UDHËZUES PËR SIGURINË DIXHITALE

Albanian Media Institute
Instituti Shqiptar i Medias

UDHËZUES
PËR
SIGURINË DIXHITALE

Kejsi Bozo dhe Kristina Lani

Instituti Shqiptar i Medias, 2025

Përmbajtje

Hyrje

Në një botë gjithnjë e më të ndërlidhur dixhitalisht, ku kufiri mes jetës personale dhe asaj profesionale po bëhet gjithnjë e më i paqartë, siguria dixhitale nuk është më një luks apo zgjedhje, por një domosdoshmëri. Ky udhëzues është konceptuar si një mjet praktik dhe gjithëpërfshirës, kryesisht për ata që ushtrojnë gazetarinë, por vlen njësoj për këdo që vepron, informon apo angazhohet në hapësirat dixhitale.

Gazetarët, për shkak të natyrës së punës së tyre, e cila përfshin kërkimin, mbledhjen dhe shpërndarjen e informacionit, janë veçanërisht të ekspozuar ndaj rreziqeve dixhitale. Nga ndërhyrjet e paautorizuara në pajisje dhe profile në rrjete sociale, të survejimi i qëllimshëm, nga *phishing*-u deri te ngacmimet sistematike online, kërcënimet janë të shumta dhe shpesh të sofistikuara. Ndaj, mbrojtja e të dhënave personale, ruajtja e sigurisë së pajisjeve, si dhe kuptimi i legjislacionit përkatës nuk janë më thjesht çështje teknike, por aspekte thelbësore të etikës profesionale dhe të drejtës për informim të sigurt.

Ky udhëzues përpiqet të tejkalojë qasjet tradicionale ndaj sigurisë dixhitale. Përveç masave teknike themelore, ai trajton çështje të ndërlikuara rrallë here të prekura më pare si të drejtat e autorit, plagjiatura, dhe ndikimet e inteligjencës artificiale. Përdorimi i mjeteve të duhura, adoptimi i praktikave të sigurta, dhe vetëdijësimi për rreziqet dhe përgjegjësitë në epokën dixhitale janë elementë të pandashëm të gazetarisë së përgjegjshme dhe të qytetarisë kritike.

Në vijim, ky udhëzues synon të jetë një shoqërues praktik dhe një ndihmë konkrete për të gjithë ata që kërkojnë jo vetëm të mbrohen vetë, por edhe të ushtrojnë rolin e tyre në shërbim të së vërtetës në mënyrë të sigurt dhe të ndërgjegjshme.

1. Rëndësia e sigurisë dixhitale në fushën e gazetarisë

Vërehet gjithnjë e më shumë, dhe jo vetëm në gazetari, një thirrje, dëshire apo dhe vrull për të trajtuar çështje në lidhje me sigurinë dixhitale. Patjetër që dhe me pare siguria dixhitale ka qene me rëndësi, por specifikisht që nga infodemia që shoqëroi pandeminë COVID-19 u vu në pah sa vulnerabël është shoqëria, por dhe në veçanti fusha e medias, gazetarisë dhe informacionit me gjerësisht, ndaj disa rreziqeve te cilëve i ekspozohemi me praninë dhe ndërveprimin tone *online*.

1.1 Çfarë është siguria dixhitale?

Siguria dixhitale është aftësia për të mbrojtur veten, të dhënat dhe komunikimet në mjedisin *online*. Kjo përfshin praktikisht çdo aspekt të pranisë dhe ndërveprimit *online*: mbrojtja e llogarive personale dhe profesionale, ruajtja e konfidencialitetit dhe sigurisë në komunikime, ose parandalimi i humbjes apo manipulimit të informacionit, nder shume të tjera.

1.2 Pse është me rëndësi për gazetarët?

Gazetarët janë ndër më të ekspozuarit ndaj disa rreziqeve si:

- Survejimi (nga aktorë shtetërorë ose jo-shtetërorë);
- Sulme kibernetike që mund të sjellin rrjedhje informacioni si për shembull ekspozimin e burimeve;
- Ngacmime online, në veçanti gjatë raportimeve të ndjeshme;
- Manipulime të përmbajtjes dhe informacionit (*deepfake*, montime, sulme me qëllim diskreditimi).

1.3 Llojet më të zakonshme të kërcënimeve dixhitale

Lloji i kërcënimit	**Çfarë është?**	**Shembull për gazetarë**
Phishing	Email-e apo mesazhe mashtruese për të vjedhur të dhëna të ndjeshme si fjalëkalimet	Email i rremë që duket si nga redaksia
Spyware	Program që përgjon aktivitetet në pajisje	Instalohet pa dijeni për të mbikëqyrur komunikimin

Lloji i kërcënimit	**Çfarë është?**	**Shembull për gazetarë**
Ransomware	Bllokon pajisjen dhe kërkon pagesë	Sulm që enkripton skedarët e punës
Doxxing	Publikimi i të dhënave personale pa leje	Emri, adresa, numri i telefonit shpërndahen publikisht
Deepfake	Video ose audio të montuara e të falsifikuara	Shfaqje e gazetares me deklarata që nuk i ka bërë

1.4 Përmbajtja e këtij manuali:

Në kapitujt në vijim, do të trajtohen:

- Mbrojtja e të dhënave personale;
- Siguria e pajisjeve;
- Email-i dhe lundrimi i sigurt në Internet;
- Menaxhimi i të dhënave;
- Ngacmimi dhe bullizmi online;
- Siguria në rrjetet sociale;
- Çështjet etike: Të drejtat e autorit (copyright) dhe plagjiatura;
- Ligjet dixhitale;
- Inteligjenca Artificiale (IA) dhe Siguria Dixhitale.

2. Mbrojtja e të dhënave personale

Qofte në dimensionin personal apo profesional, gazetaret janë veçanërisht të ekspozuar ndaj kërcënimeve të të dhënave personale.

Të dhënat personale janë çdo informacion që mund të identifikoje një individ, pra, emri dhe mbiemri, numri i telefonit/celularit, e-mail-i, ose adresa e banimit, por jo vetëm. Gjithashtu konsiderohen të dhëna personale fjalëkalimet (*password*-et), vendndodhja (*location*), dhe adresa IP (*IP address*).

Zbulimi i të dhënave personale mund të cenoje jo vetëm punën dhe llogarite (*account*-et) online të gazetarit, por gjithashtu mund të shkaktoje sulme dixhitale ose madje dhe fizike kundër gazetarit dhe të afërmeve të tij/saj, si dhe dëmtim të reputacionit profesional.

2.1 Fjalëkalimet

Mënyra kryesore dhe me e thjeshte për të mbrojtur të dhënat personale është krijimi i fjalëkalimeve të forta dhe të sigurta.

Një fjalëkalim i sigurt:

- Ka të paktën 12-16 karaktere;
- Duhet të jetë unik për çdo llogari;
- Përfshin shkronja të mëdha, të vogla, numra dhe simbole;
- Nuk përmban emra ose të dhëna personale të individit të cilat mund të jene të identifikueshme lehtësisht.

Gjithashtu, këshillohet të përdoret një *password manager* si për shembull KeePassXC, i cili është një program që mban të gjitha fjalëkalimet në mënyre të enkriptuar. Nuk këshillohet të shënohen fjalëkalimet në një mjet fizik, siç mund të jete një fletore, sepse ky mjet mund të jete lehtësisht i aksesueshëm nga pale të padëshiruara.

