrim-leximin biznesor dhe financiar. Projekti finansohet nga BE-ja përmes Delegacionit të BE-së në Mal të Zi, kurse bashkëfinansohet nga Ministria e Administratës Publike të Qeverisë së Malit të Zi.

VLADA CRNE GORE
MINISTARSTVO JAVNE UPRAVE

Përmbajtja e këtij botimi është përgjegjësi e vetme e Fondacionit SHARE dhe QAQ-së dhe në asnjë mënyrë nuk mund të interpretohet si qëndrim zyrtarë i Bashkimit Evropian ose i Ministrisë së Administratës Publike Qeverisë së Malit të Zi.

MANUAL PËR GAZETARINË E EPOKËS DIGJITALE:

mbrojtja teknike dhe ligjore

Podgoricë, korrik 2020

PËRMBAJTJA

Hyrje

Decentralizimi i shkëmbimit të lajmeve midis qytetarëve, nga të cilët pothuajse të gjithë janë te pajisur teknikisht aq sa të mund të inçizojnë, përpunojnë dhe dërgojnë brenda momentit informacionet në anën tjetër të botës, u ka paraqitur gazetarëve një sfidë të vështirë. A ka më kuptim ky profesion sot, kur të gjithë janë bërë media për vete? A munden mediat t'ia dalin mbanë të fitojnë vëmendjen e audiencës në një treg të mbingopur me përmbajtje informative dhe argëtuese, të vetëdijshëm se u mungojnë si njohuritë ashtu dhe burimet për të lundruar në mjedisin digjital?

Në një kohë kur shumë aktivitete private dhe publike kanë kaluar nga hapësira fizike në atë online, grumbullimi dhe verifikimi i të dhënave kërkon një njohuri të mirë të teknologjisë. Është e nevojshme të kuptohet logjika e re e krijimit dhe përpunimit të të dhënave, parametrave të rinjë të hulumtimit të cilët zbatohen në internet, si dhe rreziqet e ndryshme të sigurisë që paraqiten në këto kushte. Hapësirat informatike janë gjithashtu të kufizuara nga normat e reja ligjore të cilat ndikojnë, në një masë të rëndësishme, në rolin e gazetarëve në arritjen e interesit publik.

Manuali i cili gjindet para juve ofron përgjigjje në disa nga pyetjet kryesore teknike dhe ligjore të gazetarisë moderne, qoftë ajo realizuar brenda një organizate mediatike apo në mënyrë të pavarur.

Çfarë është interneti?

Infrastruktura e internetit në Mal të Zi

Që kur filloi zbatimi i Strategjisë kombëtare për zhvillimin e shoqërisë së informacionit në Mal të Zi në vitin 2016, është bërë përparim në

zhvillimin e infrastrukturës dhe rrjetëve për qasje më të shpejtë në internet. Sipas Ministrisë së Ekonomisë, 80 përqind e familjeve malazeze kanë lidhje interneti aktive me bandë të gjerë.

Në raportin e Agjencisë për Komunikime Elektronike dhe Shërbimet Postare (EKIP) mbi gjendjen e tregut të komunikimeve elektronike për prill 2020 për internet, numri i përgjithshëm i lidhjeve me bandë të gjerë, pavarësisht nga teknologjia e përdorur për qasje është 181,483 (1,021 lidhje më shumë se në mars). Krahasuar me marsin, numri i lidhjeve me bandë të gjerë është më i lartë për 0.57%, kurse krahasuar me të njëjtën periudhë të vitit të kaluar, numri i lidhjeve me bandë të gjerë është më i lartë me 12.72%.

Domeni *.me*

Domeni kombëtarë i internetit i Malit të Zi është domeni.ME. Ky domen është një domen kombëtarë i nivelit më të lartë (ccTLD) i cili është globalisht i disponueshëm për regjistrim, që do të thotë se çdokush mund ta regjistrojë atë-është i disponueshëm për publikun e gjërë. Domen .ME mund të regjistrohet nga korriku i vitit 2008, dhe regjistruesit janë si nga Mali i Zi, ashtu edhe nga SHBA-të, Kina, Kanada, Britania e Madhe, Franca dhe Gjermania. Sidoqoftë, ekzistojnë domenet e nivelit të tretë, të cilët janë të hapur vetëm për qytetarët e Malit të Zi, sikurse janë gov.me, edu.me, co.me, net.me, org.me, priv.me dhe its.me. Në vitin 2016 është arritur një milion domene, kryesisht për shkak të rritjes së tregut për emrat e domeneve në Kinë. Ky numër ra në vitin 2017 në 900.000 domene, sepse disa nuk u rinovuan, kështu që rritja u ngadalësua. Që nga ai vit, shënohet një rritje e qendrueshme nga 6% në vit.

Paketë interneti

Interneti është një rrjet global i pajisjeve, dhe çdo pajisje qoftë server, ruter, tablet, kompjuter ose celular që është i lidhur me internet ka një IP adresë. I gjithë infomacioni i transmetuar në internet, midis ruterëve, serverëve dhe hosteve tjerë ndahet në pjesë më të vogla të të dhënave, të njohura si pako interneti. Çdo paketë përbëhet nga një kokë dhe përmbajtje. Koka (eng. headers) paraqet një lloj meta të dhënash. Ruteri i ofruesit të internetit përcakton adresën e destinacionit të secilës paketë dhe përcakton se ku do ta dërgojë atë. Paketa e internetit duhet të arrijë në destinacionin e caktuar në një sekond dhe gjatë asaj kohe ajo kalon hapësira të mëdha. Paketa e internetit fillon të "udhëtojë" nga routeri i shtëpisë, përmes routerit kryesorë të qytetit, deri tek data qendra kryesore e ofruesit të internet në vend. Pastaj, interneti kalon nga një vend i caktuar deri tek "kryqëzimi i internetit" (Internet Exchange Point - IXP) më të madh në kontinent-në rastin e Europës, është Frankfurti. Nëse internet përmbajtja e dëshiruar pritet në Amerikën Veriore, paketa do të kalojë oqeanin përmes kabllove nënujore, për të arritur në qendrën e të të dhënave ku do të ruhet.

Në vetëm një sekond, paketa e internetit kalon mijëra kilometra dhe kufij të shumtë shtetërorë, kalon nga një ofrues i internetit në tjetrin, të cilët operojnë nën regulla të ndryshme ligjore dhe interesa komerciale, hidhet nga një kryqëzim internetit në tjetrin dhe lë gjurmë të ekzistencës së tij në çdo pikë të rrugës.

Kur paketa e internetit arrinë destinacionin e saj përfundimtar, ajo do të ruhet dhe do të presë që të jetë subjekt i analizës. Mirëpo, paketa nuk do të ruhet vetëm në atë vend. Gjatë udhëtimit të saj, ajo do të klonohet dhe ruhet në disa vende, në disa qendra tjera të dhënash, serverë për ruajtjen e të dhënave të ofruesve të internetit, në shtete të ndyshme dhe

tek agjencionet e ndryshme shtetërore apo kompani private.

Në fund, paketa do të përdoret në shumë mënyra, si pjesë e një enigme të madhe për të analizuar sjelljen, preferencat dhe interesat e përdoruesve, ose një pjesë e vogël që do të shënojë dikë si terorist potencial ose ta dallojë nga ai.

Rrjedhjet e të dhënave në internet

Analiza e rrugës së të dhënave në internet është e rëndësishme në mënyrë që të krijohet një imazh i rrjedhjes së infomacioneve përmes rrjetit global, si dhe për të hartuar vendndodhjet kryesore dhe lojtarët. Trafiku i të dhënave nga një vend shkon në disa pika dhe në fakt bëhet më i centralizuar. Pikat e centralizimit janë pika të energjisë dhe sa më shumë ruterë ose ofrues të internetit të takohen në një pikë, aq më e madhe është rëndësia e asaj pike, ruterit ose serverit.

Është e rëndësishme të dihet se kush i kontrollon këto subjekte, sepse ata kanë kontroll mbi internetin në vend dhe mund ta abuzojnë atë pushtet. Sa i përket largimit të të dhënave nga vendi, sikurse centralizimi i rrjedhës lokale të të dhënave përmes një ruteri të vetëm, të dhënat kalojnë përmes disa pikave kryesore para se të largohen nga vendi.

Interneti nuk është aq i decentralizuar sa duket në shikim të parë, kryesisht sepse përbëhet nga vendet kryesore për tranzit dhe matjen e të dhënave, të ashtuquajturat "kryeqendra" të rrjedhësë së të dhënave, të vendosura në vetëm 13 vende. Kjo strukturë sot dallon shumë nga ai rrjeti i decentralizuar i konceptuar fillimisht, idejë nga fillimi i internetit. Ofruesit e internetit mund të konsiderohen edhe si kontrollues të internetit. Çdo censurë, filtrim ose ngadalësim

i mundshëm i trafikut në internet kryesisht do të bëhet në bashkëpunim me ofruesit e internetit. Hartësimi i pikave të lidhjes së ofruesve kombëtarë dhe ndërkombëtarë të internetit dhe analizimi i topologjisë së rrjetit mundëson një kuptim më të mirë të pikës kryesore të kësaj infrastrukture, gjegjësisht, ku mund të ndodhë censura, filtrimi apo ngadalësimi i mundshëm i trafikut.

Analiza e rrjedhjes së të dhënave për 100 faqet më të vizituara të përdoruesve të internetit në Serbi, të lidhur përmes rrjetit SBB, ka treguar se, mbas disa pikave lokale, i gjithë trafiku shkon vetëm në disa pika, dhe se 63% e të paketëve të internetit largohen nga vendi. Ndryshe nga vendet evropiane, sikur janë Hungaria, Çekia, Gjermania, Holandia dhe Britania, nëpër të cilat të dhënat nga Serbia zakonisht vetëm kalojnë, ruajtja (hosting) e të dhënave zhvillohet kryesisht në Amerikën e Veriut, më saktësisht në SHBA.

Interneti në epokën e koronavirusit

Shpërthimi i pandemisë ka kushtëzuar rritjen e përdorimit të shërbimeve të komunikimit elektronik, dhe me atë rritjen e konsiderueshme të trafikut telekomunikues, siç njoftohet nga Agjencia e Komunikimeve Elektronike dhe Shërbimeve Postare (EKIP). Rritja më e madhe ka ndodhur në gjysmën e dytë të marsit, kur trafiku i internetit u rrit për rreth 25%. Në total për muajin mars është realizuar 54% më shumë trafik interneti sesa në të njëjtin muaj vitin e kaluar. Rrjetet elektronike për komunikim morën masa në kohën e pandemisë që rritja e përdorimit të shërbimeve të komunikimeve elektronike të kalojë pa mbingarkesë dhe ngadalësim të trafikut.

Siguria digjitale

Gazetarët dhe punonjësit e medias, puna e të cilëve varet nga konfidencialiteti dhe siguria e të dhënave, si dhe nga burimet me të cilët ata komunikojnë, duhet të kenë shumë më kujdes për përdorimin e teknologjisë. Një pikë e kompromentuar mund të rrezikojë sigurinë digjitale të një redaksie të tërë, por edhe të burimeve të tyre.
Në ditët e sotme, e gjithë puna gazetareske bazohet në përdorimin e teknologjisë-praktikisht të gjitha informacionet konfidenciale gjenden në celularë dhe kompjutera.

Ekzistojnë shumë faktorë të cilët ndikojnë në sigurinë apo pasigurinë e një sistemi. Para së gjithash, këta janë faktorët teknologjik, gjegjësisht a është sistemi teknologjikisht i kompromentuar ose i prekshëm dhe cili është niveli i sigurisë që vetë pajisjet dhe programet e instaluara ofrojnë. Mirëpo, ekzistojnë dhe faktorët njerëzorë, sikur janë zakonet e përdoruesit, të cilat janë shumë të rëndësishme.

Është rregull i përgjithshëm që siguria nuk është një tipar i lindur i sistemeve digjitale, dhe se në sigurinë e tyre duhet punuar vazhdimisht. Përparësi e mjedisit digjital qendron në faktin se përdoruesit mund të ndikojnë në një farë mase në mbrojtjen e tyre dhe të të tjerëve. Masat më të rëndësishme mbrojtëse janë në dispozicion të gazetarëve dhe çdokujt që merren me publikimin e infomacioneve.

Kriptimi

Komunikimi në mjedisin online realizohet përmes kanaleve të cilët mund të prishen nga kushdo që ka njohuri dhe burime të mjaftueshme.

Prandaj, është e nevojshme të kodohet përmbajtja e komunikimit, ose të kriptohet, në mënyrë që të sigurohet që mesazhi do të lexohet vetëm nga ata të cilëve u është drejtuar, gjegjësisht, të cilët e kanë çelësin për dekodim.

Rëndësia e mbrojtjes së të dhënave personale, sekreteve të biznesit, por edhe mbrojtjes së sekretit të burimeve gazetareske, në mjedisin modern digjital praktikisht nënkupton që kriptimi është bërë pjesë përbërëse e rutinës së përditshme të punës në media.

