Udhërrëfyes për mbrojtjen e të drejtës së privatësisë në hapësirën digjitale

(Udhëzime praktike për profesionistët ligjor)

Janar, 2024

Financuar nga Bashkimi Evropian

Ky projekt zbatohet nga

ЦЕНТАР ЗА ПРАВНИ ИСТРАЖУВАЊА И АНАЛИЗИ
CENTER FOR LEGAL RESEARCH AND ANALYSIS

MYLA

IMPRESUM

Titulli: Udhërrëfyes për mbrojtjen e të drejtës së privatësisë në hapësirën digjitale (Udhëzime praktike për profesionistët ligjor)

Botues: Qendra për hulumtime dhe analiza ligjore
Shoqata maqedonase e juristëve të rinj

Për botuesin: Lidija Stojkova Zafirovska, QHAL
Aleksandra Cvetanovska, SHMJR

Autor: Aleksandar Gogjo

Kontribut: Dr. Eva Suhrada Kirshmaer
Doc. d-r. Irena Bojaxhievska

Redaktimi: Qendra për hulumtime dhe analiza ligjore

Lekturë: Dejan Vasilevski

Dizajni grafik: Vertigo

Redaktor: Lidija Stojkova Zafirovska

Shtypur nga: Polyesterday

Tirazhi: 30

Vend dhe viti i botimit: Shkup, 2024

Ky publikim është realizuar në kuadër të projektit "Drejtësia efektive për mbrojtjen e lirive themelore dhe të drejtës së privatësisë në hapësirën online", të financuar nga Bashkimi Evropian. Përmbajtja e publikimit është përgjegjësi e vetme e autorëve dhe në asnjë mënyrë nuk mund të konsiderohet se pasqyron pikëpamjet e Bashkimit Evropian.

PËRMBAJTJA

LISTA E SHKURTESAVE

GDPR - General Data Protection Regulation

LMDHP - Ligji për mbrojtjen e të dhënave personale

KP - Kodi penal

LPP - Ligji për procedurën penale

LPC - Ligji për procedurën civile

LMO - Ligji për marrëdhëniet obligative

LPPA - Ligji për procedurën e përgjithshme administrative

LKA - Ligji për kontestet administrative

BE - Bashkimi Evropian

TAIEX - Technical Assistance and Information Exchange instrument

GJEDNJ - Gjykata evropiane për të drejtat e njeriut

GJED - Gjykata evropiane e drejtësisë

KEDNJ - Konventa evropiane për të drejtat e njeriut

APKB - Asambleja e përgjithshme e Kombeve të Bashkuara

TIK - Teknologjitë informative dhe kompjuterike

AMDHP - Agjencia për mbrojtjen e të dhënave ersonale

MPB - Ministria e punëve të brendshme

PTHP - Prokuroria themelore publike

PP - Prokuroria publike

„PRIVATËSIA NUK ËSHTË NJË PRIVILEGJ, ËSHTË NJË E DREJTË THEMELORE E NJERIUT“

VIVIANE REDING

HYRJE

Në vend të një parathënie, një e dhënë që mund të pasqyrojë shumë qartë madhësinë e fenomenit me të cilin po përballemi.

Sipas një hulumtimi të bërë në vitin 2022 në faqet e internetit që gjithashtu përmbajnë media sociale dhe kanë humbur më shumë të dhëna të përdoruesve (pa hyrë në fatin e këtyre të dhënave dhe dëmet e mundshme që kanë ndodhur), situata është si më poshtë:

1. "Jahu"- 3,5 miliardë

Më shumë se 3,5 miliardë përdorues janë prekur nga një shkelje e të dhënave të Jahu, duke përfshirë tre miliardë të kapur në shkeljen e vitit 2013.

2. „Fejsbuk“ – 2,1 miliardë

Katër shkelje të veçanta në vitin 2019 rritën numrin e përdoruesve të „Fejsbuk“ të cilëve iu vodhën të dhënat e tyre në mbi dy miliardë.

3. "Linkedin" – 1,1 miliardë

Shumica e 1.1 miliardë përdoruesve të LinkedIn, të dhënat e të cilëve u ekspozuan, u prekën nga një shkelje në vitin 2021 që rezultoi në shitjen e 700 milionë të dhënave.

4. „Majspejs“ - 719 milionë

Këto tre shkelje zbuluan të dhënat e 719 milionë përdoruesve të „Majspejs“. Faqja tani joaktive kishte vetëm shtatë milionë përdorues në vitin 2019.

5. "Sina Weibo" – 538 milionë

Të dhënat e 539 milionë përdoruesve të faqes kineze të mediave sociale, duke përfshirë 172 milionë numra telefoni, u nxorën në shitje në vitin 2020.

6. "Tuiter" – 370 milionë

"Tuiter" konfirmoi në qershor se një haker kishte fituar qasje në detajet e kontaktit për 5,4 milionë llogari, duke shtuar numrin e përgjithshëm të përdoruesve të prekur në faqen e mikroblogjeve.

7. “Kuora” – 100 milionë

Kuora, një faqe interneti ku përdoruesit mund të bëjnë dhe t'u përgjigjen pyetjeve, zbuloi se fjalëkalimet dhe pyetjet e sigurisë të njëqind milionë përdoruesve u zbuluan në një hakerim në vitin 2018.

8. "Dailymotion" - 85 milionë

Një haker vodhi më shumë se 85 milionë adresa unike të postës elektronike dhe emra përdoruesish nga sistemet e platformës së ndarjes së videove të "Dailymotion", si dhe fjalëkalime për 18.3 milionë llogari në një bastisje të vitit 2016.

9. “Tambler” – 65 milionë

Në vitin 2016, "Tambler" raportoi se siguria e tij ishte kompromet uar tre vjet më parë, duke rezultuar në të dhënat e vjedhura të llogarisë së 65 milionë njerëzve.

10. "Instagram" – 49 milionë

Rreth 49 milionë përdorues të platformës së shpërndarjes së fotografive në pronësi të "Facebook", "Instagram", u ekspozuan pasi një server i pambrojtur u zbulua në internet në vitin 2019.[1]

Transformimi dixhital i shoqërisë sonë është padyshim një nga tranzicionet më të shpejta dhe më të thella të qytetërimit që kemi përjetuar ndonjëherë. Kjo epokë digjitale po na çon të komunikojmë gjithnjë e më shumë në internet, për informacion, argëtim, konsum ose punë. Pandemia me KOVID-19 ka zbuluar potencialin e shërbimeve dixhitale që u kanë mundësuar njerëzve të vazhdojnë të komunikojnë dhe të angazhohen dhe na kanë bërë më rezistent Por mbeten shumë pyetje në lidhje me pasojat e këtij transformimi dhe ndikimin e tij në të drejtat e njeriut.

Çështja e privatësisë ka qenë prej kohësh shumë aktuale në jetën tonë të përditshme, por përdorimi në rritje i hapësirës virtuale dhe zhvillimi i teknologjisë, siç është inteligjenca artificiale, po i sjell këto debate edhe më shumë në qendër të vëmendjes. Në vend që të zvogëlojnë diskriminimin ose pabarazinë, disa sisteme algoritmike të vendimmarrjes mund ta përkeqësojnë atë, veçanërisht në sferën publike. Me përdorimin e veçorive të parashikueshme në sistemin e drejtësisë, duket se del edhe një burim i ri i ligjit. Mjetet e njohjes së fytyrës sjellin koncepte të tilla si fizionomia dhe besimi se karakteristikat e sjelljes mund të deduktohen nga karakteristikat fizike.

Gëzimi i plotë i të drejtave tona në hapësirën kibernetike vjen me mbrojtje adekuate nga rreziqet në mjedisin online. E drejta e jetës private, dinjiteti njerëzor, siguria, integriteti i personit, mosdiskriminimi kërcënohen nga krimi kibernetik.[2]

1 https://businessplus.ie/tech/social-media-lost-user-data/

2 ECHR Symposium: Human Rights in the Digital Sphere.

QËLLIMI DHE FUSHËVEPRIMI

Ky udhërrëfyes synon të jetë një lloj mjeti praktik, ku të gjitha konceptet, kornizat ligjore, kërcënimet, parimet, aktorët, mekanizmat, mjetet juridike dhe procedurat e parashikuara në legjislacionin dhe praktikën e Republikës së Maqedonisë së Veriut do të përmblidhen në një dokument, si dhe disa dilema praktike, shembuj dhe fjali të tilla si Gjykata evropiane për të drejtat e njeriut dhe Gjykata evropiane e drejtësisë.

Shembujt dhe udhëzimet e dhëna në këtë udhërrëfyes duhet t'u shërbejnë organeve shtetërore, kryesisht AMDHP-së, por edhe aktorëve në gjyqësor (gjyqtarëve, prokurorëve publikë, avokatëve) në Republikën e Maqedonisë së Veriut, si dhe të gjithë personave juridikë dhe fizikë, kur merren me çështje të mbrojtjes së të dhënave, nëse ata mbikëqyrin ose mbikëqyrin zbatimin e rregulloreve, vendosin për ankesa ose padi në lidhje me trajtimin, përpunimin ose keqpërdorimin e të dhënave personale, zbulojnë dhe/ose ndjekin penalisht kryerësit e veprave penale dhe veprave penale, ofrojnë ndihmë juridike ose duhet vetë të respektojnë mbrojtjen e të dhënave në kuadër të kryerjes së veprimtarisë së tyre. Në të njëjtën kohë, këto shembuj dhe udhëzime sigurisht rekomandohen të lexohen për të gjithë personat fizikë dhe juridikë, të cilët janë në një mënyrë ose në një tjetër të përfshirë ose u kërkohet të respektojnë rregullat dhe rregulloret që rregullojnë këtë sferë, të njohin rreziqet dhe sfidat dhe të jenë në gjendje të përdorin në mënyrë të përshtatshme mjetet në dispozicion të tyre për të mbrojtur veten, për të minimizuar rreziqet për të drejtat e tyre për privatësinë dhe mbrojtjen e të dhënave personale në hapësirën kibernetike, si dhe për të përdorur mekanizmat ligjorë dhe mjetet juridike në mënyrë të përshtatshme dhe efektive brenda rendit ligjor vendas, dhe sigurisht në atë ndërkombëtar.

Parimet kryesore

Dokumenti bazohet në parimet kryesore për përgatitjen e një "Udhërrëfyesi për mbrojtjen e të drejtës së privatësisë në hapësirën digjitale", të cilat u përgatitën si rezultat i misionit të ekspertëve TAIEX që u zbatua në periudhën nga 31 tetori deri më 2 nëntor 2023 në Republikën e Maqedonisë së Veriut. Qëllimi i misionit TAIEX ishte të ofrojë mbështetje dhe këshilla për përgatitjen e "Udhëzimeve për palët e interesuara gjyqësore për privatësinë dhe mbrojtjen e të dhënave në Republikën e Maqedonisë së Veriut", në përputhje me GDPR dhe acquis të BE-së në këtë fushë.

Ky dokument përmban rekomandimet dhe i trajton ato në mënyrë më të detajuar në përputhje me rrethanat.

Disa nocione kryesore

Për qëllimet e këtij udhërrëfyesi, së pari duhet të përcaktojmë konceptet më themelore që përfaqësojnë thelbin e temës.

"Të dhëna personale"

do të thotë çdo informacion në lidhje me një person fizik të identifikuar ose të identifikueshëm ("subjekti i të dhënave"); një person fizik i identifikueshëm është ai që mund të identifikohet, drejtpërdrejt ose tërthorazi, në veçanti duke iu referuar një identifikuesi të tillë si emri, numri i identifikimit, të dhënat e vendndodhjes, identifikuesi në internet ose një ose më shumë faktorë specifikë për identitetin fizik, fiziologjik, gjenetik, mendor, ekonomik, kulturor ose social të atij personi fizik.

"Kategoritë e veçanta të të dhënave"

janë të dhëna personale që zbulojnë informacione në lidhje me prejardhjen racore ose etnike të një personi fizik, mendimet politike, besimet fetare ose filozofike, ose anëtarësimin në sindikatë, si dhe të dhëna gjenetike, të dhëna biometrike, të dhëna shëndetësore, ose të dhëna gjinore ose orientimi seksual. Ata i nënshtrohen një regjimi të veçantë (neni 13 i LMDHP-së).

"Përpunim"

do të thotë çdo operacion ose grup operacionesh që kryhet mbi të dhënat personale ose në grupe të të dhënave personale, qoftë me mjete të automatizuara ose jo, të tilla si mbledhja, regjistrimi, organizimi, strukturimi, ruajtja, përshtatja ose modifikimi, marrja, konsultimi, përdorimi, zbulimi me transferim, shpërndarje ose ndryshe vënia në dispozicion, rreshtimi ose kombinimi, kufizimi, fshirja ose shkatërrimi.

„Kontrollues"

do të thotë një person fizik ose juridik, pushtet publik, agjenci ose organ tjetër, i cili vetëm ose së bashku me të tjerët përcakton qëllimet dhe mjetet e përpunimit të të dhënave personale; kur qëllimet dhe mjetet e këtij përpunimi përcaktohen nga legjislacioni i Bashkimit Evropian ose i shtetit anëtar, kontrolluesi ose kriteret specifike për emërimin e tij mund të parashikohen nga legjislacioni i Bashkimit Evropian ose i shtetit anëtar.

„Përpunues"

do të thotë një person fizik ose juridik, pushtet publik, agjenci ose organ tjetër që përpunon të dhënat personale në emër të kontrolluesit.

„Pranuesii“

nënkupton një person fizik ose juridik, organ publik, agjenci ose organ tjetër të cilit i zbulohen të dhënat personale, qoftë palë e tretë ose jo. Megjithatë, organet publike që mund të marrin të dhëna personale në kuadër të një hetimi të veçantë në përputhje me ligjin nuk do të konsiderohen si marrës. Përpunimi i këtyre të dhënave nga organet publike duhet të jetë në përputhje me rregullat e zbatueshme të mbrojtjes së të dhënave në përputhje me qëllimet e përpunimit.

Hapësira kibernetike (cyber space)

Një nocion i prezantuar nga romancieri fantastiko-shkencor William Gibson në vitin 1984.

Hapësira kibernetike është vendi ku ndërveprimi njerëzor ndodh përmes rrjeteve kompjuterike, përmes postës elektronike, lojërave ose simulimeve.[3] Nocioni hapësirë kibernetike – (A) nënkupton një rrjet të ndërvarur të infrastrukturave të teknologjisë së informacionit; dhe (B) përfshin internetin, rrjetet e telekomunikacionit, sistemet kompjuterike dhe përpunuesit dhe kontrollorët e inkorporuar.[4]

3 https://www.lexisnexis.co.uk/legal/glossary/cyberspace#:~:text=%27Cyberspace%27%20is%20where%20human%20interaction,through%20email%2C%20games%20or%20simulations

4 https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=50-USC-119985075-325479117&term_occur=999&term_src=title:50:chapter:35:section:1708

01
KORNIZA LIGJORE

KORNIZA LIGJORE

Në ligj, ekziston diskutimi dhe konfuzioni nëse ekziston edhe një kornizë e vetme ligjore që mund të bashkojë të drejtat e njeriut, të dhënat personale dhe t'i referohet hapësirës kibernetike. Për shkak të natyrës së saj ndërkufitare, me në qendër informacionin, hapësira kibernetike paraqet një sfidë për qasjen e shtetit ndaj qeverisjes. Nga njëra anë, infrastruktura fizike që përbën hapësirën kibernetike i nënshtrohet juridiksionit dhe institucionit kombëtar. Nga ana tjetër, rrjedha e të dhënave dhe informacionit përmes asaj infrastrukture mund të kalojë vazhdimisht nëpër juridiksione (të shumëfishta) territoriale, duke e bërë të vështirë për një juridiksion të ushtrojë "kontroll efektiv" mbi këtë rrjedhë informacioni. Kjo ka bërë që shumë të bëjnë thirrje për zhvillimin e një normativiteti të ri, domethënë për të futur regjime për rregullimin e hapësirës kibernetike.

Në ditët e sotme, nuk ka dyshim se parimet e së drejtës ndërkombëtare duhet të jenë të zbatueshme në hapësirën kibernetike. Është më pak e qartë se si këto parime përkthehen në praktikë.

Rrjedhimisht, ky hendek midis politikës dhe praktikës çon në pasiguri ligjore dhe madje edhe boshllëqe ligjore që mund të minojnë mbrojtjen e të drejtave të njeriut të përdoruesve të internetit. Prandaj, organizatat ndërkombëtare dhe rajonale kanë ndërmarrë veprime për iniciativa, me qëllim identifikimin dhe interpretimin se si zbatohen parimet ligjore ekzistuese të së drejtës ndërkombëtare në hapësirën kibernetike.[5]

Megjithatë, qëllimi është që të gjitha përparimet e reja teknologjike të sillen në normën ligjore sa më shumë që të jetë e mundur, në mënyrë që ato të jenë në gjendje të normalizohen dhe të rregullojnë sjelljen. Nëse kjo nuk bëhet në mënyrë të detajuar, boshllëqet ligjore plotësohen sipas normës më përkatëse.

5 Guide to Good Governance in Cybersecurity, 2019, ©DCAF – Geneva Centre for Security Sector Governance, Geneva – 2019.

1.1. Normat ligjore të brendshme, Kushtetuta, Ligji për mbrojtjen e të dhënave personale, rregulla të tjera

Në kuadër të rendit të brendshëm juridik, natyrisht, është Kushtetuta, si akti më i lartë, dhe ligjet.

LMDHP është legjislacioni që rregullon më drejtpërdrejt çështjet e mbuluara në këtë udhërrëfyes. Ligje të tjera procedurale dhe materiale, si LPPC LPP, LPPA, LKA, Ligji për marrëdhëniet obligative, Ligji për komunikimet elektronike, Ligji për mediat, etj., janë secila pjesë e mozaikut për mbrojtjen e të dhënave personale, të drejtën e privatësisë dhe të drejtave të njeriut.

Sipas Kushtetutës[6], instrumentet ndërkombëtare janë pjesë përbërëse e rendit juridik vendas dhe kanë epërsi. Ato do të analizohen në fushën e instrumenteve ligjore ndërkombëtare.

1.2. Instrumentet juridike ndërkombëtare

1.2.1. Deklarata universale për drejtat e njeriut dhe Pakti ndërkombëtar për të drejtat civile dhe politike

Në kuadër të rendit ndërkombëtar, përgjithësisht pranohet që ligji ndërkombëtar për të drejtat e njeriut, përfshirë Deklaratën universale për të drejtat e njeriut dhe Paktin ndërkombëtar për të drejtat civile dhe politike, zbatohet në hapësirën digjitale. Kjo u konfirmua nga Këshilli për të drejtat e njeriut (KDNJ) në rezolutën A/HRC/20/L.13, e cila përcaktoi se "të njëjtat të drejta që njerëzit kanë jashtë linje duhet të mbrohen gjithashtu në internet". Kjo rezolutë është e rëndësishme sepse ishte hera e parë që organi ndërkombëtar deklaroi shprehimisht se mbrojtja e të drejtave të njeriut vlen edhe për hapësirën kibernetike. Pas zbulimeve të Snouden, APKB vendosi të krijojë një raportues të ri special për të drejtën e privatësisë në mënyrë që t'i përgjigjet më mirë privatësisë në epokën digjitale dhe të krijojë një mjedis më të sigurt digjital në vitin 2015. Raportuesi special për të drejtën e privatësisë ka mandat për të kryer vizita shtetërore, për të bërë rekomandime dhe për të trajtuar ankesat individuale.