2.2 Two-factor authentication (2FA)

Verifikimi me dy hapa ose siç njihet me gjerë në termin në anglisht, *two-factor authentication*, shton një shtresë të dytë sigurie dhe një forme të dytë vërtetimi përveç fjalëkalimit.

Zakonisht kryhet përmjet një aplikacioni (p.sh. bankat), një numër telefoni (SMS) ose një llogari *back-up* (*recovery email*).

Një metodë tjetër është nëpërmjet përdorimit të një çelësi fizik sigurie (*physical security key*), gjë që ofron këtë shtresë të shtuar sigurie edhe në rast se pajisjet që përdoren për 2FA kompromethohen.

Aplikacione për 2FA:

- Google Authenticator (Android / iOS)
- Authy
- Microsoft Authenticator (Android / iOS)

2.3 Reduktimi i gjurmës dixhitale

Termi **gjurmë dixhitale** i referohet të dhënave që lëmë pas online si pasoje e thjeshte e përdorimit të internetit.

Kontrolloni rregullisht:

- Privatësinë e postimeve në rrjete sociale.
- Kush ka akses në email-in dhe dokumentet tuaja.
- Faqet ku keni krijuar llogari në të kaluarën.

Pastroni rrjetet sociale:

- Fshini postime që përmbajnë të dhëna personale.
- Limitoni çfarë mund të shohin audienca të ndryshme (miqtë/familjarët kundrejt ndjekësve në tërësi).
- Mos publikoni vendndodhjen në kohë reale, veçanërisht nëse puna që po kryeni (p.sh. në terren) është e ndjeshme.

Mashtrimet më të zakonshme për vjedhje të dhënash

- Email i rremë nga “banka”, “gazeta” apo “bashkëpunëtorë” që kërkojnë të klikoni një *link*. Ky është një shembull i *phishing*, koncept që do zhvillojmë me tej në këtë udhëzues.
- Mesazh që thotë se llogaria juaj është bllokuar dhe kërkon të “konfirmoni fjalëkalimin”.
- Thirrje telefonike që kërkon një kod verifikimi.

3. Siguria e pajisjeve

Pajisjet dixhitale të gazetareve, siç janë telefonat celular, kompjuterat dhe tablet-et, ruajnë informacione tejet të ndjeshme që kërkojnë mbrojtje maksimale. Kompromet imi i një pajisjeje mund të sjelle pasoja katastrofike jo vetëm për punën gazetareske, por gjithashtu për sigurinë personale të gazetarit dhe të burimeve të tij.

Pajisjet e gazetareve mund të përmbajnë:

- Dokumente konfidenciale dhe materiale investigative;
- Kontakte të burimeve dhe informatorëve;
- Foto, video dhe materiale të ndjeshme;
- Biseda komunikimi me kolege apo informatorë;
- Të dhëna financiare dhe personale.

Për rrjedhojë, nëse pajisja kompromet ohet, pasojat mund të jene ligjore, reputacionale dhe personale, me potencial për dem madje fizik.

3.1 Bazat e sigurisë për çdo pajisje

Mbrojtja e pajisjeve fillon me masa të thjeshta por kritike që duhet të zbatohen në çdo telefon, kompjuter ose tablet.

Një pajisje e sigurt:

- Ka të aktivizuar bllokimin e ekranit me PIN kompleks, fjalëkalim të gjate, ose në mënyre biometrike (gjurmë gishti/njohje fytyre).
- Është e përditësuar rregullisht, si sistemi operativ ashtu dhe aplikacionet.
- Ka të instaluara aplikacione vetëm nga burime zyrtare (App Store/Google Play).
- Sigurohuni që prejardhja e aplikacioneve të jete zhvilluesi zyrtar i aplikacionit në fjalë. Për shembull, nëse doni të instaloni Microsoft Word në pajisjen tuaj, shkarkoni opsionin që ka si *developer* Microsoft Corporation.
- Nuk përdoret nga persona të tjerë pa mbikëqyrje të plotë.
- Nuk duhet të këtë fjalëkalime të ruajtura në "Notepad" apo “Notes” ose dokumente të pambrojtura.

Gjithashtu, këshillohet të përdoret një menaxher fjalëkalimesh i enkriptuar për ruajtjen e sigurt të të gjitha kredencialeve.

3.2 Mbrojtja nga vjedhjet dhe humbjet

Humbja ose vjedhja e një pajisjeje mund të hapë rrugë për:

- Akses të paautorizuar në email, rrjete sociale apo llogari bankare;
- Ekspozim të informacionit të burimeve;
- Instalim të *software*-it me qellim spiunimi (*spyware*);
- Përfaqësim të rremë në emër të gazetarit,

Veprimet që duhen ndërmarrë:

- Aktivizoni funksionin "Find My Device" ose "Find My iPhone".
- Enkriptoni diskun e plotë të kompjuterit ose telefonit.
- Përdorni kabëll apo pajisje fizike për mbyllje (*laptop lock*) në ambiente publike.
- Vendosni opsionin për fshirje të plote të pajisjes (*remote wipe*) në rast humbjeje apo vjedhjeje.
- Bëni *backup*-e të rregullta të të dhënave të rëndësishme.

3.3 Mbrojtja nga *spyware* dhe *keyloggers*

Spyware është një program që instalohet fshehurazi dhe ndjek çdo veprim që bën në pajisjen tuaj. Për gazetaret, ky lloj *software*-i mund të kompromet oje tërësisht punën investigative.

Keyloggers janë një lloj i veçantë *spyware*-i që regjistron çdo tast që shtypet, duke përfshirë fjalëkalime dhe informacione të ndjeshme.

Shenjat e mundshme të një infektimi:

- Pajisja punon me ngadalë se zakonisht;
- Bateria shkarkohet shpejt;
- Aplikacione të panjohura në sistem;

- Trafik interneti i papritur;
- Mesazhe apo email-e të dërguar pa dijeninë tuaj.

Si të mbroheni:

- Mos klikoni në *link*-e të dyshimta nga email-e apo mesazhe.
- Mos hapni file të panjohura në USB që nuk janë të juajat.
- Shmangni lidhjen me Wi-Fi falas pa VPN.
- Instaloni vetëm aplikacione nga burime të besueshme.
- Përdorni antivirus të përditësuar.

3.4 Përdorimi i sigurt i pajisjeve në terren

Gazetaret që raportojnë nga protesta, zona të ndjeshme apo kryejnë pune investigative përballen me rreziqe të veçanta dhe duhet të zbatojnë masa shtese sigurie.

Rreziqet specifike në terren:

- Konfiskimi i pajisjeve nga autoritetet;
- Instalimi i forcuar i *spyware;*
- Gjurmimi i vendndodhjes në kohë reale;
- Aksesi fizik në pajisje gjate ndalimeve.

Strategji mbrojtjeje:

- Përdorni telefon rezervë për kontakte të ndjeshme.
- Fikni pajisjet gjate udhëtimit në zona të pasigurta.
- Përdorni aplikacione për fshirje të menjëhershme të të dhënave në rast rreziku.
- Aktivizoni enkriptimin automatik të të gjitha të dhënave.
- Krijoni pseudonime dhe identitete të veçanta për punë të ndryshme.
- Ruani backup-et në vende të sigurta, jo në pajisje.