Shumica e sistemeve informative nuk janë të kriptuara paraprakisht, por u nënshtrohen disa prej segmenteve individuale të tyre, sipas nevojës. Mund të kriptohet komunikimi, gjegjësisht përmbajtja e mesazheve që shkëmbehen, kurse mund të kriptohen edhe disqet në të cilët ruhen të dhënat. Kriptimi i komunikimit i referohet, para së gjithash, shërbimeve të postës elektronike dhe të ashtuquajturit chat-a, si dhe lundrimit të sigurtë nëpër internet.

Mbrojtja e postës elektronike

Teknologjia që qendron pas postës elektronike ka shumë defekte të sigurisë, që do të thotë se përdoruesi nuk ka kontroll të plotë mbi qasjen në metadata dhe përmbajtjen e postave elektronike të tyre, veçanërisht kur përdoren serviset publike sikur Gmail.

Një nga mënyrat më të mira të kriptimit të postës është PGP (Pretty Good Privacy). Mungesa e këtij programi paraqitet tek implementimi i cili kërkon aftësi digjitale më të avancuara. Poashtu, duhet që të dy palët në komunikim të përdorin PGP në mënyrë që programi të mund të vendoset si mekanizëm i komunikimit të mbrojtur. Përveç kësaj, ekzistojnë shërbime sikur janë ProtonMail ose Tutanota, të cilët

e kanë të integruar kriptimin e komunikimit midis përdoruesve të këtij shërbimi.

Derisa shkrim-leximi digjital i publikut të gjërë të ngrihet në një nivel më të lartë, është e veshtirë të pritet që të gjithë do të përdorin PGP-në, por për kontakte specifike të gazetarëve, sikur janë sinjalizuesit ose zyrtarët publikë të cilët merren me çështje të ndjeshme, të tilla si siguria kombëtare, duhet insistuar në vendosjen e komunikimit me postë të kriptuar në një nga mënyrat e disponueshme.

Përveç postës elektronike, për komunikim përdoren edhe chat shërbime të ndryshme. Këto shërbime jo rrallë përdoren nga burimet për të përcjellë gazetarëve me shpejtësi ndonjë informatë jozyrtare, të pavetëdijshëm nga rreziqet të cilave u ekspozohen. Megjithatë, ekzistojnë edhe chat aplikacione të cilat mundësojnë komunikim të kriptuar- sikur Signal, Telegram dhe WhatsApp.

Kërkim i sigurt në internet

Për kërkim në internet përdoren programe të veçanta (eng. browsers). Kërkimi teknik paraqet qasje në përmbajtjen në internet duke përdorur protokolle gjegjëse të internetit. Ekzistojnë zgjidhje të ndryshme (Mozilla Firefox, Google Chrome, Brave Browser, Microsoft Edge) dhe të gjitha në një farë mënyre kryejnë të njëjtin funksion, por në mënyrë që kërkimi të jetë i sigurt, është e nevojshme vendosja e parametrave shtesë dhe instalimmi i komponentave shtesë (eng. plugins), sikur është HTTPS Everywhere.

Niveli themelor nënkupton përdorimin e protokolleve të sigurta siç janë SSL ose TLS. Këto teknologji kriptojnë komunikimin midis klijentëve dhe serverëve dhe ashtu mbrojnë në mënyrë efektive nga sulmet e akterëve

"në mes" (eng. Man-in-the-Middle). Në këtë mënyrë mundësohet transmetimi i sigurt i të dhënave të ndjeshme në internet sikur janë emrat e përdoruesve, kodet ose të dhënat personale konfidenciale, si numrat e dokumentave personale, të dhëna mbi karta të pagesës, numrat e llogarive bankare etj.

Kriptimi i disqeve

Sasi të mëdha të të dhënave shpesh ruhen në pajisje të ndryshme, nga të cilat për kriptim rëndësi kanë disqet lokale dhe pajisjet portative (USB flash memoria dhe hard disqet eksterne)

Kriptimi i diskut përshin krijimin e një shtrese mbrojtjeje e cila i pamundëson personat e paautorizuar të hyjnë në përmbajtjen e cila gjindet në disk, nëse ata vijnë në zotërim të tij. Për të hyrë në përmbajtje duhet shkruar fjalëkalimi, kurse nganjëherë vendosen edhe parametra shtesë siç janë vërtetimi me dy nivele, çertifikata digjitale ose të dhënat biometrike.

Për kriptimin e disqeve lokale dhe transmetuese mund të përdoret softueri i hapur dhe falas VeraCrypt, i cili posedon një numër të madh të funkcioneve sipas nevojave të përdoruesit.

Në disa raste mund të jetë i nevojshëm kriptimi hibrid. Psh. me memorie flash USB, në një transakcion paraqitet nevoja për të kriptuar transferimin nga një disk në flash memorje dhe pastaj kriptimi kryhet në vetë memorjen. Nga ana tjetër teknologjia cloud gjithashtu i kushtëzon mekanizmat e veçantë të kriptimit sepse vetë teknologjia është një hibrid i transmetimit dhe ruajtjes.

Azhurnimi i softuerit

Çdo ditë zhvillohen lloje të reja të sulmeve teknologjike dhe softuerëve me qëllim të keq, dhe aplikacionet anti-malware azhurnojnë listat e tyre çdo ditë dhe kështu mundësojnë që programi ti zbulojë llojet më të reja të malware-ve. Çdo sistem ka mangësi të cilat mund të shfrytëzohen për të fituar qasje të paautorizuar në sistem. Cyber kriminelët vazhdimisht punojnë në gjindjen dhe hulumtimin e mangësive sistemike, shfrytëzimi i të cilave do të mundësonte ndëhyrje në sistem. Për këtë është e rëndësishme që të azhurnohen rregullisht të gjitha aplikacionet brenda sistemit, duke filluar nga sistemi operativ, përmes anti-malware aplikacioneve deri te aplikacionet të cilat përdoren çdo ditë. Rekomandohet që aplikacionet të konfigurohen ashtu që të njoftojnë përdoruesin që duhet të azhurnojë softuerin, dhe të mos lejojnë që automatikisht të shkarkohen verzionet e azhurnuara të programit.

Kujdes nga malware-ët

Malware është softuer i krijuar për të dëmtuar një sistem infomacioni. Llojet më të dalluar të malware-ve janë viruset kompjuterike, por ekzistojnë edhe lloje tjera sikur janë trojanë dhe krimba (eng. worms). Çdo lloj malware-sh ka mënyrën e vetë funksionimi, dhe për këtë arsye dëmtimi i shkaktuar nga secili prej tyre është i një shkalle të ndryshme. Malware-i mund të kryejë operacione të ndryshme, nga ridrejtmi në faqe të internetit të rrëme, deri te destabilizimi i një sistemi të tërë. Ekziston edhe një lloj i veçantë i malware-ve i cili regjistron çdo hyrje përmes tastierës dhe u dërgon të dhënat palëve të treta (eng. keylogger).

Gjithashtu, ekziston një lloj malware-i i cili ka aftësi të dërgojë me mijëra email nga kompjuteri i infektuar. Malware-i shpërndahet në mënyra të ndryshme- më shpesh vetë përdoruesit e shkarkojnë me ndonjë nga aktivitetet e tyre, megjithëse sulmuesit mund të përdorin edhe

ndonjë nga mangësitë ende të pazbuluar të programeve të instaluara. Përveç një programi të mirë anti-malware, është e nevojshme që të ndërrohen shprehitë- të mos shkarkohen aplikacionet e pasigurta, të mos hapen lidhjet dhe adresa emaili të dyshimta, ose të mos vizitohen faqet e pasigurta të internetit.

Kompleksiteti i kodit

Rregulli themelor gjatë krijimit të kodeve është që ata të mos përmbajnë të dhëna mbi përdoruesin dhe as fjalë të plota të gjuhës natyrore, sepse ashtu mund të zbulohen lehtësisht me metodën e provës dhe gabimit. Ekzistojnë gjeneratorë të kodeve komplekse me karaktere të rastit, por ato kode mbahen mend shumë vështirë. Zgjedhje e mirë është krijimi i kodeve gjoja të rastësishme të cilat mbahen mend lehtë, por merren me mend vështirë.

Poashtu, është e rëndësishme të konfigurohen pyetje të mira sigurie për rivendosjen e fjalëkalimit/kodit. Duhet patur kujdes që përgjigjja në pyetje sigurie të mos jetë përgjithësisht e njohur dhe në dukje e rastësishme.

Përveç kodeve komplekse, duhet aktivizuar dhe vërtetimi në dy nivele (eng. two-step authentication), në raste kur një gjë e tillë është e mundur. Kjo është një metodë vërtetimi që përveç vendosjes së fjalëkalimit kërkon edhe një hap shtësë, më së shpeshti shkrimi i kodit që fitohet përmes mesazhit SMS ose aplikacionit në celular. Një kod cilësor dhe mekanizma të tjerë të mbrojtjes së hyrjes janë të pashmangshme në rrugën drejt një sistemi të sigurt, por po aq e rëndësishme është edhe mënyra e ruajtjes. Nuk rekomandohet që fjalëkalimet të shënohen në fletore, copa letre apo të ruhen në celular. Mënyrë e sigurtë e ruajtjes janë softuerët të cilët i ruajnë fjalëkalimet

në bazën e të dhënave në format të kriptuar, kështu që, edhe nëse kompjuteri në të cilin ruhen është shënjestër e sulmeve, fjalëkalimet nuk e humbin integritetin e tyre. Shembuj të softuerëve të cilët mund të gjenerojnë fjalëkalime të rastit dhe të gjata, dhe ti ruajnë në bazë të sigurtë të pajisjes janë KeePass i KeePassXC. Më shumë mbi temën mund të gjeni edhe në Manual "Siguritë themelore digjitale".

Liria e shprehjes dhe mediat online në mjedisin digjital

E drejta për lirinë e shprehjes është e mbrojtur me nenin 10 të Konventës Evropiane për Mbrojtjen e të Drejtave të Njeriut dhe Lirive Themelore. Në paragrafin e parë të këtij neni thuhet se çdokush ka të drejtën e lirisë së shprehjes, ndërsa në paragrafin e dytë sqarohet se në cilat raste kjo e drejtë mund të kufizohet. Shtetet anëtare të Këshillit të Evropës kanë detyrime pozitive dhe negative në lidhje me nenin 10, gjegjësisht, janë të ftuara që në mënyrë aktive të promovojnë mbrojtjen dhe rrespektimin e të drejtave, por edhe të përmbahen nga ndërhyrja në ushtrimin e së drejtës për lirinë e shprehjes. Sipas nenit 10, paragrafi 2, ndërhyrja e shtetit në këtë të drejtë duhet të përmbushë kritere të rrepta: ajo duhet të përcaktohet me ligj, të jetë e nevojshme në një shoqëri demokratike, dhe të ketë një qellim legjitim. Mbrojtja që jep neni 10 përfshin informacione dhe mendime që mund të trondisin, ofendojnë dhe shqetësojnë, prandaj, në bazë të kësaj, të gjitha kufizimet e lirisë së shprehjes duhen zbatuar në mënyrë kufizuese.

Edhe pse neni 10 i Konventës nuk përmend në mënyrë eksplicite lirinë e medias, ajo është e përfshirë në lirinë e shprehjes. Roli i medias si "qen vrojtimi" është e një rëndësie të madhe në çdo shoqëri demokratike dhe të hapur, dhe me ardhjen e teknologjise së re atë rol e marrin gjithnjë e më shumë aktor, sepse tregu tradicional i medias ka ndryshuar plotësisht me paraqitjen e internetit, duke krijuar forma të reja të medias dhe komunikimit. Gjegjësisht, mjedisi digjital përfshin një hapësirë publike që sipas karakteristikave të veta është përgjithmonë në dispozicion të të gjithë aktorëve, duke u ofruar mundësi që në mënyre të drejtpërdrejt të marrin pjesë në shkëmbimin e informacioneve në nivel global.

Përveç mediave të mirënjohura tradicionale të tilla si media e shkruar, radioja dhe televizioni si dhe faqet e tyre në internet, tani ekzistojnë edhe shumë forma të mediave online. Është vështirë të hartohen dhe klasifikohen format e reja, por më tipike janë portalet informative, blogjet, shërbime për kërkimin e përmbajtjeve, rrjetet sociale, faqet për ndarje të videove, grumbulluesit e lajmeve, etj. Të gjitha këto forma na ofrojnë mundësinë të marrim dhe dërgojmë infomacione, por shtrohet pyetja se cilat forma të internetit duhen konsideruar "media" në aspektin e rregullimit të medias, si dhe cilat të drejta dhe përgjegjësi ekzistojnë në raste individuale. Interneti në këtë mënyrë i fshin plotësisht kufijtë, duke ndryshuar sistemet e vendosura dhe duke destabilizuar rregullat ekzistuese të informimit publik, çfarë krijon sfida të reja si për rregullatorët, ashtu edhe prodhuesit e përmbajtjes mediatike.

