SMART Balkans

Civil Society for Shared Society in the Western Balkans

INSTITUTI LIBERAL PASHKO

Forcimi i Privatësisë dhe Sigurisë së të dhënave për Grupet Vulnerabël në Tiranë

HYRJE

Zhvillimi i shpejtë i teknologjisë ka sjellë ndryshime të thella në çdo aspekt të jetës. Sot, përdorimi i kompjuterëve, internetit dhe mediave sociale është bërë i zakonshëm dhe i aksesueshëm për të gjithë. Komunikimi virtual përmes rrjeteve sociale dhe aplikacioneve në telefonat mobile është mënyra kryesore e ndërveprimit midis individëve në shoqërinë moderne.

ÇFARË ËSHTË PRIVATËSIA DHE SIGURIA E TË DHËNAVE?

Privatësia dhe siguria e të dhënave janë dy aspekte kritike në epokën digjitale. Ato përfshijnë mbrojtjen e informacionit personal nga keqpërdorimi, qasja e paautorizuar dhe manipulimi.

PSE ËSHTË E RËNDËSISHME KJO TEMË?

Në epokën e informacionit, të dhënat personale janë një pasuri e vlefshme. Ato mund të përdoren për përfitime, por gjithashtu edhe të keqpërdoren në forma të ndryshme:

- **Mashtrime kibernetike** ku të dhënat merren nga hacker-a për qëllime kriminale.
- **Keqpërdorimi** nga korporata që mbledhin të dhëna pa miratim.
- **Sulmet** ndaj individëve vulnerabël që nuk kanë njohuri mbi sigurinë digjitale.

QËLLIMI I TEMËS

Forcimin e mbrojtjes së privatësisë dhe sigurisë së të dhënave

Rritjen e ndërgjegjësimit mbi rreziqet dhe masat e mbrojtjes.

Aftësimin e individëve për të menaxhuar në mënyrë të sigurt informacionin e tyre personal.

Zbatimin e standardeve ndërkombëtare dhe kombëtare në mbrojtjen e të dhënave.

Reduktimin e rrezikut të abuzimit dhe keqpërdorimit të të dhënave.

KUSH JANË GRUPET VULNERABËL?

- Fëmijët dhe të rinjtë.
- Personat me aftësi të kufizuara.
- Minoritetet dhe komunitetet e margjinalizuara.
- Personat e moshuar

NDIKIMI NË GRUPET VULNERABËL

- Në një realitet ku informacionet personale janë gjithnjë e më të ekspozuara, grupet vulnerabël përballen me sfida të veçanta në mbrojtjen e privatësisë dhe sigurisë së të dhënave. Këto kategori shpesh nuk kanë mjete, njohuri apo mbështetjen e nevojshme për të mbrojtur informacionet e tyre, duke u bërë objektiv i manipulimeve, mashtrimeve dhe abuzimeve digjitale.

FËMIJËT DHE TË RINJTË

- Të rinjtë janë një nga grupet më të ekspozuara në internet. Shpesh ata ndajnë informacione pa menduar për pasojat, duke u bërë viktima të keqpërdorimit të të dhënave, profilizimit të pashmangshëm nga platformat digjitale dhe sulmeve kibernetike, si cyberbullying dhe mashtrimet online. Mungesa e edukimit mbi privatësinë mund t'i vërë ata në rrezik të identitetit të vjedhur ose të manipulimit psikologjik.

PERSONAT ME AFTËSI TË KUFIZUARA

- Kjo kategori mund të përballet me sfida në qasjen e informacionit dhe në menaxhimin e privatësisë. Ata shpesh mbështeten në teknologji për të komunikuar dhe për të marrë shërbime, por mungesa e masave të duhura të sigurisë mund të çojë në shkelje të të dhënave, abuzim ekonomik dhe diskriminim nga platforma digjitale, të cilat mund t'i përjashtojnë ose t'i ekspozojnë pa dashje.