3.5 Mashtrimet më të zakonshme qe synojnë pajisjet

Sulmuesit përdorin metoda të ndryshme për të aksesuar pajisjet e gazetareve. Disa shembuj janë:

- **Email-e të rreme** qe duket sikur dërgohen nga shërbime të njohura (Google, Apple) dhe kërkojnë të "verifikoni llogarinë";
- **USB të infektuar** qe instalojnë automatikisht *malware* kur lidhen me kompjuter;
- **Rrjet Wi-Fi i rreme** qe duplikon rrjete të njohura me qellim “kapjen” e të dhënave të ndjeshme;
- **Aplikacione false** qe imitojnë ato origjinale në App Store ose Google Play;
- **Thirrje telefonike** qe pretendojnë të jene nga mbështetja teknike dhe kërkojnë akses në pajisje.

Një term i veçantë qe shpesh shfaqet në kontekstin e sigurisë dixhitale është ***social engineering***. *Social engineering* i referohet përdorimit të ndikimit psikologjik për të manipuluar dike qe të beje gabime sigurie ose të japë informacione të ndjeshme. Kjo mund të kryhet nëpërmjet telefonit, email-it, ose madje dhe takimeve fizike.

Si mund të dalloni një tentative mashtrimi? Disa shenja paralajmërimi:

- Kërkesa urgjente për informacione të ndjeshme;
- Presion psikologjik ("llogaria do të mbyllet");
- Kërkesa për aksesim të pajisjes nga larg (*remote control*);
- Komunikim nga adresa email të dyshimta.

4. Email-i dhe lundrimi i sigurt në Internet

Email-i dhe shfletimi i internetit janë ndër mjetet më të përdorura në punën e gazetarëve, por gjithashtu, pikërisht sepse janë pjese e rutinës së përditshme, kthehen ndër mjetet më të rrezikshme. Një klikim, një email qe hapni apo një faqe ueb qe vizitoni mund të hapë rrugë për sulme dixhitale që kompromet ojnë të dhënat personale, identitetin profesional dhe sigurinë e burimeve.

Gazetarët janë synim i veçantë për sulme përmes email-it dhe internetit sepse:

- Punojnë me informacione të ndjeshme;
- Komunikojnë me burime të ndryshme;
- Shpesh duhet të aksesojnë materiale nga burime të panjohura;
- Përdorin rrjete publike për punë në terren.

Rreziqet kryesore përfshijnë:

- **Sulme *phishing* -** mashtrime që nxisin të japësh të dhëna personale;
- **Shkarkime të rrezikshme -** viruse dhe *malware*;
- **Gjurmim *online* -** monitorim përmes *cookies* ose adresës IP;
- **Faqe të rreme** që imitojnë portale dhe faqe ueb serioze;
- **Kompromet im të llogarive** e-mail dhe sociale.

4.1 Zbulimi i email-eve mashtruese (*phishing*)

Phishing është një teknikë sulmi kibernetik ku sulmuesit dërgojnë email-e që duken legjitime për të vjedhur informacione të ndjeshme si fjalëkalime, të dhëna bankare ose të dhëna personale.

Shembuj të zakonshëm ndaj gazetarëve:

- Email nga "redaksia" që kërkon verifikim të llogarisë;
- Mesazh nga "bashkëpunëtorë" me *link*-e qe çojnë në dokumente të rëndësishme;
- Njoftim nga "shërbime teknike" për problem e sigurie;
- Ftesë për interviste ose një event me *file* të bashkëngjitur të dyshimtë.

Si mund të dalloni një email mashtrues?

- **Adresa e dërguesit -** kontrolloni me kujdes, shpesh ka gabime të vogla, si për shembull germa qe mund të ngatërrohen ose adresa email-i të panjohura ose qe duken të çuditshme;
- **Përmbajtje urgjente -** "Vepro tani!", "Llogaria do të mbyllet!", "Emergjencë sigurie";
- **Kërkesë për të dhëna -** asnjë shërbim legjitim dhe serioz nuk kërkon fjalëkalime përmes email-it;
- ***Link*-e të dyshimta -** URL që nuk përputhen me organizatën që pretendojnë të përfaqësojnë;
- **Gabime gjuhësore -** drejtshkrim i dobët ose përdorim i çuditshëm i gjuhës.

Një teknikë e zakonshme është ***spoofing* -** kur sulmuesit falsifikojnë adresën e dërguesit për t'u shtirur sikur email-i vjen nga një burim i besueshëm.

Çfarë mund të bëni nëse keni dyshime:

- Mos klikoni *link*-e brenda email-it pa verifikuar burimin.
- Kontrolloni adresën e dërguesit – shihni përtej emrit qe ju del në ekran dhe kontrolloni adresën email.
- Verifikoni – kontaktoni personin ose organizatën nëse dyshoni
- Raportoni email-in si spam ose fshijeni menjëherë.
- Skanoni *file*-et e bashkëngjitura me antivirus para se t'i hapni.

4.2 Përdorimi i sigurt i email-it

Është thelbësore qe gazetaret të përdorin shërbime email-i që ofrojnë enkriptim dhe mbrojtje të avancuar kundër sulmeve.

Shërbimet e këshilluara:

- **Proton Mail** - email i enkriptuar me mbrojtje ndaj *phishing*
- **Tuta** (Tutanota më parë) – email i sigurt me enkriptim *end-to-end*

- **Signal** - për komunikim të shpejte (*instant* messaging) të enkriptuar, por ofron mundësinë për të shkëmbyer *file* si dhe opsionin për mesazhe qe zhduken. mesazhe të shkurtra të enkriptuara

Disa këshilla:

- Përdorni adresa të ndryshme për punën dhe për jetën personale.
- Mos iu përgjigjni email-eve nga burime të panjohura.
- Përdorni firma (*signatures*) profesionale për të konfirmuar identitetin.
- Bëni backup të rregullt të email-eve të rëndësishëm.
- Aktivizoni verifikimin me dy hapa (2FA) për llogarinë tuaj të email-it.

4.3 Lundrimi i sigurt në internet

Shfletimi i pasigurt mund të çojë në infeksione të pajisjes me *malware*, gjurmim të aktiviteteve dhe ekspozim të të dhënave personale.

Si mund të dalloni një faqe të pasigurt?

- URL (*link*-u në vetvete) nuk fillon me "http**s**://" ;
- *Browser*-i qe përdorni për lundrim ju paralajmëron për certifikata të dyshimta;
- *Pop-up* të shumta me reklama;
- Kërkesa për shkarkime të pakërkuara;
- Faqe ueb që kërkojnë informacione personale pa arsye.

Një term i rëndësishëm është ***man-in-the-middle attack*** - kur dikush ndërhyn në komunikimin midis jush dhe një faqeje ueb për të vjedhur informacione.

Mbrojtja gjatë lundrimit:

- Përdorni *browser* të sigurt si Mozilla Firefox, Brave ose Tor Browser.
- Instaloni shtesa mbrojtëse (*extensions*) si uBlock Origin, Privacy Badger ose Ghostery.
- Kontrolloni certifikatat - kërkoni ikonën e drynit në adresën URL.

- Përdorni VPN gjithmonë në rrjete publike.
- Përditësoni rregullisht *browser*-in dhe *extensions*.

4.4 VPN dhe mbrojtja e privatësisë

VPN (*Virtual Private Network*) krijon një tunel të enkriptuar midis pajisjes tuaj dhe internetit, duke fshehur kështu aktivitetin dhe vendndodhjen.

Rrjetet publike përbëjnë rrezik për gazetaret:

- **Sulmues** që monitorojnë trafikun e rrjetit;
- **Faqe të rreme** që imitojnë rrjete të njohura;
- **"Kapje" e kredencialeve** të llogarive të ndjeshme;
- **Gjurmim i vendndodhjes** në kohë reale.