Sfida kryesore me të cilën përballën rregullatorët është çështja e statusit gazetaresk, gjegjësisht, pyetja se kush është gazetar dhe kush jo, dhe si koncepti modern i "gazetarisë qytetare" ndikon në kuptimin tradicional të profesionit. Rekomandimet e Komitetit të

Ministrave të Këshillit të Evropës nga viti 2011 përcaktojnë gjashtë kritere për identifikimin e medias, ndërsa udhëzimet për statusin e gazetarëve u dhanë në vitin 2012 nga raportuesi special i atëhershëm i Kombeve të Bashkuara për lirinë e shprehjes. Përkatësisht, Frank La Ru në raportin e tij është përcaktuar për të ashtuquajturin përkufizim funksional të një gazetari sipas të cilit ai është secili që vëzhgon, përshkruan, dokumenton dhe analizon ngjarje, deklarata, politika dhe çdo propozim që mund të ndikojë në shoqëri, me qëllim sistematizimin e informacioneve të tilla, mbledhjen e fakteve dhe analizimin, për të informuar një pjesë të shoqërisë ose shoqërinë në tërësi. Mjedisi digjital me vetë praninë në rrjet na mundëson pjesëmarrje në sferën e medias, gjë që nuk ishte më parë. Interneti konsiderohet gjithashtu një hapësirë ku të gjithë mund të thonë çfarë të duan dhe ku nuk zbatohen rregullat e gazetarisë tradicionale. Në këtë hapësirë të gjithë kanë shansat e njëjta për të dërguar një informacion dhe në këtë mënyrë të ndikojnë në opinionin publik, në të njëjtën mënyrë si gazetaria e edukuar etikisht, me formë editoriale, që respekton të gjitha rregullat.

Rezulati i diskutimit mbi statusin gazetaresk në një mjedis të ndryshuar do të ndikojë drejtpërdrejt në përcaktimin e fushës së disa lirive dhe të drejtave, siç është mbrojtja e sekretit të burimit të informacionit ose e drejta e përjashtimit nga aplikacioni i rreptë i regjimit të ri evropian të mbrojtjes së të dhënave personale. Nga ana tjetër, ky mjedis i ri digjital ndikon në mënyrë dramatike në pozitën e kujtdo që përfshihet në informimin e publikut, profesionalisht apo përkohësisht. Njohuria digjitale, cyber siguria dhe njohuria e teknikave dhe mjeteve për mbledhjen e infomacionit dhe mbrojtjen e të dhënave në mjedisin online, janë bërë pjesë përbërëse e aftësive themelore gazetareske.

Online mediat dhe rregullorja e mediave

Në Mal të Zi është në fuqi Ligji për Mediat i vitit 2002. Procesi i miratimit të Ligjit të ri në Kuvend është në proces, i harmonizuar me një sërë ndryshimesh teknologjike dhe shoqërore që kanë ndodhur ndërkohë, dhe që pritet të përmirësojnë ndjeshëm sferën e medias.

Ndryshe nga Ligji në fuqi i cili rëndit në mënyrë taksative atë që konsiderohet të jetë media (neni 6), në propozimin e Ligjit të ri, ky përkufizim mungon. Në vend të tij, propozimi i Ligjit të ri përmban përkufizimin e përmbajtjes mediatike dhe, ndër tjera, në nenin 6 thuhet që përmbajtja mediatike përfshin informacion, analizë, koment, mendim dhe të ngjajshme. Përveç kësaj, në të njëjtin nen të propozimit është e vendosur një dispozitë e paqartë që thotë se "media nënkupton aktorët e përfshirë në prodhimin dhe shpërndarjen e përmbajtjes mediatike me kontroll editorial ose mbikëqyrje të asaj përmbajtjeje të orjentuar drejt një numri të pacaktuar njerëzish". Gjithashtu, në nenin 26 futet termi botimet në internet dhe jepet përkufizimi i tij: një medium, përmbajtja e të cilit hapet përmes internetit, dhe që nuk është një shërbim mediatik audioviziv. Në përputhje me kriteret e dhëna, kjo do të nënkuptojë se çdo informacion, analizë, koment, mendim e të ngjashme, i prodhuar nën kontrollin editorial ose mbikëqyrjen e asaj përmbajtjeje të orjentuar drejt një numri të pacaktuar të personave mund të konsiderohet një botim në internet.

Në përkufizim i tillë i gjërë i botimit në internet mund të çojë te ajo që të gjitha llojet e mediave online, përfshirë edhe bllogjet, platforma në internet dhe celularë, forume, llogari Twitter, faqet në Facebook dhe shërbime të tjera të internetit që përdoren për të informuar publikun për çështje me interes publik, mund të konsiderohen media në përputhje me ligjin. Ndryshe nga Ligji aktual për media, në këtë mënyrë gjerësisht rregullohet hapësira online, çfarë mund të çojë në pasoja të mëdha për

lirinë e shprehjes si një të drejte të garantuar dhe për shkëmbimit e lirë të informacionit.

Në versionet e mëparshme të Projektligjit për media, në fillim vendoset domethënja e termeve, përfshirë edhe çfarë janë mediat, të cilat mund të shihen në Opinionin ligjor dhe komentet mbi projektligjin e porositur nga Misioni i OSBE-së në Mal të Zi.

Në përgjithësi, nga aspekti i rregullores, në media online duhet shikuar si në përmbajtje të hartuara editorialisht dhe të cilat kanë për qëllim informimin e publikut për çështje nga interesi publik. Një nga zgjedhjet mund të jetë që ligjvënësi të lënë opcionin për media që, nësë dëshirojnë, të regjistrohen si media dhe në atë mënyrë të marrin statusin e duhur me të gjitha të drejtat dhe detyrimet. Mediat e paregjistruara online duhet të kenë mundësinë të mbeten jashtë fushës së Ligjit për media, sepse rregulloret e medias imponojnë përgjegjësi të shumta të cilat mund të mbingarkojnë aktorët që nuk kanë ambicie të jenë media në kuptim zyrtar. Me fjalë të tjera, vetëm ata që regjistrohen vullnetarisht duhet të konsiderohen si medium për në kuptim të ligjit që rregullon këtë fushë. Sidoqoftë, as aktorët të cilët zgjedhin të mos regjistrohen nuk qendrojnë plotësisht jashtë fushës së të gjitha ligjeve-mbi ta aplikohen rregullat e përgjithshme ligjore mbi kompensimin e dëmeve nëse e shkaktojnë atë.

Çështje të reja etike

Gazetarët reagojnë në mënyrë të ndryshme ndaj ndryshimeve teknologjike. Kështu, disa mbrojnë qendrimin se gazetaria është gjithmonë e njëjtë, pavarësisht nga mjetet e realizimit të përdorura, ndërsa të tjerët sot veçojnë "gazetarinë me dron" nga llojet e tjera të veçanta, që i nënshtrohen ligjeve të ndryshme, të tilla si shtypi, radioja, televizioni ose gazetaria në internet.

Në varësi të vërtetimit mbi ndikimin që formati mund të ketë në praktikat mediatike, ndryshojnë edhe qasjet ndaj standardardeve etike. Një rrymë tregon që kërkesa e saktësisë dhe plotësisë së infomacionit ose përgjegjësisë për një të pavërtetë të botuar, gjithmonë do t'i rezistojë testit të ndryshimit teknologjik, pa marrë parasysh sa dramarike mund të jenë ato. Rryma tjetër beson se kushtet e reja për prodhimin dhe shpërndarjen e lajmeve kanë ndryshuar rrënjësisht vetë konceptet e së vërtetës, privatësisë ose interesit publik, dhe për këtë arsye kodi gazetaresk duhet të ndryshohet.

Lista e sfidave të mundshme që u paraqiten gazetarëve nga interneti nuk është përfundimtare, ngashme me atë kur flasim për ndikimin e teknologjive informative në rrethanat socio-politike ose ekonomike. Mediat dhe gazetarët mësojnë nga gabimet e tyre, duke u mbështetur në nivele të mirë-vendosura të vetërregullimit-nga vëmendja individuale gazetareske, vetëdija për kufizimet dhe paragjykimet e tyre, sfidat etike me të cilat përballen përmes mekanizmave editorial (kodet e brendshme, gjobat dhe shpërblimet, kontrolli editorial, ombudsmani i lexuesve) deri të shoqatat profesionale, kombëtare dhe ndërkombëtare.

Disa nga çështjet më të rëndësishme etike për gazetarinë në internet deri më tani janë të grupuara rreth verifikimit të besueshmërisë së burimeve, përdorimit të përmbajtjeve të botuara nga pikëpamja e mbrojtjes së të drejtës së autorit, transparencës dhe përgjegjësisë (korrigjimi i gabimit, konflikti i interesit) dhe balancimi i interesave komercial dhe publik (reklama e fshehtë, përmbajtje e ndjeshme- dhuna, pornografia, gjuha e urrejtjes).

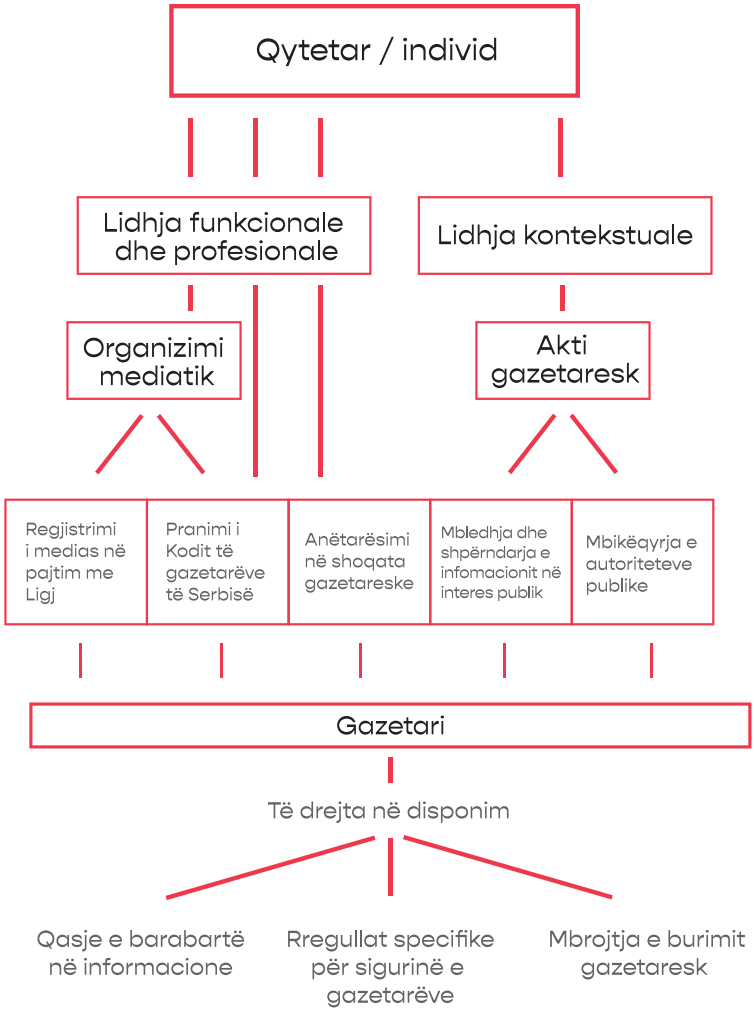
Rritja e dy rreziqeve themelore për gazetarinë etike - shpejtësia dhe konkurrenca - do të thotë që gazetarët profesionistë konkurrojnë në internet me korporatat gjigante nga njëra anë, dhe gazetarët amatorë, nga ana tjetër. Në kushte të tilla mbështetja përfundimtare është integriteti gazetaresk. Pavarësisht nëse ata përdorin informacionin e audiencës (eng.

crowdsourcing) për të mbledhur dhe verifikuar saktësisë së informacionit, nëse ata shkruajnë një blog në një kapacitet privat ose si punonjës të një organizatë mediatike, përgjegjësia personale e gazetarëve do të jetë në fund të fundit kapitali i tyre me reputacion në tregun mediatik. Një analizë e hollësishme e biznesit mediatik në mjedisin e ri teknologjik dhe ligjor mund të gjendet në manualin "Korniza rregullatore dhe modelet e biznesit të mediave online".

Statusi i gazetarëve

Çështja e statusit është e një rëndësie jashtëzakonisht të madhe kur flasim për dy të drejta- mbojtjen e sigurisë së gazetarëve dhe mbrojtjen e burimit të infomacionit. Shpesh mbizotëron interpretimi sipas të cilit të drejtat e veçanta vlejnë vetëm për gazetarët profesionistë, anëtarët e shoqatave profesionale, gjegjësisht personave të angazhuar në një nga mediat e regjistruara.

Sidoqoftë, duke marrë parasysh ndryshimet drastike në mjedisin mediatik, vëmëndje e rëndësishme duhet ti kushtohet harmonizimit të standardeve ekzistuese me parimet inovative që mbrojtja gazetareske u përket edhe pjesëmarrësve në komunikim publik që nuk kanë status zyrtarë të gazetarit, por vazhdimisht ose kohë pas kohe ndërmarrin akte gazetareske, gjegjësisht informojnë audiencën për çështje me interes publik.
Me fjalë tjera, individët mund të kenë privilegje dhe përgjegjësi kur janë profesionalisht të lidhur me ndonjë organizate mediatike, një shoqatë gazetarësh ose organ vetërregullues, gjë që është e gjitha e njohur për ne, ose përmes vetë aktit gazetaresk, gjegjësisht nga mbledhja dhe shpërndarja e infomacionit në mënyrë që të arrihet interesi publik dhe të kontrollohet qeveria.



