CEDI

KONRAD ADENAUER STIFTUNG

SI TË MBROSH TË DHËNAT PERSONALE NË EPOKËN E TEKNOLOGJISË

Për informacione ose komente nund të drejtoheni në:

CEDI – QENDRA PËR ZHVILLIM DHE INTEGRIM EUROPIAN
Rr. Asim Zeneli, Nr. 15
Tiranë, Shqipëri
Tel: +355 695288494
qendra.cedi@gmail.com

KONRAD ADENAUER STIFTUNG, ALBANIA
Blv. Dëshmorët e Kombit
Kulla Binjake 1, K.11, Ap. 3
Tiranë, Shqipëri
Tel: +355 4 22 66525
www.kas.de/albanien

Përgatiti: MSc. Klara Kodra & MSc. Ina Xhepa

Përmbajtja

A e dini se?

- Ligji që garanton të dhënat personale të shtetasve shqiptar është ligji Nr. 9887, datë 10.03.2008 “Për Mbrojtjen e të Dhënave Personale”, i ndryshuar në 2012 & 2014.

- Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale është institucioni, që mbikqyr dhe kontrollon mbrojtjen e të dhënave personale.

- Autoriteti Kombëtar i Certifikimit Elektronik dhe Sigurisë Kibernetike (AKCESK) është institucioni, që mundëson mbrojtje në internet të fëmijëve, duke adresuar të gjitha rreziqet, kërcënimet dhe dëmet që fëmijët mund të hasin në botën digjitale.

- 11% e përdoruesve në internet në SHBA kanë qenë viktima të vjedhjes së të dhënave personale (detaje të kartave të kreditit, detaje të llogarisë bankare).[1]

1 https://mytechdecisions.com/network-security/10-online-privacy-facts/

- 41% e fëmijëve në SHBA nga mosha 8-17 vjeç kanë llogari publike në rrjetet sociale.
- 28 janari është Dita e Mbrojtjes së të Dhënave Personale.
- Në SHBA 1 në 50 fëmijë janë viktimë e vjedhjes së identitetit.[2]
- Vjedhja e indentitetit të fëmijëve është më e vështirë për tu zgjidhur nga autoritetet në krahasim më vjedhjen e identitetit të një të rrituri.
- 54% e fëmijëve që përdorin rrjetet sociale nuk supervizohen nga prindërit, fakt i cili shton 3 herë më tepër rrezikun për vjedhjen e identitetit të tyre.
- 85% e nënave në Shqipëri pranojnë që e përdorin internetin për t`i mbajtur të zënë fëmijët.[3]
- 83% e amerikanëve kanë tableta dhe 77% kanë smartfonë.
- Fëmijët e grupmoshës 8-12 vjeç qëndrojnë në internet mesatarisht rreth 6 orë në ditë, ndërsa mosha 13-18 vjeç deri në 9 orë.[4]

2 © 2021 Escalent https://javelinstrategy.com/research/child-identity-fraud-web-deception-and-loss

3 https://www.portalishkollor.al/kuriozitet/mbrojtja-e-femijeve-ne-internet-udhezues-per-prinderit

4 Po aty.

Përkufizime

- **Adresa e IP**, ose siç quhet ndryshe Protokolli i Internetit tuaj është një seri numrash që identifikon çdo pajisje e cila lidhet me internetin.[5]

- **Interneti** është sistem global i rrjetave të ndërlidhura kompjuterike, të cilat bëjnë shkëmbimin elektronik të të dhënave (tekst, muzikë video, fotografi, etj.,) nëpërmjet përdorimit të kabllove të bakrit, fibrave optike, lidhjeve pa tela dhe teknologjive të tjera. Këto informacione mund të lexohen, shikohen apo shkarkohen nga përdoruesit e tjerë. Pra interneti mundëson praktikisht komunikimin nga një pajisje kompjuterike në tjetrën.[6]

- **IMEI** është një kod identifikimi unik nga 15-17 shifra me të cilin është i pajisur çdo aparat telefonik. Ky kod shërben për të identifikuar të dhënat personale që konsistojnë në thirrjet hyrëse ose

5 https://www.avast.com/c-ëëhat-is-an-ip-address

6 https://www.idp.al/wp-content/uploads/2017/10/Kuadri_i_aftesimit_te_mesuesve.pdf

dalëse, nga organet të njohura nga legjislacioni shqiptar apo inteligjencës digjitale duke lokalizuar pajisjen tuaj telefonike me një saktësi prej disa metrash nga vendi ku pajisja ndodhet.[7]

- **Rrjete sociale** janë adresa në internet ose aplikacione që lejojnë përdoruesit të lidhen, komunikojnë, të shpërndajnë informacion dhe të krijojnë marrëdhënie me personat e tjerë që janë përdorues të rrjeteve sociale.[8] [P.sh Instagram, TikTok, Facebook etj].

- **Cyber-Bullying** është një formë e bullizmit përmes teknologjisë e njohur në Shqipëri si "Bullizmi kibernetik" dhe që përfshin: dërgimin, postimin, shpërndarjen e materialeve me përmbajtje negative, fallco, keqdashëse, të cilat kanë lidhje me një person tjetër.

- Bullizmi kibernetik mund të bëhet përmes shpërndarjes së informacioneve personale të dikujt duke i shkaktuar këtij të fundit poshtërim apo turpërim.[9]

- **E dhënë personale** është çdo informacion që mundëson identifikimin e një personi si: Emri, mbiemri, datëlindja, adresa postare ose e e-mailit, numri i telefonit, numri identifikues, numri i patentës, shenjat e gishtërinjve, ADN-ja, fotografitë, numri i sigurimeve shoqërore, llogari bankare (të dhëna financiare). Këto të dhëna identifikojnë individët, qoftë direkt ose indirekt.[10]

7 https://www.techtarget.com/whatis/definition/IMEI-International-Mobile-Equipment-Identity

8 https://www.techtarget.com/whatis/definition/social-media

9 https://www.stopbullying.gov/cyberbullying/ëëhat-is-it

10 Këshilluesit e Vegjël për Sigurinë Online AKCESK dhe UNICEF, Tiranë 2018

- **E-Mail** është postë elektronike, e cila është një mënyrë komunikimi që kryhet duke përdorur mjetet elektronike për të shpërndarë mesazhe elektronike në sistemin kompjuterik.[11]

- **Profili Online** është informacion i postuar në internet publikisht dhe/ose privatisht.[12]

- **Virus** është një software që dëmton kompjuterin: vjedhje të dhënash, fshirje skedarësh. Viruset zakonisht shkaktohen dhe instalohen aksidentalisht nga skedar në internet.[13]

- **Social Networking** është një faqe interneti ku dikush lidhet me ata që ndajnë interesa personale apo profesionale.[14]

- **Blogging** është një praktikë në rritje ku njerëzit dërgojnë mesazhe në Web në formë ditari.[15]

- **Fëmijë** është çdo person nën moshën 18 vjeç.

11 Po aty

12 Po aty

13 Po aty

14 Po aty

15 Po aty

Hyrje

Në një botë ku Interneti përshkon pothuajse çdo aspekt të jetës moderne, mbajtja e përdoruesve të rinj të sigurt në internet është një çështje gjithnjë e më urgjente për çdo vend. Interneti ka evoluar përtej njohjes dhe është një burim pafundësisht i pasur për fëmijët për të luajtur dhe për të mësuar. Ai është bërë gjithashtu një vend shumë më i rrezikshëm për ata që e përdorin atë pa mbikqyerjen e një të rrituri.