VPN të rekomanduara:

- **Proton VPN** - version falas i disponueshëm, por në përgjithësi duhet patur parasysh qe duhet paguar për një VPN sa më të plotë.
- **Mullvad** - nuk kërkon të dhëna personale për regjistrim.
- **Windscribe** - mbrojtje e mirë me çmim të arsyeshëm.
- **Tor** - për anonimitet maksimal (më i ngadaltë), përbën një lloj të veçantë VPN-je i cili mund të aksesojë pjesë të internetit jo lehtësisht të aksesueshme (*deep web* dhe *dark web*).

4.5 *Cookies* dhe gjurmimi *online*

Cookies janë *file* të vegjël që faqet përdorin për të ruajtur në pajisjen tuaj preferencat tuaja në faqe ueb specifike, por shpesh përdoren për gjurmim dhe reklamë të shenjëstruar (*targeted advertising*).

Tracking cookies janë lloj i veçantë *cookies* që gjurmojnë lëvizjet tuaja nëpër faqe të ndryshme, duke krijuar një profil të detajuar të sjelljes tuaj *online*.

Si mund t'i dëmtojnë gazetarët?

- Ndërtim profili pa dijeninë tuaj;
- Ekspozim i interesave dhe burimeve të informacionit;
- Reklama të shenjëstruara që mund të zbulojnë projekte investigative;
- Mundësi për gjurmim nga organizata të dyshimta.

Mbrojtja nga gjurmimi:

- Përdorni "Private/Incognito Mode" për kërkime të ndjeshme.
- Bllokoni *cookies* me *extensions* si Privacy Badger.
- Pastroni rregullisht historikun dhe *cookies*.
- Mos pranoni të gjitha *cookies* - refuzoni ato jo të nevojshme.
- Përdorni *browser* të ndryshëm për punë dhe përdorim personal.

4.6 Rreziqet nga shkarkimet dhe bashkëngjitjet

Shkarkimet nga burime të pasigurta janë një nga mënyrat më të zakonshme të infektimit me *malware*.

Lloje të zakonshme sulmesh:

- *File* PDF të infektuar që instalojnë *spyware* kur hapen;
- Aplikacione të rreme që imitojnë ato origjinale;
- Foto dhe video që përmbajnë kod të fshehur;
- Arkiva ZIP/RAR me përmbajtje të rrezikshme.

Si të dalloni një shkarkim të dyshimtë?

- Bashkëngjitje nga dërgues të panjohur;
- *File* të llojeve jo të zakonshme (.exe, .scr, .bat);
- Shkarkime automatike pa kërkesën tuaj;
- *File* që pretendojnë të jenë diçka tjetër.

Masa mbrojtëse:

- Skanoni çdo *file* me antivirus para se ta hapni.

- Përdorni VirusTotal.com për të kontrolluar *file* të dyshimta.

- Hapni file të rrezikshme në *sandbox* ose *virtual machine*.
- Mbani backup të rregullt në rast infeksioni.

4.7 Mashtrime më të sofistikuara

Sulmuesit vazhdimisht zhvillojnë **teknika të reja për të mashtruar**, si:

- *Spear phishing* - sulme të shenjëstruara që përdorin informacione personale.
- *Watering hole attacks* - infektim i faqeve që vizitohen shpesh.
- *Business Email Compromise* - mashtrimi i kolegëve për të kryer veprime të rrezikshme.

5. Menaxhimi i të dhënave

Menaxhimi i sigurt i të dhënave është një nga pikat më kritike të sigurisë dixhitale për gazetarët. Të dhënat që ruhen dhe përdoren në punë përfshijnë dokumente konfidenciale, kontakte burimesh, materiale investigative dhe informacione të ndjeshme që kërkojnë mbrojtje maksimale.

Gazetarët punojnë me informacione që mund të jenë thelbësore jo vetëm për karrierën e tyre, por edhe për sigurinë e burimeve dhe integritetin e proceseve demokratike.

Humbja, vjedhja ose ekspozimi i këtyre të dhënave mund të ketë pasoja të renda.

Të dhënat kritike për një gazetar përfshijnë:

- Dokumente investigimi dhe artikuj në përpunim;
- Lista të burimeve dhe bashkëpunëtorëve;
- Audio/video të intervistave dhe pamjeve ekskluzive;
- Email-e dhe biseda të ndjeshme;
- Foto, vendndodhje dhe *file* të ndarë *online;*
- Të dhëna financiare dhe personale.

Humbja ose ekspozimi i këtyre të dhënave mund të ketë pasoja serioze për gazetarin dhe për burimet e tij, duke përfshirë rreziqe për sigurinë fizike, dëmtim të reputacionit dhe probleme ligjore.

5.1 Rëndësia e kopjeve rezervë (*backup*)

Backup nënkupton kopjen rezervë e të dhënave, që ruhet në një vend të dytë për çështje sigurie. Kjo është mbrojtja më themelore kundër humbjes aksidentale apo të qëllimshme të informacionit.

Rreziqet pa *backup*:

- Defekt i *hardware*-it që shkatërron të gjitha *file*-et;
- Sulme *ransomware* që bllokojnë aksesin në të dhëna;

- Vjedhje ose humbje e pajisjes;
- Fshirje aksidentale e dokumenteve të rëndësishme;
- Korruptim i *file*-eve gjatë transferimit.

Disa këshilla praktike:

- Bëni *backup* të paktën 1 herë në javë.
- Ruani *backup*-et në vendndodhje të ndryshme (një *cloud* + një disk të jashtëm).
- Përdorni opsionin e *backup*-it automatik, aty ku është e mundur.
- Testoni rregullisht nëse *backup*-et funksionojnë.

Mjete të këshilluara:

- **Google Drive / Dropbox** (me 2FA) - për të dhëna me rëndësi të ulët
- **Tresorit** - e enkriptuar dhe e sigurt për gazetarë
- **Disk të jashtëm me enkriptim**
- **pCloud** - *cloud* me enkriptim të avancuar

5.2 Enkriptimi i të dhënave

Enkriptimi është procesi i kodimit të informacionit që vetëm ju (ose një përdorues i autorizuar) mund ta lexojë. Edhe nëse dikush akseson pajisjen ose skedarët tuaj, nuk mund t'i lexojë pa çelësin e dekriptimit.

Enkriptimi është veçanërisht i rëndësishëm për gazetarët sepse:

- Mbron identitetin e burimeve;
- Parandalon aksesin e paautorizuar në materiale investigative;
- Ofron mbrojtje ligjore në disa juridiksione;
- Ruan konfidencialitetin e komunikimeve.

Kur duhet të përdorni enkriptimin?

- Kur ruani dokumente hetimore dhe konfidenciale.
- Kur ndani *file* me bashkëpunëtorë.
- Kur mbartni informacione të ndjeshme në USB apo disk të jashtëm.

- Kur ruani kontakte burimesh dhe informatorësh të ndjeshëm.
- Kur arkivoni intervista dhe materiale multimediale.

Mjete për enkriptim të lehtë:

- **Cryptomator** - për *file* në *cloud*, i thjeshtë për t'u përdorur
- **VeraCrypt** - për disqe lokale dhe USB, më i avancuar
- **7-Zip** me fjalëkalim - për kompresim të sigurt
- **BitLocker** (Windows) ose **FileVault** (Mac) - enkriptim i plotë i diskut

Një term i rëndësishëm është ***end-to-end encryption*** - enkriptim që siguron se vetëm dërguesi dhe marrësi mund të lexojnë përmbajtjen, pa mundësi ndërhyrjeje nga palë të treta.