6 Neni 110 Marrëveshje ndërkombëtare

RAPORT I GRUPIT TË EKSPERTËVE QEVERITARË TË OKB-SË

Raporti i OKB-së i vitit 2015 përshkruan rekomandimet e mëposhtme për sjelljen e përgjegjshme të shtetit, për të kontribuar në një hapësirë kibernetike të hapur, të sigurt, të qëndrueshme, të arritshme dhe paqësore:

NORMAT POZITIVE:

- Shtetet duhet të bashkëpunojnë për të rritur stabilitetin dhe sigurinë në përdorimin e TIK-ut dhe për të parandaluar praktikat e dëmshme të TIK-ut.
- Shtetet duhet të marrin parasysh të gjithë informacionin përkatës në lidhje me atribuimin në mjedisin TIK.
- Shtetet duhet të marrin masat e duhura për të mbrojtur infrastrukturat kritike kombëtare nga kërcënimet e TIK-ut dhe t'u përgjigjen kërkesave të duhura për ndihmë nga një shtet tjetër.
- Shtetet duhet të ndërmarrin hapa të arsyeshëm për të siguruar integritetin dhe për të parandaluar përhapjen e mjeteve keqdashëse të TIK-ut dhe teknikave të TIK-ut.
- Shtetet duhet të inkurajojnë raportimin e përgjegjshëm mbi dobësitë e TIK-ut dhe shkëmbimin e informacioneve në lidhje me të.

NORMAT KUFIZUESE:

- Shtetet nuk duhet të lejojnë me vetëdije që territori i tyre të përdoret ndërkombëtarisht dhe për veprime të gabuara duke përdorur TIK.
- Shtetet duhet t'i përmbahen rezolutave të Asamblesë së Përgjithshme të Kombeve të Bashkuara në lidhje me të drejtat e njeriut.
- Shtetet nuk duhet të zbatojnë me vetëdije mbështetje për veprimtarinë e TIK-ut në kundërshtim me detyrimet e tyre sipas të drejtës ndërkombëtare.
- Shtetet nuk duhet të kryejnë ose mbështesin me vetëdije aktivitete për të dëmtuar sistemet e informacionit të ekipeve të autorizuara të reagimit ndaj emergjencave.

1.2.2. Rregullorja (BE) 2016/679 (General Data Protection Regulation)

Kjo rregullore përcakton rregullat në lidhje me mbrojtjen e personave fizikë në lidhje me përpunimin e të dhënave personale dhe rregullat në lidhje me lëvizjen e lirë të të dhënave personale. Ajo mbron të drejtat dhe liritë themelore të personave fizikë, dhe në veçanti të drejtën e tyre për mbrojtjen e të dhënave personale.

Sipas saj, lëvizja e lirë e të dhënave personale në kuadër të Bashkimit Evropian nuk do të kufizohet dhe as ndalohet për arsye që lidhen me mbrojtjen e personave fizikë në lidhje me përpunimin e të dhënave personale.[7]

7 Regulation (EU) 2016/679 (General Data Protection Regulation), член 1.

Kjo rregullore zbatohet për përpunimin e të dhënave personale në kontekstin e aktiviteteve të krijimit të një kontrolluesi ose përpunuesi në Bashkimin Evropian, pavarësisht nëse përpunimi bëhet në Bashkimin Evropian apo jo[8]

1.2.3. Rezoluta e OKB-së për krijimin e një kulture globale të sigurisë kibernetike

Një rezolutë tjetër e rëndësishme e APKB është A/RES/57/239 për krijimin e një kulture globale të sigurisë kibernetike që njeh krimin kibernetik si një sfidë të madhe të sigurisë kibernetike[9]

1.2.4. Parimet zdhëzuese të Kombeve të Bashkuara për biznesin dhe të drejtat e njeriut

Për më tepër, instrumenti i OKB-së i rëndësishëm për identifikimin e normave në hapësirën kibernetike janë Parimet udhëzuese të Kombeve të Bashkuara për biznesin dhe të drejtat e njeriut (të njohura edhe si "Parimet Ragi"), të miratuara në vitin 2011. Parimet ofrojnë udhëzime për shtetet dhe bizneset në lidhje me mbrojtjen e të drejtave të njeriut. Parimet Ragi bazohen në kornizën e OKB-së – "Respekto, mbro dhe shëro". Në pjesën hyrëse të këtyre parimeve udhëzuese thuhet se "ndërmarrjet e biznesit si organe të specializuara të shoqërisë që kryejnë funksione të specializuara janë të detyruara të respektojnë të gjitha ligjet në fuqi dhe të respektojnë të drejtat e njeriut."

Në kontekstin e rregullimit të formave të caktuara të gjuhës ilegale online – gjuhës së urrejtjes, raporti i Komisionerit të lartë të OKB-së për të drejtat e njeriut, i miratuar nga Këshilli i të drejtave të njeriut në vitin 2013 (i njohur si "Plani për veprim i Rabatit"), identifikon kriteret, shërben për të identifikuar gjuhën e urrejtjes dhe mund të ofrojë udhëzime edhe në fushën online.

1.2.5. Konventa Evropiane për të drejtat e njeriut

Një nga instrumentet më të spikatura ligjore të shekullit të 20-të, Konventa, gjatë interpretimit të saj përmes nenit 8, jep një përkufizim se çfarë do të thotë e drejta e privatësisë në kontekstin e kohës moderne. Sipas KEDNJ-së, neni 8 dhe interpretimi i tij është objekti ku i përket e drejta e mbrojtjes së privatësisë, të dhënave personale dhe përdorimit të tyre, si dhe mbrojtja e të drejtave në hapësirën e internetit. Këshilli i Evropës e ka GJEDNJ-në si organin që interpreton konventën dhe siguron mbrojtje përmes ankesave individuale. Për t'u thirrur në nenin 8, kërkuesi duhet të demonstrojë se ankimi i tij ose i saj bie në të paktën një nga katër interesat e listuara në nen, përkatësisht: jeta private, jeta familjare, shtëpia dhe korrespondenca.

8 Ibid., Neni 3.

9 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/22/PDF/N0255522.pdf?OpenElement

se ankimi i tij ose i saj bie në të paktën një nga katër interesat e listuara në nen, përkatësisht: jeta private, jeta familjare, shtëpia dhe korrespondenca.

Sigurisht, disa gjëra mbulojnë më shumë se një interes. Së pari, Gjykata përcakton nëse kërkesa e aplikantit është brenda objektit të nenit 8. Në vijim, Gjykata shqyrton nëse ka pasur ndërhyrje në atë të drejtë apo nëse janë angazhuar detyrimet pozitive të shtetit për të mbrojtur të drejtën. Kushtet sipas të cilave shteti mund të ndërhyjë në gëzimin e të drejtës së mbrojtur renditen në pikën 2 të nenit 8, përkatësisht, në interes të sigurisë kombëtare, sigurisë publike ose mirëqenies ekonomike të vendit, me qëllim parandalimin e çrregullimit ose krimit, për mbrojtjen e shëndetit ose moralit, ose për mbrojtjen e të drejtave dhe lirive të të tjerëve. Kufizimet lejohen për sa kohë që ato janë "në përputhje me ligjin" ose "të përshkruara me ligj" dhe janë "të nevojshme në një shoqëri demokratike" për të mbrojtur një nga qëllimet e përshkruara më sipër. Në vlerësimin e testit të domosdoshmërisë në një shoqëri demokratike, Gjykata shpesh duhet të balancojë interesat e kërkuesit të mbrojtur nga neni 8 dhe interesat e palës së tretë të mbrojtur nga dispozitat e tjera të Konventës dhe protokollet e saj.[10]

1.2.6. Konventa e Këshillit të Evropës për krimin kibernetik

Nevoja për të unifikuar dhe sistemuar në nivel global normat materiale dhe procedurale në fushën e krimit kibernetik dhe provave elektronike u pasqyrua në Konventën për krimin kibernetik të Këshillit të Evropës (në vijim: Konventa). Megjithëse ka pasur përpjekje të mëparshme për të përcaktuar normat materiale që rregullojnë bashkëpunimin juridik ndërkombëtar, Konventa, nga gjithëpërfshirja, fleksibiliteti dhe mundësia e përfshirjes së lehtë në legjislacionin kombëtar, edhe pse fillimisht e destinuar për vendet e Evropës, është bërë një mekanizëm i njohur për komunikim të lehtë midis vendeve të botës.

Konventa për krimin kibernetik pasohet më vonë nga Konventa për mbrojtjen e të drejtave personale në procesin e automatizuar të përpunimit të të dhënave personale [11]me ndryshimet dhe Protokollin shtesë për rrjedhën e autorizuar të të dhënave personale jashtë shtetit[12], Protokollin shtesë të Konventës për krimin kibernetik për mbrojtjen nga racizmi dhe ksenofobia[13], Konventën për mbrojtjen e fëmijëve nga shfrytëzimi seksual [14] dhe ngacmimi seksual dhe Direktivat e BE-së.

Këshilli i Evropës miratoi Konventën për krimin kibernetik në Budapest më 23.11.2001. Gjithsej 58 vende janë nënshkruese të Konventës, 28 prej tyre me ratifikim. Konventa u nënshkrua nga vendi ynë më 23.11.2001, u ratifikua më 15.09.2004 dhe hyri në fuqi më 01.01.2005.

10 https://www.echr.coe.int/documents/d/echr/guide_art_8_eng

11 https://azlp.mk/wp-content/uploads/2022/11/Zakon_za_ratifikacija_na_Konvencijata_108.pdf

12 https://azlp.mk/wp-content/uploads/2022/11/Dopolnitelen_protokol_Konvencija_108.pdf

13 https://www.pravdiko.mk/wp-content/uploads/2013/11/Dopolnitelen-protokol-na-Konventsijata-za-kompjuterski-kriminal-za-inkriminatsija-na-dela-od-rasistichki-i-kesnofobistichki-vid-ETS-189.doc

14 http://www.childrensembassy.org.mk/WBStorage/Files/Konvencija%20na%20Sovetot%20na%20Evropa%20za%20zastita%20na%20deca%20od%20seksualna%20zloupotreba.pdf

Konventa përmban materiale, norma procedurale dhe norma për bashkëpunimin ndërkombëtar. Dispozitat në fushën e së drejtës materiale kanë të bëjnë me: qasjen e paautorizuar, përgjimin e paautorizuar, ndërhyrjen në të dhëna, ndërhyrjen në sistem, keqpërdorimin e një pajisjeje, falsifikimin e lidhur me kompjuterin, mashtrimin e lidhur me kompjuterin, veprat penale të pornografisë së fëmijëve, veprat penale që lidhen me shkeljen e të drejtave të autorit dhe të drejta të tjera të lidhura me to.

Sipas Protokollit shpjegues të Konventës mbi krimin kibernetik të vitit 2001, zhvillimet e shpejta në fushën e teknologjisë së informacionit kanë një ndikim të drejtpërdrejtë në të gjitha pjesët e shoqërisë moderne. Integrimi i sistemeve të telekomunikacionit dhe informacionit lejon ruajtjen dhe transmetimin, pavarësisht nga distanca, të të gjitha llojeve të komunikimit, gjë që hap një gamë të tërë mundësish të reja. Këto zhvillime u nxitën nga shfaqja e superautostradave dhe rrjeteve të informacionit, duke përfshirë internetin, përmes të cilit praktikisht të gjithë do të jenë në gjendje të kenë qasje në çdo shërbim elektronik të informacionit, pavarësisht se ku janë. Nëpërmjet shërbimeve të komunikimit dhe informacionit, përdoruesit krijojnë një lloj hapësire të përbashkët, të quajtur "hapësirë kibernetike", e cila përdoret për qëllime të ligjshme, por gjithashtu mund t'i nënshtrohet keqpërdorimit dhe konfidencialitetit të sistemeve kompjuterike dhe rrjeteve të telekomunikacionit ose ato konsistojnë në përdorimin e rrjeteve të tilla në shërbimet e tyre për të kryer shkelje tradicionale. Natyra ndërkufitare e veprave të tilla, për shembull, kur kryhen përmes internetit, bie ndesh me territorialitetin e organeve kombëtare të zbatimit të ligjit.[15]

1.2.7. Konventa për mbrojtjen e personave në lidhje me përpunimin automatik të të dhënave personale

Sipas Memorandumit shpjegues të kësaj Konvente, e drejta për respektimin e jetës familjare dhe private parashikohet në nenin 8 të KEDNJ-së. Kjo e drejtë interpretohet më tej nga praktika gjyqësore e Gjykatës dhe plotësohet dhe përforcohet nga Konventa 108 e Këshillit të Evropës.

Jeta private është një nocion që nuk është i ndjeshëm ndaj përkufizimit shterues. Gjykata theksoi se neni 8 mbulon një gamë të gjerë interesash, përkatësisht jetën private dhe familjare, shtëpinë dhe korrespondencën, duke përfshirë postën, komunikimet telefonike dhe postën elektronike në vendin e punës. Jeta private i referohet të drejtës së një personi për imazhin e tij, për shembull me ndihmën e fotografive dhe videove. Gjithashtu i referohet identitetit dhe zhvillimit personal të një personi, të drejtës për të krijuar dhe zhvilluar marrëdhënie me qeniet e tjera njerëzore. Gjithashtu mbulohen aktivitete të natyrës profesionale ose afariste.

15 https://rm.coe.int/16800cce5b

02

E DREJTA E PRIVATËSISË DHE MBROJTJA E TË DHËNAVE

II.

E DREJTA E PRIVATËSISË DHE MBROJTJA E TË DHËNAVE

Duke analizuar këto dy nocione, ato nuk përfaqësojnë sinonime. Në praktikë, ka debate të ndryshme në lidhje me finesën e këtyre dy të drejtave. Por një gjë është e qartë, e drejta e privatësisë është një nocion më i gjerë sesa mbrojtja e të dhënave.

2.1. E drejta e privatësisë

Privatësia nuk është vetëm një e drejtë individuale, por edhe një vlerë shoqërore. Ajo është ngulitur në konceptin e individualizmit, lirisë dhe të drejtës për mbrojtjen e individit. Në disa shtete, për shembull në Shtetet e Bashkuara, privatësia shpesh konsiderohet një element i lirisë, domethënë është e drejta për të qenë i lirë nga ndërhyrjet nga shteti. Privatësia është një nga të drejtat themelore dhe pothuajse çdo vend në botë, në një farë mënyre, njeh privatësinë, qoftë në kushtetutën e tyre ose në dispozita të tjera, sepse e drejta për privatësi ose jetë private është e ngulitur në Deklaratën Universale për të drejtat e njeriut (neni 12), Konventën evropiane për të drejtat e njeriut (neni 8) dhe Kartën evropiane të të drejtave themelore (neni 7).

Një nga dallimet imanente është se privatësia njihet si një e drejtë universale e njeriut, ndërsa mbrojtja e të dhënave nuk është (të paktën jo ende).[16]

2.2. Koncepti i mbrojtjes së të dhënave

Mbrojtja e të dhënave i referohet mbrojtjes së çdo informacioni në lidhje me një person fizik të identifikuar ose të identifikueshëm, duke përfshirë emrat, datat e lindjes, fotografitë, videot, adresat e postës elektronike dhe numrat e telefonit. Informacione të tjera, të tilla si adresat IP dhe përmbajtja e komunikimit – të lidhura ose të ofruara nga përdoruesit e fundit të shërbimeve të komunikimit – konsiderohen gjithashtu të dhëna personale.

Nocioni i mbrojtjes së të dhënave rrjedh nga e drejta e privatësisë. Të dyja janë të dobishme në ruajtjen dhe promovimin e vlerave dhe të drejtave themelore; dhe në ushtrimin e të drejtave dhe lirive të tjera – të tilla si liria e fjalës ose e drejta e tubimit.

Mbrojtja e të dhënave ka qëllime të sakta për të siguruar përpunimin e drejtë (mbledhjen, përdorimin, ruajtjen) e të dhënave personale si nga sektori publik ashtu edhe nga ai privat.[17]

16 https://edps.europa.eu/data-protection/data-protection_en
17 Ibid.

2.3. Mbrojtja nga identifikimi indirekt

Të gjithë aktorët e listuar në këtë udhërrëfyes që punojnë ose vijnë në kontakt me të dhënat është e rëndësishme të dinë se informacioni që ata kanë mund të çojë në identifikimin indirekt të një individi të caktuar dhe për këtë arsye edhe këto të dhëna në dukje të ndërmjetme ose indirekte marrin trajtimin e të dhënave personale. Kështu, ato i nënshtrohen sistemit të mbrojtjes sipas GDRP/LMDHP.

Nëse një individ nuk mund të identifikohet drejtpërdrejt nga informacioni i përpunuar nga profesionisti (për shembull, kur hiqen të gjithë identifikuesit), kjo nuk do të thotë se individi nuk mund të identifikohet ndryshe, për shembull, nga informacioni i mbajtur më parë nga profesionisti (ai që përdor, përpunon) ose informacioni që duhet të marrë nga një burim tjetër. Në mënyrë të ngjashme, një palë e tretë mund të përdorë informacionin e mbajtur nga profesionisti, kështu që nëse e kombinon atë me informacione të tjera në dispozicion të asaj pale të tretë, procesi mund të çojë në identifikimin e individit.

Në një rast të tillë, barra e vlerësimit bie mbi secilin aktor të renditur në këtë udhërrëfyes, i cili duhet të vlerësojë se çfarë informacioni ka të ngjarë të përdoret për përpunim, gjë që do të çonte në zbulimin e individit, domethënë identifikimin e tij për të shmangur publikimin ose zbulimin pa dashje të informacionit që mund të shoqërohet me informacione të tjera dhe (në mënyrë të papërshtatshme) identifikimin e individit.

Cili është informacioni që mund të zbulojë një individ në mënyrë indirekte?

Nuk ka listë shteruese, por afërsisht një informacion i tillë, domethënë kombinimi i tyre mund të çojë në identifikimin e individit:

- numri i regjistrimit të automjetit,
- numri i pasaportës, ose
- një kombinim i kritereve të rëndësishme (për shembull, mosha, profesioni, vendbanimi).

Pika kryesore e identifikimit indirekt është kur informacioni kombinohet me informacione të tjera që më pas dallojnë dhe lejojnë identifikimin e individit.

2.4. E drejta për mbrojtjen e të dhënave

Privatësia dhe mbrojtja e të dhënave janë dy të drejta të përfshira në Traktatet e BE-së dhe në Kartën e BE-së për të drejtat themelore.[18] Karta përmban një të drejtë të qartë për mbrojtjen e të dhënave personale (neni 8). Me hyrjen në fuqi të Traktatit të Lisbonës në vitin 2009, Karta e të drejtave themelore i dha të njëjtën vlerë ligjore si traktatet kushtetuese të BE-së. Kështu, institucionet dhe organet e BE-së dhe shtetet anëtare janë të lidhura me të. Për më tepër, neni 16 i Traktatit për funksionimin e Bashkimit Evropian (TFEU) e detyron BE-në të vendosë rregulla për mbrojtjen e të dhënave për

18 https://edps.europa.eu/data-protection/data-protection_en

përpunimin e të dhënave personale. BE-ja është unike në parashikimin e një detyrimi të tillë në kushtetutën e saj.