MINORITETET DHE KOMUNITETET E MARGJINALIZUARA

- Këto grupe mund të jenë më të rrezikuara për shkak të diskriminimit sistematik, përdorimit abuziv të të dhënave për profilizim dhe monitorimit të paautorizuar nga institucionet apo palët e treta. Shpesh informacionet e tyre përdoren për qëllime të dëmshme, duke i lënë pa mbrojtje dhe duke u kufizuar aksesin në shërbime të barabarta.

PERSONAT E MOSHUAR

- Personat e moshuar shpesh nuk kanë edukim teknologjik të mjaftueshëm për të kuptuar mekanizmat e privatësisë dhe sigurisë së të dhënave. Ata mund të bien viktima të mashtrimeve financiare, keqpërdorimit të informacionit të tyre mjekësor dhe sulmeve kibernetik, duke humbur aksesin në financat e tyre ose duke u manipuluar nga individë të pandërgjegjshëm.

RREZIQET DHE SFIDAT

- **Sulmet kibernetike**: Phishing, malware, hacking.
- **Keqpërdorimi i të dhënave personale:** Rrjetet sociale, informacioni publik.
- **Mbikëqyrja dhe kontrolli:** Si mund të ndikojë mbikëqyrja e tepërt në të drejtat e individit?
- **Dezinformimi dhe manipulimi:** Rreziqet që vijnë nga informacioni i pavërtetë.

SULMET KIBERNETIKE: PHISHING, MALWARE, HACKING

- **Phishing:** Teknikë manipulimi ku sulmuesit dërgojnë e-maile ose mesazhe të rreme që duken të besueshme për të mashtruar përdoruesit që të japin informacione sensitive, si fjalëkalime apo numra kartash.
- **Malware:** Softuer i dëmshëm që futet në pajisjet e përdoruesve për të vjedhur të dhëna, për të monitoruar aktivitetet ose për të shkaktuar dëmtime të sistemit.
- **Hacking:** Depërtimi i paautorizuar në sisteme të mbrojtura për të marrë informacion ose për të dëmtuar funksionimin e tyre.

- **Si të mbrohemi? Përdorimi i antivirusëve, fjalëkalimeve të sigurta, autentifikimit me dy faktorë, dhe mos hapja e mesazheve nga burime të panjohura janë mënyra efektive për të zvogëluar rrezikun.**

KEQPËRDORIMI I TË DHËNAVE PERSONALE: RRJETET SOCIALE DHE INFORMACIONI PUBLIK

- **Rrjetet Sociale:** Platforma si Facebook, Instagram dhe TikTok grumbullojnë dhe analizojnë të dhënat e përdoruesve për reklama të personalizuara. Në disa raste, të dhënat e përdoruesve mund të keqpërdoren ose të shpërndahen pa lejen e tyre.
- **Informacioni Publik:** Shpërndarja e paautorizuar e informacioneve personale, si adresat, numrat e telefonit ose të dhënat financiare, mund të çojë në mashtrime identiteti dhe probleme ligjore.
- **Profilizimi digjital:** Kompanitë dhe institucionet përdorin informacionin personal për të krijuar profile mbi sjelljet dhe preferencat, ndonjëherë pa transparencë të plotë për përdoruesit.

- **Si të mbrohemi? Përdorimi i cilësimeve të privatësisë, kontrolli i informacionit të shpërndarë, ndjekja e politikave të mbrojtjes së të dhënave, dhe mos ndarja e tepërt e informacioneve personale në internet.**

MBIKËQYRJA DHE KONTROLLI: NDIKIMI NË TË DREJTAT E INDIVIDIT

- **Monitorimi i të dhënave nga qeveritë dhe korporatat:** Në shumë vende, informacioni personal monitorohet për arsye sigurie apo reklamimi. Ky mbikëqyrje mund të jetë një rrezik për të drejtat civile dhe autonominë individuale.
- **Kamerat e vëzhgimit dhe teknologjitë e njohjes së fytyrës:** Njohja biometrike mund të përdoret për arsye sigurie, por gjithashtu mund të krijojë një sistem mbikëqyrjeje masive që cenon privatësinë.
- **Rregullat e privatësisë në aplikacionet digjitale:** Shumë aplikacione dhe faqe interneti mbledhin të dhëna pa pëlqimin e qartë të përdoruesit, duke krijuar profilizim të pavetëdijshëm dhe ndikim në sjelljet digjitale.