5.3 Shkëmbimi i *file*-eve në mënyrë të sigurt

Gazetarët shpesh duhet të ndajnë dokumente me kolegë, bashkëpunëtorë ose burime. Dërgimi i dokumenteve të ndjeshme përmes email-eve të zakonshëm ose platformave të pasigurta mund të përbëjë rreziqe si:

.

- Ndërhyrje gjatë transferimit (*man-in-the-middle*).
- Ruajtje e përhershme në servera të palëve të treta.
- Akses nga administratorët e platformave.
- Rrjedhje të dhënash nga shkelje sigurie.
- Mungesë kontrolli në lidhje me kush mund t'i aksesojë *file*-et.

Disa këshilla:

- Përdorni platforma që ofrojnë **enkriptim *end-to-end***.
- Vendosni **afate skadimi dhe fjalëkalime** për *file*-et e ndarë.
- **Ruani *file*-et vetëm përkohësisht në *cloud***, jo përgjithmonë.
- **Verifikoni identitetin e marrësit** para se të dërgoni diçka.
- Përdorni **kanale të veçanta komunikimi** për të ndarë fjalëkalime.

Shërbime të sigurta për ndarje *file*-esh:

- **OnionShare** - për dërgesa anonime përmes Tor
- **Proton Drive** - *cloud* me mbrojtje të avancuar
- **Tresorit** - për bashkëpunim të sigurt ndërmjet gazetarësh

5.4 Ruajtja e *file*-eve në kompjuter

Mënyra se si organizoni dhe ruani *file*-t në pajisjen personale ndikon drejtpërdrejt në sigurinë e tyre, si dhe në sigurinë tuaj.

Gabime të zakonshme:

- Ruajtje e dokumenteve të ndjeshme në *desktop;*
- Përdorim i emrave të qartë për *file* konfidenciale;
- Mosenkriptim i dosjeve me materiale investigative;
- Përzierje e *file*-eve personale me ato profesionale.

Disa rregulla për t'u patur parasysh:

- Krijoni dosje të koduara për projektet e ndjeshme.
- Mos lini asnjë *file* të rëndësishëm në *desktop* ose në dosje të pambrojtura.
- Përdorni emra të koduar për *file*-t konfidencialë.
- Ndani qartë materialin personal nga ai profesional.
- Mos përdorni USB të pasigurta që nuk janë tuajat.

5.5 Menaxhimi i fjalëkalimeve dhe kredencialeve

Gazetarët kanë nevojë ndoshta më shumë se askush tjetër për akses në shumë llogari, platforma dhe shërbime. Menaxhimi i dobët i kredencialeve mund të kompromentojë të gjithë punën.

Më parë në këtë udhëzues u ndalem tek fjalëkalimet dhe rëndësia e fjalëkalimeve të forta dhe të sigurta për të ruajtur llogarite tuaja. Edhe pse duket diçka e rëndomtë, një fjalëkalim

i sigurt dhe jo i përsëritur në llogari të tjera mund të shpëtojë punën, madje edhe jetën tuaj.

Gjithashtu këshilluam përdorimin e një *password manager*, një aplikacion që ruan dhe gjeneron fjalëkalime të sigurta për të gjitha llogaritë tuaja, duke kërkuar vetëm një fjalëkalim kryesor (*master password*).

Një *password manager*:

- Gjeneron fjalëkalime të forta dhe unike për çdo llogari.
- Ruan të gjitha kredencialet në mënyrë të enkriptuar.
- Plotëson automatikisht fjalëkalimet në faqe dhe aplikacione të mirëfillta. Kjo krijon gjithashtu një mbrojtje të shtuar ndaj *phishing* në raste kur sulmi kryhet nëpërmjet një faqe ueb të klonuar me qëllim që të vidhen kredencialet tuaja.
- Sinjalizon fjalëkalimet e kompromet uara.
- Mundëson akses të sigurt nga pajisje të ndryshme.

Menaxherë fjalëkalimesh të rekomanduar:

- **Bitwarden** - falas dhe *open source*
- **KeePassXC** - i pavarur, ruhet lokalisht
- **1Password** - i paguar por me veçori të avancuara
- **Dashlane** - i lehtë për t'u përdorur

6. Ngacmimi dhe bullizmi online

Ngacmimi dhe bullizmi online përfshijnë përdorimin e platformave dixhitale, siç mund të jenë mediat sociale, aplikacionet e mesazheve ose forumet, për të synuar individë me sjellje të dëmshme agresive, kërcënuese dhe fyese, apo me anë përhapjes së informacionit të rremë ose presionit psikologjik.
Ndryshe nga bullizmi tradicional, ai online mund të jetë anonim, mund të zgjasë në kohë dhe është shpesh i përhapur gjerësisht, duke lënë kështu efekte psikologjike afatgjata.

Format më të zakonshme ndaj gazetarëve:

- Komente poshtëruese ose seksiste.
- Përhapje e lajmeve të rreme për figurën personale/profesionale.
- Publikim i të dhënave personale (*doxxing*).
- Kërcënime për jetën, punën apo familjen.
- Trolling i organizuar në formë fushate.

Një term i veçantë që shpesh shfaqet në kontekstin e sigurisë dixhitale është *doxxing*. Doxxing i referohet aktit të zbulimit publik të informacionit privat ose personalisht të identifikueshëm në lidhje me një individ pa pëlqimin e tij, shpesh me qëllim keqdashës.

Metodat e *doxxing* ndryshojnë, por zakonisht përfshijnë mbledhjen e informacionit përmes:

- *social engineering* - përdorimi i ndikimit psikologjik për të manipuluar dikë që të bëjë gabime sigurie ose të japë informacione të ndjeshme;
- rrjedhjes së të dhënave;
- shfrytëzimit të databazave publike;
- gjurmimit të adresave IP;
- kërkimit në profile të mediave sociale.

Informacioni i ekspozuar mund të përfshijë të dhëna tepër të ndjeshme si adresa e shtëpisë, numrat e telefonit, adresat e email-it, detajet e vendit të punës ose edhe të

dhënat financiare. Për më tepër, doxxing mund të sjellë pasoja fizike si vjedhja e identitetit apo edhe ndjekja (*stalking*) e gazetarit, përveç pasojave psikologjike të qarta.

6.1 Si ta dallojmë ngacmimin/bullizmin online?

Ngacmimi nuk është thjesht kritikë. Ai kthehet në sistematik, personal dhe synon të trembë ose të heshtë dikë.

Shenja për t'u marrë seriozisht:

- Përsëritje të sulmeve nga të njëjtat llogari ose grupe.
- Kërcënime eksplicite (p.sh. "do të pendohesh", "do të të ndodhë diçka").
- Ndikim emocional (frikë, ankth, izolim).
- Përdorimi i fotove ose përmbajtjes personale me qëllim diskreditimin e personit.

6.2 Çfarë duhet të bësh nëse përballesh me ngacmim online?

- **Shmangni përballjen direkte**.
- **Ruani prova:** bëni *screenshots* të mesazheve, komenteve, profileve të sulmuesve.
- **Raportoni:** përdorni mjetet e raportimit në platformat sociale.
- **Bllokoni përdoruesit** që shfaqin sjellje kërcënuese.
- **Njoftoni redaksinë** ose kolegët për ngjarjen.
- **Shkruani një raportim incidenti** për ndihmë të mëtejshme ligjore.