Një nga çështjet e privatësisë për fëmijët lidhet me përmbajtjen e dhunshme dhe të papërshtatshme, me mashtruesit në Internet, abuzimin seksual dhe shfrytëzimin. Këto janë disa nga fenomenet me të cilat po përballën fëmijët e ditëve të sotme kur lundrojnë të pasigurtë në internet. Kërcënimet po shtohen dhe autorët e këtyre veprimve vijnë nga vende të ndryshme.[16]

16 Manual për Fëmijët Për Sigurinë në Internet, botim i vitit 2022 nga AKCESK ne bashkepunim me ITU-në.

Teknologjia në ditët e sotme është e pranishme kudo dhe në jetën e gjithkujt dhe mund të gjendet në forma nga më të ndryshmet. Një ndikim të jashtëzakonshëm ka pasur edhe pandemia e COVID-19, gjatë së cilës bota u mësua të funksionontе thuajse krejtësisht në mënyrë digjitale. Nga ky moment çdo gjë nisi të digjitalizohet dhe teknologjia u bë akoma më e pranishme në jetët e të gjithëve. Jeta reale dhe ajo virtuale u bashkuan me njëra-tjetrën, duke qenë se dalja nga shtëpia dhe kontakti fizik me njerëzit ishte i ndaluar dhe i rrezikshëm. Digjitalizimi dhe teknologjia ndihmuan në vazhdimin e jetës. Shkollat zhvilluan mësimet e tyre përmes internetit, kompanitë dhe punonjësit filluan gjithashtu të punonin virtualisht. Si pasojë, teknologjia filloi të përdorej akoma më shumë dhe për rrjedhojë të zhvillohej me ritme të shpejta, bashkë me këtë zhvillim vijnë dhe disa rreziqe të shtuara.

Me zhvillimet e mëdha teknologjike, **të dhënat personale**, janë ato që rrezikohen më tepër. Siç mund ta kuptojmë edhe prej emërtimit, këto të dhëna lidhen ngushtësisht me personin që i zotëron ato. Duke qenë se këto të dhëna janë shumë të rëndësishme, ato duhet të mbrohen në mënyrë të veçantë nga ligji dhe institucionet. Në vendin tonë ekziston një ligj i posaçëm për mbrojtjen e këtyre të dhënave[17]. Ndërsa institucioni, që mbikëqyr dhe kontrollon mbrojtjen e të dhënave personale quhet Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale.

Epoka në të cilën po jetojmë njihet si epoka e digjitalizimit. Fëmijët janë një nga grupet subjektet kryesore të dhënat personale të të cilëve duhen mbrojtur në mënyrë të veçantë. Kjo ndodh pasi fëmijët jo gjithmonë janë në dijeni të çdo rreziku që mund t'ju vijë nga përdorimi i pakujdesshëm i internetit.

17 I ndryshuar me ligjin nr. 48/2012, datë 26.04.2012 & I ndryshuar me ligjin nr.120/2014.

Interneti sot përdoret gjerësisht nga fëmijët e moshave të ndryshme.[18] Një studim i vitit 2014 i zhvilluar nga World Vision Albania, që ka intervistuar 900 fëmijë shqiptarë të grupmoshës 13-18 vjeç, ka evidentuar se 47% e kësaj grupmoshe janë kontaktuar online nga një individ gjatë vitit të fundit. Fëmijët janë të "zbuluar" dhe shumicën e kohës të pa mbikqyrur, si dhe të pambrojtur gjatë lundrimit të tyre në internet. Ju mund të jeni viktima të vjedhjes së të dhënave personale, siç mund të jenë emri, fotografitë, llogaritë e rrjeteve sociale, bullizmit kibernetik etj.

Për këto arsye, kemi vendosur të përgatitim këtë broshurë me qëllim sensibilizimin dhe ndërgjegjësimin tuaj, prindërve dhe mësuesve për mbrojtjen e të dhënave tuaja personale. Duke qenë se kjo epokë teknologjike ju jep mundësi të shumta për të lundruar në internet dhe për të shpërndarë detaje të ndryshme nga jeta juaj, përdorimi sa më i kujdesshëm i internetit luan një rol kyç në mbrojtjen e të dhënave personale.

18 https://www.idp.al/wp-content/uploads/2017/02/Studimi_privatesia_dhe_siguria_e_te_dhenave_botim_2016.pdf

I. Mbrojtja e të dhënave personale në epokën digjitale

1.1. Si lindi mbrojtja e të dhënave personale dhe mekanizmat ndërkombëtare

Të dhënat personale lidhen ngushtësisht me të drejtën e privatësisë dhe sigurinë e sistemeve që përpunojnë këto të dhëna. Në bazë të kësaj të drejte, të gjithëve i'u lind e drejta që të dhënat e tyre personale të mbrohen, të mos keqpërdoren si dhe të mos bëhen publike. Për këtë do të flasim se ku e ka zanafillën mbrojtja e këtyre të dhënave.

Në vitet **1970** kompjuterat po përdoreshin gjithnjë e më shumë për të përpunuar informacion rreth personave. Po ashtu me zhvillimin e tregëtisë ndërkufitare, e cila solli përfitime mjaft të mira ekonomike, nisën të ngriheshin shqetësime mbi mbrojtjen e privatësisë dhe për rrjedhojë lindi nevoja për vendosjen e një ekuilibri dhe më tej standardeve përsa i përket mbrojtjes së privatësisë dhe tregëtisë së lirë.[19]

19 https://www.youtube.com/watch?v=hFbmkFUFGpk

Dy kanë qenë instrumetet e para të rëndësishme që kanë vendosur standardin dhe njëherësh njohur të drejtën e privatësisë.

1948 *Deklarata Universale e të drejtave të Njeriut (DUDNJ)* në nenin 12 të saj parashikon se drejta e jetës private garantohet si e drejtë themelore, por nuk del qartazi mbrojtja e të dhënave personale.

1948 *George Orwell shkruan romanin 1984* i cili flet mbi të ardhmen, mbikqyrjen, censurën. Në këtë libër flitet për super-shtetin e Oqeanisë në cilin banorët nuk kanë privatësi. Hapësirat publike dhe private janë të mbushura me kamera dhe mikrofona. Edhe mendimi kontrollohet nga agjentë të fshehtë të "Policisë së Mendimit".[20]

1950 U përgatit dhe u nënshkrua *Konventa Evropiane për të Drejtat e Njeriut*. Kjo Konventë mbron të drejtat e njeriut për qytetarët e 46 shteteve anëtare dhe njëherësh parashikon të drejtën e respektimit të jetës private dhe e jetës në familje. Sipas Konventës kjo e drejtë nuk mund të shkelet përveçse kur ligji e lejon një gjë të tillë.[21]

Në nivelin e Bashkimit Evropian *Rezolutat e BE-së 73/22 dhe 74/29* mbrojnë në mënyrë të dedikuar të drejtën e privatësisë.

20 https://safecomputing.umich.edu/privacy/history-of-privacy-timeline

21 ©Council of Europe

1980 Organizata për Zhvillim dhe Bashkëpunim Ekonomik (OECD) nxori *Udhëzues për Mbrojtjen e Privatësisë dhe Rrjedhjen Ndërkufitare të të Dhënave Personale*. Udhëzuesit kishin dy qëllime kryesore: të pasqyronin standardet e privatësisë dhe të lehtësonin rrjedhjen e lirë të informacionit sipas parashikimeve të ligjit.[22]

1981 Këshilli i Evropës miratoi *Koventën 108*, e cila ishte instrumenti i parë ndërkombëtar me fuqi detyruese në fushën e mbrojtjes së të dhënave personale. Ajo ndalonte procesimin e të dhënave personale specifike që lidheshin me: racën, bindjet politike, shendëtin, denimet penale etj.