- **Si të mbrohemi? Leximi dhe kuptimi i politikave të privatësisë, përdorimi i VPN, kontrolli i aplikacioneve që përdorin të dhënat tuaja dhe mos dhënia e lejeve të panevojshme në pajisjet digjitale janë strategji të efektshme për zvogëlimin e ekspozimit ndaj mbikëqyrjes.**

DEZINFORMIMI DHE MANIPULIMI: RREZIQET NGA INFORMACIONI I PAVËRTETË

- **Fake News:** Lajmet e rreme përhapen shpejt në rrjetet sociale dhe mediat digjitale, duke ndikuar në perceptimin e realitetit dhe vendimmarrjen e qytetarëve.
- **Manipulimi psikologjik:** Disa entitete përdorin informacionin personal për të ndikuar mendimet, sjelljet dhe zgjedhjet e njerëzve përmes teknikave të marketingut dhe propagandës digjitale.
- **Deepfake dhe përmbajtjet e rreme:** Teknologjitë e reja mund të krijojnë imazhe, video dhe audio të falsifikuara që duken të vërteta, duke mashtruar publikun dhe duke krijuar probleme etike.

- **Si të mbrohemi? Verifikimi i burimit të informacionit, konsultimi me burime të besueshme, shmangia e shpërndarjes së informacionit pa verifikim, dhe raportimi i përmbajtjeve manipuluese janë mënyra efektive për të luftuar dezinformimin.**

LEGJISLACIONI PËR MBROJTJEN E TË DHËNAVE

- Ligjet shqiptare mbi mbrojtjen e të dhënave personale.
- Rregullat e GDPR dhe ndikimi i tyre në Shqipëri.
- Roli i AKSHI-së dhe institucioneve të tjera.

LIGJET SHQIPTARE MBI MBROJTJEN E TË DHËNAVE PERSONALE.

Shqipëria ka miratuar një kuadër ligjor të mbrojtjes së të dhënave personale, i cili përcakton standardet për mbledhjen, ruajtjen dhe përdorimin e informacionit personal nga individët, kompanitë dhe institucionet. Ligji kryesor në këtë fushë është:

Ligji nr. 9887, datë 10.03.2008 "Për mbrojtjen e të dhënave personale"

Ky ligj synon të mbrojë të drejtat e individëve duke rregulluar:

- Mënyrën e mbledhjes dhe përpunimit të të dhënave personale.
- Kushtet e ruajtjes dhe ndarjes së informacionit.
- Të drejtat e qytetarëve për akses në të dhënat e tyre dhe për korrigjimin e tyre.
- Rregullat për transferimin e të dhënave jashtë Shqipërisë.

RREGULLAT E GDPR DHE NDIKIMI I TYRE NË SHQIPËRI.

Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave (GDPR), e miratuar nga Bashkimi Europian në vitin 2016 dhe e zbatuar në 2018, ofron një qasje më të fortë për të mbrojtur të dhënat personale, duke imponuar detyrime strikte mbi:

- **Transparencën dhe pëlqimin**: Individët duhet të informohen qartë për mënyrën se si përpunohen të dhënat e tyre dhe të japin pëlqimin në mënyrë të vetëdijshme.
- **E drejta për të harruar**: Çdo individ ka të drejtën të kërkojë që të dhënat e tij të fshihen nga sistemet digjitale.
- **Siguria e të dhënave**: Kompanitë dhe institucionet janë të detyruara të përdorin teknika të enkriptimit dhe mbrojtjes së informacionit për të minimizuar rreziqet e sulmeve kibernetike.
- **Raportimi i shkeljeve**: Në rast të një shkeljeje të sigurisë së të dhënave, subjekti duhet ta raportojë atë brenda 72 orëve.
- **Sanksionet**: Ndërmarrjet që nuk zbatojnë GDPR mund të përballen me gjoba deri në 4% të të ardhurave globale.