6.3 Si të mbroni veten online për të parandaluar sulmet?

- Kontrolloni privatësinë e llogarive në rrjetet sociale.
- Limitoni informacionet personale që ndani publikisht.
- Mos përdorni të njëjtën foto në profile profesionale dhe personale.
- Përdorni pseudonime për rrjete sociale jo-zyrtare.
- Monitoroni emrin tuaj me mjete si Google Alerts.

7. Siguria në rrjetet sociale

Rrjetet sociale janë bërë mjete kyçe për gazetarët, si për të ndërtuar besueshmërinë profesionale ashtu dhe për mbledhjen e informacioneve, monitorimin e medias dhe raportimin. Megjithatë, këto platforma përfaqësojnë edhe një nga pikat më të dobëta të sigurisë dixhitale sepse çdo postim, koment apo ndërveprim mund të ekspozojë informacione të ndjeshme.

Gazetarët janë shënjestër të sulmeve në rrjetet sociale sepse:

- Kanë audienca të mëdha dhe të ndryshme;
- Ndajnë informacione profesionale dhe personale;
- Shpesh përdorin platformat për komunikim me burime.

Rreziqet kryesore për gazetarët përfshijnë:

- **Sulme *trolling*** dhe ngacmime sistematike;
- **Vjedhje identiteti** përmes përdorimit të fotove dhe informacioneve;
- ***Doxxing*** - publikim të dhënash personale për intimidim;
- **Manipulim përmbajtjesh** - përdorim jashtë kontekstit të postimeve;
- **Gjurmim dhe monitorim** i aktiviteteve dhe lëvizjeve.

7.1 Mbrojtja e llogarive personale dhe profesionale

Llogaritë e rrjeteve sociale janë shpesh objektivi i parë i sulmuesve sepse përmbajnë informacione personale dhe ofrojnë qasje të drejtpërdrejtë te publiku.

Sulmet më të zakonshme përfshijnë:

- *Hacking* i llogarive përmes fjalëkalimeve të dobëta.
- *Phishing* përmes mesazheve të rreme nga "miq" ose "bashkëpunëtorë".
- *Social engineering* - manipulim psikologjik për të marrë informacione.
- Instalim *malware*-i përmes *link*-eve të dyshimta.
- Përdorim i informacioneve publike për sulme të shënjestruara.

Masa mbrojtëse kyçe:

- **Aktivizoni verifikimin me dy hapa (2FA)** në çdo platformë që e ofron mundësinë.
- **Përdorni fjalëkalime të ndryshme** për çdo platformë.
- **Mos klikoni në mesazhe të dyshimta** që duken si oferta apo thirrje urgjente.
- **Mos jepni të dhëna personale** në *inbox* ose komente publike.
- **Kontrollo rregullisht sesionet aktive** për të monitoruar akses të paautorizuar.

7.2 Kontrolli i privatësisë dhe dukshmërisë

Gazetarët duhet të gjejnë ekuilibrin midis transparencës profesionale dhe mbrojtjes së privatësisë personale. Ky ekuilibër është veçanërisht vulnerabël në platformat sociale.

Sigurohuni qe profilet tuaja në rrjete sociale janë të mbrojtura mire. Cila është audienca juaj? Kushdo mund të shohë gjithçka, apo e ndani përmbajtjen publike nga përmbajtja për miq? Çfarë informacione personale keni ndarë publikisht? Mund të gjeheni lehtësisht përmes kërkimeve? Keni publikuar diçka qe mund t'ju dëmtoje profesionalisht apo dhe personalisht?

7.3 Ndarja e përmbajtjes me kujdes

Disa të dhëna nuk duhen publikuar asnjëherë në platforma sociale:

- Vendndodhja në kohë reale gjatë ngjarjeve të ndjeshme;
- Foto të burimeve ose të intervistuarve pa leje;
- Informacione rreth jetës familjare ose adresës së shtëpisë;
- Projekte investigative para se të publikohen;
- Detaje të sigurisë personale (udhëtime, rutina ditore);
- Mendime politike ekstreme që mund të dëmtojnë objektivitetin dhe reputacionin tuaj,

7.4 Identifikimi i llogarive të rreme dhe *bot*-eve

Fake accounts dhe ***bot*-et** përdoren shpesh për të manipuluar opinionin publik dhe për të sulmuar gazetarët.

Si mund të dalloni një llogari të rreme?

- **Profil i paplotë** - pak informacione personale, foto të vjedhura ose *stock* (foto tipike të marra nga p.sh. Google Images).
- **Aktivitet i dyshimtë** - postime vetëm politike ose kontroverse.
- **Miqësi të çuditshme** - shumë miq por pa ndërveprime reale.
- **Gjuhë e standardizuar** - përdorim i të njëjtave konstrukte gjuhësore në postime të shumta.
- **Frekuenca e aktivitetit** - postime në orë të papritura ose me model të rregullt.
- **Reagime të shpejta** - komente menjëherë pas publikimit.

Bot networks ose ***sock puppets*** janë grupe llogarish të rreme që kontrollohen nga të njëjtët persona për të amplifikuar mesazhe të caktuara.

8. Çështjet etike: Të drejtat e autorit (*copyright*) dhe plagjiatura

Në epokën dixhitale, gazetarët përballen me sfida të shumta në ruajtjen e standardeve etike gjatë prodhimit të përmbajtjes me cilësi të lartë. Të drejtat e autorit (copyright) dhe plagjiatura janë nder këto sfida të tilla por të cilat fatkeqësisht shpesh anashkalohen, ndërsa mund të ndikojnë ndjeshëm në besueshmërinë dhe statusin ligjor të një gazetari.

8.1 Të drejtat e autorit (*copyright*)

Çfarë janë të drejtat e autorit (copyright)?

E drejta e autorit është një koncept ligjor që u jep krijuesve të drejta ekskluzive për veprat e tyre origjinale. Këto të drejta zakonisht përfshijnë mundësinë për të riprodhuar, shpërndarë, shfaqur dhe krijuar vepra të prejardhura nga krijimi origjinal. Për gazetarët, mbrojtja e të drejtave të autorit prek artikuj, fotografi, video dhe forma të tjera të medias që ata prodhojnë.

Aspektet kryesore të legjislacionit të të drejtës së autorit

- **Origjinaliteti**: Vepra duhet të jetë origjinale, e krijuar nga një autor. Ndërsa vetë idetë nuk janë të mbrojtura, mënyra si janë të shprehura po.
- **Fiksimi**: Vepra duhet të jetë e fiksuar në një medium të prekshëm, siç është teksti i shkruar ose regjistrimi audioviziv.
- **Kohëzgjatja**: Mbrojtja e të drejtës së autorit përgjithësisht zgjat për jetën e autorit plus një numër të caktuar vitesh (p.sh., 70 vjet pas vdekjes së autorit në shumë juridiksione, përfshirë ai i Republikës së Shqipërisë).
- **Përdorimi i drejtë (*fair use*)**: Lejon përdorimin e kufizuar të materialit të mbrojtur me të drejtë autori pa leje për qëllime si kritika, komentimi, raportimi i lajmeve, mësimdhënia, studimi akademik ose kërkimi.

Legjislacioni

Shqipëria është palë në Konventën e Bernës për Mbrojtjen e Veprave Letrare dhe Artistike që nga marsi i vitit 1994.