2.5. Rregulloret për mbrojtjen e të dhënave personale

Në prill 2016, BE miratoi një kornizë të re ligjore – Rregulloren e përgjithshme të mbrojtjes së të dhënave (GDPR) dhe Direktivën për mbrojtjen e të dhënave për fushën e zbatimit të ligjit dhe policisë.

I zbatuar plotësisht në të gjithë BE-në në maj të vitit 2018, GDPR është pjesa më gjithëpërfshirëse dhe progresive e legjislacionit për mbrojtjen e të dhënave në botë, e përditësuar për të adresuar implikimet e epokës digjitale.

Republika e Maqedonisë së Veriut e ka transpozuar këtë rregullore përmes miratimit të LMDHP-së.

03
QASJA HORIZONTALE

QASJA HORIZONTALE

Mbrojtja e të dhënave është një çështje horizontale, që në thelb do të thotë se në çdo sektor specifik duhet të merret parasysh Ligji për mbrojtjen e të dhënave personale (LMDHP) për çdo çështje ligjore që i nënshtrohet zgjidhjes. Për më tepër, duhet të merren parasysh edhe ligjet që mund të përmbajnë dispozita specifike të sektorit për mbrojtjen e të dhënave (ligji i telekomunikacionit, ligji për e-tregti, ligji për mediat, etj.) që duhet të zbatohen në përputhje me rrethanat. Këto rregulla duhet të merren parasysh edhe gjatë zgjidhjes së një situate konkrete ligjore.

Përveç ligjeve, gjatë vlerësimit të çështjeve që lidhen me mbrojtjen e të dhënave, do të merret parasysh praktika gjyqësore e Gjykatës evropiane për të drejtat e njeriut (GJEDNJ), duke marrë parasysh aspiratat e vendit tonë ndaj Bashkimit Evropian dhe arsyetimin përkatës ligjor të Gjykatës evropiane të drejtësisë (GJEDNJ). Gjithashtu mund të jetë e dobishme t'i referoheni udhëzimeve dhe mendimeve të Këshillit evropian për mbrojtjen e të dhënave (një këshill ku përfaqësohen të gjitha organet për mbrojtjen e të dhënave të shteteve anëtare të BE-së).

3.1. Parimet e mbrojtjes së të dhënave

LMDHP përcakton parimet që rregullojnë përpunimin e të dhënave personale.

Këto parime përfshijnë:

- ligjshmëria,
- drejtësia dhe transparencë,
- kufizimi i qëllimit,
- minimizimi i të dhënave,
- saktësia e të dhënave,
- kufizimi i magazinimit,
- integriteti dhe konfidencialiteti,
- përgjegjësi[19]

19 LMDHP, neni 9.

3.1.1. Ligjshmëria

Përpunimi i të dhënave personale konsiderohet i ligjshëm vetëm nëse kryhet për një nga arsyet që lejohen, respektivisht të përcaktuara në legjislacion[20]

3.1.2. Drejtësia

Kur të përmbushet ligjshmëria si parim, atëherë kalojmë në krijimin e përpunimit të drejtë respektivisht fer. Kjo do të thotë se subjekti i të dhënave personale duhet të jetë i vetëdijshëm se të dhënat e tij personale do të përpunohen. Kjo do t'i lejojë atij të marrë një vendim të informuar nëse pajtohet me një përpunim të tillë dhe do t'i lejojë atij të përmbushë të drejtat e tij në lidhje me mbrojtjen e të dhënave të tij personale.

20 Ligjshmëria e përpunimit të të dhënave personale
Neni 10
(1) Përpunimi i të dhënave personale është i ligjshëm vetëm nëse dhe në masën që plotësohet të paktën një nga kushtet e mëposhtme:
– subjekti i të dhënave personale ka dhënë pëlqimin për përpunimin e të dhënave të tij personale për një ose më shumë qëllime specifike,
– përpunimi është i nevojshëm për të përmbushur një kontratë ku subjekti i të dhënave personale është palë kontraktuese ose për të ndërmarrë aktivitete me kërkesë të subjektit të të dhënave personale para hyrjes të tij/saj në kontratë,
– përpunimi kërkohet për të përmbushur një detyrim ligjor të kontrolluesit,
– përpunimi është i nevojshëm për të mbrojtur interesat thelbësore të subjektit të të dhënave personale ose të një personi tjetër fizik,
– përpunimi është i nevojshëm për kryerjen e punëve me interes publik ose në ushtrimin e autoritetit publik të kontrolluesit të përcaktuar me ligj,
– përpunimi është i nevojshëm për qëllime të interesave legjitime të kontrolluesit ose të një pale të tretë, përveç kur këto interesa nuk mbizotërojnë mbi interesat ose të drejtat dhe liritë themelore të subjektit të të dhënave personale që kërkojnë mbrojtjen e të dhënave personale, në veçanti kur subjekti i të dhënave personale është fëmijë.
(2) Dispozitat e pikës 1, pika 6, të këtij neni, nuk zbatohen për përpunimin e të dhënave personale nga institucionet shtetërore në zbatimin e kompetencave të tyre.
(3) Baza ligjore për përpunimin e të dhënave personale të përmendura në pikën 1, pika 3 dhe 5, të këtij neni, përcaktohet me ligj. Ligji detyrimisht parashikon: kushtet që përcaktojnë ligjshmërinë e përpunimit nga kontrolluesi, qëllimet e përpunimit, kategoritë e të dhënave personale që i nënshtrohen përpunimit, kategoritë e subjekteve të të dhënave personale; subjektet të cilëve mund t'u zbulohen të dhënat personale, si dhe qëllimet për të cilat zbulohen të dhënat personale, kufizimet në qëllimet e përpunimit, periudhën e ruajtjes, operacioneve dhe procedurave të përpunimit, duke përfshirë masat për të siguruar përpunimin e ligjshëm dhe të drejtë, me qëllim përmbushjen e qëllimit të interesit publik dhe të jetë proporcionale me ndjekjen e qëllimit legjitim. Ligji duhet të përmbajë edhe vlerësimin e ndikimit të mbrojtjes së të dhënave personale në rastet e parashikuara në nenin 39 të këtij ligji.
(4) Nëse të dhënat personale përpunohen për një qëllim të ndryshëm nga qëllimi për të cilin janë mbledhur fillimisht, me anë të të cilit përpunimi nuk kryhet në bazë të pëlqimit të subjektit të të dhënave personale ose në bazë të një ligji, i cili është një masë e nevojshme dhe proporcionale për të mbrojtur qëllimet e përcaktuara në nenin 27 paragrafi 1 i këtij ligji, atëherë kontrolluesi, për të përcaktuar nëse përpunimi për qëllime të tjera është në përputhje me qëllimin fillestar për të cilin janë mbledhur të dhënat personale, është i detyruar, ndër të tjera, të marrë parasysh:
– çdo lidhje midis qëllimeve për të cilat mblidhen të dhënat personale dhe qëllimeve për përpunimin e mëtejshëm të synuar,
– kontekstin në të cilin janë mbledhur të dhënat personale, veçanërisht në lidhje me marrëdhëniet midis subjekteve të të dhënave personale dhe kontrolluesit,
– natyra e të dhënave personale, dhe në veçanti nëse kategoritë e veçanta të të dhënave personale përpunohen në përputhje me nenin 13 të këtij ligji ose të dhënat personale në lidhje me dënimet penale dhe veprat penale përpunohen në përputhje me nenin 14 të këtij ligji – pasojat e mundshme të përpunimit të mëtejshëm të parashikuar për subjektet e të dhënave personale,
– ekzistenca e masave mbrojtëse të përshtatshme që mund të përfshijnë enkriptimin ose pseudonimizimin.

3.1.3. Transparenca

Lidhur drejtpërdrejt me parimin e përpunimit të drejtë është parimi i transparencës, që do të thotë se kontrolluesi duhet të jetë i hapur dhe i qartë për subjektin e të dhënave personale gjatë përpunimit të të dhënave të tij personale. Në vend të njoftimit aktual të Agjencisë për mbrojtjen e të dhënave personale për grumbullimin e të dhënave personale të përpunuara, me rregullat e reja ligjore kontrolluesi është i detyruar të informojë subjektet e të dhënave personale për këtë. Raportimi duhet të jetë në kohë, duke përdorur një gjuhë të qartë dhe të thjeshtë.

3.1.4. Kufizimi i qëllimit

Kufizimi i qëllimit nënkupton që kontrolluesit mund të përpunojnë vetëm të dhënat personale për të përmbushur qëllime konkrete, të qarta dhe legjitime. Kjo do të thotë që kontrolluesit duhet së pari të identifikojnë qëllimin specifik për të cilin po përpunojnë të dhënat personale dhe që identifikuan qëllimin specifik për të përfaqësuar kuadrin në të cilin zhvillohet përpunimi. Përpunimi i mëtejshëm (dytësor), për një qëllim të ndryshëm nga ai i pari, mund të jetë i ligjshëm vetëm nëse konsiderohet i pajtueshëm me qëllimin fillestar për të cilin janë përpunuar fillimisht të dhënat personale.

3.1.5. Vëllimi minimal i të dhënave

Parimi i përpunimit të një vëllimi minimal të të dhënave do të thotë që kontrolluesit do të përpunojnë vetëm ato të dhëna personale që janë përkatëse, relevante dhe të kufizuara në atë që është e nevojshme për të arritur qëllimin. Kontrolluesi duhet të sigurojë që përpunimi është me të vërtetë i nevojshëm dhe se vëllimi i përpunimit të të dhënave personale është proporcional me qëllimin e përpunimit.

3.1.6. Saktësia

Parimi i saktësisë nënkupton që kontrolluesi duhet të zbatojë masat e duhura për të dhënat personale që përpunon. Ato do të jenë të sakta dhe, nëse është e nevojshme, të përditësuara, si dhe masat për fshirjen dhe korrigjimin në kohë të të dhënave personale që janë të pasakta ose jo të plota.

3.1.7. Kufizimi i afatit të ruajtjes

Sipas këtij parimi, të dhënat personale do të ruhen në një formë që lejon identifikimin e subjekteve të të dhënave personale jo më shumë se sa është e nevojshme për të përmbushur qëllimet për të cilat kryhet përpunimi. Me fjalë të tjera, përpunimi i të dhënave personale do të kryhet vetëm për aq kohë sa është e nevojshme për të përmbushur qëllimin për të cilin janë përpunuar të dhënat personale.

3.1.8. Integriteti dhe konfidencialiteti

Të dhënat personale mund të përpunohen vetëm në një mënyrë që siguron një nivel të përshtatshëm të sigurisë së të dhënave personale duke zbatuar masat e duhura teknike ose organizative. Për të mbrojtur të dhënat personale, kontrolluesit duhet të zbatojnë një sistem të sigurisë së informacionit që përshkruhet më hollësisht në kapitullin e shtatë të këtij doracaku. Gjatë vlerësimit dhe krijimit të sistemit të sigurisë së informacionit, është praktikë e zakonshme dhe e mirë që ekipi të përbëhet nga avokatë dhe persona teknikë për të përcaktuar në mënyrë më të përshtatshme strategjitë dhe politikat e kontrolluesit.

3.1.9. Përgjegjësia

Përgjegjësia në fushën e të dhënave personale është rrugë dykahëshe. Gjithkush është i detyruar të kujdeset për mbrojtjen e të dhënave të tij personale dhe të mos i ekspozojë ato në publik ose t'i vërë ato në rrezik për t'u keqpërdorur. Sigurisht, përgjegjësia bie edhe mbi këdo që në çfarëdo mënyre kryen përpunimin, ruajtjen dhe asgjësimin e të dhënave personale të vëna në dispozicion të tyre në bazë të bazave dhe qëllimeve të përcaktuara me ligj.

04

PËRDORIMI I TË DHËNAVE PERSONALE PËR QËLLIME TË LIGJSHME DHE NË BAZË TË PUNËS SË LIGJSHME LIGJORE

PËRDORIMI I TË DHËNAVE PERSONALE PËR QËLLIME TË LIGJSHME DHE NË BAZË TË PUNËS SË LIGJSHME LIGJORE

Koncepti i besimit të të dhënave personale, përkatësisht përpunimi, ruajtja dhe asgjësimi i tyre për qëllime ligjore nënkupton marrjen e pëlqimit nga subjekti. Në raste të caktuara, pëlqimi nuk kërkohet, kur ekzistojnë arsye dhe rrethana ligjërisht të vlefshme dhe të arsyetuara. Megjithatë, detyra e kujdesit mbetet e njëjtë.

4.1. Pëlqimi

Në ditët e sotme, me fluksin e teknologjive të reja, nuk ka pothuajse asnjë faqe interneti, aplikacion, rrjet social ose lloj tjetër të rrjetit të ndarjes së të dhënave që nuk ka rregullat e veta që na kërkojnë të pajtohemi me to para se t'i përdorim ato. Këto rregulla janë kryesisht në formën e rregullave të përdorimit, rregullave dhe politikave të biskoatave dhe/ose politikës së privatësisë, EULA (End User License Areement, etj.). Në thelb, pëlqimi është lidhja e një marrëdhënieje kundëraktuale, e cila mund të ndërpritet sipas kushteve të specifikuara në ato rregulla, respektivisht kontratë Parimet që duhet të respektohen gjatë dhënies së pëlqimit janë si më poshtë:

4.1.1. Pëlqimi i dhënë në mënyrë të lirë

• Nënkupton zgjedhjen që subjekti i të dhënave personale ka për të dhënë pëlqimin ose jo, si dhe mundësinë për ta tërhequr atë në çdo kohë. Në vlerësimin nëse pëlqimi është dhënë lirisht, duhet të merret parasysh nëse subjekti i të dhënave personale është i kushtëzuar nga zbatimi i një kontrate në të cilën ai është palë kontraktuese.

4.1.2. Pëlqimi konkret

• Nënkupton që subjekti është pajtuar vetëm për një përpunim specifik të të dhënave të tyre personale. Nëse kontrolluesi kryen përpunimin e të dhënave personale në disa procese, duhet të jepet pëlqim i veçantë për secilin proces veç e veç.

4.1.3. Pëlqimi i informuar

• Nënkupton që subjekti i të dhënave personale ka dhënë pëlqimin e tij/saj pasi i janë paraqitur më parë të gjitha detajet e përpunimit të gjuhës dhe në një formë që është e kuptueshme në mënyrë që ai/ajo të mund të vlerësojë në mënyrë adekuate ndikimin që përpunimi mund të ketë mbi të.

4.1.4. Pëlqim i padyshimtë

• Nënkupton që deklarata e dhënë ose veprimi konfirmues i subjektit nuk lë vend për dyshim në qëllimin e tij/saj për t'u pajtuar për përpunimin e të dhënave personale të tij/saj.

4.2. Kur nuk kërkohet pëlqimi

Sipas LMDHP-së, pëlqimi i subjektit të të dhënave nuk është baza e vetme ligjore për përpunimin e të dhënave.

Për shembull, përpunimi i të dhënave mund të bazohet gjithashtu në një ligj të veçantë ose interes të ligjshëm të ndjekur nga kontrolluesi ose një palë e tretë, përveç rasteve kur këto interesa mbizotërohen nga interesi i të drejtave dhe lirive themelore të subjektit të të dhënave. Kjo dispozitë, respektivisht postulat, duhet të interpretohet ngushtë, që i referohet në mënyrë specifike atyre rasteve kur do të ishte i nevojshëm pëlqimi i subjektit të të dhënave.

Në praktikë, kjo dispozitë zbatohet për krimin kibernetik, për shembull, për rastet kur kryerësit veprojnë nën një profil të rrejshëm (nën emrin e një personi tjetër), përdorin të dhëna personale për të kryer mashtrim, ose kur përpunojnë të dhëna në lidhje me pornografinë e fëmijëve, ose kur publikojnë fotografi dhe informacione të tjera të ndjeshme në lidhje me të tjerët në internet për të dëmtuar dinjitetin dhe reputacionin e këtyre personave duke i ekspozuar ato në publik.

4.3. Të drejtat e subjektit të të dhënave personale

Subjekti duhet:

- Të informohet për identitetin e kontrolluesit dhe përfaqësuesit të tij në Republikën e Maqedonisë së Veriut;
- Të fitojë njohuri për mbledhjen e të dhënave personale;
- Të dijë se çfarë të dhënash personale ruhen rreth tij në formë elektronike ose në letër;
- Të njohë qëllimet e përpunimit të të dhënave të tij personale;
- Të njohë përdoruesit ose kategoritë e përdoruesve të të dhënave;
- Të mos japë pëlqimin për përdorimin e të dhënave për qëllime tregtare ose transferimin e tyre tek palët e treta për qëllime të tilla;
- Të ketë qasje në të dhënat dhe t'i korrigjojë ato.

IV.

Për shembull:

"Facebook" përdor të dhënat e marra nga përdoruesit e rrjetit të tij social për të ofruar tregje më të synuara për reklamuesit. "Google" është në gjendje të identifikojë interesin e përdoruesve ose faqeve të internetit të vizituara duke analizuar pyetjet e kërkimit të përdoruesve të shërbimit të tij në motorin e kërkimit, si një bazë tregtare për reklamat e synuara. Kur krijoni një llogari me "Facebook" ose "Google", ekziston një politikë privatësie për të cilën pajtoheni para se të vazhdoni të klikoni "regjistrohu" ose "OK".

4.4. Parimi i proporcionalitetit

Proporcionaliteti nënkupton një ekuilibër midis mjeteve të përdorura dhe qëllimit të synuar. Parimi i proporcionalitetit nënkupton vendosjen e një ekuilibri të arsyeshëm midis përpunimit të të dhënave dhe qëllimit të synuar. Me fjalë të tjera, do të thotë që përpunimi i të dhënave është në masën që ai përmbush qëllimin.

Për të zvogëluar mangësitë dhe rreziqet për gëzimin e të drejtave të privatësisë dhe mbrojtjes së të dhënave, është e rëndësishme që kufizimet të përmbajnë masa mbrojtëse të përshtatshme.

Kur e drejta e privatësisë dhe mbrojtja e të dhënave, nga njëra anë, dhe të drejtat e tjera të njeriut, nga ana tjetër, janë kontradiktore, parimi i proporcionalitetit është mjeti kryesor ligjor që përdoret për të balancuar të drejtat e ndryshme të njeriut. Pastaj, duhet të bëhet një test për balancim.

Testi i proporcionalitetit sillet rreth tre hapave: përshtatshmëria (nëse përzierja është me të vërtetë e përshtatshme për të arritur qëllimin e pretenduar), domosdoshmëria (gjithashtu "alternativa më pak kufizuese" ose "dëmtimi minimal"; nëse masa e marrë është alternativa më pak kufizuese) dhe proporcionaliteti në kuptimin e ngushtë (nëse përfitimet e arritura tejkalohen nga kufizimet e shkaktuara). Për më tepër, përpunimi i të dhënave duhet të bazohet në ligjin kombëtar dhe të ndjekë një qëllim të ligjshëm.