ROLI I AKSHI-SË DHE INSTITUCIONEVE TË TJERA.

Institucionet shqiptare që monitorojnë dhe zbatojnë legjislacionin mbi mbrojtjen e të dhënave janë:

Autoriteti i Mbikëqyrjes së Të Dhënave Personale (IDP)

IDP është institucioni kryesor që mbikëqyr zbatimin e ligjit për mbrojtjen e të dhënave personale. Disa nga funksionet kryesore të tij përfshijnë:

- Inspektimin e subjekteve publike dhe private që mbledhin të dhëna personale.
- Rregullimin e procedurave të mbrojtjes së të dhënave dhe zbatimin e ligjit nr. 9887.
- Këshillimin e individëve mbi të drejtat e tyre për privatësinë.
- Vendosjen e masave administrative dhe sanksioneve ndaj subjekteve që shkelin ligjet mbi privatësinë.

SI MUND TË MBROHEMI?

- Mbrojtja e të dhënave personale është një proces që kërkon kujdes dhe vigjilencë të vazhdueshme. Në botën digjitale, ku informacionet qarkullojnë me shpejtësi, individët mund të minimizojnë rreziqet duke përdorur strategji të sigurta.
- Më poshtë janë masat kryesore të sigurisë që duhet të aplikojmë për të mbrojtur të dhënat tona.

1. PËRDORIMI I FJALËKALIMEVE TË SIGURTA DHE AUTENTIFIKIMI ME DY FAKTORË

- **Pse është e rëndësishme?**

  Fjalëkalimi është **vija e parë e mbrojtjes** kundër qasjes së paautorizuar. Një fjalëkalim i dobët mund të bëhet lehtësisht objekt i sulmeve si **hacking** dhe **phishing**.

- **Si të krijojmë një fjalëkalim të sigurt?**

- Përdor **kombinime të karaktereve**, duke përfshirë shkronja të mëdha dhe të vogla, numra dhe simbole.
- Mos përdor **informacione të lehta për t'u gjetur** (datëlindje, emri i fëmijës, etj.).
- Ndrysho fjalëkalimet **rregullisht** dhe shmang përdorimin e njëjtit fjalëkalim në platforma të ndryshme.
- Përdor një **menaxher fjalëkalimesh** për të ruajtur dhe krijuar kombinime të forta.

1. PËRDORIMI I FJALËKALIMEVE TË SIGURTA DHE AUTENTIFIKIMI ME DY FAKTORË

Ky mekanizëm **shton një shtresë ekstra sigurie** duke kërkuar një kod shtesë për qasje, zakonisht të dërguar në telefon ose email.

- **Përfitimet:**
- Redukton mundësinë e vjedhjes së fjalëkalimit.
- Bën më të vështirë qasjen e paautorizuar edhe nëse dikush di fjalëkalimin tuaj.
- Shumica e platformave si **Google, Instagram, Facebook, Bankat Online** e mbështesin këtë veçori.

2. RREGULLAT E SIGURISË NË INTERNET

- **Pse është e rëndësishme?**

  - Sulmet kibernetike **përdorin dobësitë** në sistemet tona për të fituar akses në informacionet personale. Mbrojtja e pajisjeve tona është **thelbësore** për të reduktuar këto rreziqe.