*Manuali "Korniza rregullatore dhe modelet e biznesit të mediave online

Pyetja prandaj mund të shihet përmes një lidhjeje profesionale dhe kontekstuale. Dallimi midis këtyre dy aspekteve qendron në faktin se në një marrëdhënie profesionale mbrojtja gazetareske supozohet, kurse tek një marrëdhënie kontekstuale u takon vetë qytetarëve të dëshmojnë se po ndërmarrin një akt gazetaresk që u mundëson atyre privilegje gazetareske, dhe kështu mbrojtje.

Rregulla të përgjithshme mbi privilegjet dhe përgjegjësitë

Ekzistojnë dallime në status midis mediave të regjistruara dhe formave të paregjistruara të raportimit, të cilat përcaktojnë rregulla mbi privilegjet dhe përgjegjësitë në lidhje me përmbajtjen e botuar. Pyetja themelore është se cili ligj do të zbatohet, sepse për mediat e regjistruara zbatohet Ligji për media, kurse për aktorët e paregjistruat zbatohet Ligji për detyrimet.

Kur flasim për media të regjistruara, ekziston një numër privilegjesh, por edhe përgjegjësish të cilat janë të përcaktuara nga Ligji për Media.

Privilegjet

Mbojtja e burimit të informacionit

Një nga standardet më të rëndësishëm të profesionit të gazetaresisë është mbrojtja e burimeve të informacionit, si një trashëgimi e lirive të medias dhe gjendet në shumë dokumente, deklarata dhe rekomandime ndërkombëtare. Gazetarët kanë të drejtë të mbrojnë identitetin e burimeve të tyre dhe të publikojnë informacione. Ushtrimi i këtij privilegji është thelbësor për raportimin mbi të gjitha çështjet me interes publik për të cilat publiku përndryshe nuk mund të ketë dijeni.

Siç raporton organizata *Article 19* në botimin e saj mbi mbrojtjen e burime gazetareske, gazetaria e pavarur varet pikërisht nga shkëmbimi i lirë i infomacioneve midis mediave dhe qytetarëve. Individët, gjegjësisht burimet dalin me informacione sekrete dhe të ndjeshme, duke u mbështetur tek gazetarët që t'ia përcjellin publikut të gjërë për t'i informuar mbi çështje me interes publik. Më shumë mbi këtë temë mund të gjeni në manualin "Mbrojtja e sekretit të burimeve të informacionit".

Në nenin 23. paragrafi 3 të Ligjit aktual për Media thuhet se një gazetar dhe persona të tjerë të cilët gjatë kryerjes së punës gazetareske hasin informacione të cilat mund të tregojnë identitetin e burimit, nuk janë të detyruar të zbulojnë burimin e informacionit i cili dëshiron të mbetet i panjohur. Nëse kjo dispozitë interpretohet gjerësisht, mund të kuptohet në një mënyrë që të mos ketë kufizime, gjegjësisht, se e drejta për mbrojtjen e sekretit të burimeve gazetareske është absolute.

Sidoqoftë, ky nuk është rasti me Projektligjin (neni 30, paragrafi 1) i cili ka të njëjtën gjë si premisë themelore - që gazetari nuk është i detyruar të zbulojë një burim informacioni- kurse në paragrafin e rrallës kufizohet që një gazetar është i detyruar të zbulojë, në bazë të kërkesës së prokurorit, një burim informacioni kur kjo është e nevojshme për mbrojtjen e interesave të sigurisë kombëtare, integritetit territorial, mbrojtjes shëndetsore dhe zbulimit të veprave penale për të cilët është i parashikuar dënimi me burg prej pesë ose më shumë vitesh.

Këto përjashtime gjerësisht të përcaktuara mund të paraqesin një rrezik për gazetarët, gjegjësisht, burimet e tyre të cilat mund të pësojnë pasoja të dëmshme nëse identiteti i tyre zbulohet në gjykatë.

Veçanërisht problematike është që ky artikull mund të përdoret për të përsekutuar gazetarë që hetojnë punet e zyrtarëve publikë dhe njerëzve të tjerë të fuqishëm, me pretekstin e "mbrojtjes së sigurise kombëtare" e të ngjajshme.

Qasja në infomacion dhe akreditimi për raportim

Një marrëdhënie formale profesionale që përcakton qartë statusin gazetaresk lehtëson në mënyrë të konsiderueshme qasjen në infomacion dhe kredite për raportim. Është një parim i njohur që organizatorët e ngjarjeve të llojeve të ndryshme të japin akreditime për raportim mediave të regjistruara, kurse të tjerët nuk janë në gjendje të akreditohen.

Qasje në fondet shtetërore - burimet financiare për ushtrimin e të drejtës së qytetarëve në informim

Kur flasim për qasje në fondet shtetërore dhe burimet financiare të cilat ndahen për të arritur interesin publik, gjegjësisht të drejtën e qytetarëve për t'u informuar mbi çështje me rëndësi për komunitetin e tyre, si rregull, të drejtë në këtë kanë mediat e regjistruara. Subjektet e paregjistruara si media në përputhje me Ligjin dhe në regjistrin përkatës, nuk mund të llogarisin në mbështetje nga buxhetet publike.

Ligji aktual, si dhe projektligji i ri kanë pak a shumë të njëjtin qendrim, që fondet e caktuara ndahen nga buxheti shtetëror dhe dallimi qendron në atë për çfarë ndahen këto fonde, gjegjësisht, për çfarë përmbajtjesh. Ligji aktual cakton fonde për përmbajtjet programore që janë të rëndësishme për zhvillimin e shkencës dhe arsimit, zhvillimin e kulturës, informimin e personave me dëgjim dhe shikim të dëmtuar, si dhe fondet për përmbajtjen e specifikuar të programit

në gjuhën e pakicave kombëtare (neni 3). Neni 17 i projektligjit e përcakton pak më gjerësisht këtë fushë, dhe finansohen projektet nga fusha e informimit në mënyrë që shteti i siguron burimet financiare për ofrimin e shërbimeve publike përmes Fondit për Inkurajimin e Pluralizmit dhe Diversitetit të Medias. Përveç kësaj, shteti siguron një pjesë të fondeve për përmbajtje mediatike jokomerciale me interes publik, në gjuhët e popujve pakicë dhe të komuniteteve tjera kombëtare të pakicave dhe përmbajtje mediatike jokomerciale me interes publik në mediat e shtypura jofitimprurëse. Në përputhje me të dy aktet, mënyra dhe kushtet përcaktohen në mënyrë plotësuese nga një akt i organit kompetent për punët e informacionit ose Ministria e Kulturës.

Përgjegjësitë

Detyrimi i vëmëndjes gazetareske – "gazetaria e përgjegjshme"

Detyrimi themelor i gazetarëve është të veprojnë me vëmendjen e duhur gazetareske. Kjo do të thotë që ata nuk duhet të kenë besim të verbër në burimet e informacionit dhe kur raportojnë, ata janë të detyruar që të kontrollojnë informacionin nga disa burime të pavarura para se ta publikojnë. Kjo është veçanërisht e vërtetë për rrjetet sociale dhe burimet e tjera të informacionit në internet – teoritë e konspiracionit dhe trillimet e plota që përfundojnë në media zakonisht lindin në një cep të largët të internetit.

Është e rëndësishme të theksohet se gazetarët, redaktorët dhe botuesit e mediave mund të jenë përgjegjës para gjykatës për kompenzimin e dëmit të shkaktuar për shkak të mosrespektimit të vëmëndjes gazetareske.

Është interesante që Ligji aktual parashikon vetëm përgjegjësinë e autorit dhe themeluesit të medias, ndërsa përgjegjësia e kryeredaktorit nuk parashikohet, gjë që është mjaftë e pazakontë në praktikën krahasuese. Kjo ndryshon në propozimin e ligjit të ri, në të cilin thuhet, ndër të tjera se përgjegjësi për dëmin e shkaktuar kanë themeluesi, kryeredaktori dhe gazetari, nëse vërtetohet se ata kanë vepruar në kundërshtim me vëmëndjen e duhur gazetareske. Përgjegjësia e kryeredaktorit në punën gazetareske është e padiskutueshme, pikërisht sepse rolet e tij kryesore janë përzgjedhja dhe kontrolli i përmbajtjes që do të publikohet në media.

Më përkufizimin e gazetarisë së përgjegjshme, prozimi paraqet një risi dhe thotë se një gazetarë është i detyruar që "para se të publikojë një informacion në lidhje me një ngjarje, fenomen ose person të caktuar, me vëmëndjen e duhur gazetareske, të kontrollojë origjinën, vërtetësinë dhe plotësinë e saj".

Poashtu, kur flasim për përgjegjësitë, Projektligji rregullon në mënyrë eksplicite edhe hjekjen e komenteve nga faqet e internetit. Fillimisht thuhet që komenti është përmbajtje e postuar në faqen e internetit nga një përdorues i regjistruar. Meqenëse përkufizimi i një publikimi në internet është jashtëzakonisht i gjërë, atëherë, në këtë përkufizim ligjor mund të përfshihen forma të ndryshme të të shprehurit në internet. Dispozita që një koment duhet krijuar nga një përdorues i regjistruar çon në komplikime shtesë: çfarë ndodhë nëse media online nuk ka detyrim të regjistrojë përdoruesin në faqen e saj?

Themeluesi i botimit në internet gjithashtu merr përsipër të heqë një koment që është padyshim përmbatje e paligjshme dhe që shkel të drejtat e mbrojtura me ligj, pa vonesë dhe jo më vonë se brenda 24 orëve nga momenti i zbulimit ose raportimit të një personit tjetër.

Nëse kjo ndodh, përsoni me të cilin ka të bëjë komenti ka të drejtë të kërkojë heqjen e përmbajtjes nga gjykata kompetente.

Sidoqoftë, në sferën digjitale, çdo sekond publikohet një sasi jashtëzakonisht e madhe e përmbajtjeve të krijuara nga vetë përdoruesit, duke e bërë, shpeshherë, të pamundur kontrollin e çdo komenti të postuar. Mekanizmi i përshkruar në Projektligj është procedura e ashtuquajtur "notice and take down (NTD)", e cila e përshkruan procedurën në të cilën përmbajtja e diskutueshme hiqet pasi të njoftohet personi i interesuar. Kjo procedurë bazohet në dispozitat e Direktivës se Bashkimit Evropian mbi Tregtinë Elektronike 2000/31/EC dhe është e pranishme në të gjitha shtetet anëtare të BE-së, por zbatohet në mënyra të ndryshme. Në fakt, pasiguri ligjore krijon pikërisht ndryshimi në interpretim gjatë procesit të aplikimit në nivelin kombëtar.

Në proposim theksohet edhe se botimi në internet është i detyruar të përshkruajë rregullat e komentimit dhe t'i publikojë ato. Rregullat e komentimit janë shumë të rëndësishme për përdoruesit dhe është e nevojshme që ata të informohen se si mediat online trajtojnë komentet, si dhe mbi të drejtat dhe detyrimet të cilat i referohen përmbajtjes që ata synojnë të postojnë. Këshilli i shtypit në Serbi ka zhvilluar një Manual për përshtatjen e rregullave për nevojat e medive online i cili flet më hollësisht për rregullat e komentimit dhe modelet e ndryshme që media online mund të zbatojë.

Se zgjidhjet ekzistuese u nënshtrohen ende interpretimeve të ndryshme në lidhje me traditën juridike, konfirmohet edhe nga vendimi i Këshillit Kushtetues të Francës, i miratuar në qershor të vitit 2020, më të cilin u deklaruan antikushtetuese dispozitat kryesore të të ashtuquajturit Ligj të Aviacionit. Një nga dispozitat e diskutueshme

ishte detyrimi i ofruesve të shërbimeve në internet për të hequr brenda 24 orëve përmbajtjen e raportuar nga përdoruesit si "padyshimtë e paligjshme", në përputhje me një listë të përcaktuar më parë të shkeljeve ligjore. Gjithashtu, është shfuqizuar edhe dispozita sipas së cilës, në rastin e përmbajtjes terroriste dhe përmbajtjes në lidhje me shfytëzimin seksual të fëmijeve, ndërmjetësuesit në internet janë të detyruar që përmbajtjet e tilla ti heqin brenda një ore nga raporti i paraqitur nga organet administrative. Këshilli ka theksuar në vendimin e tij se dispozita të tilla rrezikojnë lirinë e shprehjes dhe komunikimit dhe nuk janë proporcionale, të nevojshme dhe të përshtatshme.

Pasiguria më e madhe krijohet nga afati kohor dhe pyetja se kush e merr vendimin se çfarë përbën përmbajtje të paligjshme ose cilat janë ato të drejta të mbrojtura në përputhje me Ligjin. Vëmendje të veçantë i duhet kushtuar edhe faktit që diçka e tillë kërkon burime shtesë brenda mediave online, gjegjësisht, është e nevojshme të keni njerëz të trajnuar që janë në gjendje të bjenë vendime të tilla këtij lloji. Nëse përmbajtja nuk hiqet, media është në rrezik të procesit gjyqësor; nëse përmbajtja hiqet, media rrezikon të bëhet censor që kufizon të drejtën për lirinë e shprehjes.