05

SIGURIA E HAPËSIRËS KIBERNETIKE – SIGURI KIBERNETIKE DHE HIGJIENA KIBERNETIKE

SIGURIA E HAPËSIRËS KIBERNETIKE – SIGURIA KIBERNETIKE DHE HIGJIENA KIBERNETIKE

Veçanërisht në rrjetet sociale, të dhënat personale private janë në dispozicion të palëve të treta, ndonjëherë edhe të publikuara dhe për këtë arsye të disponueshme për të gjithë. Ato gjithashtu mund të përmbajnë informacione private, si fotografi personale dhe informacione që – në botën analoge - nuk do të ishin lehtësisht të disponueshme. Shumë shkelje të mbrojtjes së të dhënave ndodhin në mjedisin online. Personat që kryejnë një shkelje të mbrojtjes së të dhënave shfrytëzojnë rrezikun e internetit, dhe nganjëherë të pakujdesit së përdoruesit, dhe përpunojnë të dhënat personale të përdoruesve për qëllimet e tyre.

5.1. Tre lloje të sigurisë kibernetike

Fusha e sigurisë kibernetike përfshin një gamë të madhe mjetesh dhe teknikash, të cilat në thelb përfshijnë:

5.1.1. Sigurinë e të dhënave

Hakerët shpesh kërkojnë të dhëna. Ata duan të shohin ose të vjedhin informacione që janë jashtë kufijve. Arsyet e tyre janë të ndryshme. Në disa raste, një haker thjesht vjedh informacione si numrat e kartave të kreditit për t'i shitur ato në tregun e zi (Dark web). Në raste të tjera, qëllimi nuk është fitimprurës, por të dëmtojë duke publikuar të dhëna personale ose, në mënyrë alternative, të marrë vetëm të dhënat vetë, për të kënaqur orekset politike, të biznesit ose të tjera. Siguria e të dhënave përfshin mbrojtjen e të dhënave nga qasja e paautorizuar. Përfshin politikat e enkriptimit të të dhënave, teknologjitë dhe politikat e kontrollit të qasjes në të dhëna.

5.1.2. Siguria e rrjetit

Në mënyrë që një sulm kibernetik të funksionojë, pothuajse në çdo situatë, është së pari e nevojshme që hakeri të fitojë qasje në rrjetin e objektivit. Mbrojtja e rrjetit është një nga fushat më serioze të sigurisë kibernetike dhe zakonisht është fokusi i investimeve të rëndësishme. Siguria e rrjetit është një grup rregullash dhe konfigurimesh të dizajnuara për të mbrojtur integritetin, konfidencialitetin dhe qasjen e rrjeteve kompjuterike dhe të dhënave duke përdorur teknologjitë softuerike dhe harduerike.

5.1.3. Siguria e aplikacioneve

Hakerët gjithashtu duan të hyjnë në aplikacione softuerike si Enterprise Resource Planning (ERP), CRM,, serverët e postës elektronike dhe të ngjashme. Prania brenda aplikacionit është një mënyrë e shkëlqyer për të spiunuar objektivin ose për të prishur funksionimin e tij. Siguria e aplikacionit ka shumë aspekte, por zakonisht kombinon politikat (për shembull, kujt i lejohet qasja në aplikacion dhe "prapavijën" e tij administrative) dhe kontrollet mbi ndërfaqet e programimit të aplikacionit (API) që lejojnë programe të tjera softuerike të kenë qasje në aplikacion.

5.2. Llojet e kërcënimeve

Në përputhje me rrethanat, ndaj të cilëve mund të drejtohen, kërcënimet ndahen në:

- Kërcënimet ndaj personave
- Kërcënimet ndaj pronës
- Kërcënimet ndaj sistemit

Ekzistojnë shtatë lloje të zakonshme të kërcënimeve të sigurisë kibernetike. Kërcënimi kibernetik është një metodë për të sulmuar një mjet të të dhënave. Ky nuk është sulmi i vërtetë. Është më shumë si një plan për sulm. Ka fjalë për fjalë qindra miliona kërcënime kibernetike atje. Në përgjithësi, ato janë si më poshtë:

VIRUSET/MALUER – Virusi është një formë e kodit maluar që instalohet vetë në pajisjen tuaj. Pasi të jetë inkorporuar, virusi mund të bëjë një numër gjërash të ndryshme të këqija, duke përfshirë ngrirjen e sistemit, vjedhjen e të dhënave dhe madje rrëmbimin e pajisjes për qëllime kriminale si minierat e kriptovalutave pa lejen tuaj, për shembull, "kriptojacking".

VJEDHJA E IDENTITETIT – Vjedhja e identitetit është një krim ku një haker vjedh mjaft nga informacionet tuaja private, personale (p.sh. numri i sigurimeve shoqërore, data e lindjes, adresa, etj.) Për të qenë në gjendje t'ju imitojë. Duke u shtirur si ti, një haker mund të jetë në gjendje të vjedhë para nga llogaria jote bankare, të hapë llogari me kartë krediti në emrin tënd dhe shumë më tepër.

SULMET ME FJALËKALIM – Nëse një haker ka fjalëkalimin tuaj, ai ose ajo mund të hyjë në llogaritë tuaja. Sulmet e fjalëkalimeve përdorin softuer të veçantë për të hamendësuar fjalëkalimet, shpesh duke provuar mijëra mundësi para se të hamendësoni atë të saktë.

„TROJANËT" – Ashtu si kali i famshëm i trojës i kohëve të lashta, Trojan është një sulm kibernetik që depërton në rrjetin e objektivit nën pretendime të rreme. Për shembull, një haker mund të fusë një virus në një dokument PDF dhe ta dërgojë atë tek ju si një shtojcë emaili. Kur hapni PDF-në, skedari ngulit virusin në sistemin tuaj ndërsa dokumenti hapet në Acrobat Reader.

RANSOMUER – Një variant i maluer që kodon të dhënat e tua dhe të bën të paguash një shpërblim, zakonisht në bitkoin, për t'i zhbllokuar ato.

V.

- FISHING – Një përpjekje, zakonisht përmes postës elektronike, për t'ju mashtruar të klikoni në një hiperlink që do të vendosë maluer në kompjuterin tuaj. Një formë më e sofistikuar sulmi, e njohur si spiar fishing, përfshin sulmuesin që shtiret si një mik ose koleg, zakonisht për t'ju bërë të ndani kredencialet e hyrjes në llogari. Fiishing është një teknikë socio-inxhinierike që përdoret për të vjedhur të dhëna ose mashtrime. Kjo bëhet duke dërguar reklama të rrejshme përmes faqeve të rrejshme të internetit tek përdoruesit e besuar. Reklamat zakonisht shfaqin promovime të shitjeve për një larmi mallrash, duke përfshirë, për shembull, aksesorë ose automjete me çmime shumë të ulëta. Kjo bëhet për të tërhequr viktimat e mundshme për të shkëmbyer informacione të ndjeshme, të tilla si informacione personale, emra përdoruesish dhe fjalëkalime, si dhe detaje të kartës së pagesës dhe bankës.

- KËRCËNIMI I AVANCUAR I VAZHDUESHËM (APT) – APT janë ndoshta kërcënimet më të fuqishme kibernetike. APT është projektuar për t'u futur fshehurazi, pastaj për t'u fshehur në rrjetin tuaj për muaj të tërë, pa u vënë re. Ai lëviz anash, duke u instaluar vazhdimisht në pjesë të ndryshme të infrastrukturës suaj derisa të aktivizohet. Atëherë, mund të shkaktojë dëme të jashtëzakonshme.

5.3. Higjiena kibernetike

Higjiena kibernetike i referohet një sërë praktikash dhe masash që mund të merrni për të ruajtur sigurinë tuaj digjitale dhe për t'u mbrojtur nga kërcënimet kibernetike. Ashtu si praktikat e higjienës personale, të tilla si larja e duarve dhe larja e dhëmbëve, ndihmojnë në parandalimin e përhapjes së baktereve dhe sëmundjeve, praktikat e higjienës kibernetike ndihmojnë në parandalimin e përhapjes së maluer, virusëve dhe sulmeve kibernetike.

06

“AKTORË” TË NDRYSHËM NË BAZË TË PRIVATËSISË DHE MBROJTJES SË TË DHËNAVE PERSONALE

VI.

"AKTORË" TË NDRYSHËM NË BAZË TË PRIVATËSISË DHE MBROJTJES SË TË DHËNAVE PERSONALE

Çështja e mbrojtjes së të dhënave personale është komplekse. Është një konglomerat masash, aktivitetesh, autoritetesh, personash dhe kompanish që jo gjithmonë kanë kufij dhe kompetenca të qarta dhe të kufizuara.

6.1. Kuvendi i Republikës së Maqedonisë së Veriut

Organi ligjvënës parashikon ndër të tjera kornizën kushtetuese dhe ligjore në këtë fushë. Për qëllimet e këtij udhërrëfyesi, është e rëndësishme të theksohet se koncepti i një organi të pavarur mbikëqyrës është zbatuar në rendin ligjor të Republikës së Maqedonisë së Veriut, përmes Agjencisë për mbrojtjen e të dhënave personale, e cila, nga ana tjetër, është përgjegjëse para Kuvendit të Republikës së Maqedonisë së Veriut për punën e saj.[21]

6.2. Agjencia për mbrojtjen e të dhënave personale

Si organ i pavarur rregullator, pavarësia e këtij institucioni është themeluar dhe afirmuar jashtëzakonisht qartë dhe fuqishëm. Agjencia është plotësisht e pavarur politikisht, financiarisht dhe funksionalisht në ushtrimin e kompetencave, detyrave dhe kompetencave të saj dhe drejtori, deputeti dhe punonjësit e saj nuk mund të marrin dhe të kërkojnë udhëzime nga organet shtetërore, organet e komunës, organet e Qytetit të Shkupit dhe nga çdo person tjetër juridik dhe/ose fizik.

Kjo agjenci kryen funksionin e saj mbikëqyrës përmes mbikëqyrjes, e cila mund të jetë:

- mbikëqyrje e rregullt,
- mbikëqyrje të jashtëzakonshme, dhe
- mbikëqyrje e kontrollit.

21 LMDHP, neni 57.

Në kuadër të kompetencave të saj, AMDHP mund të iniciojë procedura për kundërvajtje dhe të vendosë gjoba ndaj një kontrolluesi që do të kryejë shkelje të mbrojtjes së të dhënave, e cila është sjellje e dënueshme në përputhje me dispozitat e LMDHP-së.

Gjyqësori është përgjegjës për punën e tij para Kuvendit, dhe kontrolli i vendimeve të tij ushtrohet nga gjyqësori, në përputhje me parimin kushtetues në nenin 15 të Kushtetutës dhe nenin 6 të KEDNJ-së. [22] Sipas LMDHP-së, Agjencia nuk është kompetente për të mbikëqyrur gjykatat kur vepron brenda funksioneve të tyre gjyqësore, përveç mbikëqyrjes së ligjshmërisë së veprimtarive të ndërmarra në përpunimin tjetër të të dhënave personale të kryera nga gjykatat në përputhje me ligjin.

6.3. Gjykatat

Sipas Kushtetutës, mbrojtja gjyqësore ndaj akteve të administratës shtetërore dhe organeve shtetërore është e garantuar. Gjithashtu, e drejta e qasjes në gjykatë me kushte të barabarta për të gjithë është gjithashtu një e drejtë e garantuar. Në Republikën e Maqedonisë së Veriut, gjykatat organizohen sipas parimit të gjykatave të rregullta. Gjykatat e rregullta organizohen sipas parimit të kompetencës lëndore dhe në ndarjen më themelore ndahen në gjykata civile, penale nga njëra anë dhe gjykata administrative nga ana tjetër.

Gjykata në këtë fushë paraqitet në një rol të dyfishtë. I pari si kontrollues i të dhënave që ka, sepse gjyqtarët nuk janë imunë nga detyrimi për të ndjekur ligjet për mbrojtjen e të dhënave. Për shembull, gjatë kryerjes së veprimeve të tyre, ata duhet të marrin parasysh parimin e minimizimit të të dhënave (ata mund të mbledhin/përpunojnë vetëm të dhënat personale që janë të nevojshme për procedurën) dhe të anonimizojnë siç duhet gjykimet e tyre. Vetëm të dhënat personale të rëndësishme për zgjidhjen e çështjes do të përpunohen në procesverbal. Vëmendje e veçantë duhet t'i kushtohet masës në të cilën palët kanë qasje në dosje. Për shembull, i dyshuari nuk duhet të ketë qasje në të dhënat personale të viktimës ose dëshmitarëve, të tilla si adresa, numri i telefonit dhe të dhëna të tjera që janë të ndjeshme në këtë drejtim.

Për më tepër, gjykata paraqitet në cilësinë e një aktori në mbrojtjen e interesit publik dhe privat në lidhje me të dhënat personale. Këto cilësi do të diskutohen më hollësisht më poshtë.

6.3.1. Gjykatat administrative

Gjykatat administrative janë ndër të tjera kompetente për t'i dhënë mbrojtje gjyqësore vendimeve të Agjencisë së mbrojtjes së të dhënave personale, pra ato ofrojnë mbrojtje ligjore në fushën e çështjeve administrative, në lidhje me mbrojtjen

22 Kushtetuta e Republikës së Maqedonisë së Veriut, neni 15
Garantohet e drejta e ankesës ndaj akteve juridike individuale të miratuara në procedurë të shkallës së parë përpara një gjykate, organi administrativ ose organizate ose institucionesh të tjera që ushtrojnë kompetenca publike.

e të dhënave personale dhe zbatimin e LMDHP-së. Këto gjykata sigurojnë parimet e kushtetutshmërisë dhe ligjshmërisë (në një kuptim më të gjerë, së bashku me zbatimin e standardeve ndërkombëtare).

6.3.2. Gjykatat civile (fusha civile)

Çështja e mbrojtjes së të dhënave personale dhe të drejtave të njeriut, veçanërisht në hapësirën kibernetike, nuk kufizohet vetëm në mbrojtjen e të dhënave dhe sigurimin që të dhënat e dikujt të ruhen siç duhet. Pasoja e përpunimit, ruajtjes ose zbulimit të dobët të të dhënave natyrisht mund të përbëjë shkelje të të drejtave personale, për të cilat sigurohet mbrojtje e përshtatshme para gjykatave civile, për kompensimin e dëmeve. Raste të tilla rregullohen nga rregulli nemo iudex sine actore, si dhe principi actori uncubit probatio. E para do të thotë se gjykata nuk vepron ex officio, por vetëm kur thirret për të shqyrtuar një kërkesë (padi) të spikatur, dhe i takon paditësit të provojë se elementet janë përmbushur nga norma ligjore të cilës i referohet.[23] Në raste të tilla, sipas parimeve të përgjithshme të kompensimit të dëmit, paditësi zakonisht duhet të provojë se:

- ekziston një veprim i dëmshëm (i cili mund të jetë me sjellje aktive ose me mosveprim) dhe aq i përshtatshëm për ta përshkruar, domethënë për ta shpjeguar atë;
- ekziston një dëmtues i identifikuar, i cili është përgjegjës për një veprim të tillë ose nuk ka marrë masa mbikëqyrjeje për të parandaluar veprime të tilla ose për të korrigjuar mosveprimin duke vepruar dhe identifikuar atë;
- është shkaktuar dëm në çdo formë, dhe kryesisht dëm jomaterial si rezultat i shkeljes së të drejtave personale, të cilat duhet të shpjegohen në mënyrë adekuate në atë që përbëhet;[24]
- ekziston një lidhje respektivisht një nexus midis veprimit të dëmshëm dhe dëmtuesit;
- dëmi do të kuantifikohet siç duhet duke përdorur rregullat e provës dhe mjetet e provës në dispozicion;
- nëse dëmi nuk mund të kuantifikohet, respektiivisht kuantifikimi i tij do të shkaktonte vështirësi të konsiderueshme, atëherë Gjykata mund të vendosë për një vlerësim falas.[25]

23 Baza e përgjegjësisë
Neni 141
(1) Personi që dëmton tjetrin me faj është i detyruar ta kompensojë atë.
(2) Për dëmet e shkaktuara nga objektet ose aktivitetet nga të cilat lind një rrezik në rritje i dëmtimit të mjedisit, përgjegjësia do të zbatohet pavarësisht nga faji.
(3) Dëmi, pavarësisht nga fajësia, do të jetë përgjegjës edhe në raste të tjera të parashikuara me ligj.
Dëmi
Neni 142
Dëmi është zvogëlimi i pasurisë së dikujt (dëmi i zakonshëm) dhe parandalimi i rritjes së tij (përfitimi i humbur), si dhe shkelja e të drejtave personale (dëmi jomaterial).
Kërkesë për heqjen e rrezikut të dëmit
Neni 143
(1) Gjithkush mund t'i kërkojë tjetrit të heqë dorë nga burimi i rrezikut nga i cili i kanoset një dëm i konsiderueshëm ose një numër i pacaktuar personash, si dhe të përmbahet nga veprimtaria që rezulton në ngacmim ose rrezik të dëmit, nëse shfaqja e shqetësimit ose dëmit nuk mund të parandalohet me masat e duhura.
(2) Gjykata, me kërkesë të personit në fjalë, urdhëron marrjen e masave të duhura për parandalimin e shfaqjes së dëmtimit ose shqetësimit ose për heqjen e burimit të rrezikut, në kurriz të mbajtësit të burimit të rrezikut, nëse ai vetë nuk e bën këtë.
(3) Nëse dëmi ndodh në kryerjen e një aktiviteti të përfitimit publik për të cilin është marrë një leje nga autoriteti kompetent, mund të kërkohet vetëm kompensim për dëmin që tejkalon kufijtë normalë (dëmi i tepërt).
(4) Në rastin e përmendur në pikën 3 të këtij neni, mund të kërkohen masa të justifikuara shoqërore për të paranda-luar shfaqjen e dëmit ose për ta zvogëluar atë.
Kërkesë për ndalimin e shkeljes së të drejtave personale
Neni 144
(1) Secili ka të drejtë të kërkojë nga një gjykatë ose organ tjetër kompetent të urdhërojë ndërprerjen e një veprimi që cenon të drejtën e tij personale dhe të urdhërojë heqjen e pasojave që rrjedhin nga ky veprim

24 Si kompensohet dëmi jomaterial
Neni 187-a
Dëmi jomaterial do të kompensohet në mënyrë jomateriale (kënaqësia morale) dhe materiale (kënaqësia materiale) në rastet e parashikuara me ligj.
Publikimi i një aktgjykimi ose korrigjimi
Neni 188
Në rast të shkeljes së të drejtave personale, i dëmtuari mund të kërkojë, dhe gjykata mund të urdhërojë, në kurriz të dëmtuesit, publikimin e aktgykimit, respektivisht korrigjimin, tërheqjen e deklaratës me të cilën është kryer shkelja ose diçka tjetër që mund të arrijë qëllimin që arrihet me kompensimin e drejtë monetar.
Kompensim i drejtë monetar
Neni 189
(1) Në rast të shkeljes së të drejtave personale, nëse gjykata konstaton se serioziteti i shkeljes dhe rrethanat e çështjes e justifikojnë atë, ajo do të japë kompensim të drejtë monetar, pavarësisht nga kompensimi për dëmin material, si dhe në mungesë të tij.
(2) Gjatë vendosjes së kërkesës për kompensim të drejtë monetar, gjykata do të marrë parasysh forcën dhe kohëzgjatjen e dëmtimit me të cilin janë shkaktuar dhimbjet fizike, dhimbjet mendore dhe frika, si dhe qëllimin për të cilin shërben kompensimi, por edhe të sigurojë që kompensimi të mos bjerë në kundërshtim me aspiratat që nuk shoqërohen me natyrën dhe qëllimin e tij shoqëror.
(3) Për shkelje të së drejtës së reputacionit dhe të drejtave të tjera personale të personave juridikë, nëse gjykata konstaton se serioziteti i shkeljes dhe rrethanat e çështjes e justifikojnë atë, ajo do të japë kompensim të drejtë monetar, pavarësisht nga dëmi material, si dhe në mungesë të tij.
(4) Përveç këtyre rregullave, në raste të caktuara, kur rregullohet ndryshe me një ligj tjetër, do të zbatohen rregullat e atij ligji.