1989 *Konventa e OKB-së për të Drejtat e Fëmijës* garanton mbrojtje për të gjitha aspektet e jetës së një fëmije. Konventa shpjegon sesi të rriturit dhe qeveritë duhet të punojnë bashku për të siguruar gëzimin e këtyre të drejtave nga të gjithë fëmijët. Konventa në nenet 10 dhe 16 të saj garanton mbrojtje për jetën familjare dhe private të fëmijëve.

1995 *Direktiva për Mbrojtjen e të Dhënave Personale* në BE ri-harmonizoi legjislacionin por njëherësh solli dhe disa ndryshime të nevojshme.

2009 Mbrojtja e kësaj të drejte në kuadër të Bashkimit Evropian përbëhet nga *Karta e të Drejtave Themelore e BE-së*. Kështu, në nenin 7 të Kartës parashikohet e drejta e privatësisë duke specifikuar se *çdokush ka të drejtën e respektimit të jetës se tij private dhe familjare, banesës dhe korrespondencës.* Ndërsa në nenin 8 parashtrohet se *çdo individ gëzon të*

22 https://ccdcoe.org/incyder-articles/the-oecd-issues-revised-privacy-guidelines/

drejtën e mbrojtjes së të dhënave personale që i përkasin dhe se këto të dhëna duhet të përpunohen me drejtësi për qëllime specifike dhe mbi parimin e bashkëpunimit të personave të interesuar ose te tjera parime bazë të lejuara nga ligji. Çdokush ka të drejtën të njhet me të dhëna që lidhen me vete atë dhe të drejtën për t'i ndryshuar ato.

2018 Komisioni Evropian e vijoi punën e tij për vite me radhë sidomos midis 2009 deri më 2016 për të zëvendësuar Direktivën e vitit 1995 me *Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave Personale (GDPR)*, e cila hyri në fuqi në 2018. GDPR është **ligji më i fortë për privatësinë dhe sigurinë në botë**, e cila mbron më mirë të dhënat personale. Njëherësh GDPR rriti përgjegjësinë dhe kompetencat shtesë për autoritetet mbikëqyrëse. Në po këtë vit, Këshilli i Evropës bëri modernizimin e Konventës 108[23], e njohur tani si *Konventa 108+*,[24] duke ndjekur dy objektiva kryesore që lidheshin me trajtimin e sfidave që rrjedhin nga përdorimi i teknologjive të reja të informacionit dhe komunikimit si dhe forcimin e zbatimit efektiv të Konventës.

23 Deri më tani palë në këtë konventë janë 55 shtete. Edhe Shqipëria e ka nënshkruar dhe bërë pjesë të legjislacionit të saj këtë Konventë.

24 Shqipëria ka miratuar me anë të Ligjit nr. 49/2022 dhe Ligjit nr. 49/2022, datë 12.05.2022, "Për ratifikimin e Protokollit ndryshues të Konventës "Për mbrojtjen e individëve, në lidhje me përpunimin automatik të të dhënave personale **(Konventa 108+)** si edhe me Ligjin nr. 45/2022 Ligji nr. 45/2022, datë 28.04.2022 "Për ratifikimin e Konventës së Këshillit të Evropës "Për aksesin në dokumenta zyrtare (Konventa 205)"

1.1.1 Mekanizmat inctitucionale ndërkombëtare

Gjykata Evropiane e të Drejtave të Njeriut, në Strasburg është arbitri i Konventës Evropiane për të Drejtat e Njeriut e cila merr në shqyrtim kërkesat e individëve për shkelje mbi të drejtat e njeriut nga shtetet antare në të clat bën pjesë dhe Shqipëria.

Organi kompetent në interpretimin e legjislacionit të BE-së është ***Gjykata e Drejtësisë të Bashkimit Evropian*** në Luksemburg, e cila garanton mbrojtjen e të drejtave themelore të njeriut brenda BE-së.

Komiteti për të Drejtat e Fëmijës[25], i cili përbëhet nga 18 ekspertë të pavarur, është organi monitorues i Konventës për të Drejtat e Fëmijës dhe tre Protokollet e saj Opsionale.

1.2. Mbrojtja e të dhënave personale në Shqipëri

Shqipëria nuk ka ende një ligj që mbron posaçërisht të dhënat personale të fëmijëve, por kjo nuk do të thotë që këto të drejta nuk mbrohen.[26] Le të mësojmë pak më tepër sesi është zhvilluar në Shqipëri në rend kronologjik mbrojtja e jetës pivate dhe mbrojtja e të dhënave personale.

1925 *Statuti Themeltar të Republikës së Shqipërisë (1925)* mbronte paprekshmërinë e banesës dhe fshehtësinë e korrespondencës postare, megjithëse kuptimi i këtyre të drejtave nuk ishte ai i sotmi.

25 Shqipëria e ka ratifikuar këtë Konventë në vitin 1991.

26 Manual Mbrojtja e të dhënave personale, sfidë e shoqërive post modern, CEDI& KAS

1928 Në këtë vit ndodhi ndryshimi nga Republikë në monarki dhe për rrjedhojë dhe Statuti Themeltar i Republikës së Shqipërisë ndryshoi në *Statutin Themeltar të Mbretërisë Shqiptare*. Megjithatë mbrojtja ngeli e njëjtë si në ligjin e mëparshëm.

1976 *Kushtetuta e Republikës Populllore Socialiste të Shqipërisë*, e parashikonte të drejtën për jetë private dhe familjare, por ajo ishte e cunguar. Pavarësisht se njihej fshehtësia e korrespondencës në Kushtetutë, kjo e drejtë nuk respektohej si e tillë nga vetë sistemi, duke ndërhyrë në korrespondencën e njerëzve, sidomos në komunikimet e bëra me jashtë.

1998 *Kushtetuta e Republikës së Shqipërisë* e ka konceptuar të drejtën për jetë private dhe familjare më të plotë nga sa është njohur deri në atë kohë nga ligji. Edhe pse Kushtetuta nuk e përmend spefikisht të drejtën për respektimin e jetës private dhe familjare (e drejta e privatësisë), Gjykata Kushtetuese i identifikon këto të drejta tek nenet 35 (mbrojtja e të dhënave personale), neni 36 (liria dhe fshehtësia e korrespondencës), neni 37 (paprekshmëria e banesës).

1999 U miratua *ligji i parë për mbrojtjen e të dhënave personale* në shtetin demokratik, ku rolin e mbrojtjes së këtyre të dhënave e kishte Avokatit të Popullit (Ombudsman).

2008 Në këtë vit u shfuqizua ligji i parë dhe hyri në fuqi *ligjin nr. 9887/2008 "Për mbrojtjen e të dhënave personale"*, që është në fuqi deri në këto momente.

Gjatë 3 mujorit të katërt të vitit 2023 *pritet të miratohet një ligj i ri* për mbrojtjen e të dhënave personale i cili është i përafruar plotësisht me Rregulloren e Përgjithshme për Mbrojtjen e të Dhënave Personale në BE (njohur shkurtimisht si "GDPR") dhe që garanton mbrojtje të këtyre të dhënave sipas standardeve evropiane.


Protection

1.2.1 Cilat janë institucionet që mbrojnë të dhënat personale në vendin tonë?

Institucioni që merret me mbrojtjen e të dhënave personale në Shqipëri është ***Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale***, i cili gëzon të drejtën të kryejë hetime administrative, të ketë akses në përpunimin e të dhënave personale dhe të mbledhë të gjithë informacionin e nevojshëm për të kryer detyrat e tij mbikëqyrëse. Komisioneri mund të urdhërojë bllokimin, fshirjen, shkatërrimin ose pezullimin e përpunimit të paligjshëm të të dhënave personale.