E drejta e përgjigjjes dhe korrigjimit

Gabime në gazetari ndodhin, me pasoja më të lehta ose më të vështira, por në një kohë kur është pothuajse e pamundur të hiqet përmbajtja plotësisht nga interneti, pasojat e gabimeve mund të jenë të përhershme.

Legjislacioni i medias në të gjithë botën njeh institutet e së drejtës për t'u përgjigjur ose korrigjuar informacionin, saktësisht për t'i dhënë mundësi palës raportuese të marrë kënaqësi pa filluar procedura ligjore, nëse konsideron se është e dëmtuar.

Duke pasur parasysh që e drejta e përgjigjjes dhe korrigjimit hap mundësi për abuzim, legjislacioni mediatik në përgjithësi njeh kufizime kur mediat nuk janë të detyruar të publikojnë një përgjigjje.

Ligji aktual rregullon në detaje të drejtën e përgjigjjes dhe korrigjimit, në mënyrë që çdokush ka të drejtë të kërkojë publikimin e përgjigjjes dhe korrigjimit nëse ndonjë nga të drejtat e tij është shkelur, brenda 30 ditëvë nga dita e publikimit të përmbajtjes. Është përshkruar mënyra në të cilën bëhet botimi, si dhe kur media nuk është e detyruar të publikojë përgjigjjen ose korrigjimin. Në rast kur media është e detyruar ta publikojë përgjigjjen ose korrigjimin dhe nuk e bën këtë, është e rregulluar edhe procedura e padisë.

Përveç dispozitave të përgjithshme, në Projektligj thuhet se në botime në internet përgjigjja dhe korrigjimi duhen botuar jo më von se 12 orë pas marrjes dhe duhet të lidhen me përmbajtjen mediatike të cilës i referohen.

Është e rëndësishme që edhe mediat online të jenë të vetëdijshme që metodat tradicionale të botimit të përgjigjjes dhe korrigjimit duhet të përshtatën me mjedisin e ri, prandaj është e nevojshme të vendoset një praktikë se si do të bëhet kjo kur bëhet fjalë për faqet e internetit. Një pikë e mirë fillestare janë Udhëzimet për zbatimin e Kodit të gazetarëve të Serbisë në mjedisin online.

Arsye të veçanta për përjashtimin e përgjegjësisë

Përveç krijimit të përmbajtjes origjinale, media transmeton gjithashtu infomacione ose thënie me rëndësi për publikun. Megjithëse në parim ekziston përgjegjësia për të gjithë përmbajtjen e publikuar në një medium, në situata të caktuara media mund të referohet në

standarde të përjashtimit nga përgjegjësia për dëmin e shkaktuar nga infomacioni i transmetuar.

Një shembull i qartë është informacioni i diskutueshëm i transmetuar me besnikëri nga një tubim publik, ose i botuar në një emision të transmetuar drejtpërdrejtë, me kusht që në të dyja rastet gazetari të veprojë me kujdesin e duhur gazetaresk.

Ligji aktual për media nuk ka dispozita të veçanta në lidhje me përjashtimin nga përgjegjësia, megjithëse ato janë të një rëndësie të jashtëzakonshme në raste të caktuara. Projektligji e parashikon këtë në një mënyrë të tillë që përgjegjësia e përbashkët e themeluesve të medias, kryeredaktorit dhe gazetarëve nuk do të ekzistojë nëse përmbajtjen e cila ka shkaktuar dëmin e kanë publikuar me vëmendjen e duhur gazetareske, dhe ajo përmbajtje është:

- e transmetuar me besnikëri nga një seancë të autoriteteve legjislative, ekzekutive ose gjyqësore, organ të qeverisjes shtetërorë ose lokale, nga një tubim publik ose i transmetuar nga një akt i një organi, institucioni publik ose personi tjetër të besuar me autoritet publik;
- me interes publik dhe e transmetuar si citim nga një medium tjetër ose i publikuar brenda një intervistë, përveç nëse ndonjë pjesë e caktuar përmban fyerje dhe shpifje të dukshme;
- bazuar në informacione për të cilat gazetari dhe kryeredaktori kishin arsye të mira për të besuar se ishin të plota ose të vërteta, dhe kishte një interes të ligjshëm publik për t'u informuar.

Vetërregullimi

Rrespektimi i standardeve etike të profesionit gazetaresk është detyrim i çdo raportimi mbi tema me interes publik, qofshin ata gazetarë profesionistë ose qytetarët që kryejnë aktin gazetaresk.

Parimet themelore të gazetarisë etike janë praktikisht universale, siç janë vërtetësia, paanësia, drejtësia ose përgjegjësia, më shtesa dhe sqarime të ndryshme nga konteksti lokal, zhvillimi historik dhe përvoja. Kështu, disa dispozita të kodit dëshmojnë për mbrojtjen kundër presionit komercial në shoqëritë perëndimore gjatë gjysmës së dytë të shekullit XX, ndërsa ndalimet e qarta të diskriminimit shoqëruan luftën për përfshirjen shoqërore dhe barazinë. Epoka e përhapjes së lajmeve të rreme dhe "fakteve alternative" sot paraqet një sfidë të veçantë ndaj parimit të vërtetësisë.

Kodi i Etikës për gazetarët e Malit të Zi u miratua në vitin 2002, dhe u plotësua në vitin 2015 dhe 2018, kur u përfshinë edhe udhëzimet për media online.

Organet vetë-rregulluese

Në Mal të Zi nuk ekziston një organ i vetëm që merret me çështje të etikës gazetareske dhe pajtueshmërinë me Kodin. Në vend të kësaj, gjatë viteve janë themeluar disa organe, disa nga të cilat janë akoma aktive, ndërsa të tjerat janë mbyllur. Gjithashtu, në disa media ekziston edhe instituti i ombudsmenit.

Deri më tani, në Mal të Zi nuk është krijuar një mekanizëm i unifikuar i vetërregullimit kolektiv. Fillimisht ishte Organi vetë-rregullues gazetaresk, të cilin e kanë themeluar bashkërisht shoqatat e

gazetarëve dhe media individuale, por ai pushoi së funksionuari në vitin 2010. Pastaj, disa media të shkruara filluan Këshillin e Mediave për Vetërregullim, që ka përcjellë punën e mediave dhe ka prurë vendime në lidhje me ankesa, herë pas here pezullonte punën dhe përsëri rifillonte. Disa media lokale dhe të shkruara kanë krijuar në vitin 2012 Këshillin vetë-rregullues për shtypin lokal, i cili deri më sot ka publikuar vetëm një raport mbi punën e mediave, dhe nuk është e qartë nëse ky organ ekziston ende. Nga ana tjetër, disa media kanë themeluar ombudsmenë të cilët janë kryesisht funkcionalë edhe sot – ND Vijesti, Dan, Monitor, TV Vijesti (sipas të dhënave në dispozicion vetëm deri në vitin 2018).

Ndryshe nga ai aktual, propozimi i ligjit të ri për media njeh rëndësinë e vetërregullimit, dhe thotë se media mund të krijojë një organ vetë-rregullues kolektiv, por gjithashtu që secili medium mund të krijojë një organ të brendshëm vetë-rregullues.

Mekanizmat e vetërregullimit janë të një rëndësie jetike për një profesion që është i pavarur nga kontrolli i shtetit, dhe i cili i përmbush detyrimet e tij ndaj publikut duke rishikuar vazhdimisht cilësinë e punës së tij. Megjithëse mekanizmat e brendshëm janë jashtëzakonisht të dobishëm për media individuale ose grup mediash të ndërlidhura, një platformë e vetme vetë-rregulluese mund të përmirësojë ndjeshëm zbatimin e plotë të standardeve etike në raportimin ditor. Mekanizmi i cili vazhdimisht kontrollon se si interpretohen parimet e kodit gazetaresk në lidhje me sfidat e ekosistemit të mediave të reja është gjithashtu një mbështetje e rëndësishme për mediat e reja online.

Mediat dhe mbrojtja e të dhënave personale

Kuadri ligjor për mbrojtjen e të dhënave personale

Të merresh me gazetari do të thotë gjithashtu të përpunosh të dhëna të ndryshme personale, për qellime të ndryshme dhe në kontekste të ndryshme. Pavarësisht rolit të tyre në një medium të caktuar, gazetarët, redaktorët ose punonjësit në mbështetjen administrative duhet të jenë të vetëdijshëm për detyrimet që kanë në lidhje me përpunimin e të dhënave personale me të cilat kanë kontakt në punën që bëjnë. Përndryshe, për media e ndonjëherë edhe për individët, mund të ndodhin pasoja dhe sanksione ligjore negative, me rrezik të madh dhe dëmtim të mundshëm të reputacionit të tyre.

Viteve të fundit, kuadri ligjor i cili rregullon trajtimin e të dhënave personale ka pësuar ndryshime të mëdha në pothuajse të gjitha shtetet evropiane. Në nivelin e të gjithë Bashkimit Evropian, me 25 maj 2018 ka filluar zbatimi i Rregullores së Përgjithshme të Mbrojtjes së të Dhënave (eng. General Data Protection Regulation, GDPR). Ky akt ligjor ka rëndësi për të gjitha shtetet jashtë Bashkimit Evropian për dy arsye. Arsyeja zyrtare është që vetë neni 3(2) i GDPR-së përcakton kushtet në të cilat do të zbatohet për subjektet që nuk janë të themeluar në BE, por përpunojnë të dhëna të personave të cilët janë të vendosur në BE. Arsyeja e dytë është se shtetet jashtë BE-së përfshijnë në legjislacionin e tyre kombëtar ligje që parashikojnë të njëjtat standarde të larta - si për të lëvizur më pranë tregut evropian,

ashtu edhe për të shpallur standarde të larta në fushën e të drejtave të njeriut, përfshirë edhe të drejtën për privatësi.

Qe nga fillimi i zbatimit të GDPR-së ka pasur njoftime se Ligji për mbrojtjen e të dhënave personale do të miratohet edhe në Mal të Zi, i cili do të përfshijë rregullat e reja të BE-së në legjislacionin e brendshëm. Sidoqoftë, në kohën e shkrimit së këtij udhëzuesi nuk ekziston një projektligj i kësaj rregullore në dispozicion publik.

Çështje e zbatimit të rregullave të GDPR-së është e një rëndësie të veçantë për punën e gazetarëve. Përkatësisht, GDPR-ja në nenin 85 rregullon në mënyrë specifike situatat e përpunimit të të dhënave kur bëhet fjalë për infomimin e publikut. I quajtur gjerësisht "përjashtim gazetaresk" i përfshirë në këtë artikull të GDPR-së u referohet situatave kur gazetarët nuk duhet të rrespektojnë të gjitha rregullat ligjore gjatë përpunimit të të dhënave personale, nëse kjo është e nevojshme për kryerjen e punës gazetareske. Rregulla, të tilla si "përjashtimi gazetaresk" nuk janë të përfshira në Ligjin aktual të Malit të Zi mbi mbrojtjen e të dhënave. Ky fakt, në situata të caktuara mund të jetë burim i pasigurisë ligjore.

Konceptet themelore në fushën e mbrojtjes së të dhënave personale

Të dhëna mbi për personin ose të dhëna personale është një term i gjerë në kuptimin e rregullores juridike. Aktualisht, Ligji i Malit të Zi në mënyrë koncize përcakton të dhënat personale si të gjitha informacionet që lidhen me një person fizik identiteti i të cilit është përcaktuar ose mund të përcaktohet. Në thelb të këtij përkufizimi është ideja që të dhënat personale janë çdo informacion që ka të bëjë me një person fizik dhe që, në mënyrë të pavarur ose me

informacione të tjera, mund të kontribuojë në identifikimin e një personi të caktuar. Disa të dhëna, të tilla si numri unik i identifikimit, gjurmë gishtash ose emër dhe mbiemër, kontribuojnë drejtpërdrejt në identifikimin. Sidoqoftë, personale konsiderohen edhe të gjitha ato të dhëna që në mënyrë indirekte mund të çojnë në të njëjtin rezultat, siç janë përshkrimi i karakteristikave psikologjike, fjalëkalimet dhe llogaritë e mesazheve, adresat e postës elektronike, historia e veprimtarive në internet dhe veçanërisht në rrjetet sociale (meta të dhënat, ndarjet, pëlqimet, klikimet), historia e kërkimit në internet, adresa IP e kompjuterit ose smartphone-it dhe të ngjashme.