25 LPC
Neni 209
Nëse përcaktohet se pala ka të drejtë për kompensim për dëmet, shumën monetare ose sendet e zëvendësueshme, por shuma ose sasia e sendeve nuk mund të përcaktohet ose mund të përcaktohet vetëm nga vështirësi joproporcionale, gjykata do të vendosë për këtë në një vlerësim të lirë.

6.3.3. Kompensimi për dëmet sipas LMDHP-së

Është interesante se LMDHP ka dispozita për kompensimin e dëmeve që janë lex specialis. Sipas parimit lex specialis derogit legi generali[26], në pamje të parë duket se këto dispozita zëvendësojnë dispozitat e përgjithshme dhe parimet e kompensimit të dëmeve. Megjithatë, dispozita e referuar në LMDHP i referohet shkeljes së dispozitavetë parë duket se këto dispozita zëvendësojnë dispozitat e përgjithshme dhe parimet e kompensimit të dëmeve. Megjithatë, dispozita e referuar në LMDHP i referohet shkeljes së dispozitave të këtij ligji.[27]

26 VIII MJETET JURIDIKE DHE PËRGJEGJËSIA
E drejta për të parashtruar kërkesë në Agjenci
Neni 97
(1) Çdo subjekt i të dhënave personale ka të drejtë të parashtrojë një kërkesë në Agjenci, nëse vlerëson se përpunimi i të dhënave të tij personale shkel dispozitat e këtij ligji, duke mos vënë në pikëpyetje asnjë mjet tjetër administrativ ose gjyqësor të mbrojtjes ligjore.
(2) Agjencia njofton kërkuesin për rrjedhën dhe rezultatin e procedurës, duke përfshirë mundësinë e mbrojtjes gjyqësore në përputhje me nenin 98 të këtij ligji.
(3) Forma dhe përmbajtja e formës së kërkesës së përmendur në pikën 1 të këtij neni përcaktohen nga drejtori i Agjencisë.
(4) Agjencia do të vendosë nëse gjatë procedurës së palës së kundërt do të zbulojë të dhënat personale të kërkuesit, si dhe të dëshmitarit.
(5) Agjencia, për kërkesën e paraqitur, të përmendur në pikën 1, të këtij neni, kryen mbikëqyrje në përputhje me këtë ligj.
E drejta për mbrojtje gjyqësore efektive ndaj vendimeve të Agjencisë
Neni 98
(1) Çdo person fizik ose juridik ka të drejtë për mbrojtje gjyqësore efektive kundër vendimit ligjërisht të detyrueshëm të Agjencisë në lidhje me të, duke mos vënë në dyshim asnjë mjet tjetër administrativ ose jashtëgjyqësor të mbrojtjes ligjore.
(2) Çdo subjekt i të dhënave personale, duke mos vënë në pikëpyetje mjete të tjera administrative ose jashtëgjyqësore të mbrojtjes ligjore, ka të drejtën e mbrojtjes gjyqësore efektive, kur Agjencia, në përputhje me kompetencat e përcaktuara në nenet 65 dhe 66 të këtij ligji, nuk ka vepruar sipas kërkesës ose nuk ka njoftuar subjektin e të dhënave personale brenda tre muajve për rezultatin e procedurës mbi kërkesën e paraqitur sipas nenit 97 të këtij ligji. E drejta për mbrojtje gjyqësore efektive kundër kontrolluesit ose përpunuesit
Neni 99
(1) Çdo subjekt i të dhënave personale, duke mos vënë në pikëpyetje mjetet e disponueshme administrative ose jashtëgjyqësore të mbrojtjes ligjore, përfshirë të drejtën për të paraqitur një kërkesë në Agjenci, në përputhje me nenin 97 të këtij ligji, ka të drejtën e mbrojtjes gjyqësore efektive, kur vlerëson se i janë shkelur të drejtat e përcaktuara me këtë ligj, si rezultat i përpunimit të të dhënave të tij personale në kundërshtim me këtë ligj.
(2) Subjekti i të dhënave personale ushtron të drejtën e përmendur në pikën 1 të këtij neni duke paraqitur ankesë në gjykatën kompetente në përputhje me ligjin.
Përfaqësimi i subjekteve të të dhënave personale
Neni 100
(1) Subjekti i të dhënave personale ka të drejtë të autorizojë një shoqatë, të paraqesë një kërkesë në emër të saj në lidhje me mbrojtjen e të dhënave të tij personale dhe të ushtrojë të drejtat e përmendura në nenet 97, 98 dhe 99 të këtij ligji, si dhe kur parashikohet me ligj për të ushtruar të drejtën e kompensimit të përmendur në nenin 101 të këtij ligji.
(2) Statuti i shoqatës, i përmendur në pikën 1, të këtij neni, i krijuar në përputhje me ligjin, duhet të përcaktojë objektivat e interesit publik, karakterin e tij jofitimprurës, si dhe kjo duhet të veprojë në mënyrë aktive në fushën e mbrojtjes së të dhënave personale dhe në mbrojtjen e të drejtave dhe lirive të subjekteve të të dhënave personale. E drejta për kompensim të dëmit dhe përgjegjësia
Neni 101
(1) Çdo person që ka pësuar dëm material ose jomaterial si pasojë e shkeljes së këtij ligji, ka të drejtë të marrë dëmshpërblim nga kontrolluesi ose përpunuesi për dëmin e pësuar.
(2) Çdo kontrollues i përfshirë në përpunimin e të dhënave personale do të jetë përgjegjës për dëmin e shkaktuar nga ai përpunim që shkel dispozitat e këtij ligji. Përpunuesi do të jetë përgjegjës për dëmin e shkaktuar nga përpunimi vetëm nëse nuk ka respektuar detyrimet sipas këtij ligji që janë të dedikuara posaçërisht për përpunuesit ose kur ka vepruar jashtë udhëzimeve ligjore të kontrolluesit ose në kundërshtim me to.
(3) Kontrolluesi ose përpunuesi përjashtohet nga përgjegjësia në bazë të pikës 2 të këtij neni, nëse provon se nuk është në asnjë mënyrë përgjegjës për ngjarjen që ka shkaktuar dëmin.
(4) Kur mëshumë se një kontrollues ose përpunues është i përfshirë në të njëjtin përpunim ose një kontrollues dhe përpunues marrin pjesë në të njëjtin përpunim dhe kur, në përputhje me paragrafët 2 dhe 3 të këtij neni, ata janë përgjegjës për çdo dëm të shkaktuar nga përpunimi, atëherë çdo kontrollues ose përpunues do të konsiderohet përgjegjës për të gjithë dëmin, në mënyrë që të sigurohet kompensimi efektiv i dëmit ndaj subjektit të të dhënave personale (përgjegjësi e përbashkët dhe e disa).
(5) Kur kontrolluesi ose përpunuesi sipas pikës 4 të këtij neni ka paguar kompensim të plotë për dëmin e shkaktuar, kontrolluesi ose përpunuesi ka të drejtë të kërkojë nga kontrolluesit ose përpunuesit e tjerë të përfshirë në kompensimin e njëjtë të përpunimit të të dhënave personale që korrespondon me pjesën e tyre të përgjegjësisë për dëmin e shkaktuar, në përputhje me kushtet e përcaktuara në pikën 2 të këtij neni.
(6) Procedura për ushtrimin e të drejtës së kompensimit të dëmit të këtij neni zhvillohet përpara një gjykate kompetente në përputhje me ligjin.

27 LMDHP, neni 101.

6.3.4. Gjykatat penale (fusha penale)

Ashtu si gjykatat civile, gjykatat penale administrojnë gjithashtu drejtësinë dhe gjykimin në rastet që prekin çështjen e trajtuar në këtë udhërrëfyes. Ato gjithashtu kanë parimin nemo iudex sine actore, si dhe parimin actori incubit probatio. Në procedurat penale, parimi imperativ që është mbi të gjitha është prezumimi i pafajësisë.

Gjykatat penale nuk janë vetëm aktorë kur gjykojnë çështje që kanë si të mirë shoqërore të mbrojtur – të dhënat personale dhe të drejtat e njeriut, por në të njëjtën kohë janë edhe garantues të atyre të drejtave, në aspektin e të gjithë pjesëmarrësve, dhe veçanërisht të personave që dyshohen ose akuzohen për krime. Mbi të gjitha, bëhet fjalë për rolin e gjykatave penale në sferën e masave të posaçme hetimore, lejimin, kohëzgjatjen, paraqitjen, ruajtjen dhe shkatërrimin e tyre.

Megjithatë, kur flasim për gjykatat kur ato thirren për të gjykuar për vepra penale individuale, krahasuar me LMDHP-në, në praktikë ka një mbivendosje të caktuar të elementeve që lidhen me atë që përbën veprim penal sipas dispozitave të Ligjit për mbrojtjen e të dhënave personale d he Kodit penal.

Nëse analizohen dispozitat për kundërvajtje në LMDHP, çdo shkelje i referohet një dispozite të caktuar të ligjit dhe veprimi në kundërshtim me atë dispozitë sjell përgjegjësi për kundërvajtje.

Vepra penale që është më afër temës së trajtuar nga ky udhërrëfyes është Keqpërdorimi i të dhënave personale, sipas nenit 149 të Kodit Penal.[28] Ekzistenca e kësaj vepre penale preferon që në formën e saj bazë të ekzistojë:

- Veprim i kundërligjshëm që është në kundërshtim me ligjin! (Megjithëse asociacioni i parë është se për LMDHP, megjithatë, mund të ketë dispozita për trajtimin e të dhënave personale edhe në ligje të tjera, kështu që nuk është vetëm LMDHP.)
- Actus reus është mbledhja, përpunimi ose përdorimi i të dhënave personale.
- Një veprim i tillë bëhet pa pëlqimin e personit, të dhënat e të cilit janë keqpërdorur.

Veprimet e kryerjes së shkeljeve përshkruhen më hollësisht në dispozitat kundërvajtëse të LMDHP-së. Vepra penale, megjithatë, siç përshkruhet, ka një shtrirje relativisht të gjerë. Kur pyetet se çfarë përbën ndryshim midis kundërvajtjes dhe veprës penale, kur akti i ekzekutimit është relativisht i njëjtë, përgjigja mund të qëndrojë në faktin se vepra penale, të paktën në formën e saj themelore, nuk ka grumbullim të të dhënave,

28 Keqpërdorimi i të dhënave personale;
Neni 149
(1) Personi, i cili në kundërshtim me kushtet e përcaktuara me ligj pa pëlqimin e qytetarit, mbledh, përpunon ose përdor të dhënat e tij personale, dënohet me gjobë ose me burgim gjer në një vit.
(2) Dënimi i përmendur në paragrafin 1 do të shqiptohet ndaj një personi që hyn në një sistem informativ kompjuterik të të dhënave personale me synimin për t'i përdorur ato për vete ose për një tjetër për të arritur ndonjë përfitim ose për t'i shkaktuar dëm një tjetri.
(3) Nëse vepra penale e përmendur në pikat 1 dhe 2 është kryer nga një zyrtar gjatë kryerjes së shërbimit, ai dënohet me burgim nga tre muaj deri në tre vjet.
(4) Përpjekja është e dënueshme.
(5) Nëse veprën e përmendur në këtë nen e kryen një person juridik, dënohet me gjobë

dhe ndërsa në rastin e veprave penale, ato zbatohen kur bëhet fjalë për mbledhjen e të dhënave. Megjithatë, një rregull i përgjithshëm dhe universal nuk mund të ekzistojë dhe çdo rast duhet të vlerësohet individualisht, me të gjitha faktet dhe rrethanat që e rrethojnë atë.

Gjykatat penale, përkatësisht procedimet, nuk thirren vetëm për të vepruar në këtë vepër penale, por edhe në vepra të tjera penale që synojnë përdorimin e paligjshëm të të dhënave personale. Kështu, një mori veprash penale kanë si pikë kontakti pak a shumë të dhëna personale, dhe këto janë disa prej tyre:

- Publikimi i paautorizuar i të dhënave personale – neni 148;
- Zbulimi i paautorizuar i një sekreti – neni 150;
- Përgjimi i paautorizuar dhe regjistrimi i zërit – neni 151;
- Inçizimi i paautorizuar – neni 152;
- Prodhimi dhe shpërndarja e pornografisë së fëmijëve – neni 193-a;
- Dëmtimi dhe ndërhyrja e paautorizuar në një sistem kompjuterik – neni 251;
- Krijimi dhe futja e viruseve kompjuterike – neni 251-a;
- Mashtrimi kompjuterik – neni 251-b;
- Falsifikim kompjuterik – neni 379-a;
- Terrorizmi – neni 394-b;
- Shpërndarja e materialit racist dhe ksenofobik përmes sistemit kompjuterik - neni 394 - ç;
- Zhvatja – neni 258;
- Shantazh – Neni 259.

Megjithatë, gjykatat penale jo vetëm që thirren për të gjykuar, por gjithashtu kanë detyrimin të ruajnë të dhënat e marra nga masat MPH, prova të caktuara, veçanërisht prova elektronike/digjitale, materiale të ADN-së, materiale biologjike, etj.

6.4. Prokuroria publike

Prokuroria publike është pjesë e aparatit gjyqësor të një vendi, si një nga hallkat e nevojshme. E organizuar sipas parimit të hierarkisë, por edhe ligjshmërisë dhe legalitetit, mundësive të kufizuara, PP-ja ka për detyrë të ndjekë penalisht kryerësit e krimeve që lidhen me mbrojtjen e të dhënave dhe të drejtat e njeriut në hapësirën kibernetike. Kohët e fundit, prokuroria publike po përballet me një fluks serioz të punëve të gjeneratës së re, të nxitura dhe të udhëhequra nga teknologjitë e reja, për shembull, gjuha e urrejtjes në rrjetet sociale dhe të ngjashme. Në secilin rast individual, shqyrtohet se çfarë përbën një fjalim fitimtar, d.m.th. shprehje, në krahasim me një më të mprehtë, i cili përmban elementet e krimit. Në fakt, shtypja e normës ligjore mund të kryhet vetëm pas sqarimit të plotë të fakteve dhe rrethanave, pra, pas një hetimi të plotë dhe të plotë.

Mesazhi has raste kur nevojiten prova dhe/ose informacione nga i ashtuquajturi VASP (Virtual Assets Service Provider), d.m.th. Ofruesi i shërbimeve të mjeteve virtuale (Bitcoin, FTH, Litecoin, etj.). Ka vetëm një në Republikën e Maqedonisë së Veriut deri më tani.

Një rast tipik nga praktika është mashtrimi i personave të interesuar për tregti, respektivisht blerja e aseteve virtuale (kriptovalutave) dhe kur u japin të dhënat e tyre personale këtyre ofruesve, disa prej tyre janë regjistruar ligjërisht në disa juridiksione, por disa jo. Interesante është se edhe pse ato mund të jenë të vendosura fizikisht në një territor, në fakt, ato janë të dhëna, domethënë regjistrime që ndodhen më shpesh jashtë vendit, në ndonjë server, në ndonjë juridiksion tjetër, për shembull në bankat virtuale, etj.

Përsëri, të gjitha keqpërdorimet e të dhënave personale, respektivisht privatësia, maten dhe vlerësohen rast pas rasti, duke bazuar në të gjitha faktet dhe dëshmitë e mbledhura.

Për të pasur baza për dyshim, dhe më vonë dyshim arsyetuar se është kryer një vepër penale, tipike e nenit 149 të Kodit Penal, është e nevojshme të ketë një nivel minimal të rrezikimit, jo vetëm për të marrë ose përfituar të dhënat, por edhe për t'i përdorur ato në kundërshtim me ligjin.

Megjithatë, kjo vepër penale nuk është gjithmonë se përmban të gjitha elementet, sepse qëllimi i keqpërdorësit është t'i përdorë ato për përfitimin e tyre të paligjshëm ose për një qëllim tjetër. Kështu, nuk është e rrallë që të dhënat personale të merren për t'u përdorur për të marrë kredi të shpejta, për të ushtruar të drejta të tjera si rezultat i këtyre të dhënave (sigurimet shoqërore, pensioni), për të kryer mashtrime në sigurime, etj. Të gjitha këto situata kanë fakte të ngjashme, por produkti përfundimtar në terma të një norme ligjore të përfshirë nuk duhet të jetë vetëm akti i nenit 149 por edhe si rezultat i këtij keqpërdorimi të të dhënave, mund të përfshihen një ose më shumë vepra penale. Qoftë në një bashkim real ose ideal.

6.4.1. Sigurimi i rrugëve të dëshmive ose Chain of Custody

Në raste të tilla, është jashtëzakonisht e rëndësishme të sigurohet paprekshmëria e dëshmive, domethënë të dhënat e marra gjatë hetimit. Nëse dëshmitë nuk kanë një lëvizje të qartë përmes zinxhirit të personave dhe organeve përmes të cilave kalojnë, siguria e tyre nuk garantohet, jo vetëm fizike, por edhe nga pikëpamja e të mos qenit të ndjeshëm ndaj ndryshimit ose modifikimit, atëherë ata humbasin vlerën e dëshmisë.

Nga pikëpamja praktike, duhet të theksohet se këto raste sipas përkufizimit kërkojnë përfshirjen e ekspertëve/ekspertëve teknikë për të nxjerrë të dhënat e nevojshme në një procedurë. Këtu duhet të theksohet qartë se roli i personave teknikë është të shpjegojnë përmbajtjen e të dhënave, për sa i përket vendit ku u gjetën, kush i zotëron ato, respektivishrt kush është përgjegjës për to (metadatat, kush i krijoi, kush i mblodhi, në cilat media, kur dhe sa herë dhe si u modifikuan), por jo të dëshmojnë, respektivisht të japin mendim për të dhënat. Qëllimi përfundimtar është të krijohet, respektivisht të provohet një lidhje midis të dhënave dhe të dyshuarit. Sigurisht, për të përmbushur interesat e procedurës së drejtë, mbrojtja do të ketë të drejtën e shqyrtimit të ndërsjellë të këtij personi.

6.5. Avokatia

Avokatia si pjesë e gjyqësorit ka një rol shumë specifik në këtë fushë. Nga njëra anë, ekziston detyrimi ligjor dhe etik në përputhje me aktet dhe kodin e dhomës për ruajtjen dhe përpunimin e të dhënave personale për klientët e vet, dhe nga ana tjetër, ekziston detyrimi i duhur për t'i mbrojtur ata, edhe kur këto të dhëna kanë kuptim në një procedurë të caktuar. Mbi të gjitha, i referohet detyrimit për mbajtjen e sekretit të avokatit, atij që i është besuar gjatë punës, si dhe të drejtës për të mos dëshmuar për atë që avokati ka mësuar gjatë punës së tij dhe marrëdhënies me palën e tij.