Shembull

P.sh. *Nëse marrim shembullin e Shqipërisë, para krijimit të platformës E-Albania, nëse një person dëshironte të merrte një dokument si Certifikatë Personale apo Certifikatë Familjare, duhet të shkonte pranë institucionit të Gjendjes Civile. Ndryshe ndodh sot, me zhvillimin e teknologjisë dhe digjitalizimin e regjistrave të të dhënave personale të personave, një dokument i tillë mund të aksesohet dhe të merret në mënyrë elektronike përmes platformës E-Albania pa qenë nevoja të shkohet në zyrën e Gjendjes Civile e të kërkohet një gjë e tillë.*

Por **KUJDES** *Institucionet përgjegjëse kanë detyrë të garantojnë mbatjen e sigurtë dhe përpunimin e të dhenave të gjendjes civile.*

Gjithashtu, institucione të ndryshme ruajnë të dhënat tuaja personale edhe nëse ju nuk mund ti aksesoni ato online. Kjo vjen si pasojë e digjitalizimit të regjistrave të të dhënave personale. Për këtë arsye, me zhvillimet teknologjike sado lehtësira mund të krijohen shtohen edhe rrezike të reja.

Shembull

P.sh. Një rrezik është edhe rasti i sulmeve kibernetike, siç ndodhi në Shqipëri në korrik 2022, ku viktimë e këtyre sulmeve ishte databaza e Agjencisë Kombëtare të Shoqërisë së Informacionit (AKSHI),[27] *e cila është agjencia që ruan dhe mirëmban shumicën e sistemeve të adminstratës publike. Të dhënat personale të shumë shtetasve shqiptarë dhe të huaj janë vjedhur gjatë këtij sulmi. Ky sulmi pati një rrezikshmëri të lartë pasi autorët mund t`i keqpërdorin këto informacione në mënyra të ndryshme dhe shantazhuese.*

Dalim në konkluzionin se nëse një sistem qeveritar arrin të depërtohet nga një sulm kibernetik, atëhere llogaritë e ndryshme në internet, apo sistemet e kompanive private siç janë bankat që kanë akses në të dhëna personale janë edhe më të rrezikuara. Për këto arsye është e nevojshme që të kemi një informacion të qartë dhe të gjerë lidhur me mbrojtjen e të dhënave personale në epokën digjitale në të cilën po jetojmë.

Gjithashtu, në nenin 134/e të Kushtetutës, thuhet se Komisioneri për të drejtën e informimit dhe mbrojtjen e të dhënave personale, në rast se ka një çështje që cenon interesat që Komisioneri përfaqëson, atëhere ai mund të vërë në lëvizje ***Gjykatën Kushtetuese***, institucion “roje” i Kushtetutës dhe të drejtave të mbrojtura prej saj.

27 ©AKSHI 2022

Ligji shqiptar për të realizuar një mbrojtje sa më të mirë të të dhënave personale dhe sigurisë së tyre në rrjetet publike ka parashikiuar një mbrojtje më të mirë për fëmijët, kjo jo vetëm në Ligjin për të Drejtat e Fëmijëve[28] edhe në ligjin "Për Sigurinë Kibernetike"[29], ku autoriteti përgjegjës është ***Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK)***, me qëllim t'ju vijë në ndihmë fëmijëve dhe të rinjve për raportuar përmbajtje të paligjshme/dëmshme të hasura gjatë lundrimit në internet duke krijuar një mjedis më të sigurt elektronik për fëmijët dhe të rinjtë në vend.[30]

Pasi u njohëm me historikun e evoluimit për mbrojtjen e të dhënave personale dhe privatësisë në kapitullin e ardhshëm do të njohim mënyrat sesi duhet të mbrohemi në internet dhe nga se duhet të kemi kujdes.

28 Ligji nr. 18/2017 "Për të drejtat e fëmijëve".

29 Ligji nr. 02/2017 "Për sigurinë kibernetike".

30 https://cesk.gov.al/raporto/

II. Të mbrojmë të dhënat tona personale

2.1. Të përmirësojmë njohuritë mbi mbrojtjen e të dhënave personale

Me siguri që prindërit dhe mësuesit ju kanë thënë, që duhet të mbroni të dhënat tuaja personale, duhet të bëni kujdes kur shpërndani informacion, fotografi, video me bashkëmoshatarët tuaj, qofshin këta edhe persona shumë të afërt.

Në rastet e personave, që nuk i njihni fare apo nuk kanë moshën tuaj, më të rriturit duhet t`ju paralajmërojnë të jeni shumë të kujdesshëm dhe në asnjë mënyrë të mos shpërndani këtë informacion. Në kapitullin e parë ne u njohëm më ligjet vendase dhe ato ndërkombëtare që mbrojnë jetën private dhe të dhënat personale dhe cilat institucione janë roja e këtyre akteve ligjore.

Tashmë jemi gati të eksplorojmë se çfarë duhet të mbrojmë. Ndonjëherë ne nuk e mendojmë se ndarja e të dhënave personale mund të na dëmtojë ne ose shokët tanë qoftë dhe përmes shpërndarjes së një informacioni, që në dukje mund të jetë i padëmshëm, siç p.sh. ndodh rëndom me ndarjen e fotografive në rrjtet sociale. Po për këtë do të flasim në vijim.

Fillimisht do të rikujtojmë dhe një herë se çfarë janë të dhënat personale.

Të dhënat personale janë çdo informacion për një person [individ], që është i identifikuar ose i identifikueshëm.

Të dhëna personale janë:

- Emri
- Mbiemri
- Adresa e shtëpisë
- Fotografia
- Shenjat biometrike në pasaportë ose Kartën e Identitetit
- Profesioni – Kualifikimet
- Të ardhurat
- Numri i telefonit

Por ka dhe një kategori e caktuar e të dhënave personale që konsiderohet që informacioni është më sensitiv për personin. Të dhëna të tilla quhen **të dhëna sensitive**[31] dhe në këtë kategori renditen:

- origjina racore ose etnike
- bindjet politike
- anëtarësimi në sindikata
- besimi fetar apo filozofik
- dënimet penale
- të dhëna për shëndetin dhe jetën seksuale.

31 Ligji nr. 9887, datë 10.03.2008 “Për Mbrojtjen e të Dhënave Personale” i ndryshuar.

Pra, disa të dhëna personale mund të konsiderohen veçanërisht sensitive, për shkak të natyrës intime të jetës private, mund të jenë burim i diskriminimit, ose mund t'i referohen të miturve.

Shpesh na ndodh që të ndajmë informacione me miqtë, shokët, prindërit tanë, por ndodh dhe që disa nga këto informacione nuk do donim t'i ndanim me të gjithë pasi i konsiderojmë private [jo se nuk lejohen apo janë të paligjshme për t'u ndarë].

Ju mund të keni 35 shokë në klasë, ose mund të keni 10 shokë në lagje, por informacione të caktuara zgjidhni ti ndani me një rreth shumë më të ngushtë, p.sh 2 ose 3 persona. Pra, në jetën e përditshme ne zgjedhim personat me të cilët duam të ndajmë informacionet.

Paralelisht e njëjta gjë ndodh në botën e internetit. Ju zgjidhni, që informacionin ta ndani me një grup të caktuar "shokësh" që ju i keni pranuar dhe ndjekur për të qenë miqtë tuaj virtualë.