Një gamë e tillë e gjerë informacionesh që konsiderohen të dhëna personale është pasojë, ndër të tjera, e digjitalizimit në rritje të një numri në rritje të aktiviteteve sociale dhe personale. Në mjedisin online, shumë të dhëna të tilla personale bëhen lehtësisht të disponueshme për publikun. Është e rëndësishme të theksohet se të gjitha të dhënat personale janë, në parim, nën të njëjtën mbrojtje ligjore. Me fjalë të tjera, fakti që disa informacione janë bërë publike, edhe me vullnetin e vetë personit, nuk do të thotë që ligji nuk e mbron atë dhe se palët e treta mund t'i disponojnë lirisht këto informacione. Gjithashtu, mediat, si pjesë e përpunimit të tyre të të dhënave personale, i bëjnë ato të dhëna publike të disponueshme në baza ditore. Prandaj, është jashtëzakonisht e rëndësishme që gjatë kryerjes së punës së tyre ata të mos kalojnë kufirin me të cilin në mënyrë të panevojshme dhe të paligjshme shkelin privatësinë e personave që kanë të drejtën e mbrojtjes ligjore të të dhënave personale.

Disa të dhëna personale janë nga natyra e tyre shumë të ndjeshme, sepse me përpunimin e tyre depërtohet më thellë në privatësi si një të drejtë themelore të njeriut. Prandaj, rregulloret sigurojnë një shkallë më të lartë të mbrojtjes së këtyre të dhënave, gjegjësisht

ato përshkruajnë kushte më të rrepta për përpunimin e tyre. **Në kategorinë e të dhënave të veçanta,** sipas Ligjit aktual të Malit të Zi, përfshihen të dhëna në lidhje me origjinën racore ose etnike, mendimin politik, besimin fetarë ose filozofik, anëtarësimin në sindikata, si dhe të dhëna që lidhen me statusin shëndetësor ose jetën seksuale.

Subjekti ndaj të cilit një person fizik - bartës i të dhënave mund të ushtrojë të drejtat e tij quhet **operator**. Operatori mund të jetë i çdo forme juridike ose subjektive, megjithëse si rregull do të jenë persona juridikë ose organe shtetërore. Ajo që e bën një subjekt operator është fakti që ky subjekt ka përcaktuar qëllimin dhe mënyrën e përpunimit të të dhënave personale. Në hapësirën mediatike, është, si rregull, vetë media, dhe jo gazetarë ose redaktorë individualë. Sidoqoftë, edhe një gazetar që, për shembull, ka blogun e tij, mund të konsiderohet operator në kushte të caktuara.

Përveç operatorit, në përpunimin e të dhënave shpesh marrin pjesë edhe **përpunuesit**. Këta janë subjekte që nuk kanë përcaktuar qëllimin për të cilin përpunohen të dhënat, as nuk e kanë përcaktuar mënyrën - por i kanë siguruar operatorit mjetet (p.sh. pajisjet, aplikacionin ose softuerin) për përdorim gjatë përpunimit. Për shembull, një përpunues në kontekstin e medias është një kompani IT që krijoi dhe mirëmban si faqen e internetit, ashtu edhe programet softuerë që gazetarët përdorin në punën e tyre të përditshme. Roli i përpunuesit është, mbi të gjitha, të sigurojë që të dhënat të jenë të sigurta, gjegjësisht të mos ndodhin incidente të tilla si "rrjedhja" ose humbja e të dhënave. Me një kontratë të veçantë me operatorin, ata marrin përsipër që pajisjet e përdorura për përpunimin e të dhënave personale të jenë të sigurta.

Regullat themelore që duhet të ndiqen gjatë përpunimit të të dhënave personale

Përgjegjësia që përpunimi i të dhënave personale të jetë i ligjshëm i takon operatorit (d.m.th., jo përpunuesit). Shtrirja e detyrimeve të tij në parim mund të ndahet në detyrime materiale dhe formale. Detyrimet materiale u referohen rregullave kryesore që duhet të shoqërojnë çdo proces të përpunimit të të dhënave, nga fillimi në fund, gjegjësisht, nga mbledhja e të dhënave deri te fshirja e tyre. Këto rregulla janë të përfshira në parimet e GDPR-së, por ato janë gjithashtu të përshkruara edhe nga Ligji aktual i Malit të Zi.

Logjika e këtyre rregullave themelore është si vijon: (i) para fillimit të përpunimit, operatori duhet të **përcaktojë dhe përkufizojë qartë qëllimin** që do të arrihet me përpunimin, kurse qëllimi duhet të jetë i justifikuar dhe i ligjshëm (kufizimi i qëllimit); (ii) kur përcaktohet qëllimi, duhet të përcaktohet **nëse ekziston një bazë ligjore** që lejon përpunimin për një qëllim specifik, ku bazat ligjore në dispozicion janë të rregulluara nga vetë ligji (ligjshmëria); (iii) për një qëllim të përcaktuar mund të mbledhen vetëm **ato të dhëna personale që janë vërtet të nevojshme** dmth. pa të cilat realizimi i qëllimit nuk do të ishte aspak i mundur (minimizimi); (iv) duhet të merren masat e nevojshme për të siguruar që **të dhënat janë të sakta,** të korrigjohen kur është e nevojshme si dhe të azhurnohen rregullisht (saktësia); (v) si dhe masat e nevojshme në rrethana specifike për të pasur qasje në të dhëna vetëm nga ata të autorizuar për ta bërë këtë dhe asnjë palë e tretë, **në mënyrë që të dhënat të mos humbasin, shkatërrohen ose dëmtohen** (integriteti dhe konfidencialiteti) (vi) të dhënat të cilat janë mbledhur për një qëllim specifik **duhet të fshihen ose anonimohen** menjëherë pasi që të arrihet ai qëllim (kufizimi i ruajtjes); (vii) subjektet, të dhënat e të

cilëve përpunohen duhet të informohen **në mënyrë të qartë dhe lehtësisht të arritshme** për përpunimet specifike që kanë të bëjnë me ata, duke respektuar të drejtat e tyre (transparenca dhe drejtësia).

Përveç rregullave materiale që duhet të rrespektohen për çdo përpunim specifik, operatorët gjithashtu kanë disa detyrime zyrtare, siç janë detyrimi për të lidhur kontratë me përpunuesit dhe detyrimi për të mbajtur **shënime për përpunimin** që ata kryejnë. Sipas ligjit aktual të Malit të Zi, ekziston edhe detyrim për të regjistruar koleksionet e të dhënave në Agjencinë për Mbrojtjen e të Dhënave Personale dhe Qasjen e Lirë në Informacion. Sidoqoftë, pritet që ligji i ri në përputhje me GDPR-në të shfuqizojë detyrimin për t'u regjistruar dhe që këto koleksione, gjegjësisht shënime do bëhen vetëm brenda te operatori. Qëllimi i regjistrave është që operatori të ketë në një vend një pasqyrë të të gjitha llojeve dhe proceseve të përpunimit që ai kryen brenda veprimtarisë së tij, me informacionin e duhur që përshkruan ato procese, nga të cilat mund të vërtetohet nëse operatori ndjek me të vërtetë rregullat themelore.

Nuk ka asnjë detyrim të përcaktuar që operatori të ketë një politikë **të privatësisë**, dmth. një dokument që përkufizon publikisht marrëdhëniet e tij me privatësinë dhe të dhënat personale dhe informon qytetarët për të drejtat e tyre. Sidoqoftë, rregulloret përmbajnë rregulla të hollësishme në lidhje me çfarë duhet gjithë kontrolluesit të informojnë personat, të dhënat e të cilëve ata përpunojnë. Praktika ka treguar se politika e privatësisë është një mënyrë për të përmbushur detyrimin e njoftimit. Për shumicën e mediave të pranishme në internet, disponueshmëria e një dokumenti të tillë është çështje e praktikës së mirë dhe standardeve tashmë të vendosura.

Përjashtim gazetaresk

Regjimi i ri i mbrojtjes së të dhënave personale trajton lirinë e shprehjes dhe informacionit si një rast të veçantë të përpunimit për të cilin zbatohen rregulla pak më të ndryshme. Përpunimi i të dhënave personale, në këtë kontekst, në parim përjashtohet nga zbatimi i disa dispozitave të ligjit në lidhje me parimet e përpunimit, të drejtat e qytetarëve dhe detyrimet e administruesve dhe përpunuesve – me kusht që në një rast të veçantë kjo të jetë e nevojshme. Një rregullim i tillë është i nevojshëm për të pajtuar në praktikë konfliktin midis dy të drejtave themelore: lirisë së shprehjes dhe informacionit nga njëra anë, dhe të drejtës për privatësi nga ana tjetër. Kurdoherë që ky konflikt mbizotëron në favor të lirisë së shprehjes dhe interesit publik, hulumtimi gazetaresk dhe botimi i informacionit në media do të lirohen nga detyrimi për të mbrojtur të dhënat personale. Nga këndvështrimi i zbatimit të ligjeve që mbrojnë të dhënat personale, një zgjidhje e tillë zakonisht quhet "përjashtim gazetaresk".

Rastet specifike në të cilat është e mundur të mbështetemi në një përjashtim gazetaresk ende nuk janë testuar në praktikë, kryesisht të modeluara në zbatimin e GDPR-së për shkak të rëndësisë së tij në fushën ligjore evropiane. Sidoqoftë, tashmë është e mundur të parashikohen konflikte të mundshme midis mbrojtjes së të dhënave personale dhe vetë aktit të gazetarisë. Dyshimet dhe rreziqet në zbatimin e përjashtimit pasqyrohen në interpretimin e termave të tilla si gazetaria, gazetari, media, interesi publik dhe të ngjashme.

Në atë kuptim, pyetja themelore dhe fillestare është – për kë është menduar përjashtimi gazetaresk? Çështje të tilla si kush është gazetar, çfarë përmbajtje mund të konsiderohet gazetari dhe cili është interesi publik që gazetaria plotëson – po bëhen gjithnjë e më

të rëndësishme në kontekstin e aktivizimit të përjashtimit për qëllime gazetareske. Kështu, duhet të kemi parasysh se përpunimi i të dhënave personale në këtë rast të veçantë të lirisë së shprehjes dhe informacionit nuk do të thotë një përjashtim i zbrazët për përpunimin e të dhënave personale por, siç përshkruhet nga GDPR-ja, "vetëm nëse këto kufizime janë të nevojshme për të harmonizuar të drejtën për mbrojtjen e të dhënave personale me lirinë e shprehjes dhe informacionit".

Për organizatat e medias si rregull, do të jetë më e lehtë të mbështeten në përjashtimin nëse ato mund të paraqesin politika dhe procedura të përshtatshme të brendshme, pajtueshmëri me kode dhe menaxhim adekuat të bazës së të dhënave, ndërsa e gjithë kjo mund të jetë një sfidë më e madhe për gazetarinë personale (eng. freelancer). pa mbështetjen e organizatës mediatike.

Sipas praktikës gjyqësore të gjykatave evropiane, termi "gazetar" që mund të mbështetet në një përjashtim gazetaresk duhet të interpretohet gjerësisht, ku rëndësi thelbësore ka nëse qëllimi i botimit të caktuar ishte "zbulimi i informacionit, mendimeve dhe ideve për publikun", siç mund të shihet në gjykimin e Gjykatës së Drejtësisë të Bashkimit Evropian në çështjen "Sergejs Buivids v. Datu valsts inspekcija" në të cilën u vendos që këto rregulla të vlejnë edhe për "youtuber" kur plotësohen kushtet e caktuara.

Në mungesë të udhëzimeve më specifike në nivelin e BE-së, akoma të përkatshme janë udhëzimet e Komisionit Britanik për Zbatimin e Direktivës së Vjetër Evropiane mbi Mbrojtjen e të Dhënave të cilat japin propozime konkrete për analizimin e përjashtimit gazetaresk, i cili mund të ndahet në katër elemente: (1) të dhënat përpunohen vetëm për gazetari, art ose letërsi, (2) me qëllim të botimit të materialeve

të caktuara, (3) me një besim të arsyeshëm që botimi është për interes publik dhe (4) me një besim të arsyeshëm se harmonizimi nuk është i pajtueshëm me gazetarinë.

Mbledhja dhe përpunimi i të dhënave personale është një pjesë thelbësore e punës gazetareske dhe, megjithëse rregullat e reja ngrisin nivelin e mbrojtjes së të dhënave personale, pozicioni i gazetarëve që respektojnë standardet ligjore dhe profesionale nuk duhet të ndryshojë ndjeshëm. Transferimi i barrës mund të ketë implikime praktike mbi gazetarët për të përcaktuar nëse interesi i ligjshëm publik tejkalon të drejtën për privatësi, veçanërisht në kontekstin e gazetarisë hulumtuese. Ekziston gjithashtu një rrezik që rregullat e mbrojtjes së të dhënave personale të keqpërdoren me qëllim të goditjes së mediave "të papërshtatshme". Sidoqoftë, duke qenë se ky problem është njohur tashmë, është e rëndësishme të vendoset ligjërisht një përjashtim gazetaresk mbi bazën e të cilit gazetarët mund të kundërshtojnë praktika të tilla. Në atë kontekst, megjithëse Ligji aktual i Malit të Zi për mbrojtjen e të dhënave personale nuk e njeh përjashtimin gazetaresk si të tillë në tekst, sipas njoftimeve që rregullat e GDPR-së së shpejti do të përfshihen në sistemin e brendshëm ligjor, pritet që kjo çështje të zgjidhet në mënyrë të përshtatshme.