Nga ana tjetër, avokatia është një profesion publik dhe për këtë arsye mbledh të dhëna për të cilat, nga ana tjetër, është gjithashtu përgjegjës, si të gjitha subjektet e tjera. Sidomos sot, në epokën digjitale, kur të dhënat janë gjithnjë e më shumë në formë digjitale. Me rritjen e komunikimit të avokatit me palët e tij dhe me organet, rriten edhe detyrimet. Kjo do të thotë që avokatët nuk kanë imunitet kur bëhet fjalë për të dhënat personale dhe aspektin e të drejtave të njeriut në hapësirën kibernetike, por kanë një detyrim pozitiv për të ruajtur dhe treguar mundësinë e keqpërdorimit.

Një nga detyrimet më të mëdha të Avokatit të Popullit është njohja në mënyrën e duhur dhe sa më të plotë të teknologjive të reja dhe aspekteve normative të tyre, në mënyrë që të jetë në gjendje të njohë rreziqet e paraqitura prej tyre në lidhje me abuzimet, në mënyrë që të jetë në gjendje të ofrojë këshilla ligjore në kohë, të sakta dhe efektive. Nga ana tjetër, përmes këtyre postulateve, ata duhet të jenë në gjendje të përdorin siç duhet kompetencat procedurale dhe materiale kur paraqiten në rolin e një ndihmësi procedural, pra një përfaqësuesi dhe një mbrojtësi në procedura (civile, administrative, penale, kundërvajtje, etj.).

Gjatë procedurave, avokati ka mundësi të marrë konstatime respektivisht gjetje dhe mendime nga persona të aftë dhe këshilltarë teknikë njësoj si prokurori në procedurat penale dhe në kushte të barabarta me palën tjetër. Folëm për postulatet që zbatohen në këto kushte të mësipërme në seksionin për prokurorin publik.

6.6. Policia

Kur flasim për policinë, sigurisht, asociacioni i parë është se roli i saj nga pikëpamja e subjektit të këtij udhërrëfyes është në zbulimin e kundërvajtjeve dhe veprave penale. Sipas krijimit të sistemit të drejtësisë penale në Republikën e Maqedonisë së Veriut, ekzistojnë dy lloje të hetimeve, përkatësisht para-hetime, të ndërmarra nga zyrtarët policorë. Është një hetim reaktiv dhe proaktiv. Postulatet dhe shembujt që vlejnë për veprimet e prokurorisë publike vlejnë edhe për policinë, respektivisht policinë gjyqësore.

Në të dhënat personale, policia duhet të përshtatet në përputhje me zhvillimin e shoqërisë dhe shfaqjen e formave të reja të kriminalitetit.

Veprat penale të kryera përmes sistemeve kompjuterike dhe/ose internetit, që synojnë shkeljen e të drejtës së privatësisë, si një e drejtë e njeriut, dhe që synojnë shkeljen e të dhënave personale, mund të përshkruhen në katër mënyra:

1. Këto janë veprime të paligjshme që përbëjnë shkelje të të mirave të rëndësishme individuale dhe shoqërore për të cilat ligji parashikon sanksion penal.
2. Ato bëhen në mënyrë specifike, duke përdorur mjete dhe qëllime specifike të veprës penale – dhe kjo është me përdorimin e sistemeve dhe rrjeteve kompjuterike.
3. Këto vepra janë nën mbrojtje të veçantë – për shembull, siguria e sistemeve dhe rrjeteve kompjuterike, transmetimi i të dhënave kompjuterike të ruajtura në tërësi ose në një pjesë të caktuar.
4. Qëllimi i kryerësit të këtyre veprave është përfitimi i kundërligjshëm (i prekshëm ose i paprekshëm) ose dëmtimi i të tjerëve.[29]

Megjithatë, policia nuk mund të shihet si një entitet i izoluar në luftën kundër kriminalitetit, pasi shkeljet e ligjit nuk janë gjithmonë vepra penale dhe anasjelltas. Ajo që mbulohet nga rregullorja që parashikon të dhënat personale dhe mbrojtja e tyre nuk është gjithmonë nën juridiksionin respektivisht kompetencat e policisë. Kështu, për shembull, kur bëhet fjalë për keqpërdorimin e të dhënave personale, juridiksioni përcaktohet këtu nga policia, sepse ndoshta ekziston një bazë për dyshimin e një vepre penale. Në të kundërt, nëse bëhet fjalë për një menaxhim të paligjshëm të mbledhjes së të dhënave personale, megjithëse të njëjtat fakte mund të shkaktojnë prima facie dyshimin për një vepër penale dhe një shkelje rregullatore sipas LMDHP-së, kjo e fundit ka të ngjarë të mbizotërojë, pasi ekziston ende një grumbullim i të dhënave personale, të cilat për çfarëdo arsye mund të kenë parregullsi të caktuara në menaxhimin e saj, pa pasur vepër penale.

29 I. Marcella, Albert J. II. Greenfield, Robert, Cyber Forensics, CRC Press, 2005, f. 48.

Nëse marrim parasysh se

vepra penale = veprim (mosveprim) + **kundërligjshmëri** + **të përshkruhet si një qëndrim i dënueshëm** +

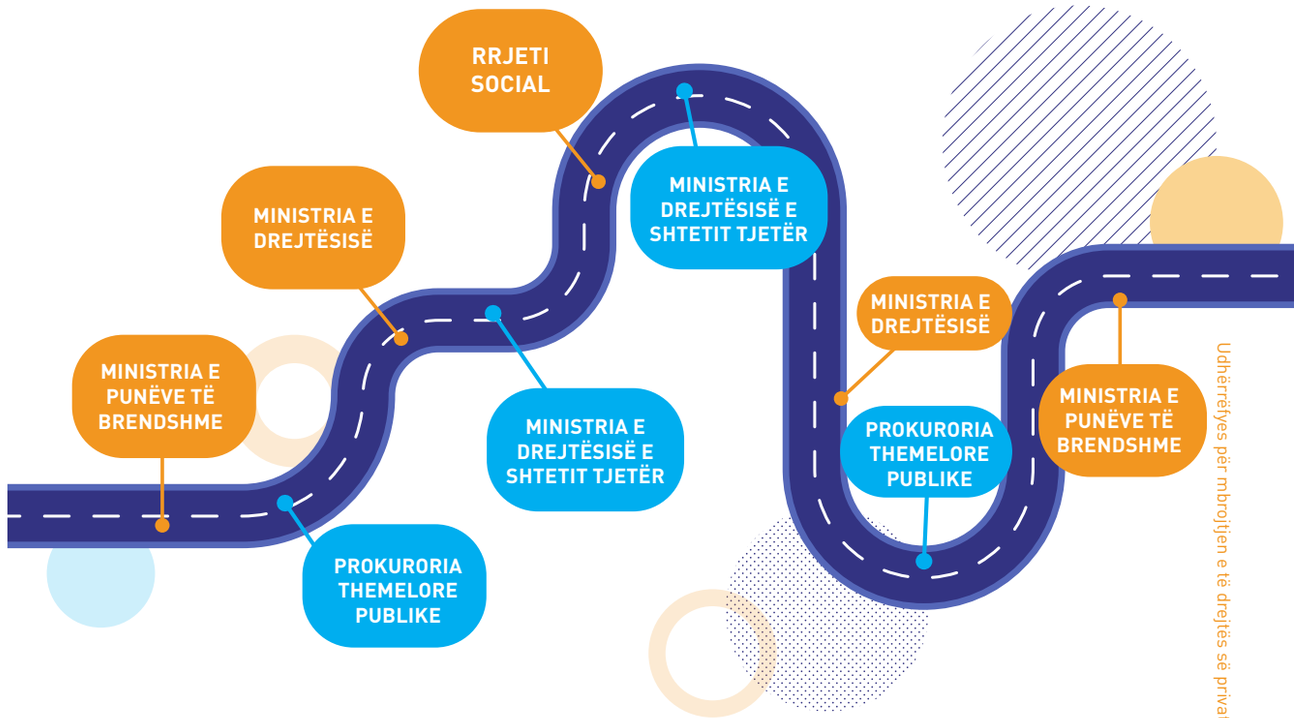
vullnetar ndaj krimit (qëllim/ neglizhencë)

Atëherë mungesa e ndonjërit prej këtyre elementëve do të thotë se nuk ka vepra penale. Por kjo nuk përjashton ekzistencën e ndonjë delikti tjetër.

Kështu, për shembull, për fshirjen e profileve të rrejshme në rrjetet sociale, ekziston juridiksioni respektivisht kompetenca me LMDHP, ndërsa për pasojën që ka ndodhur si pasojë e krijimit të profilit të rrejshëm (dëmtim, mashtrim, zhvatje, etj.) policia do të kishte juridiksion respektivisht do të ishte kompetente, sepse është vepër penale e parashikuar nga Kodi Penal.

Një lloj i veçantë i procedurave janë kërkesat për ndihmë juridike ndërkombëtare, të cilat janë të shpeshta, duke pasur parasysh rrethanat që të dhënat personale në internet nuk janë të vendosura në territorin e një vendi, por përkundrazi, ato mund të jenë jo vetëm në një vend të huaj, por edhe në disa prej tyre. Së fundi, nuk është e pazakontë të identifikohen subjektet që operojnë sisteme të tilla, që do të thotë se duhet të kërkohet ndihmë juridike ndërkombëtare. Megjithëse jetojmë në një shoqëri ku kryesisht komunikohet në mënyrë elektronike, këto procedura janë të shkruara në mënyrë rigoroze, përfshijnë një mori institucionesh dhe ka shumë pritje për reagime.

Rruga e asaj ndihme juridike ndërkombëtare duket kështu:



6.7. Organet shtetërore

Organet shtetërore gjithashtu kanë një rol të rëndësishëm për të luajtur. Ato shfaqen kryesisht si kontrollues të të dhënave personale dhe kanë koleksione të të dhënave personale që mund të jenë të shkallës më të lartë të mbrojtjes. Në procedurat administrative, mbrojtja mund të kërkohet, veçanërisht për të drejtat e subjekteve të të dhënave (p.sh. e drejta e qasjes, korrigjimi, fshirja dhe kundërshtimi) ose përcaktimi i paligjshmërisë së përpunimit të të dhënave (pasi kjo nuk është në përputhje me parimet e mbrojtjes së të dhënave dhe/ose dispozitat e tjera në lidhje me ligjshmërinë e përpunimit të të dhënave).

6.8. Organizatat e shoqërisë civile

Organizatat e shoqërisë civile kanë një rol të jashtëzakonshëm në ndërtimin e institucioneve demokratike dhe zhvillimin e vetëdijësimit për rëndësinë e mbrojtjes së të drejtave të njeriut, duke përfshirë ato në hapësirën e internetit. Përmes trajnimeve, fushatave, përfaqësimeve strategjik dhe pjesëmarrjes në krijimin e politikave të qarta, organizatat e shoqërisë civile shpesh janë mjeti kryesor në rritjen e vetëdijësimit në shoqëri dhe ndërtimin e mekanizmave mbrojtës.

VI.

6.9. Kompanitë

Gjatë operacioneve të tyre të përditshme, kompanitë mbledhin dhe përpunojnë të dhënat personale dhe kështu luajnë rolin e kontrollorëve. Detyrimi i tyre është i dyfishtë, si ndaj rregullatorit, respektivisht legjislacionit, për të qenë në përputhje me kërkesat ligjore për mbrojtje, ashtu edhe ndaj personave, të dhënat e të cilëve ata ruajnë dhe përpunojnë, pra punonjësit e tyre, por edhe ndaj të tretëve që nuk janë në punësim, por të dhënat e të cilëve ata kanë qasje.

Këtu duhet përmendur në mënyrë të veçantë konglomeratet e mëdha ndërkombëtare, respektivisht kompanitë shumëkombëshe që mbledhin të dhëna brenda kompetencave të tyre, respektivisht shërbimet dhe produktet që ato ofrojnë. Këto përfshijnë rrjetet sociale të pashmangshme (Facebook, Instagram, X, LinkedIn, etj.) dhe ofruesit e shërbimeve të internetit (Google, Yahoo, etj.).

6.10. Individët

Një nga rregullat bazë të mbrojtjes së të dhënave është, në fakt, se është detyrimi kryesor i individit. Gjithkush ka të drejtën e privatësisë, por edhe detyrimin për t'u kujdesur për sigurinë e të dhënave të veta. Kohët e fundit, me zhvillimin e teknologjisë, janë personat fizikë ata që, me veprimin e tyre, respektivisht me mosveprimin e mbikëqyrjes së duhur, zbulojnë të dhënat e tyre dhe kështu ekspozohen ndaj rreziqeve. Kështu, për shembull, shembuj eklatant janë ndarja e një kodi PIN të kartës së pagesës, lënia e të dhënave të llogarisë në faqet e internetit pa kontrolluar besueshmërinë e tyre, dhënia e informacionit mjekësor kudo, hapja e emaileve të dyshimta që synojnë instalimin e softuerit me qëllim të keq, etj. Prandaj, individët nuk janë vetëm viktima, por edhe një aktor aktiv në fushën e mbrojtjes së të dhënave, sepse vetë-mbrojtja ndonjëherë është mbrojtja më e mirë.

07

TË DHËNAT PERSONALE, TË DREJTAT E NJERIUT DHE ÇËSHTJA E ARBITRABILITETIT

VII.

TË DHËNAT PERSONALE, TË DREJTAT E NJERIUT DHE ÇËSHTJA E ARBITRABILITETIT

Zbatimi i Rregullores së përgjithshme të mbrojtjes së të dhënave (GDPR) të 25 majit 2018 shkaktoi një valë reagimesh përtej komunitetit të arbitrazhit.

Shkurtimisht, pyetja është nëse të dhënat personale janë një fushë e së drejtës që është e arbitrazhit, domethënë mund të bien nën një nga regjimet për zgjidhjen alternative të kontesteve (arbitrazhi), dhe jo vetëm vendase, por edhe ndërkombëtare. Zbatimi i Ligjit për mbrojtjen e të dhënave personale gjatë procedurës së arbitrazhit mund të jetë me të vërtetë shumë kompleks (dhe potencialisht i rëndë) dhe mund të imponojë detyrime shtesë për palët (institucionet e arbitrazhit) të përfshira në procedurë, të cilat duhet të merren shumë seriozisht duke pasur parasysh rreziqet e përgjegjësisë që rrjedhin nga GDPR.

Pavarësisht nga rëndësia e zbatimit të GDPR-së në arbitrazhin ndërkombëtar, mendimi mbizotërues duket se është se do të ishte për të ardhur keq të konsiderohej se regjimet e reja ligjore që rregullojnë dhe mbrojnë të dhënat (siç është GDPR) janë vetëm një burim shqetësimi për komunitetin global të arbitrazhit. Përkundrazi, këto regjime ligjore që krijojnë detyrime të reja ligjore ka të ngjarë të gjenerojnë sfida të reja ligjore dhe konteste ligjore që përsëri mund t'i paraqiten arbitrazhit dhe mekanizmave të tjerë alternativë për zgjidhjen e mosmarrëveshjeve në rrethana të caktuara. Rrjedhimisht, nuk është për t'u habitur që ofruesit e arbitrazhit dhe zgjidhjes alternative të mosmarrëveshjeve (ADR) janë shfaqur në mënyrë që të ofrojnë mjete online për zgjidhjen e kontesteve në lidhje me GDPR (posaçërisht për kontestet e shkeljes së të dhënave). Në çdo rast, është e qartë se në ekonominë tonë të drejtuar nga të dhënat, në të cilën të dhënat janë dhe do të jenë një nxitës kryesor i inovacionit dhe fuqia, fushëveprimi dhe rëndësia strategjike e 'kontesteve për të dhënat', përgjithësisht të përcaktuara si mosmarrëveshje në lidhje me kushtet e mbrojtjes, qasjen në të dhëna dhe/ose përdorimin e të dhënave në rrethana të caktuara, do të (vazhdojnë) të rriten ndjeshëm në të ardhmen.[30]

30 Using arbitration and adr for disputes about personal and non-personal data: what lessons from recent developments in Europe? – ARIA – Vol. 30, No. 2, Jacques de Werra, Mars, 2020.

7.1. Përgjegjësia për të mbrojtur privatësinë dhe të dhënat personale në kuadër të rendit ligjor vendas dhe në kuadër të rendit ligjor ndërkombëtar

Në rendin shtëpiak, përgjegjësia i takon kontrolluesit ose përpunuesit ose personit tjetër juridik ose fizik që ka kryer ndonjë shkelje të privatësisë. Me fjalë të tjera, nëse një person fizik kryen një vepër penale në kuadër të fushës të së drejtës penale kundër një personi tjetër juridik ose fizik, është sui generis, në kuadër të rendit juridik vendas. Sigurisht, kryerësi i çdo keqtrajtimi (me veprim aktiv ose pasiv) mund të jetë edhe shteti. Ajo është e barabartë në rendin e saj juridik të brendshëm sipas aftësisë së saj të huaj me aktorët e tjerë.

Në rendin juridik ndërkombëtar, shteti ka gjithmonë subjektivitet juridik.

Pse e hapim këtë temë në këtë udhërrëfyes?

Zakonisht, organet vendase, kur vendosin brenda kompetencave të tyre, i përmbahen normave të rendit juridik vendas gjatë ushtrimit të kompetencave të tyre kushtetuese dhe ligjore, pa marrë parasysh standardet ndërkombëtare në të cilat shteti ka aderuar dhe ato janë bërë pjesë e rendit të brendshëm.

Në shekullin e njëzetë, dhe tani veçanërisht në shekullin e njëzet e një, sfida më e madhe e çdo rendi juridik është të kuptojë se, megjithëse shtetet janë sovrane dhe të pavarura, megjithatë rendi juridik që ka pranuar normat ndërkombëtare nuk është ekskluzivisht i tyre, por është pjesë e një rendi juridik ndërkombëtar më të madh dhe më të gjerë. Sigurisht, në shkallën aktuale të zhvillimit të ligjit, ky është një përfitim civilizues dhe një atribut i çdo shoqërie demokratike.

Organet vendase që vendosin brenda rendit juridik të Republikës së Maqedonisë së Veriut kanë një detyrim, jo një opsion, për të zbatuar standardet ndërkombëtare, d.m.th. rregulloret. Një detyrim i tillë lind jo vetëm nga Kushtetuta, por edhe nga një mori rregulloresh të tjera, për shembull Ligji për gjykatat, Ligji për përgjegjësinë civile për fyerje dhe shpifje, etj.

Një postulat i tillë do të shpjegohet më së miri me sa vijon: Shtetet mund të mbajnë përgjegjësi për veprimet dhe mosveprimet e tyre, për mospërmbushjen e detyrimeve të marra përsipër ndërkombëtarisht, etj. Megjithatë, gjërat janë pak më komplekse kur bëhet fjalë për të kuptuar burimet e kësaj doktrine, kur bëhet fjalë për operacionet e përditshme të çdo organi administrativ dhe gjyqësor në Republikën e Maqedonisë së Veriut, megjithëse ligje të caktuara synojnë qartë gjykimet e huaja, si mund të zbatohet drejtpërdrejt, së bashku me pikëpamjet dhe arsyetimet e shprehura në to.