Pyetjet që shtrohen janë:

- A i njihni të gjithë këta shokë/shoqe?
- A do donit që vendndodhjen tuaj, një foto poshtë shtëpisë apo në kafenenë që preferoni të shkoni ta dijë çdo njeri, qoftë dhe ky një i njohur i largët, që ju mbase e keni takuar vetëm një here?

Çdo situatë që parashtruam më sipër mund t'ju vendosë në rrezik ju, duke ju dhënë informacione të mjaftueshme keqbërësve, që mund të dinë vendin që ju preferoni, të dinë që jeni me pushime, ku e keni shkollën dhe ku jetoni.


SECURITY

Sa më i madh të jesh, aq më shumë mendimi yt duhet të merret parasysh. Kjo gjë ndodh si në familje ashtu dhe mes miqve tuaj.

Shembull

P.sh. nëse nuk doni që prindërit të publikojnë fotot, videot tuaja, atëherë ju keni të drejtë tua kërkoni atyre mos e bëjnë këtë gjë. E njëjta gjë dhe me shokët/shoqet tuaja. Nëse ju nuk jeni dakord që fotot tuaja të ndahen në internet atëherë ju duhet ti kundërshtoni.

Por me të drejtat vijnë dhe detyrimet. A do ta bënit të njëjtën gjë për shokët/shoqet tuaja.

Kur je para ekranit të kompjuterit një foto që keni bërë në klasë, një foto "gallatë" për ju, mund të mos jetë për shokun/shoqen që është pjesë e saj. Përpara se të bëni publikime merrni lejën dhe miratimin e çdo personi që është pjesë e fotos.

Këto janë të drejtat dhe detyrimet tuaja përsa i takon privatësisë. Rregullat janë të njëjta kudo dhe për gjithësecilin. Mbroni privatësinë tuaj.

2.2. Risqet e përdorimit të rrjeteve sociale

Tashmë do të kalojmë në një seksion që ndoshta në dukje mund të mos ju duket me rëndësi, por që paraqet rrezikshmëri të lartë.

Një fotografi e ndarë për dëshirë, një videolojë dhe komunikim me miq virtualë mund të jenë një rrezik për ju. Informacioni i shpërndarë mes miqve mund të kopjohet në mënyrë të thjeshtë e më pas të shpërndahet në mënyrë të pakujdesshme. Edhe pse ju mendoni se një fotografi nuk konsiderohet e dhënë apo informacion personal, gaboheni pasi ajo është e tillë pasi tregon fytyrën tuaj apo informacione të ndryshme të rëndësishme për ju.

Për këtë arsye, **duhet të keni shumë kujdes kur vendosni të shpërndani një fotografi në rrjete sociale apo t'ja dërgoni atë miqve tuaj përmes mesazheve**. Nëse keni postuar diçka në rrjete sociale është shumë e vështirë ose e pamundur që të ktheni mbrapsht informacionin që keni shpërndarë me anë të këtij postimi. Ndërsa, nëse një fotografi ia dërgoni një mikut tuaj, është thuajse e sigurt që kjo fotografi tashmë do të qëndrojë e ruajtur në pajisjen që miku juaj është duke përdorur. Në këtë moment lind rreziku, që fotografia tuaj të shpërndahet tek persona të ndryshëm të cilët ju nuk i njihni dhe që mund të keqpërdorin fotografitë tuaja e t'i shpërndajnë ato tek persona të tjerë. Njësoj si të rriturit, edhe fëmijët mund të jenë në rrezik kur bëhet fjalë për të dhënat personale. Të mos harrojmë se një fotografi që mund t'ja tregoni dikujt në jetën e përditshme në fund të ditës ajo mbetet e juaja, dhe dikush që thjesht e ka parë nuk ka mundësi ta riprodhojë dhe ta shpërndaje atë te të tjerët.

P.sh. ekziston një rrezik që identiteti i fëmijëve të vidhet dhe keqpërdoret nga persona të panjohur në rrjete sociale.

Vjedhja e identitetit për shkak të shfaqjes dhe zbulimit të më shumë informacioneve apo të dhënave personale seç duhet apo rekomandohet ndodh rëndom tek shumë të rritur. Për këtë arsye ky fenomen është akoma më i rrezikshëm tek fëmijët, duke qenë se fëmijët janë më pak të kujdesshëm gjatë përdorimit të internetit dhe rrjeteve sociale, ata pa vetëdijen e tyre ose në mënyrë të paqëllimshme mund të japin shumë detaje personale online, gjë që sjell një mundësi të lartë që identiteti i tyre të vidhet nga të tjerët.[32]

Edhe pse në përgjithësi, ju (fëmijët) i përdorni rrjetet sociale për lojra apo për të komunikuar me miqtë tuaj të cilët i njihni nga jeta e përditshme, duhet patur kujdes me atë që shpërndani me ta.

Pjesa e lojrave online ka një rrezikshmëri të theksuar për të dhënat tuaja personale, por gjithashtu edhe të prindërve tuaj. Edhe pse lojrat, ashtu si rrjetet sociale kanë një limit moshe të caktuar, jo të gjithë e respektojnë ose janë të sinqertë për këtë limit. Rreziqet që mund të vijnë nga luajtja e lojrave në internet mund të jenë nga më të ndryshmet.

Le të shikojmë më poshtë sesi ju mund të bini preh e keqpërdoruesve vetëm duke luajtur një lojë online.

Duke qenë se **lojrat kryesisht të viteve të fundit i krijojnë mundësi lojtarit që të komunikojë me pjesëtarët e tjerë të skuadrës gjatë lojës, kjo sjell një rrezik për të dhënat e fëmijëve që mund të vidhen nga keqbërës.** Shembulli më i thjeshtë është ai i dikujt që është i rritur dhe komunikon nëpërmjet lojës me një fëmijë. Dihet se komunikimi është i drejtpërdrejtë, por diferenca e moshës mund të jetë e madhe. Pra, nga njëra anë kemi një lojtar, që është fëmijë nën moshën 18 vjeç dhe nga ana tjetër kemi

32 internetmatters.org


SCANNING...

një person të rritur mbi 18 vjeç. Sigurisht që një fëmijë nuk i di të gjitha rreziqet që mund t'i vijnë gjatë lundrimit në internet, dhe është akoma më e vështirë, që të ruhet dhe të mendojë se ka rreziqe të tilla nga luajtja e një loje, për këtë arsye rrezikshmëria rritet.

Një person keqbërës gjatë komunikimit me një fëmijë nëpërmjet një videoloje mund të pyesë për informacione të ndryshme të cilat mund të jenë personale dhe në këtë mënyrë mund të vijojnë me vjedhjen e informacioneve të tjera. Pra, nëse dikush pyet një fëmijë gjatë luajtjes së një loje për të dhëna personale të tipit: emrin, vendin ku fëmija banon, vendin ku fëmija shkon në shkollë, ku e kalon kohën e lirë, me çfarë sporti merret, ku i punojnë prindërit etj., vendin e tyre të lindjes, vendin e lindjes së prindërve, datëlindjen e tyre apo të prindërve të tyre, një emër të kafshës shtëpiake etj., duhet të jeni shumë të kujdesshëm dhe të mos i jepni këto të dhëna.

Keqbërësve **iu mjaftojnë disa të dhëna kryesore për të vjedhur një llogari tuajën apo të prindërve tuaj,** duke qenë se njerëzit në përgjithësi vendosin në fjalëkalimet e tyre fjalë apo numra, që kanë të bëjnë me jetën e tyre siç mund të jetë viti i lindjes apo data e lindjes.[33] Në këtë mënyrë dikush me njohuri në vjedhjen e llogarive të rrjeteve sociale dhe të fjalëkalimeve mund të gjej fjalëkalimin tuaj ose të një llogarie në internet të prindërve tuaj dhe ta vjedhë atë. Kjo mund të sjellë **pasoja të ndryshme si vjedhje më pas të llogarive bankare, shantazhime të ndryshme** etj.