Në nivelin kombëtar, ekziston **Ligji Nr. 35/2016 për të drejtat e autorit dhe të drejtat e tjera të lidhura me to (ndryshuar me ligjin nr. 37/2022).**

Vlen të theksohet qe neni 12.1.d i Ligjit Nr. 35/2016 përjashton “lajmet dhe informacion[et] e shtypit, [të cilat] ka[në] karakter të thjeshte informimi” nga objektet e mbrojtura nga e drejta e autorit. Ndonëse kjo le hapësirë për interpretim, një artikull, reportazh, apo punim investigativ i një gazetari/e, i cili nuk është thjesht riprodhim faktesh por përmban përpunim materiali, duhet të jete absolutisht objekt i mbrojtur nga e drejta e autorit në Shqipëri.

8.2 Plagjiatura

Çfarë është plagjiatura?

Plagjiatura është paraqitja e punës ose ideve të dikujt tjetër si të tuat pa reference dhe pa i dhënë atribuimin e duhur autorit. Në gazetari, plagjiatura minon besimin midis gazetarit dhe audiencës, pasi komprometon integritetin e informacionit që raportohet. Për me teper, plagjiatura jo vetëm shkel standardet etike, por dëmton edhe reputacionin e gazetarit dhe të botimit, duke sjelle në humbjen e besueshmërisë dhe në pasoja ligjore. Gazetaria etike kërkon transparencë dhe ndershmëri, duke siguruar që të gjitha burimet të përmenden siç duhet.

Llojet e plagjiaturës:

- **Plagjiaturë e drejtpërdrejtë**: Kopjimi e tekstit nga një burim tjetër pa i dhënë atribuim.
- **Plagjiaturë mozaiku**: Parafrazimi i punës së një burimi pa citim të duhur.
- **Vetë-plagjiaturë**: Ripërdorimi i punës së dikujt të botuar më parë pa e përmendur, gjë që mund të jetë problematike nëse kjo paraqitet si përmbajtje e re.

Si ta shmangni plagjiaturën?

- **Citoni burimet me saktësi**: Atribuo gjithmonë citimet, statistikat apo idetë burimeve të tyre origjinale.
- **Përdorni thonjëza**: Kur citon drejtpërdrejt një burim, fut tekstin e cituar në thonjëza dhe jep një citim.

- **Parafrazoni me përgjegjësi**: Kur parafrazoni, sigurohuni që teksti i rifrazuar të jetë mjaftueshmerisht i ndryshëm nga origjinali. Në çdo rast, edhe në parafrazim duhet dhënë atribuimi i duhur autorit.
- **Përdorni mjete zbulimi të plagjiaturës**: Përdorni mjete si Grammarly Plagiarism Checker, PlagScan, ose Turnitin (në institucione akademike) për të kontrolluar punën tuaj për plagjiaturë të paqëllimshme para dorëzimit.
- **Kuptoni konceptin e përdorimit të drejtë (*fair use*):** Jini të vetëdijshëm për limitet e përdorimit të drejtë dhe kërkoni leje kur është e nevojshme. **Rregullat e pergjithshme për *fair use* janë**:

Kushti	**Lejohet?**
Përdor pjesë të shkurtër për citim	Po, duke qartësuar burimin
Merr gjithë përmbajtjen	Jo, edhe nëse e citojmë
Përfshin elemente edukues ose kritikë	Mund të lejohet
Synon përfitim financiar	Shmangeni

Për foto dhe video, përdorni **Creative Commons** dhe tregoni autorin si dhe licencën.
Gazetarët duhet të njohin mirë kompleksitetet e të drejtave të autorit dhe plagjiaturës me qëllim që të ruajnë integritetin dhe detyrat ligjore si dhe respektin ndaj etikes së zanatit të tyre. Kjo kërkon kuptimin e ligjeve të të drejtave të autorit dhe përmbajtjen e standardeve etike, me qellim qe puna të jete origjinale dhe të respektoje të drejtat e pronësisë intelektuale. Kështu, gazetarët mbështesin parimet e gazetarisë etike dhe kontribuojnë në një diskurs publik të besueshëm dhe të informuar.

9. Ligjet dixhitale

Siguria dixhitale është një fushë në zhvillim të vazhdueshëm dhe ligji shpesh has vështirësi në kapjen e ritmit të inovacioneve të kësaj fushe, pavarësisht nëse përdoren për qëllime të mira apo të këqija.

Gazetaret duhet të mbeten të informuar dhe të përditësuar në lidhje me ligjet që ndikojnë punën e tyre në hapësirën dixhitale: të drejtat e autorit (të shpjeguara me hollësisht në kapitullin e mësipërm), të dhënat personale, përmbajtjet online dhe mbrojtjen nga ngacmimi apo sulmet kibernetike.

- **E drejta e autorit dhe pronësia intelektuale**

Ligji nr. 35/2016 "Për të drejtat e autorit dhe të drejtat e lidhura me të" mbron:

- Artikujt origjinalë
- Video, audio dhe foto të krijuara nga gazetari
- Të drejtën për të mos u kopjuar pa leje
- Të drejtën për të kërkuar dëmshpërblim në rast përdorimi të paautorizuar

Edhe përmbajtjet që ndahen në internet kanë **mbrojtje ligjore**, përfshirë postimet në rrjetet sociale.

- **Mbrojtja e të dhënave personale**

  Ligji nr. 9887/2008 "Për mbrojtjen e të dhënave personale" u jep individëve:

  - Të drejtën për të ditur si përpunohen të dhënat e tyre
  - Të drejtën për të kërkuar fshirjen e të dhënave
  - Të drejtën për të refuzuar publikimin e informacionit personal pa leje

Ky ligj duhet patur parasysh si për gazetaret edhe për individët mbi të cilët ata raportojnë.

Vlen të përsëritet se gazetaret duhet të:

- Marrin **leje të qarta** kur publikojnë të dhëna identifikuese (foto, emra të qytetarëve, vendbanime).
- Ruajnë **anonimitetin** e personave të përfshirë kur raportojnë për raste sensitive.
- Ruajnë të dhënat e burimeve në mënyrë të **koduar dhe konfidenciale.**

- **Shpifja, fyerja dhe përhapja e lajmeve të rreme**

Sipas **Kodit Penal të Republikës së Shqipërisë**, janë të dënueshme:

  - **Shpifja (neni 120)** – përhapje e qëllimshme e informacionit të pavërtetë
  - **Fyerja publike**
  - **Përhapja e panikut** me informacione të rreme

- **Ngacmimi online dhe ndëshkimi ligjor**

Neni 121/a i Kodit Penal (neni 121/a) përcakton se ngacimi përmes rrjeteve sociale apo formave të tjera dixhitale është i dënueshëm. Veprime të tilla përfshijnë dërgimin e mesazheve kërcënuese, doxxing, fyerjen sistematike neper komente apo inbox dhe falsifikimin e përmbajtjes me qellim diskreditimin.

10. Inteligjenca Artificiale (IA) dhe Siguria Dixhitale

Inteligjenca Artificiale është duke ndryshuar totalisht peizazhin e gazetarisë, duke sjellë mundësi të reja por edhe rreziqe të mëdha për sigurinë dixhitale. Gazetarët duhet të kuptojnë jo vetëm si të përdorin IA-n në mënyrë të sigurt, por edhe si të mbrohen nga abuzimi i saj nga aktorë keqdashës.

10.1 Çfarë është Inteligjenca Artificiale?