VII.

Dokumentet dhe konventat ndërkombëtare përcaktojnë standardet minimale të trajtimit dhe procedurave kur bëhet fjalë për normat që ato përcaktojnë. Ekzistojnë instrumente të ndryshme ndërkombëtare që kanë miratuar rregulla që duhet të shqyrtohen, interpretohen dhe zbatohen brenda kornizës së ligjit vendas.

Standardet ndërkombëtare janë të zbatueshme për një sërë arsyesh:

- Së pari, çdo ligj ose korpus ligjesh nuk mund të shikohet dhe interpretohet në mënyrë të izoluar brenda rendit juridik vendas, e lëre më në rendin juridik ndërkombëtar.
- Së dyti, secili vend që zgjedh të ratifikojë ose miratojë një instrument të veçantë ligjor ndërkombëtar merr përsipër t'i përmbahet parimeve të këtij instrumenti ndërkombëtar dhe të përshtatë legjislacionin dhe/ose praktikat e tij në përputhje me rrethanat.
- Së treti, kjo kërkohet nga rregullat themelore të së drejtës ndërkombëtare në lidhje me përgjegjësinë e shteteve për veprimet e tyre të gabuara. Theksi është në rregullat dytësore të përgjegjësisë së shtetit, pra kushtet e përgjithshme sipas së drejtës ndërkombëtare që shteti të mbahet përgjegjës për veprime ose mosveprime të gabuara dhe pasojat juridike që rrjedhin prej tyre. "Draft nenet për përgjegjësitë e shteteve për akte të dëmshme ndërkombëtare me komente" (projekt nenet)[31] praktikisht kodifikojnë të drejtën zakonore ndërkombëtare dhe për këtë arsye janë të detyrueshme për të gjitha shtetet.

Sipas nenit 1, "çdo akt i dëmshëm ndërkombëtar i një shteti përfshin përgjegjësinë ndërkombëtare të atij shteti". Ndër të tjera, komenti i saj përmend nenin 1 si parimin themelor që qëndron në themel të neneve në tërësi, i cili është se shkelja e së drejtës ndërkombëtare nga një shtet përfshin përgjegjësinë e tij ndërkombëtare.

Një akt i dëmshëm ndërkombëtar i një vendi mund të përbëhet nga një ose më shumë akte ose mosveprime ose një kombinim i të dyjave. Nëse ka pasur një akt të dëmshëm ndërkombëtar varet, së pari, nga kërkesat e detyrimit që thuhet se është shkelur dhe, së dyti, nga kushtet e kuadrit për një akt të tillë, të cilat janë përshkruar në pjesën e parë.

Termi "përgjegjësi ndërkombëtare" mbulon marrëdhëniet e reja juridike që lindin sipas së drejtës ndërkombëtare për shkak të aktit ndërkombëtarisht të gabuar të një shteti. Përmbajtja e këtyre marrëdhënieve të reja juridike përshkruhet në pjesën e dytë.

Në zbatim të nenit 2, ka një veprim të dëmshëm ndërkombëtar të një shteti kur sjellja përbëhet nga një veprim ose mosveprim:

(a) sipas së drejtës ndërkombëtare që i atribuohet shtetit; dhe
(b) përbën shkelje të një detyrimi ndërkombëtar të shtetit.[32]

Një nga nenet më të rëndësishme që dallon karakterizimin e një akti të tillë dhe ndërlidhjen e tij me ligjin vendas është neni 3. Në nen thuhet se "karakterizimi i aktit të një shteti si i dëmshëm ndërkombëtarisht rregullohet nga e drejta ndërkombëtare. Ky karakterizim nuk cenohet nga karakterizimi i të njëjtit akt si i ligjshëm sipas të drejtës të brendshme.[33]"

Në rastin ELSIE, para GJND-së, këshilli i Gjykatës ka theksuar këtë rregull, duke deklaruar se:

Pajtueshmëria me ligjin vendas dhe pajtueshmëria me dispozitat e një kontrate janë çështje të ndryshme. Ajo që është shkelje e kontratës mund të jetë e ligjshme në ligjin e brendshëm dhe ajo që është e paligjshme në ligjin e brendshëm mund të jetë plotësisht e pafajshme për një shkelje të dispozitës së kontratës.

Shumë shpesh, pushtetet vendase (me të drejtë) vlerësuan se veprimet dhe/ose mosveprimet e tyre ose zbatimi/interpretimi i ligjit në një situatë të veçantë duhet të shihen nga këndvështrimi i rendit ligjor vendas. Dhe kur i mbijetojnë testit të mjeteve juridike, kjo i bën ata të ligjshëm, domethënë jo të gabuar.

Megjithatë, në mungesë të ndonjë dyshimi, ky nen synon të fshijë të gjitha interpretimet e marrëdhënies midis mënyrës se si një akt shihet nga këndvështrimi i ligjit vendas dhe ndërkombëtar dhe cili këndvështrim është i rëndësishëm, nga këndvështrimi i së drejtës ndërkombëtare.

Neni 4 i referohet sjelljes së organeve të një vendi dhe sipas këtij neni,

1. Sjellja e çdo organi shtetëror konsiderohet një akt i këtij shteti sipas së drejtës ndërkombëtare, pavarësisht nëse organi kryen një funksion legjislativ, ekzekutiv, gjyqësor apo ndonjë funksion tjetër, pavarësisht nga pozicioni që zë në organizimin e shtetit dhe pavarësisht nga karakteri i tij si organ i pushtetit qendror ose i një njësie territoriale të shtetit.

2. Organi përfshin çdo person ose subjekt që e ka këtë status sipas ligjeve të brendshme të atij shteti.[34]

Që do të thotë se parimi i atribuimit zbatohet për të gjitha organet, duke përfshirë gjykatat.

31 "Draft-nenet mbi përgjegjësitë e shteteve për aktet me komente të dëmshme ndërkombëtare", 2001, Komisioni ligjor ndërkombëtar i OKB-së.

32 "Draft-nenet mbi përgjegjësitë e shteteve për aktet me komente të dëmshme ndërkombëtare", 2001, Komisioni ligjor Ndërkombëtar i OKB-së.

33 Sa i përket të parit prej këtyre elementeve, ndoshta vendimi më i qartë gjyqësor është ai i PCIJ në trajtimin e shtetasve polakë (Trajtimi i shtetasve polakë dhe personave të tjerë me origjinë polake ose të folurit në territorin e Danzigut, Opinioni këshillimor, 1932, P.C.I.J., Seria A/B, Nr. 44, f. 4.) Gjykata mohoi të drejtën e qeverisë polake për të paraqitur pyetje në organet e Lidhjes së Kombeve në lidhje me zbatimin e disa dispozitave të Kushtetutës së Qytetit të Lirë të Danzigut me arsyetimin se: Sipas parimeve të pranuara përgjithësisht, shteti nuk mund të mbështetet, në argumentin kundër një shteti tjetër, në dispozitat e Kushtetutës së atij shteti tjetër, por vetëm në të drejtën ndërkombëtare dhe detyrimet ndërkombëtare që janë pranuar siç duhet (...) [S] anasjelltas, një shtet nuk mund të deklarohet kundër një shteti tjetër, i cili ka dispozita në Kushtetutën e tij me qëllim shmangien e detyrimeve që i imponohen nga e drejta ndërkombëtare ose traktatet në fuqi (...) Zbatimi i Kushtetutës së Danzigut mund (...) të rezultojë në shkelje të një detyrimi ndërkombëtar (...) qoftë sipas traktateve ose sipas të drejtës së përgjithshme ndërkombëtare (...) Por në raste të kësaj natyre, nuk është Kushtetuta dhe rregulloret e tjera si të tilla, por detyrimet ndërkombëtare që kërkojnë përgjegjësinë e Qytetit të lirë.

34 "Draft-nenet mbi përgjegjësitë e shteteve për aktet me komente të dëmshme ndërkombëtare", 2001, Komisioni ligjor Ndërkombëtar i OKB-së. Cituar në Judicial supervision in cases of deprivation of liberty of asylum seekers and the responsibility on the state to adhere to international legal standards. Aleksandar Godzo, Ana Dangova Hug, Dime Gjorçevski, 2021.

Në mënyrë të përmbledhur, kjo do të thotë se nëse një veprim, procedurë, etj mund të jetë plotësisht i ligjshëm nga pikëpamja e së drejtës së brendshme, i njëjti veprim, procedurë mund të jetë plotësisht në kundërshtim me të drejtën ndërkombëtare.

Është e rëndësishme për ne dhe për këtë analizë që një qëndrim i tillë është ndërtuar gjatë dekadave dhe për rastet që janë ende aktuale sot dhe përfaqësojnë një burim të argumentimit ligjor dhe ligjit.

Organet vendase, dhe veçanërisht gjykatat, duke u mbështetur ekskluzivisht në të drejtën e brendshme dhe duke injoruar praktikisht të drejtën ndërkombëtare, nuk vënë në dyshim ligjshmërinë individuale në kuptimin më të gjerë të ndonjë subjekti, por në të njëjtën kohë ia atribuojnë përgjegjësinë shtetit, autoritetet e të cilit janë, jo vetëm brenda vendit, por edhe ndërkombëtarisht.

Pra, ajo që është e ligjshme në të drejtën e brendshme nuk do të thotë gjithmonë se është në përputhje me të drejtën ndërkombëtare.

Në kontekstin e çështjes së këtij udhërrëfyesi, veçanërisht kur shteti paraqitet si aktor në fushën e mbrojtjes së privatësisë dhe të dhënave personale, është e domosdoshme të zbatohen standardet ndërkombëtare, pavarësisht nga rregullorja në rendin ligjor vendas, e cila përndryshe mund të rregullojë një çështje ose një çështje.

7.2. Mbrojtja e të dhënave dhe liria e shprehjes

Mbrojtja e të dhënave dhe liria e shprehjes janë dy të drejta themelore midis të cilave duhet të ketë një ekuilibër. Prandaj, rregullimi ligjor i kritereve që balancojnë të drejtën e mbrojtjes së të dhënave personale me lirinë e shprehjes dhe informacionit është me rëndësi të madhe. KEDNJ ka hartuar një sërë kriteresh për t'u marrë në konsideratë, të cilat janë reflektuar edhe në disa ligje kombëtare. Sipas LMDHP-së, ky proces i kushton vëmendje të veçantë:

- natyrën e të dhënave personale,
- rrethanat në të cilat merren të dhënat,
- ndikimi i informacioneve të publikuara në diskutimin e interesit publik,
- njohuritë e personit fizik në fjalë dhe lënda e informacionit,
- sjellja e mëparshme e personit fizik në fjalë,
- pëlqimin paraprak të personit fizik në fjalë,
- përmbajtjen, formën dhe pasojat e publikimit të këtij informacioni.

E drejta e shprehjes përfshin edhe të drejtën e informimit.[35]

35 LMDHP, neni 81 paragrafi 4.

7.3. Mbrojtja e të drejtës së privatësisë dhe mbrojtja e të dhënave personale përmes deklaratave përkatëse nga GJEDNJ dhe GJED

Praktika gjyqësore e GJEDNJ-së ndjek relativisht mirë arritjet teknologjike të njerëzimit, të paktën për sa i përket Këshillit të Evropës, organ i të cilit është.

Për një shikueshmëri më të mirë, praktika gjyqësore sublimohet me nëntituj, respektivisht fjalë kyçe.[36]

7.3.1. Nocioni i të dhënave personale dhe fushëveprimi i tyre

Në vendimet e saj, Gjykata shpjegon konceptin e "të dhënave personale" duke iu referuar Konventës së Këshillit të Evropës nr. 108 për mbrojtjen e individëve në lidhje me përpunimin automatik të të dhënave personale të 28 janarit të vitit 1981, i cili hyri në fuqi në vitin 1985 dhe u përditësua në vitin 2018 ("Konventa 108"), qëllimi i të cilit është "të sigurojë në territorin e secilës Palë për çdo individ (...) respektimin e të drejtave dhe lirive themelore të tij, dhe në veçanti të drejtën e tij për privatësi, në lidhje me përpunimin automatik të të dhënave personale në lidhje me të" (neni 1) [Amann v. Zvicra (GC), 2000, § 65 Haralambi kundër Rumanisë, 2009, § 77]. Gjykata ka theksuar qartë se, sipas nenit 2 të Konventës 108, koncepti i të dhënave personale përcaktohet si "çdo informacion në lidhje me një person të identifikuar ose të identifikueshëm" [Amann v. Zvicra (GC), 2000, § 65; Haralambie v. Rumania, 2009, § 77].

7.3.2. Çfarë mbulojnë

Këto të dhëna mbulojnë jo vetëm informacionin që identifikon drejtpërdrejt individin ("subjektin e të dhënave"), siç janë emri dhe mbiemri [Guillot v. Franca, 1996, §§ 21-22; Mentzen v. Letonia (dhjetor), 2004; Güzel Erdagöz kundër Turqisë, 2008, § 43; Garnaga kundër një elementi që në mënyrë indirekte identifikon një person, siç është një adresë IP dinamike (protokolli i internetit); Benedik kundër Sllovenia, 2018, §§ 107-108].

7.3.3. Personat juridikë dhe të dhënat personale

Ndërsa rezulton se çështja e mbrojtjes së të dhënave personale ka të bëjë kryesisht me individët, në lidhje me të drejtën e tyre sipas nenit 8 për të respektuar jetën e tyre private, personat juridikë gjithashtu kanë të drejtë të mbështeten në këtë të drejtë para Gjykatës nëse kanë të bëjnë drejtpërdrejt me ndonjë masë që shkel të drejtën e tyre për respektimin e "korrespondencës" ose "shtëpisë" së tyre. Ky ishte rasti, për shembull, kur kompania u urdhërua të sigurojë një kopje të të gjitha të dhënave në një server të

36 Udhërrëfyes për praktikën gjyqësore të konventës – Mbrojtja e të dhënave, Gjykata evropiane e të drejtave të njeriut, 12/98. Përditësimi i fundit: 31.08.2022.

ndarë me kompani të tjera (Bernh Larsen Holding AS dhe të tjerët v. Norvegjia, 2013, § 106) ose ku Ministria e mbrojtjes, me urdhër, përgjoi komunikimet e OJQ-ve të lirive civile (Liria dhe të tjerët kundër Mbretërisë së Bashkuar, 2008, § 56-57). Megjithatë, në rastin e masave që përfshijnë mbrojtjen e të dhënave personale të anëtarëve të një organizate fetare dhe respektimin e "jetës private" të tyre, organizata nuk u prek drejtpërdrejt dhe për këtë arsye nuk ishte "viktimë" në kuptimin e nenit 34 të Konventës (Avilkina dhe të tjerët kundër Rusisë, 2013, § 59).

7.3.4. Format e të dhënave personale

Të dhënat personale mund të marrin shumë forma të ndryshme. Për shembull:

- Informacione për parapaguesit e internetit në lidhje me adresat IP specifike dinamike të caktuara në periudha të caktuara (Benedik v. Sllovenia, 2018, §§ 108-109).
- Regjistrimet e marra për përdorim si mostra zanore, të cilat janë të një natyre të përhershme dhe i nënshtrohen një procesi analize që lidhet drejtpërdrejt me identifikimin e një personi në kontekstin e të dhënave të tjera personale (P. G. dhe J. H. v. Mbretëria e Bashkuar, 2001, § 59).
- Mostrat e qelizave dhe profilet e ADN-së [S. and Marper v. the United Kingdom (GC), 2008, §§ 70-77] ose shenjat e gishtërinjve (ibid., § 84), të cilat, pavarësisht karakterit të tyre objektiv dhe të pakundërshtueshëm, përmbanin informacione unike të personit në fjalë dhe lejonin identifikimin e tij/saj të saktë në një gamë të gjerë rrethanash (ibid., § 85).
- Informacione për një person të caktuar të marrë nga dokumentet bankare, qoftë në lidhje me detaje të ndjeshme apo veprimtari profesionale (M. N. dhe të tjerët kundër San Marino, 2015, §§ 51 e vijues).
- Të dhëna mbi profesionin e një personi të identifikuar ose të identifikueshëm të mbledhur dhe ruajtur nga policia (Khelili v. Zvicër, 2011, § 56).
- Të dhënat dhe mesazhet e përdorimit të internetit ("Yahoo") nga një punonjës në vendin e punës, të marra përmes mbikëqyrjes [Bărbulescu v. Rumania (GC), 2017, §§ 18, 74-81].
- Një kopje e të dhënave elektronike të sekuestruara në një zyrë ligjore, megjithëse nuk janë deshifruar, transkriptuar ose atribuar zyrtarisht pronarëve të tyre (Kırdök dhe të tjerët v. Turqi, 2019, § 36).
- Të dhënat e mbledhura në kontekstin e mbikëqyrjes me video të pazbuluar të një universiteti (Antoviç dhe Mirkoviç kundër Malit të Zi, 2017, § 44-45).
- Informacion mbi të ardhurat dhe pronën e tatueshme të një numri të madh individësh, pavarësisht nga fakti se publiku mund të ketë qasje në këto të dhëna nën kushte të caktuara [Satakunnan Markkinapörssi Oy dhe Satamedia Oy kundër Finlandës (GC), 2017, § 138].
- Të dhënat e lindjes dhe braktisjes së një individi, duke përfshirë informacionin e nevojshëm për të zbuluar të vërtetën në lidhje me një aspekt të rëndësishëm të identitetit personal [Gaskin kundër Mbretërisë së Bashkuar, 1989, § 39; Mikulić kundër Kroacisë, 2002, §§ 54-64 Odièvre kundër Francës (GC), 2003, §§ 28-29].
- Të dhënat e përfshira në marrëveshjen për shkurorëzim, që mbulojnë detajet e ndarjes së pronës martesore, kujdestarisë dhe vendbanimit të fëmijëve të mitur, marrëveshjen për ushqim dhe rishikimin e pasurisë/të ardhurave të kërkuesit (Liebscher kundër Austrisë, 2021, §§ 31 dhe 68).

7.3.5. Kategoritë e veçanta të të dhënave

7.3.5.1. Kategoritë e ashtuquajtura "të ndjeshme"

Sipas nenit 6 të Konventës 108, të dhënat personale që zbulojnë prejardhjen racore, mendimet politike, besimet fetare ose të tjera dhe informacionin në lidhje me shëndetin ose jetën seksuale të një individi, ose në lidhje me ndonjë dënim penal, nuk mund të përpunohen automatikisht nëse legjislacioni i brendshëm nuk parashikon masa mbrojtëse të përshtatshme. Informacionet që hyn në këto kategori, të përshkruara nga Gjykata si 'të ndjeshëm', kërkon një shkallë më të lartë mbrojtjeje nën të.