Regjistrimet e operacioneve të përpunimit që janë karakteristike për mediat

Në situatat kur media dhe gazetarët duhet të zbatojnë ligjet për mbrojtjen e të dhënave personale, ata do të kenë statusin e kontrolluesve të të dhënave dhe në atë kapacitet duhet të respektojnë rregullat e zbatueshme për kontrolluesit. Sidoqoftë, brenda veprimtarisë mediatike, ekzistojnë disa procese të përpunimit

që janë karakteristike dhe specifike, dhe për të cilat do të zbatohen rregulla të ngjashme dhe standarde sektoriale.

- Duke qenë se kufijtë e përjashtimit gazetaresk janë ende të paqartë, çështje e rëndësishme është se në cilin regjim janë të dhënat personale mbi burimet e medias, gjegjësisht nëse për mbledhjen, përdorimin dhe ruajtjen e tyre, zbatohen të gjitha rregullat si dhe për përpunimin e të dhënave të tjera personale. Përgjigja e shkurtër mund të jetë: po, në një masë të madhe. Në thelb, në lidhje me këto të dhëna, organizata e medias ka statusin e një kontrolluesi, sepse ajo vetë përcakton se për çfarë qëllimesh mund të përdoren të dhënat mbi burimet, cilat të dhëna mblidhen, për sa kohë ruhen dhe si sigurohet siguria dhe konfidencialiteti i tyre. Në mënyrë që të pajtohet me rregulloret për mbrojtjen e të dhënave personale, organizata e medias duhet të përcaktojë në rregullat e saj të brendshme të gjitha qëllimet për të cilat do të përdorë të dhënat mbi burimet, dhe të përcaktojë bazën e duhur ligjore, llojin dhe sasinë e të dhënave që mbledh, si dhe periudhat e ruajtjes. Gjithashtu, nëse konsideron që për këto të dhëna vlen një përjashtim gazetaresk - organizata e medias duhet të marrë në konsideratë dhe të analizojë çështjen paraprakisht, dhe të parashikojë nga brenda rregullat që mund të justifikojnë këtë përjashtim.
- Ligjet, si rregull, nuk përshkruajnë detyrimin e kontrolluesve për të pasur politika të privatësisë, gjegjësisht një dokument me të cilin organizata përcakton publikisht marrëdhëniet e saj me privatësinë dhe të dhënat personale. Një dokument i tillë është provuar të jetë një mënyrë e mirë për të përmbushur detyrimet e transparencës dhe informacionit të subjekteve, të dhënat e të cilëve përpunohen. Për përdoruesit e mediave

online, politika e privatësisë e disponueshme në faqe do të jetë një shenjë respekti për standardet e vendosura.

- Të ardhurat e mediave në internet gjenerohen më shpesh me shënjestrimin e përdoruesve me ndihmën e biskotave (cookies), dmth gjurmuesit. Mediat online përdorin këto mjete për të matur vizitat në faqet e tyre dhe për të përcjellë sjelljen e vizitorëve, për qëllime të analizimit të trafikut në internet, por edhe për qëllime të marketingut. Sidoqoftë, cookies dhe gjurmuesit që përdoruesit marrin kur lexojnë media online janë pjesë e një teknologjie që përfshin mbledhjen dhe përpunimin e të dhënave personale. Prandaj, transparenca e plotë për këtë çështje është gjithashtu e rëndësishme, zakonisht brenda kornizës së një politike të privatësisë ose një politike të veçantë të cookie-t. Duke qenë se kjo është një temë që mund të jetë e paqartë për një përdorues mesatar, organizata e medias duhet t'i kushtojë vëmendje të veçantë për të siguruar informacionin e duhur për teknologjitë e monitorimit dhe analitikat e përdorura në një mënyrë të thjeshtë dhe të lehtë për t'u kuptuar. Gjithashtu, nëse në këtë faqe ka cookies të palëve të treta, organizata e medias duhet të ketë një marrëdhënie të rregulluar me secilën prej tyre.
- Disa media gjenerojnë të ardhurat e tyre përmes **donacioneve direkte nga lexuesit**. Lloji i të dhënave personale të mbledhura nga lexuesit-donatorët do të kushtëzohet kryesisht nga detyrimet ligjore që kanë kontrolluesit sipas rregulloreve të kontabilitetit, taksave ose këmbimit valutor. Sidoqoftë, nëse mbledhja e të dhënave personale nuk bazohet në legjislacion, por kontrolluesi mbledh të dhëna personale shtesë për qëllimet e tij të tjera, për shembull statistikore, analitike ose marketing, atëherë është e nevojshme që kontrollori të marrë

një bazë tjetër ligjore për këtë përpunim, e cila zakonisht do të jetë pëlqimi ose një interes legjitim.

- Media të caktuara kanë zgjedhur abonimin si modelin e tyre kryesor të biznesit, i cili zbatohet në modalitete të ndryshme. Kjo do të thotë që lexuesit duhet në disa rrethana të regjistrohen dhe të paguajnë për përmbajtjen që nuk është ndryshe e disponueshme. Kështu, media krijon **baza të të dhënave parapaguese** për të cilat zbatohen rregulloret për të dhënat personale të përfshira në këto baza të të dhënave. Pavarësisht nga modaliteti, abonimi do të thotë se ekziston një marrëdhënie kontraktuale midis medias dhe lexuesve - abonuesve. Të dhënat e kërkuara për ekzekutimin e kësaj kontrate me pajtimtarin do të konsiderohen përgjithësisht të dhëna personale të tij, ndërsa baza ligjore për përpunimin e tyre do të jetë ekzekutimi i kontratës. Nëse të dhënat do të përdoren për qëllime të tjera, është e nevojshme të përcaktohet nëse për këtë qëllim të dytë duhet kërkuar pëlqimi i duhur, për shembull për të kryer sondazhe të ndryshme.

- Një nga mënyrat e komunikimit me lexuesit ekzistues dhe ata potencialë mund të jetë përmes **reklamimit të drejtpërdrejtë,** i cili, në vend të publikut të gjerë, e drejton mesazhin promovues drejtpërdrejt tek individi – me email, postë konvencionale, SMS, thirrje telefonike, etj. Baza ligjore është një çështje kryesore për operatorët që përdorin marketing të drejtpërdrejtë, dhe pëlqimi ose interesi i ligjshëm janë më së shpeshti në lojë. Bazuar në praktikën aktuale, duket se pikëpamja mbizotëruese është që dërgimi i mesazheve me reklama reklamuese për të fituar përdorues të rinj është i mundur vetëm nëse përdoruesit kanë rënë dakord të marrin mesazhe të tilla. Sidoqoftë, nëse mesazhet promovuese u

dërgohen përdoruesve ekzistues dhe përmbajtja e mesazhit është e rëndësishme për marrëdhëniet që janë vendosur tashmë me ta, atëherë është e mundur të përdoren kontaktet e përdoruesve për këtë lloj komunikimi dhe në bazë të interesit legjitim. Praktika e krijuar për komunikimin me email është që në secilin mesazh ka një lidhje në një faqe ku përdoruesi mund të tërheqë pëlqimin e tij (*unsubscribe link*).

- Rëndësia e të kuptuarit të rregullave për mbrojtjen e të dhënave personale del në pah në situatat kur gazetarët përdorin **baza të mëdha të të dhënave** në punën e tyre, gjegjësisht të dhëna nga bazat e të dhënave në dispozicion të publikut. Ligji gjithashtu mbron të dhëna të tilla personale dhe është e rëndësishme të kuptohen detyrimet dhe masat që gazetarët duhet të marrin kur trajtojnë bazat e të dhënave publike dhe të mëdha. Sasia e madhe e informacioneve në bazat e të dhënave të mëdha paraqet një sfidë serioze për gazetarët në dallimin e të dhënave të nevojshme për hulumtime dhe të gjithë të tjerëve. Të dhënat e parëndësishme të personave që janë subjekt i hulumtimit ose të dhënat e personave që nuk janë përfshirë në hulumtim nuk do të sigurojnë një bazë ligjore për përpunimin. Të dhënat e tilla duhet të trajtohen me kujdes dhe nuk duhet të përdoren, të ndahen, të lihen të pambrojtura etj. Gjithashtu, është e rëndësishme të kujtojmë se përjashtimi gazetaresk mbulon vetëm të dhënat që janë pjesë e një detyre specifike gazetareske. Pas publikimit, të dhënat e papërpunuara fshihen ose anonimohen. Përpunimi i mëtejshëm, siç është arkivimi, kërkon një bazë të veçantë ligjore.
- Në parim, mbi të dhënat e **punonjësve në media** zbatohen të njëjtat rregulla si për çdo kategori tjetër të personave.

Hyrje në OSINT

Puna e inteligjencës me burim të hapur, OSINT është akronim për "Open Source Intelligence" e cila përcaktohet si "kërkimi, mbledhja, analizimi dhe përdorimi i të dhënave publike dhe të hapura". Përveç gazetarëve hulumtues, teknikat OSINT përdoren gjithashtu nga shërbimet e inteligjencës, agjencitë private detektive, hakerat, analistët e biznesit, si dhe analistët në operacionet paqeruajtëse të Kombeve të Bashkuara.

Në epokën para digjitalizimit, burimet e të dhënave në dispozicion të publikut ishin kryesisht media tradicionale, arkivat dhe regjistrat publik të institucioneve shtetërore. Sot ne jetojmë në një botë të mbingopur me informacion të digjitalizuar, në të cilën vazhdimisht krijohen, transmetohen dhe ruhen sasi të mëdha të të dhënave. Ka gjithnjë e më shumë dosje personale, të njerëzve të tjerë, të përvetësuara, të humbura, të rrjedhura dhe të harruara të llojeve, përmbajtjeve, madhësive, qëllimeve dhe aplikime të ndryshme. Kështu, për çdo njohuri serioze, analizë dhe kuptim të informacionit, navigimi është bërë një aftësi thelbësore për mbijetesë në hapësirene njësheve dhe zerove.

Pavarësisht nëse qëllimi është që të arrijmë te burimi i një problemi, të zbulojmë abuzimin e pushtetit ose të gjejmë kuptim në një hetim, OSINT është një proces domethënës në punën e çdo gazetari, studiuesi, aktivisti, sinjalizuesi ose qytetari të interesuar që dëshiron të arrijë në mënyrë individuale deri te informacione të rëndësishme.

Çështje etike

Mbledhja dhe përdorimi i të dhënave ngre gjithmonë çështje të ndryshme ligjore dhe etike. Çfarë të bëjmë me zbulimet aksidentale që mund të dëmtojnë dëshmitarët? A është proporcionale publikimi i informacionit, a përfiton vërtet interesi publik? Pavarësisht nëse vetëm të dhënat e disponueshme nga burimet e hapura janë qasur në mënyrë të ligjshme, shpesh janë të diskutueshme situatat në "zonën gri":

- përdorimi i llogarive të rreme në rrjetet sociale shpesh është shkelje e rregullave të tyre, por ato përdoren për të mbrojtur privatësinë;
- përdorimi i të dhënave "të rrjedhura" që janë vjedhur në një moment;
- kërkimi i avancuar lejon qasje në sisteme ose pajisje të pambrojtura me një kod fabrike të qasjes i cili nuk është teknikisht i paautorizuar, por nuk është i autorizuar.

Aksesi në sasi të mëdha të të dhënave gjithashtu sjell edhe përgjegjësi të madhe. Teknikat e kërkimit mund të përmirësojnë punën hulumtuese, por gjithashtu mund të çojnë në abuzim dhe rrezikojnë privatësinë e dikujt tjetër. Prandaj është e rëndësishme të kuptohet konteksti me të cilin lidhen të dhënat dhe të udhëhiqet nga parimet themelore të etikës gazetareske.

Përgatitja dhe siguria

Para përdorimit të shumicës së mjeteve dhe teknikave OSINT, është e nevojshme të merren disa masa sigurie dhe të përgatitet sistemi

për funksionim. Hulumtimi i burimeve të hapur përfshin shumë më tepër aktivitete se zakonisht. Përveç lënies së një gjurme digjitale dhe gjurmëve personale me lundrim intensiv në internet, hapja e llojeve të ndryshme të dosjeve dhe dokumenteve me origjinë të panjohur mbart rrezikun e infektimit të sistemit me malware që mund të shkaktojë pasoja katastrofike. Kjo vlen njësoj si për incidentet aksidentale ashtu edhe për rastet shumë të shpeshta të shënjestrimit të qëllimshëm të gazetarëve hulumtues.

Ndarja

Një nga masat më të rëndësishme është ndarja, gjegjësisht ndarjen e sistemit të kërkimit nga sistemi privat për përdorim personal. Kjo kryesisht i referohet përdorimit të një kompjuteri të veçantë për aktivitetet kërkimore nga i cili do të eksportohen vetëm gjetjet përkatëse në kompjuterë ose sisteme të tjerë brenda organizatës. Nëse kompjuteri është i infektuar, sistemi formatohet dhe riinstalohet për të minimizuar dëmtimin.

Në rast se nuk ka burime materiale për një zgjidhje të tillë, ndarja e softuerit mund të kryhet edhe në dy mënyra të tjera:

1. Duke vendosur "virtualizim" - instalimi i një sistemi të veçantë operativ në një mjedis të ndarë nga sistemi operativ bazë. Një softuer i njohur falas për virtualizim me burim të hapur është VirtualBox.