Pra, duhet të **jeni shumë të kujdesshëm edhe gjatë luajtjes së lojrave në internet** si dhe gjatë komunikimit me personat me të cilët luani, sidomos me ata që nuk i njihni. Sigurohuni që nuk duhet të vendosni emrin, apo asnjë të dhënë tuajën personale kur zgjidhni emrin e përdoruesit në një lojë në

33 © 2023 Cybernews

mënyrë që identiteti juaj të mbetet i panjohur për njerëzit e panjohur, si dhe të mos ndani me të tjerët të dhëna personale siç janë ato të përmendura më sipër.

Nëse hasni një person që nuk e njihni gjatë lundrimit tuaj në internet, por qoftë edhe në jetën e përditshme, sigurohuni që të mos u tregoni asnjë prej informacioneve tuaja personale. Nga shpërndarja e informacioneve private mund të vijnë pasoja të padëshiruara siç është shpërndarja edhe më e gjerë e kësaj e këtyre informacioneve nga personi të cilit ju ia keni dërguar te persona të tjerë. Kjo sjell pasiguri për të dhënat tuaja personale, si dhe rritjen e mundësisë që ju të jeni viktimë e talljeve të ndryshme, diskriminimit apo e bullizmit për shkak të informacionit që keni shpërndarë me një mikun tuaj apo në rrjet social.

Gjithashtu, ekzistojnë **persona** të ndryshëm në internet, që **shfrytëzojnë frikën tek fëmijët**. Ata i **kërcënojnë** duke u thënë se një gjë e keqe do u ndodhi prindërve të tyre nëse nuk shpërndajnë një informacion personal me këtë person të panjohur.

Këta keqbërës në internet mund të njohin disa të dhëna në lidhje me prindërit tuaj dhe kështu ata ushtrojnë presion ndaj jush duke iu thënë se e dinë se ku prindërit e tyre punojnë apo se ku ata banojnë. Kështu, fëmijët bien në këtë grackë dhe për shkak të frikës mund të shpërndajnë një informacion tepër personal, i cili nuk duhet shpërndarë me të tjerë. **Nëse gjendeni përpara një rasti të tillë, mos hezitoni të komunikoni me prindërit ose një të afërm të besuar pasi ata do të gjejnë zgjidhjen e duhur.** Nëse me të vërtetë ekziston një rrezik, komunikimi me policinë dhe denoncimi i ngjarjes do të sigurojë që ju apo familja tuaj nuk është në asnjë rrezik. Ajo çfarë është e rëndësishme është që **të mos frikësoheni para këtyre keqbërësve**, të cilët duan të përfitojnë nga frika juaj në mënyrë që të përfitojnë dhe të marrin të dhënat tuaja personale.

Për më tepër në rastet kur ju duhet të drejtoheni për ndihmë dhe këshilla në rast rreziku në internet janë si më poshtë:

ALO 116 111 www.alo116.al/ internet-i-sigurte- raporto-online	Policia 112 dhe 129	Punonjësit e Njësisë Së Mbrojtjes së Fëmijës në Bashkinë tuaj	Drejtori i Shkollës Mësuesi, Psikologu/ Punonjësi Social në shkollë

Disa nga rrjetet sociale që mund të përdoren nga fëmijët duke filluar që nga mosha 13 vjeç e sipër janë:[34]

- TikTok
- Instagram
- Facebook
- Snapchat
- Tëitter
- Youtube
- Discord
- Twitch
- Reddit
- Ask.fm
- Omegle

16 vjeç e sipër:

- WhatsApp
- Linkedin
- Flickr
- Tumblr.

34 internetmatters.org™

Online issues

What issues could be affecting your children? Get to grips with what they may come across on the internet and how to get help if you need it. Find out what to do if you're worried about anything you or your child has seen online.

Identity Theft

Screen Time

Fake News and

Inappropriate

Cyberbullying

Self Harm

Radicalisation

Online Reputation

Online Grooming

Pornography

2.3. Si të zhvillojmë potencialin tonë si "qytetarë digjital"?

Në epokën në të cilën jetojmë, me gjithë zhvillimet teknologjike dhe internetin bombardohemi më informacion të pafundëm, i cili shpesh mund të jetë i duhuri dhe po aq shpesh apo më tepër mund të jetë i gabuar. Lehtësia për të hapur një media digjitale, një kanal në youtube, një blog i bën njerëzit që të mendojnë se mund të jenë gazetarë të paparë. Këtu qëndron sekreti dhe zgjuarsia juaj, **duke parë më kujdes burimin nga jeni duke e marrë këtë informacion** si dhe duke parë **dhe burime të tjera për t'u siguruar për informacionin që po merrni**. Kontrolloni me kujdes politikat e privatësisë të faqeve ku lundroni dhe shihni me kujdes si përdoren këto të dhëna që mblidhen nga ju.

Mbani në vëmendje, **të dhënat tuaja duhet të përpunohen në mënyrë të drejtë dhe të ligjshme.** Përpunimi i të dhënave personale duhet të plotësojë kushtet përkatëse për "përpunim", i cili nënkupton grumbullimin, përdorimin, zbulimin, mbajtjen, ndreqjen, fshirjen, transmetimin, transferimin ndërkombëtar të të dhënave personale si dhe shkatërrimin e tyre. Përpunimi i drejtë në përgjithësi kërkon transparencë me individët se si do të përdoren informacionet e tyre.

Të dhënat personale **duhet të grumbullohen për qëllime specifike dhe të ligjshme.** Të dhënat nuk duhet të përpunohen më tej apo në ndonjë mënyrë të papajtueshme me këto qëllime. Kjo kërkesë synon të sigurojë, që kontrolluesit të jenë të hapur në lidhje me qëllimet për mbledhjen e të dhënave personale dhe se përdorimi i informacionit është në përputhje me këto qëllime. Në praktikë, do të thotë se ju duhet të jeni të qartë që nga fillimi sepse i keni mbledhur të dhënat personale dhe atë që keni ndërmend të bëni me to.

Të dhënat personale duhet të jenë **të sakta dhe kur është e nevojshme të përditësohen**.

Përdorni në mënyrë të kontrolluar informacionin personal përmes:

- ***Vendosjes së një fjalëkalim ose pin mjaft të komplikuar***, duke shmangur të përdorni emrin tuaj, datën e lindjes, emrat e familjarëve ose kafshëve shtëpiake, apo çfarëdo fjale që është lehtësisht e kopjueshme. Vendosni një kod bllokimi që aktivizohet automatikisht kur telefoni është i ndezur por nuk është në përdorim për një kohë të caktuar. Gjithashtu, në këtë rast është mirë të shmangen kodet pak a shumë të lehtë për t'u zbuluar.

- ***Ruani numrin IMEI,*** të cilin mund ta gjeni në kutinë e produktit që keni blerë dhe në rast të vjedhjes ose humbjes së aparatit tuaj smartphone ose tablet mund ta përdorni për ta bllokuar në distancë.

- Sigurohuni që faqet e vizituara ***të përmbajnë protokollin e autentifikimit https***. Kujdes të veçantë duhet pasur për sigurinë në përdorimin e faqeve bankare apo dhe emailit.

- ***Instaloni antiviruse -*** Në këtë mënyrë ju mbroni paisjen tuaj me programe të sigurisë si, Firewalls - Antivirus – Antispyware.