- **Si të mbrohemi?**

  - **Përditëso softuerët dhe aplikacionet** rregullisht për të shmangur dobësitë e sigurisë.
  - **Mos hap email-e dhe mesazhe nga burime të panjohura** (mund të jenë sulme phishing).
  - **Përdor VPN kur lidheni në rrjete publike** për të mbrojtur trafikun tuaj të internetit.
  - **Instalo një antivirus cilësor** dhe aktivizo firewall-in në pajisjet tuaja.
  - **Kujdes me shkarkimet online** – shmang skedarët që nuk kanë burim të besueshëm.
  - **Verifikoni faqet ku vendosni të dhënat personale** – sigurohuni që janë të enkriptuara (https://).

3. MENAXHIMI I PRIVATËSISË NË RRJETET SOCIALE

- **Pse është e rëndësishme?**

  Rrjetet sociale janë një nga hapësirat ku më së shumti **përdoruesit ndajnë informacionet e tyre** pa menduar për rreziqet. Disa platforma grumbullojnë të dhënat për marketing, ndërsa të tjera mund të bëhen objekt i keqpërdorimit të informacionit.

- **Si të mbrohemi?**

  Kontrollo cilësimet e privatësisë dhe lejo vetëm persona të besuar të shohin profilin dhe postimet e tua.

  Shmang shpërndarjen e të dhënave personale, si adresat, vendndodhja e drejtpërdrejtë apo numri i telefonit.

  Mos prano kërkesa miqësie nga njerëz që nuk i njeh – shumë profile të rreme përdoren për mashtrim.

  Mos kliko në linke të dyshimta që mund të të çojnë në faqe mashtruese.

  Verifiko aplikacionet e lidhura me llogarinë tënde – fshiji ato që nuk i përdor më.

ROLI I KOMUNITETIT DHE INSTITUCIONEVE

- 1. Ndërgjegjësimi dhe edukimi në shkolla dhe universitete.
- 2. Roli i organizatave joqeveritare në mbrojtjen e të dhënave.
- 3. Iniciativa dhe fushata sensibilizuese për të drejtat digjitale.

1. SI MUND TË NDIHMOJNË SHKOLLAT DHE UNIVERSITETET?

- Futja e mësimeve mbi privatësinë digjitale si pjesë e kurrikulës.
- Organizimi i trajnimeve mbi sigurinë kibernetike dhe mënyrat e mbrojtjes së të dhënave.
- Krijimi i moduleve edukative për përdorimin e sigurt të internetit dhe rrjeteve sociale.
- Përdorimi i simulimeve dhe skenarëve praktikë për të rritur ndërgjegjësimin mbi rreziqet dhe mbrojtjen e informacionit.
- Angazhimi i profesorëve për të edukuar studentët mbi rëndësinë e privatësisë online.

📌 Shembull praktik:
Një shkollë e mesme mund të organizojë një seminar mbi sigurinë digjitale, ku nxënësit mësojnë për sulmet kibernetike, menaxhimin e fjalëkalimeve dhe cilësimet e privatësisë në aplikacione.

2. ROLI I ORGANIZATAVE JOQEVERITARE NË MBROJTJEN E TË DHËNAVE

Kontributet e OJF-ve në privatësinë digjitale:

- Organizimi i fushatave ndërgjegjësuese mbi rëndësinë e privatësisë online.
- Ofrimi i mbështetjes ligjore për personat e prekur nga shkeljet e privatësisë.
- Monitorimi i institucioneve dhe kompanive për të siguruar transparencë në përpunimin e të dhënave personale.
- Përdorimi i mediave dhe rrjeteve sociale për të informuar qytetarët mbi rreziqet dhe mënyrat e mbrojtjes.
- Bashkëpunimi me qeverinë dhe akademinë për të përmirësuar ligjet dhe rregulloret mbi privatësinë.

📌 Shembull praktik:
Një organizatë mund të publikojë një raport vjetor mbi keqpërdorimin e të dhënave në Shqipëri, duke identifikuar sfidat dhe rekomanduar zgjidhje.

3. INICIATIVA DHE FUSHATA SENSIBILIZUESE PËR TË DREJTAT DIGJITALE

Si mund të ndihmojnë fushatat sensibilizuese?