Inteligjenca Artificiale është një fushë teknologjie që synon të krijojë sisteme kompjuterike që simulojnë aftësitë konjitive të njeriut: të menduarit, të mësuarit dhe krijimin e përmbajtjes. Vlen të theksohet se edhe pse IA arrin ta imitoje mjaft mire “mendjen” e njeriut, nuk duhet harruar që ajo nuk ka ndërgjegje apo qellim. Me sakte, IA funksionon në baze të modeleve statistikore të ndërtuara nga analiza e miliona të dhënash ekzistuese.

Disa nga teknologjitë me të përhapura të IA-së janë:

- ***Machine Learning*** **(ML)** është procesi ku algoritmet mësojnë nga të dhënat historike dhe përdorin këtë "mësim" për të bërë parashikime. Për shembull, një redaksi mund të përdorë ML për të analizuar se çfarë lloj titujsh kanë më shumë klikime. Një rrezik i mundshëm këtu është që modelet mund të nxisin edhe me shume sensacionalizëm kur mësojnë që titullarët *clickbait* kane me shume sukses me audiencat.
- ***Generative AI*** është teknologji që krijon përmbajtje të re (tekst, imazhe, zë, video) duke përdorur algoritme të trajnuara me shumë të dhëna. Jepet një "*prompt*" (kërkesë) dhe IA gjeneron përmbajtjen. Disa shembuj në fushën e gazetarisë përfshijnë krijimin e shkrimeve për artikuj rutine si moti ose sporti, gjenerimin e materialeve vizuale për rrjete sociale, ose përkthime të shpejta të materialeve.
- ***Large Language Models*** **(LLM)** si ChatGPT janë modele të mëdha gjuhësore të trajnuara me miliarda fjalë nga interneti.

10.2 Si mund të përdoret IA nga aktorë keqdashës?

Aktorët keqdashës mund të përdorin IA për manipulim, mashtrim, diskreditim dhe survejim të gazetarëve në mënyra të sofistikuara dhe gjithnjë me të vështira për t'u zbuluar.

- **Teknologjia *deepfake*** përdor algoritme të avancuara për të ndërthurur fytyrën apo zërin e dikujt në një video ekzistuese, duke e bërë të duket sikur ai ka thënë apo bërë diçka që nuk ka ndodhur kurrë. Kjo teknologji jo vetëm mund të cënojë gazetarët, por median në tërësi.
- ***AI-phishing*** është përdorimi i IA për të krijuar mashtrime të personalizuara dhe të sofistikuara me anë të email-it. Ndryshe nga *phishing*-u tradicional, AI-phishing mund të imitojë stilin e kolegëve dhe të krijojë përmbajtje pa gabime gjuhësore.
- ***Voice cloning*** lejon krijimin e një modeli zanor nga vetëm 10-30 sekonda regjistrim. Ky model mund të përdoret për të "folur" në emrin e dikujt tjetër.
- ***Malware* i gjeneruar nga IA** është kod keqdashës i shkruar nga IA që mund të anashkalojë sistemet antivirus tradicionale duke u përshtatur automatikisht me sistemin e viktimës.
- ***Chatbot-troll farms*** janë rrjete të organizuara që përdorin IA për të gjeneruar automatikisht komente fyese, për të shpërndarë informacion të manipuluar dhe për të krijuar ndjesinë e një "opinioni publik" të rreme.

10.3 Disa rreziqe specifike për gazetarët

Gazetarët mund të synohen posaçërisht në epokën e IA për shkak të vleres së informacionit që ata mund të kenë me ane të komunikimit me burime konfidenciale, publikimit të informacionit delikat dhe ekspozimit të vazhdueshëm publik.

- ***Kompromet**imi i burimeve* është një nga rreziqet më të mëdha. IA mund të përdoret për të zbuluar burimet anonime në disa mënyra:
    - ***Stylometry AI*** analizon mënyrën e ndërtimit të fjalisë, fjalët e përdorura më shpesh dhe ritmin e frazës. Nëse një burim përdor gjithmonë fjalë të caktuara ose strukturë specifike, IA mund të jete e afte të identifikojë personin pas tekstit.

- ***Analiza e metadata*-ve** nga dokumentet që gazetari merr (PDF, Word, foto) mund të zbulojë emrin e krijuesit të dokumentit, datën e krijimit dhe vendndodhjen e pajisjes.

- ***Shënjestrimi i personalizuar*** përfshin përdorimin e IA nga aktorë keqdashës për të krijuar profile të detajuara psikologjike dhe politike të gazetarëve duke përdorur historikun e kërkimeve të tyre, ndërveprimet sociale në platforma dhe artikujt e publikuar.
- ***Automatizimi i ngacmimit*** përmes *bot*-eve të gjeneruara nga IA që shpërndajnë komente fyese, përgjigje denigruese dhe përhapje montazhesh në përmasa masive dhe të pakontrollueshme.

10.4 Mjete mbrojtëse me IA

Ekzistojnë mjete konkrete dhe të aksesueshme që gazetarët mund të përdorin për t'u mbrojtur nga rreziqet e IA dhe për të verifikuar përmbajtjen e dyshimtë.

Mjete kryesore të këshilluara:

Qëllimi	**Mjeti**	**Si ndihmon**
Verifikim i një *deepfake*	InVID, Jigsaw Assembler	Analizojnë video dhe audio për të zbuluar shenja manipulimi
Zbulim tekstesh IA	GPTZero, OpenAI Classifier	Japin probabilitetin që teksti është shkruar nga IA
Monitorim kërcënimesh	Hunchly, Maltego	Analizojnë rrjete dezinformimi dhe profile të rreme
Zbulim i AI-phishing	Microsoft Defender XDR	Skanojnë email për gjuhë të dyshimtë dhe sjellje të pazakonta
Më shumë privatësi në përdorimin e IA	Local LLaMA 3	Mundëson përdorim IA offline pa kaluar të dhënat në *cloud*

10.5 Etika, ligji dhe IA në gazetari

Përdorimi i IA në gazetari nuk është vetëm çështje teknologjie, por përfshin përgjegjësi ligjore, etike dhe shoqërore. Gazetarët kanë detyrimin të ruajnë standardet profesionale edhe kur përdorin mjete të reja.

Parimi i transparencës kërkon që gazetari të **deklarojë kur një përmbajtje është krijuar, përpunuar apo ndihmuar nga një sistem IA.** Kjo është shume e rëndësishme për të ruajtur besueshmërinë ndaj lexuesit dhe publikut, për të ndihmuar në dallimin midis informacionit të verifikuar dhe atij të krijuar në mënyre automatike, si dhe për të ulur rrezikun e akuzave për mashtrim.

Privatësia është një tjetër aspekt që kërkon kujdes të veçantë sepse futja e të dhënave personale në chatbot publik konsiderohet proçesim i të dhënave dhe mund të përbëjë shkelje ligjore sipas **GDPR** (General Data Protection Regulation, **2016/679**) si dhe **ligjit shqiptar për mbrojtjen e të dhënave personale (124/2024).**

Paragjykimet që mund të mbartë një teknologji IA janë problem serioz shpesh i anashkaluar. Nga njera ane, një IA e caktuar është e modeluar në atë mënyre specifike sepse entiteti që e krijoi atë ka qëllimet e tij vetjake. Nga ana tjetër, duhet patur parasysh gjithnjë që modelet IA janë të ushqyera nga të dhëna së të kaluarës që shpesh përmbajnë stereotipe gjinore, racizëm dhe paragjykime kulturore, përsëri në baze të entitetit që e modeloi atë.