2. Me përdorimin e një sistemi operativ që funksionon nga memoria e jashtme (flash USB, kartë SD, etj.) dhe punon në mënyrë të pavarur nga baza. Një shembull i një sistemi të tillë është Tails.

Përveç ndarjes së sistemeve të punës, ndarja në punën kërkimore përfshin edhe hapjen e adresave të postës elektronike të dedikuara për regjistrim në shërbimet e nevojshme dhe regjistrimin e mundshëm të pseudo-llogarive në rrjetet sociale të cilët në asnjë mënyrë nuk mund të lidhen me ato private. Aktualisht për postë elektronike rekomandohen shërbimet ProtonMail dhe Tutanota, dhe një shërbim interesant për gjenerimin e imazheve të profilit të njerëzve jo-ekzistues është thispersondoesnotexist.com. Gjithashtu, në disa raste, do të kërkohet një kartë SIM e paregjistruar e parapaguar.

Anonimiteti

Në shumicën e rasteve, kërkimi i avancuar përmes motorit të kërkimit është falas. Sidoqoftë, qasja në adresa dhe dokumente të caktuara mund të jetë e paligjshme ose e dyshimtë. I gjithë trafiku i internetit dhe pyetjet e kërkimit regjistrohen nga motorët e kërkimit, ofruesit e internetit, madje edhe agjencitë e inteligjencës, dhe më pas ruhen për një periudhë të pacaktuar kohe. Ky informacion mund të lidhet me një identitet dhe më vonë të përdoret kundër personit që ka hyrë në përmbajtjen në fjalë.

TOR

Një nga mënyrat më të sigurta për të maskuar trafikun në internet dhe për të mbrojtur identitetin tuaj gjatë një kërkimi në internet është shërbimi për komunikimit anonim Tor. Ndryshe nga programet e njohura si Firefox dhe Chrome, Tor dërgon të gjithë trafikun përmes një rrjeti vullnetar prej mijëra pikash, duke e bërë vendndodhjen të paarritshme për këdo që monitoron rrjetin ose kontrollon trafikun. Tor kripton të dhënat origjinale, përfshirë adresën IP dhe i dërgon ato

përmes një qarku virtual që përfshin fazat Tor të njëpasnjëshme, të zgjedhura rastësisht.

Përdorimi i Tor është bërë më i thjeshtë me kalimin e kohës, por në të njëjtën kohë disa shërbime kanë filluar të kërkojnë konfirmimin e CAPTCHA për shkak të sasisë së madhe të kërkimeve të automatizuara, të cilat ndonjëherë mund të komplikojnë dhe ngadalësojnë proceset. Gjithashtu, disa nga vendet shënojnë përdorimin e shfletuesve Tor si një aktivitet të dyshimtë, i cili nuk parandalon anonimizimin e trafikut, por edhe përcaktimin e faktit që faqet dhe kërkimet arrihen përmes rrjetit Tor.

VPN

Nëse për ndonjë arsye nuk është e mundur të përdorni Tor, një mundësi alternative por edhe më pak e sigurt është përdorimi i shërbimit VPN (Rrjeti Virtual Privat). Rrjetet private virtuale maskojnë adresën IP të përdoruesit në një adresë tjetër IP në pronësi të ofruesit të VPN. Problemi më i madh me këto shërbime është transparenca, sepse ato janë kryesisht kompani private që mund të pretendojnë të ruajnë identitetin e përdoruesve, por është shumë e vështirë të provohet.

Teknikat dhe mjetet

Dorking dhe operatorët (kërkim i avancuar)

Gjatë një kërkimi, shpesh ka nevojë për të mbledhur sa më shumë informacion mbi një temë të caktuar. Teknikat e avancuara të kërkimit në Internet mund të ndihmojnë në gjetjen e dosjeve ose gjurmë të dhënash të rëndësishme për pyetjet për të cilat kërkohet përgjigjja. Për shembull, këto mund të jenë raporte tatimore ose

vlerësime kosto dhe buxhete të qeverive lokale, informacion që nuk është i dukshëm në faqet / prezantimet e tyre, ose nuk shfaqet si rezultat i një kërkimi të thjeshtë në internet.

Për më tepër, i njohur gjithashtu si "Google hacking", Google Dorking është një teknikë e përcaktuar në vitin 2002, dhe përdoret nga redaksitë, organizatat kërkimore, auditorët e sigurisë dhe kriminelët e njohur me teknologji (kriminelët kibernetikë) duke dërguar pyetje në motorët e kërkimit për të gjetur informacione të pazbuluara ose dobësi të sigurisë dhe dobësitë e sistemit. Kjo teknikë mund të përdoret në shumicën e motorëve të kërkimit, kështu që sot ne e quajmë atë thjesht "dorking".

Dorking praktikisht nënkupton përdorimin e potencialit të plotë të motorëve të kërkimit në mënyrë që të zbuloni rezultate që nuk janë të dukshme me një kërkim normal. Kjo mundëson që me një kërkim më të imët të futet më thellë në faqet e internetit dhe dokumentet e disponueshme në internet. Kjo nuk kërkon pajisje të sofistikuar, softuer ose njohuri të veçanta teknike, por bie në kuptimin e disa fjalëve kyçe / parametrave dhe simboleve të përdorura si "operatorë" dhe "filtra" për rezultate më të sakta të kërkimit. Megjithatë, efikasiteti ndonjëherë kërkon pak këmbëngulje, kreativitet, durim dhe fat.

Kërkimi i zakonshëm në internet mbështetet në një mënyrë semantike të kërkimit të informacionit, gjegjësisht, duke futur një pyetje të drejtpërdrejtë ("Sa është buxheti i Malit të Zi?") ose duke zgjedhur fjalët kyçe ("Buxheti Mali i Zi"). Nga ana tjetër, një kërkim i avancuar do të specifikojë atë pyetje duke kombinuar elemente teknikë dhe semantikë për të përfituar nga fakti që përmbajtja në internet lexohet dhe indeksohet vazhdimisht me makinë. Elementet teknike që janë në shërbim të filtrave shtesë në këtë teknikë quhen "operatorë".

Operatorë	Shembull	Përshkrim
site:	autostrada mateshevë site:vijesti.me	Paraqet të gjitha faqet në të cilat përmenden fjalët e dhëna në kuadër të faqes së përcaktuar (vijesti.me)
filetype:	filetype:pdf site:mif.gov.me	Kërkimi i llojeve specifike të dosjeve. Shembulli tregon të gjitha dokumentet pdf të indeksuara në faqen e internetit të Ministrisë së Finansave.
OR	site:gov.me buxheti filetype:xls OR filetype:pdf	Zgjëron kërkimin në rezultate që kanë një ose më shumë pyetje. Shembulli tregon të gjitha dokumentet Excel dhe pdf mbi domenin dhe nënfushat e qeverisë së Malit të Zi.
AND	site:gov.me buxheti AND 2020 filetype:xls OR filetype:pdf	Ngushton kërkimin duke paraqitur vetëm rezultate që kanë të dy (ose më shumë) fjalë kyçe të përcaktuara nga kërkesa. Shembulli përjashton dokumentat e buxhetit para vitit 2020.
cache:	cache:niksic.me	Paraqet verzionin më të fundit të ruajtur (të memorizuar) të faqes së internetit nga shfletuesi.
“ ”	“Gazeta zyrtare MZ br.21/09 i 40/11”	Kërkimi i një pyetjeje saktësisht të përcaktuar midis citateve përjashton kombinime të tjera të termeve të dhënë.
-	buxheti malit të zi -ligji	Shenja minus përjashton rezultate të cilat përmbajnë një tjetër (ose më shumë) fjalë specifike.

Meta të dhënat, imazhe dhe vendndodhje

Të gjitha dosjet digjitale, dokumentet, fotot, muzika, postat elektronike dhe dosjet e tjerë, përveç përmbajtjes së tyre themelore, kanë edhe meta të dhënat e tyre, pra "të dhënat mbi të dhënat". Në rastin e dokumenteve tekstuale, këto janë, për shembull, koha e krijimit dhe ndryshimet e fundit, madhësia e saj, pastaj pronësia, gjegjësisht autori që ka bërë dokumentin etj. Fotografitë origjinale shpesh mbajnë me vete informacione në lidhje me vendin ku janë bërë, kështu që meta të dhënat nganjëherë japin informacione thelbësore për vërtetimin e fakteve dhe zbulimin e detajeve gjatë hulumtimit.

Sidoqoftë, me postimin e fotove në rrjetet sociale fshihen shumicën e meta të dhënave, kështu që për të kontrolluar burimin, vërtetësinë ose informacionin shtesë duhen provuar teknikat si kërkimi i kundërt i fotove. Të gjithë shfletuesit më të mëdhenj e kanë këtë mundësi dhe mjafton të kopjoni adresën e fotos në internet ose ta ngarkoni nga një kompjuter. Google aktualisht ka numrin më të madh të opsioneve për analizë, Yandex shpesh është më i mirë në njohjen e vendndodhjeve, dhe ndonjëherë ia vlen të provohen edhe shërbime të tjera si Bing ose TinEye.

Për kontrollimin dhe përcaktimin e vendndodhjes, përdoret një kombinim i hartave, imazheve rrugore dhe satelitore dhe përveç shërbimit të njohur Google Maps, i cili ofron një numër opsionesh dhe disa shtresa shikimesh, ekzistojnë edhe disa mjete të tjera që mund të jenë të dobishme në raste specifike. Aplikacioni desktop i shërbimit Google Earth ofron një pasqyrë të imazheve satelitore me kalimin e kohës, kurse shërbimi DualMaps lehtëson lundrimin hapësinor duke shfaqur një hartë, imazhe satelitore dhe perspektivë rruge të një vendi të caktuar njëkohësisht. Gjithashtu, shërbimi

vullnetar OpenStreetmap përmban shumë informacione të futur nga vetë qytetarët, në të cilët kompanitë shpesh nuk kanë akses, gjë që i bën ata një faktor të rëndësishëm në diversifikimin e të dhënave të mbledhura.

Historia e internetit dhe arkivimi

Ka dy arsye pse arkivimi i internetit është thelbësor për gazetarët dhe studiuesit:

1. Kur një kërkim çon në lidhje që nuk funksionojnë, faqe që janë ndryshuar ose prezentim të tërë të faqes që nuk ekzistojnë më.
2. Kur një kërkim çon në faqe ose informacione që janë të vlefshme, por mund të bëhen të paarritshme për arsye të ndryshme.

Në rastin e parë, do të ishte ideale të kthehen pas në kohë dhe të shkarkohet një kopje të faqes përpara se t'i ndodhte diçka. Në rastin tjetër do të ishte mençur të arkivohen me kohë dhe të parandalohet një skenar i tillë.

Një nga përpjekjet më mbresëlënëse kulturore të shoqërisë moderne është Internet Archive, biblioteka më e madhe në internet me përmbajtje multimediale. Shërbimi i saj Wayback Machine funksionon si një kapsulë digjitale e kohës dhe ofron pikërisht atë - qasje në një numër të madh faqesh me kalimin e kohës dhe arkivimin e përmbajtjes aktualisht të disponueshme për përdorim në të ardhmen.

Me ndihmën e proceseve të automatizuara, Wayback Machine mund të hyjë dhe arkivojë praktikisht çdo faqe në internet. Sidoqoftë, nuk ka modele të përcaktuara me të cilat algoritmi vendos se cilat adresa të vizitohen dhe sa shpesh për shkak të burimeve të kufizuara dhe faktorëve të tjerë që ndikojnë në të. Prandaj, nuk është gjithmonë e mundur të gjindet një version i arkivuar i një përmbajtjeje specifike të një date të caktuar, por pavarësisht, arkivi ka një sasi të madhe të të dhënave që shpesh janë një burim i domosdoshëm për kërkime. Përveç qasjes së lehtë në arkiva, ky shërbim ju lejon gjithashtu të ruani manualisht faqe specifike në një kohë të caktuar në të cilat mund të hyjnë edhe të tjerët pastaj. Ky proces është i rëndësishëm sepse shton një element të neutralitetit dhe besimit kur u referoheni burimeve të informacionit krahasuar me faqet dhe kopjet e dokumenteve të ruajtura në pajisjet personale.

Tenikat dhe burimet tjera

OSINT përfshin shumë më tepër teknika dhe mjete që mund të jenë të dobishme për lloje të ndryshme kërkimesh. Informacioni në lidhje me individë, kompani, organizata, projekte, ngjarje të rëndësishme lokale dhe globale është i kudondodhur, dhe përveç internetit të njohur "sipërfaqësor", është e mundur të kërkohet për të shumë më thellë, në shtrirjet më të largëta dhe të errëta të sferës digjitale. Për hulumtime të mëtejshme të këtyre teknikave dhe mjeteve, rekomandojmë udhëzimet Exposing the Invisible Kit dhe Open Source Intelligence – Navigator për gazetarët hulumtues, në shkrimet e të cilave morën pjesë edhe autorët e këtij manuali.


i
t
v
A


m
e
l
d
w