- Krijimi i broshurave dhe materialeve informuese mbi të drejtat e qytetarëve.
- Përdorimi i mediave sociale dhe platformave digjitale për të shpërndarë këshilla mbi privatësinë.
- Organizimi i eventeve publike ku qytetarët mund të mësojnë strategji mbrojtëse për privatësinë.
- Përfshirja e influencuesve digjitalë për të shpërndarë mesazhe edukative mbi sigurinë online.
- Zhvillimi i aplikacioneve dhe kurseve online mbi privatësinë dhe sigurinë e të dhënave.

📌 Shembull praktik:
Një kompani mund të nisë një fushatë sensibilizuese mbi sigurinë online, duke përdorur video edukative dhe grafikë që tregojnë rreziqet e ndarjes së tepërt të informacionit në rrjetet sociale.

RAST STUDIMOR

➢ Skandali i Cambridge Analytica – Manipulimi Politik përmes të Dhënave

Skandali i **Cambridge Analytica** është një nga rastet më të njohura të keqpërdorimit të të dhënave personale për **manipulim politik**. Ai zbuloi se si një kompani e analizës së të dhënave përdori informacionin e miliona përdoruesve të Facebook-ut për të ndikuar në zgjedhjet politike, duke ngritur shqetësime të mëdha mbi privatësinë dhe etikën në epokën digjitale.

SI U MBLODHËN TË DHËNAT?

Në vitin 2013, një aplikacion i quajtur "**This Is Your Digital Life**", i krijuar nga **Aleksandr Kogan**, u përdor për të mbledhur të dhënat e përdoruesve të Facebook-ut. Ky aplikacion ishte një quiz psikologjik, ku përdoruesit plotësonin një sondazh për të analizuar personalitetin e tyre.

- **Problemi kryesor:**

- Aplikacioni nuk mblodhi vetëm të dhënat e përdoruesve që e plotësuan, por edhe të dhënat e miqve të tyre në Facebook, pa pëlqimin e tyre.
- Në total, u grumbulluan të dhënat e rreth 87 milionë përdoruesve

SI U PËRDORËN TË DHËNAT PËR MANIPULIM POLITIK?

Cambridge Analytica përdori këto të dhëna për të krijuar **profile psikologjike** të votuesve dhe për të zhvilluar strategji të personalizuara për fushatat politike.

- **Fushatat ku u përdorën të dhënat:**
- Zgjedhjet presidenciale në SHBA (2016): Cambridge Analytica ndihmoi fushatën e Donald Trump.
- Referendumi i Brexit-it në Mbretërinë e Bashkuar: Cambridge Analytica ndihmoi fushatën për daljen nga BE (Leave).
- **Si funksionoi manipulimi?**
- Përdoruesit u kategorizuan sipas sjelljes dhe preferencave të tyre.
- U krijuan mesazhe të personalizuara për të ndikuar në vendimet e tyre politike.
- Reklamat u shfaqën në Facebook për të forcuar bindjet e votuesve dhe për të ndikuar në zgjedhjet e tyre.

PASOJAT E SKANDALIT

- **Reagimi i Facebook:**
- Mark Zuckerberg kërkoi falje dhe dëshmoi para Kongresit Amerikan.
- Facebook u gjobit me 5 miliardë dollarë nga Komisioni Federal i Tregtisë në SHBA.
- Në Mbretërinë e Bashkuar, Facebook pagoi një gjobë prej 500,000£ për shkelje të privatësisë.

- **Ndikimi në publik:**
- Lëvizja #DeleteFacebook u përhap në internet, duke inkurajuar përdoruesit të fshinin llogaritë e tyre.
- U rrit ndërgjegjësimi mbi rreziqet e mbledhjes së të dhënave nga kompanitë teknologjike.
- Cambridge Analytica shpalli falimentimin në vitin 2018 pas skandalit.