- ***Kujdes nga link-et që ju shfaqen në e-mail***, mesazhe, spame (junk mail) apo chat-e të ndryshme. Ato mund të përmbajnë viruse apo përmbajtje të tjera të padëshiruara.

- Bëni ***kujdes në ruajtjen e informacionit personal në smartphone dhe tablet***, sepse këto mund të humbasin, vidhen apo sulmohen nga piratët elektronikë. Për këto arsye, ju kurrë nuk duhet të mbani fjalëkalimet, kodet e hyrjes dhe të dhënat bankare në mënyrë të dukshme.

— ***2 step authorization*** është një masë sigurie që të gjithë duhet ta aktivizojmë në llogaritë tona të ndryshme. Qoftë për e-mail apo për rrjete sociale, procesi i autorizimit me dy hapa është i mundur dhe shumë efektiv. Nëpërmjet aktivizimit të këtij opsioni, ju do të keni një siguri më të lartë në llogaritë tuaja online.

Si funksionon ky opsion? Është shumë e thjeshtë, pasi e keni aktivizuar opsionin do ju kërkohet në shumicën e rasteve të vendosni numrin e telefonit tuaj në hapësirën e kërkuar. Më pas, do ju vijë një mesazh në telefon me një kod verifikimi të cilin përsëri do të duhet ta vendosni në hapësirën bosh të kërkuar. Pasi e keni verifikuar numrin tuaj të telefonit, autorizimi me dy hapa do të jetë i aktivizuar. Që nga ky moment, çdo herë që ju do të hyni në një nga llogaritë tuaja, do të njoftoheni me mesazh në telefonin tuaj. Mesazhi përmban një kod disa shifror, të cilin ju më pas duhet ta shkruani në hapësirën e kërkuar në mënyrë që të kyçeni në llogarinë tuaj. Kështu, nëse dikush ju ka vjedhur emrin e përdoruesit dhe fjalëkalimin e një llogarie tuajën në rrjet, ai/ajo nuk do të mund të kyçet në llogarinë tuaj për shkak të autorizimit me dy hapa, pasi nuk do të kenë mundësi të aksesojnë kodin i cili vjen në formë mesazhi në telefonin tuaj në kohën kur dikush po mundohet të kyçet në llogari.

2.4. Guidat e privatësisë së rrjeteve sociale

Duke qenë se është thuajse e pamundur për një fëmijë mbi moshën 13 vjeç, që të qëndrojë larg rrjeteve sociale, ka mënyra të ndryshme për ta bërë eksperiencën në këto rrjete më të këndshme dhe të sigurt nga ana juaj si fëmijë. Të dhënat tuaja personale mbrohen me ligj dhe përveç institucioneve përkatëse që mbrojnë këto të dhëna, në krahun tuaj keni gjithmonë prindërit të cilët ju mbrojnë ju dhe të dhënat tuaja në çdo moment.

Prindërit janë ata që i'u mbrojnë juve në çdo aspekt në jetën tuaj. Për këtë arsye është mirë që t'i lejoni ata të kontrollojnë aktivitetin tuaj gjatë lundrimit në internet dhe përdorimit të rrjeteve sociale. Disa nga arsyet e mira që të lejoni kontrollin prindëror gjatë përdorimit të internetit dhe rrjeteve sociale janë:

Google Safe Search është një mënyrë kontrolli që prindërit mund të përdorin për ta bërë më të sigurt lundrimin tuaj në internet. Nëpërmjet këtij opsioni, prindërit mund të vendosin se në çfarë faqesh internet ju do të keni akses, të limitojnë aksesin tuaj në faqe që mund të jenë të dëmshme për shëndetin tuaj mendor ose që mund të kenë një influencë negative te ju.

Për këtë arsye, disa nga rrjetet sociale kryesore që përdoren nga fëmijët në ditët e sotme siç janë *TikTok, apo Instagram* parashikojnë disa opsione të veçanta përmes të cilave prindi juaj mund tju ndihmojë të lundroni të sigurt në rrjete sociale të ndryshme.

P.sh., në rastin e *TikTok*, i cili është një nga rrjetet sociale më të përdorur nga fëmijët ku rreth 30% e gjithë përdoruesve të programit janë nën moshën 18 vjeçare[35], është e mundur që nëpërmjet një opsioni prindi juaj të monitorojë përdorimin e këtij aplikacioni. Një guidë e tillë mund të gjendet në Keeping TikTok family-friendly.[36] Siç mund ta shihni në seksionin e parë jepen në mënyrë të detajuar hapat që duhet të ndiqni në mënyrë që të përdorni opsionin e **"Family pairing"** dhe pas aktivizimit të këtij opsioni prindi juaj do të mund të kryejë disa veprimtari monitoruese mbi llogarinë tuaj në rrjetin social TikTok.

35 cyberpurify

36 https://www.internetmatters.org/parental-controls/social-media/tiktok-privacy-and-safety-settings/ .

Ndër to janë:

- Të vendosin një limit të kohës suaj të lundrimit në aplikacion.
- Të përcaktojnë se cilat janë ato përmbajtje të aplikacionit që nuk janë të përshtatshme për ju dhe moshën tuaj.
- Të menaxhojnë opsionet e privatësisë dhe sigurisë suaj.
- Të zgjedhin nëse llogaria juaj do të jetë publike apo private.

III. Ju mund të jeni këshilluesit

Gjatë këtyre 25 viteve, zhvillimi i teknologjisë ka qenë një nga ngjarjet kryesore në shoqërinë tonë. Me zhvillimet e shpejta të teknologjisë ka ndryshuar rrjedhimisht dhe mënyra se si fëmijët ndërveprojnë dhe marrin pjesë në jetën e përditshme të botës përreth tyre.[37]

Kështu, fëmijët në mënyrë të veçantë kanë një pafundësi mënyrash dhe mundësish për të mësuar, për të shpërndarë dhe për të komunikuar. Përdorimi i TIK sjell risi, zhvillime dhe lehtësira të mëdha për fëmijët dhe njerëzit e tjerë, por nga ana tjetër sjell edhe rreziqe të mëdha për fëmijët në veçanti.

Fëmijët janë aktori kryesor kur bëhet fjalë për mbrojtjen e të dhënave të tyre personale. Bashkëpunimi me personat më të rritur se ta dhe që janë përgjegjës për ta luan një rol kyç në sigurimin e mbrojtjes së të dhënave personale të tyre. Për këtë arsye, fëmijet duhet, përveçse të jenë të kujdesshëm gjatë lundrimit të tyre në internet, edhe të kërkojnë ndihmë nga më të rriturit për diçka që nuk e kuptojnë, apo për të dhënat që u kërkohen në internet. Në ndihmë për çdo gjë do u vijnë fëmijëve në çdo mo-

37 ©United Nations Children's Fund (UNICEF), fq. 5, 2015

ment prindërit e tyre në radhë të parë, mësuesit dhe shkolla si dhe gjithë institucionet përgjegjëse. E rëndësishme është të mos nguroni të kërkoni ndihmë në rast se një informacion apo e dhënë e juaja personale është shpërndarë kundër vullnetit tuaj.

3.1 Ti dhe Familja në përdorimin e rrjeteve sociale[38]

Kur vjen puna për edukim dhe për ndërgjegjësim, gjithmonë mendohet se është prindi ai që duhet të edukojë fëmijën për gjëra të ndryshme. Por, me ndryshimet e shpejta dhe të shpeshta të teknologjisë, ndonjëherë janë fëmijët ata që janë më të prirur drejt kuptimit më të mirë të teknologjisë.

Fëmijët mund të edukojnë prindërit për atë se çfarë ndodh në internet dhe rrjete sociale, në mënyrë që prindërit të mund të mbrojnë fëmijët e tyre dhe të dhënat e tyre personale. Fokusi kryesor qëndron tek teknologjia, kjo vjen si pasojë e digjitalizimit të thuajse çdo gjëje.

Tashmë çdo informacion personal mund të aksesohet online nga vet ju ose prindi juaj, pa patur nevojë të shkohet nëpër zyra të ndryshme shtetërore. Kjo sjell një lehtësi, por nga ana tjetër edhe një rrezikshmëri të shtuar për fëmijët të cilët mund të jenë të pakujdesshëm me të dhënat e tyre personale, gjë që do të sillte vjedhjen apo sulmimin e tyre.

Rekomandime për prindërit për mbrojtjen në mënyrë sa më të mirë të të dhënave tuaja personale:

38 *https://www.capcertified.com/the-pros-and-cons-of-parental-controls/*

- Prindërit duhet të kenë kujdes se çfarë vendosin të postojnë në rrjete sociale lidhur me fëmijët e tyre. Postime të cilat tregojnë se në çfarë shkolle, klase, apo se çfare kursesh fëmijët frekuentojnë rrisin rrezikshmërinë që dikush të mund të aksesojë të dhënat tuaja personale me keqdashje.

- Kërkojini prindërve tuaj të vendosin një shembull të mirë që ju të mund ta ndiqni atë. Duke qenë se fëmijët imitojnë veprimet e prindërve, është e sigurt se nëse një prind nuk tregohet i kujdesshëm në atë që shperndan në rrjete sociale, as fëmija nuk do ta bëjë. Nëse prindi poston çdo gjë në rrjetet sociale pa patur kujdes apo pa menduar për mundësinë e nxjerrjes së të dhënave të tij personale në rrjete sociale, atëherë edhe fëmija do të tregohet i pakujdesshëm. Kjo sjellje rrit rrezikshmërinë dhe mundësinë për vjedhje të të dhënave personale të fëmijëve.

- Kërkojini prindërve t'ju edukojnë lidhur me rreziqet në internet. Edhe pse ju mund të njihni internetin dhe teknologjinë më mirë se ata, prindërit janë ata që mund t'ju shpjegojnë në mënyrën më të mirë se çfarë rreziqesh sjell një veprim i caktuar në internet.

- Kërkojini prindërve tuaj tju monitorojnë lundrimin tuaj në internet në mënyrë që ju të jeni sa më të sigurt.

- Kërkojini prindërve që të informohen lidhur me mënyrat e mbrojtjes së të dhënave personale të tyret apo tuajat. Institucioni që merret me mbrojtjen e të dhënave personale në Shqipëri quhet "Komisioneri për të drejtën e informimit dhe mbrojtjen e të dhënave personale". Në linkun e mëposhtëm mund të gjeni broshura të ndryshme për tja treguar prindërve lidhur me fushën e të dhënave personale (https://www.idp.al/broshura-mbrojtja-e-te-dhenave-personale/)

Shtojca

Shembuj të bullizmit në rrjete sociale

A është një vajzë në klasën e 7-të, e cila ishte kontaktuar nga B, një mashkull i panjohur online. Gjatë komunikimit të tyre me videokamer, B i mbush mendjen A që ti tregojë atij pjesët e saj intime. Në këtë moment B fotografon pamjen e A, dhe më pas fillon një seri bullizmi online duke e kërcënuar A se këto foto do ti shpërndante me miqtë e saj. Ai i kërkon asaj që të merrte pjesë në një telefonatë tjetër me videokamer me persona të panjohur, ku ajo do të zbulonte përsëri pjesë intime të sajat, dhe nëse nuk e bënte këtë gjë atëher B do të shpërndante fotot intime të A.

Pasi A refuzoi ta bënte një gjë të tillë, B i shpërndau fotot e A online ku të gjithë të mund t'i shihnin. Për shkak të këtyre ngjarjeve të bullizmit online, A ndërroi shtëpi duke u zhvendosur në një qytet tjetër. Por, pavarësisht kësaj bullizuesit online nuk ndaleshin, duke vijuar me ngacmimet për shkak se kishin në dispozicion të dhënat e saj personale.

Shembull i vjedhjes së identitetit të fëmijëve

A është një djalë 18 vjeç, i cili vendos që të regjistrohet në kursin e patentës. Pas kryerjes me sukses të testimeve ai vazhdoi procedurën në mënyrë që të merrte kartonin e lejes së drejtimit. Në momentin kur ai aplikoi për të marrë këtë karton, punonjësi e njofton se ai e zotëron një leje drejtimi. I habitur, djali i shpjegon punonjësit se ai ka pak kohë që ka përfunduar kursin për marrjen e lejes së drejtimit dhe testimet dhe se është e pamundur që të ketë leje drejtimi pasi ka pak muaj që ka mbushur 18 vjeç. Në këtë moment punonjësi verifikon në lejen e drejtimit ekzistuese të dhënat e djalit së bashku me fotografinë e tij. Pasi punonjësi verifikoi fotografinë, pa se kjo leje drejtimi ekzistuese nuk i përkiste djalit që kishte përballë por dikujt tjetër. Pas denoncimit të ngjarjes nga ana e djalit A, policia doli në përfundimin se djali kishte qenë viktimë e vjedhjes së identitetit nga një person tjetër, i cili nëpërmjet vjedhjes së një llogarie të një rrjeti social të djalit kishte vjedhur dhe të dhënat e tij personale. Ky ishte një person i kërkuar nga policia, dhe për këtë arsye shfrytëzoi identitetin e djalit A. Pasojat e vjedhjes së identitetit janë të pranishme edhe sot për djalin A, pasi jo çdo gjurmë e personit që ka krijuar një leje drejtimi të falsifikuar janë fshirë nga sistemet, e kështu djali A has probleme të ndryshme me policinë pasi këta të fundit mendojnë se A ka disa gjoba të papaguara, por që në të vërtetë nuk i përkasin atij por personit që po shfrytëzonte identitetin e A.

Bibliografi

https://mytechdecisions.com/netwwork-security/10-online-privacy-facts/
https://www.comparitech.com/blog/information-security/child-data-privacy-by-country/
https://ww.internetmatters.org/resources/what-age-can-my-child-start-social-netwworking/
https://youtu.be/rPh4xjyeGz4
https://cyberpurify.com/knowwledge/how-many-kids-use-tiktok/#:~:text=According%20to%20the%20latest%20data,are%20under%2018%20years%20old.
https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf-
https://javelinstrategy.com/sites/default/files/files/reports/21-5012J-FM-2021%20Child%20Identity%20Fraud%20Study_1.pdf
https://cybernews.com/best-password-managers/most-common-passwwords/
https://www.avast.com/c-wwhat-is-an-ip-address
https://www.techtarget.com/wwhatis/definition/IMEI-International-Mobile-Equipment-Identity
https://www.techtarget.com/wwhatis/definition/social-netwworking#:~:text=Social%20netëëorks%20are%20ëëebsites%20and,uses%20of%20the%20internet%20today.
https://www.stopbullying.gov/cyberbullying/wwhat-is-it#:~:text=Cyberbullying%20includes%20sending%2C%20posting%2C%20or,into%20unlawwful%20or%20criminal%20behavior.
https://www.un.org/en/about-us/universal-declaration-of-human-rights
https://www.echr.coe.int/documents/convention_eng.pdf
https://www.exelatech.com/blog/brief-history-digitization?language_content_entity=en#:~:text=Digitization%20essentially%20began%20wwith%20the,wwe%20relax%20and%20entertain%20ourselves.