7.3.5.2. Të dhëna që zbulojnë prejardhjen racore ose etnike

Identiteti etnik i një individi duhet të konsiderohet si një element i rëndësishëm i jetës private [S. dhe Marper kundër Mbretërisë së Bashkuar (GC), 2008, § 66; Ciubotaru kundër Moldavisë, 2010, § 49]. Të dhënat janë veçanërisht shqetësuese kur mund të zbulojnë prejardhjen etnike ose prejardhjen tjetër të një personi, duke pasur parasysh ritmin e shpejtë të zhvillimit në fushën e gjenetikës dhe teknologjisë së informacionit [S. and Marper v. the United Kingdom (GC), 2008, § 71]. Mostrat dhe profilet e ADN-së përmbajnë informacion shumë të ndjeshëm dhe u lejojnë institucioneve të krijojnë lidhje gjenetike midis individëve dhe të vlerësojnë origjinën e tyre të mundshme etnike (ibid., §§ 72-77; Aycaguer v. Francë, 2017, § 33). Në rastin në lidhje me regjistrimin e prejardhjes etnike të individit në regjistrat zyrtarë, Gjykata, duke theksuar natyrën shumë të ndjeshme të regjistrimit të këtyre të dhënave, pranoi ekzistencën e një detyrimi pozitiv nga ana e shtetit për të kryer një procedurë për t'i mundësuar subjektit të të dhënave të ndryshojë etninë e tij/saj të regjistruar në bazë të provave objektivisht të verifikueshme (Ciubotaru kundër Moldavisë, 2010, § 52-59).

7.3.5.3. Data e zbulimit të mendimeve politike dhe besimeve fetare ose të tjera, përfshirë ato filozofike

Të dhënat që zbulojnë opinionet politike konsiderohen një kategori "e ndjeshme" e të dhënave personale dhe, sipas mendimit të Gjykatës, është e papranueshme që organet kombëtare ta injorojnë këtë aspekt duke përpunuar të dhëna të tilla në përputhje me rregullat e zakonshme të brendshme, pa marrë parasysh nevojën për mbrojtje (Cat kundër Mbretërisë së Bashkuar, 2019, § 112). Në rastin Catt kundër Mbretërisë së Bashkuar të vitit 2019, në lidhje me ruajtjen në një bazë të dhënash të policisë të një protestuesi paqësor, gjykatat kombëtare thjesht thirrën ligjin e përgjithshëm të mbrojtjes së të dhënave gjatë shqyrtimit të ligjshmërisë së ndërhyrjes. Gjykata konstatoi shkelje të nenit 8, duke theksuar se natyra e ndjeshme e të dhënave në fjalë duhej të përbënte një element kryesor të çështjes para gjykatave vendase, siç ishte para Gjykatës (ibid., § 112). Gjykata gjithashtu ka konstatuar shkelje të nenit 8 në M. D. dhe të tjerët v. Spanja, 2022 (§§ 63-64), në lidhje me raportin e përpiluar nga policia në lidhje me gjyqtarët që mbanin zyrat e tyre në Katalonjë dhe që kishin një manifest të nënshkruar në të cilin ata shprehën mendimin e tyre ligjor në favor të mundësisë që populli katalanas të ushtrojë të ashtuquajturën "e drejta për të vendosur", në raportin që zbulon, në veçanti, pikëpamjet politike të disa prej kërkuesve.

E drejta për mbrojtjen e të dhënave personale që zbulojnë besimet fetare ose të tjera të një individi, përfshirë ato filozofike, u shqyrtua nga Gjykata në rastet Sinan Isik kundër Turqisë, 2010 (§ 37) dhe Mokute kundër Lituanisë, 2018 (§ 117). Në lidhje me renditjen e fesë në kartat e identitetit të aplikantëve, Gjykata theksoi rëndësinë e së drejtës për mbrojtjen e të dhënave në lidhje me besimet fetare, e cila përbën një nga elementët më jetikë që përbëjnë identitetin e besimtarëve dhe konceptin e tyre të jetës, siç mbrohet nga neni 9 i Konventës (Sinan Işık kundër Turqisë, 2010, § 37).

7.3.5.4. Të dhëna që zbulojnë anëtarësimin në sindikata

Të dhënat personale që zbulojnë anëtarësimin e një individi në sindikatë mund të jenë gjithashtu "të ndjeshme" dhe për këtë arsye kërkojnë mbrojtje më të madhe. Në Catt v. Mbretëria e Bashkuar, 2019 (§ 112), policia mblodhi informacion mbi pjesëmarrjen e kërkuesit në demonstrata të organizuara nga një numër sindikatash, në veçanti emri i tij, pjesëmarrja, data e lindjes dhe adresa. Në raste të caktuara, është përshkruar edhe pamja e saj, së bashku me fotografitë e bëra gjatë demonstratave në fjalë (ibid., § 10). Përfshirja në protesta paqësore ka mbrojtje specifike sipas nenit 11 të Konventës, e cila gjithashtu përmban mbrojtje të veçantë për sindikatat (ibid., § 123). Ndërsa mbledhja nga policia e të dhënave personale të kërkuesit mund të konsiderohet e arsyetuar, nuk kishte nevojë urgjente, sipas mendimit të Gjykatës, për të ruajtur të dhënat e kërkuesit, në mungesë të ndonjë rregulli që përcakton një afat kohor maksimal të caktuar për mbajtjen e këtyre të dhënave (ibid., §§ 117-119).

7.3.5.5. Të dhënat gjenetike dhe biometrike

Gjykata ka trajtuar një sërë çështjesh që kanë të bëjnë me administrimin ose mbajtjen e:

- mostrat e qelizave [Van der Velden kundër Holandës (vendimi), 2005; Caruana kundër Maltës (vendimi), 2018; Trajkovski dhe Çipovski kundër Maqedonisë së Veriut, 2020; Boljeviq kundër Serbisë, 2020];
- Profilet e ADN-së [Van der Velden kundër Holandës (Vendimi), 2005; Schmidt kundër Gjermanisë (Vendimi), 2006; S. dhe Marper kundër Mbretërisë së Bashkuar (GC), 2008; V. kundër Holandës (Dhjetor), 2009; Peruzzo dhe Martens kundër Gjermanisë (Vendimi), 2013; Canon kundër Francës (Vendimi), 2015; Aykaguer kundër Francës, 2017; Mifsud kundër Maltës, 2019; Gaughran kundër Mbretërisë së Bashkuar, 2020; Trajkovski dhe Çipovski kundër Maqedonisë së Veriut, 2020; Dragan Petroviq kundër Serbisë, 2020];
- gjurmët e gishtërinjve [McVeigh, O'Neill dhe Evans kundër Mbretërisë së Bashkuar, 1981; Kinnunen kundër Finlandës, 1993; S. dhe Marper kundër Mbretërisë së Bashkuar (GC), 2008; Dimitrov-Kazakov kundër Bullgarisë, 2011; M. K. kundër Francës, 2013; Suprunenko kundër Rusisë (dhjetor), 2018; Gauran kundër Mbretërisë së Bashkuar, 2020; P. N. kundër Gjermanisë, 2020; Willems kundër Holandës (dhjetor), 2021];
- gjurmët e pëllëmbëve (Fq. N. v. Gjermania, 2020);
- Udhërryes për praktikën gjyqësore të Konventës – Mbrojtja e të dhënave
- Gjykata evropiane e të drejtave të njeriut 13/98 Përditësimi i fundit: 31.08.2022
- mostrat e zërit (P. G. dhe J. H. v. Mbretëria e Bashkuar, 2001; Alan kundër Mbretërisë së Bashkuar, 2002; Doerga kundër Holandës, 2004; Wind kundër Francës, 2005; Wise kundër Francës, 2005).

7.3.6. Testet e proporcionalitetit

Nëse ndërhyrja ishte e ligjshme

Gjykata ka shqyrtuar në një numër rastesh çështjen nëse kërkesa, siç përmendet në nenin 5 të Konventës 108, që të dhënat personale që i nënshtrohen përpunimit automatik duhet të jenë marrë dhe përpunuar në mënyrë të drejtë dhe të ligjshme. Në një numër rastesh, Gjykata gjeti shkelje të nenit 8 vetëm në bazë të mungesës së bazës ligjore në nivel kombëtar për të miratuar masa të afta për të ndërhyrë në të drejtat përkatëse (Taylor-Sabors kundër Mbretërisë së Bashkuar, 2002, §§ 17-19; Radu kundër Moldavisë, 2014, § 31; Mokute kundër Lituanisë, 2018, § 103-104; M. E. dhe të tjerët kundër Spanjës, 2022, §§ 61-64).

Në veçanti, në Mockutė kundër Lituanisë, 2018 (§§ 103-104), Gjykata vërejti se as Qeveria dhe as gjykatat kombëtare nuk kishin treguar ndonjë dispozitë që mund të formonte bazën ligjore për komunikimin, nga spitali psikiatrik, të informacionit mbi shëndetin e kërkuesit, i cili ishte i rritur, të nënës së tij dhe të gazetarëve. Në Taylor-Saborie kundër Mbretërisë së Bashkuar, 2002 (§§ 17-19), ku kërkuesi iu nënshtrua mbikëqyrjes policore duke "klonuar" pagerin e tij, nuk kishte asnjë sistem ligjor për të rregulluar ndjekjen e mesazheve të pagerit të transmetuara përmes një sistemi privat të telekomunikacionit. Në M.D dhe të tjerët v. Spanja, 2022 (§§ 61-64), policia përgatiti një raport në lidhje me gjyqtarët që mbanin detyrën në Katalonjë dhe që nënshkruan një manifest që përshkruan mendimin e tyre ligjor në favor të mundësisë që populli katalanas të ushtrojë të ashtuquajturën "e drejta për të vendosur", raporti që zbulon të dhënat personale, fotografitë, informacionin profesional dhe pikëpamjet politike të disa prej tyre. Gjykata vuri në dukje se përpilimi i kallëzimit nga policia nuk ishte parashikuar me ligj dhe për shkak se organet publike përdorën të dhënat personale për një qëllim të ndryshëm nga ai që justifikonte mbledhjen, ekzistenca e kallëzimit policor, i cili u hartua në lidhje me individët, sjellja e të cilëve nuk nënkuptonte ndonjë veprimtari kriminale, që përbën shkelje të nenit 8 të Konventës.

7.3.7. Nëse ndërhyrja ndoqi një qëllim legjitim

Në një numër rastesh, Gjykata ka shqyrtuar nëse kërkesa, siç përcaktohet në nenin 5 të Konventës 108, që të dhënat personale që i nënshtrohen përpunimit automatik duhet të jenë mbledhur për qëllime të qarta, të specifikuara dhe të ligjshme. Në këto raste, shqyrtimi i qëllimeve legjitime që mund të justifikojnë ndërhyrjen në ushtrimin e të drejtave të përmendura në nenin 8, siç përmendet në pikën 2, është veçanërisht i përmbajtur. Këto qëllime janë mbrojtja e sigurisë kombëtare, sigurisë publike dhe mirëqenies ekonomike të vendit, parandalimi i çrregullimit ose krimit, mbrojtja e shëndetit ose moralit, ose mbrojtja e të drejtave dhe lirive të të tjerëve. Gjykata në përgjithësi konfirmon ekzistencën e një ose më shumë prej këtyre qëllimeve legjitime të kërkuara nga Qeveria.

Gjykata mendoi, për shembull, se ruajtja në regjistrin e policisë sekrete të të dhënave për jetën private të individëve, pastaj përdorimi i këtyre të dhënave në verifikimin e kandidatëve për poste me rëndësi të sigurisë kombëtare, ndoqi një qëllimi legjitimi

për qëllimet e nenit 8, përkatësisht mbrojtjen e sigurisë kombëtare (Leander kundër Suedisë, 1987, § 49). Monitorimi i kërkuesit nga GPS, i urdhëruar nga një prokuror për të hetuar disa akte të vrasjes në tentativë për të cilat lëvizja terroriste mori përgjegjësinë dhe për të parandaluar bombardime të mëtejshme, sipas mendimit të Gjykatës, i shërbeu interesave të sigurisë kombëtare dhe sigurisë publike, parandalimit të krimit dhe mbrojtjes së të drejtave të viktimave (Uzun v. Gjermani, 2010, § 77).

7.3.8. Nëse ndërhyrja ishte "e nevojshme në një shoqëri demokratike"

Për të qenë e nevojshme në një shoqëri demokratike, çdo masë që ndërhyn në mbrojtjen e të dhënave personale sipas nenit 8 duhet të korrespondojë me një nevojë urgjente sociale dhe nuk duhet të jetë joproporcionale me objektivat legjitime të ndjekura (Z v. Finlanda, 1997, § 94; Kelly kundër Zvicrës, 2011, § 62; Vicente del Campo kundër Spanjës, 2018, § 46). Arsyet e kërkuara nga Qeveria duhet të jenë relevante dhe të mjaftueshme (Z kundër Finlandës, 1997, § 94). Ndërsa u takon institucioneve kombëtare të bëjnë vlerësimin fillestar në të gjitha këto aspekte, vlerësimi përfundimtar nëse ndërhyrja është e nevojshme mbetet subjekt i rishikimit nga Gjykata për pajtueshmërinë me kërkesat e Konventës [S. dhe Marper kundër Mbretërisë së Bashkuar (GC), 2008, § 101].

7.3.9. Gjykata evropiane e drejtësisë (GJED)

7.3.9.1. Qasja në informacione për subjektet

Më 12 janar 2023, Gjykata evropiane e drejtësisë (GJED) dha një gjykim të ri në rastin C-154/21 Österreichische Post në lidhje me informacionet në lidhje me marrësit e të dhënave personale. Një qytetar kërkoi nga Posta e Austrisë, operatori kryesor i shërbimeve postare dhe logjistike në Austri, të zbulojë identitetin e marrësve të cilëve u ka zbuluar të dhënat e tij personale. Ai u mbështet në Rregulloren e përgjithshme të BE-së për Mbrojtjen e të dhënave (GDPR). GDPR parashikon që subjekti i të dhënave ka të drejtë të marrë nga kontrolluesi informacion në lidhje me marrësit ose kategoritë e marrësve të cilëve u janë zbuluar ose do të zbulohen të dhënat e tij personale. Në përgjigje të kërkesës së qytetarit, Posta e Austrisë deklaroi vetëm se përdor të dhëna personale dhe se ua ofron ato të dhëna personale partnerëve tregtarë për qëllime marketingu. Megjithatë, lind pyetja nëse GDPR i lë një zgjedhje kontrolluesit të të dhënave për të zbuluar identitetin specifik të marrësve ose vetëm kategoritë e marrësve ose nëse i jep subjektit të të dhënave të drejtën për të njohur identitetin specifik të marrësve të të dhënave.

GJED vendosi që kjo dispozitë nuk u jep kontrolluesve të të dhënave zgjedhjen midis identifikimit të pranuesve specifikë ose kategorive të pranuesve. Në vend të kësaj, kur u përgjigjen kërkesave nga subjektet e të dhënave, kontrolluesit e të dhënave me bazë në BE duhet të zbulojnë identitetin e vërtetë të marrësve, përveç kur nuk është e mundur t'i identifikojnë ata ose mund të demonstrojnë se kërkesa për qasje është qartazi e pabazuar ose e tepruar.

7.3.9.2. E drejta e kompensimit të dëmit dhe parametrat

Më 4 mars 2023, Gjykata evropiane e drejtësisë dha vendimin e saj në rastin C-300/21, UI v Österreichische Post AG, në të cilin arriti në përfundimin se shkelja e GDPR nuk sjell të drejtën e kompensimit për individët. Sipas mendimit të Gjykatës, neni 82 kërkon përcaktimin e: (i) "dëmit", qoftë material apo jomaterial; (ii) shkeljes aktuale të GDPR-së; dhe (iii) një marrëdhënie shkakësore midis të dyjave. Megjithatë, ajo gjithashtu vendosi se e drejta për kompensim në GDPR nuk mund të varet nga individët që plotësojnë një prag të caktuar të "ashpërsisë", siç është rasti sipas ligjit austriak për momentin.

Ndër të tjera, GJED-së iu kërkua të sqarojë nëse shkelja e GDPR-së ishte e mjaftueshme për të krijuar një të drejtë për kompensim sipas nenit 82 dhe, më tej, nëse ndonjë kompensim për dëmin jomaterial mund të varet nga dëmi i pretenduar që ka "një farë peshe" mbi "ngacmimin", duke përmbushur në mënyrë efektive një prag të caktuar të "ashpërsisë" në ligjin austriak.

Në zbatim të këtij gjykimi, përcaktohen edhe standardet, pra udhëzimet për kompensimin e dëmeve. Sipas arsyetimit të GJED-së në këtë rast:

- E drejta për dëmet e parashikuara nga GDPR-ja i nënshtrohet tre kushteve kumulative: ekzistenca e shkeljes së GDPR-së, dëmi material ose jomaterial që rrjedh nga kjo shkelje dhe një lidhje shkakësore midis dëmit dhe shkeljes.
- Shkelja e GDPR-së nuk përbën kërkesë për dëmshpërblim.
- Megjithatë, kompensimi për dëmet jomateriale nuk varet nga arritja e një pragu të caktuar të materialitetit.
- I mbetet personit në fjalë të provojë se ka pësuar dëme jo materiale.
- Kriteret për vlerësimin e masës së dëmit i lihen ligjit të shteteve anëtare, duke marrë parasysh parimet e ekuivalencës dhe efektivitetit.
- Dëmet e pësuara për shkak të shkeljes së GDPR-së duhet të kompensohen "plotësisht".
- Ky kompensim i plotë nuk kërkon vendosjen e dëmeve ndëshkuese.[37]

37 https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3810075

08

SFIDAT MODERNE TË MBROJTJES SË TË DHËNAVE

VIII.

SFIDAT MODERNE TË MBROJTJES SË TË DHËNAVE

8.1. Përparimet teknologjike, algoritmet dhe inteligjenca artificiale

Në rastet që kanë të bëjnë me marrjen dhe ruajtjen nga institucionet, për qëllime të parandalimit të krimit, të shenjave të gishtërinjve, mostrave biologjike dhe profileve të ADN-së të personave të dyshuar ose dënuar për vepra penale, Gjykata ka deklaruar qartë se përdorimi i teknikave moderne shkencore nuk mund të autorizohet me çdo kusht dhe pa balancuar me kujdes përfitimet e mundshme të përdorimit të gjerë të këtyre teknikave kundër interesave të rëndësishme private [S. dhe Marper kundër Mbretërisë së Bashkuar (GC), 2008, § 112]. Çdo shtet që pretendon të ketë një rol pionier në zhvillimin e teknologjive të reja ka një përgjegjësi të veçantë për të arritur ekuilibrin e duhur në këtë drejtim (ibid., § 112). Duke marrë parasysh ritmin e shpejtë të zhvillimit në fushën e gjenetikës dhe teknologjisë së informacionit, mundësia që në të ardhmen interesat private në lidhje me informacionin e gjeneve mund të ndikohen negativisht në mënyra të reja ose në një mënyrë që nuk mund të parashikohet me saktësi sot nuk mund të zvogëlohet (ibid., § 71).

Sipas mendimit të Gjykatës, zhvillimi i shpejtë i teknikave gjithnjë e më të sofistikuara që lejojnë, ndër të tjera, teknikat e njohjes së fytyrës dhe hartëzimit që do të zbatohen në fotografitë e individëve, e bën problematike fotografimin e fotografive të tyre dhe ruajtjen dhe shpërndarjen e mundshme të të dhënave që rezultojnë. Gjykatat vendase duhet të marrin parasysh këta faktorë kur vlerësojnë domosdoshmërinë për të ndërhyrë në jetën private të personit në fjalë (Gaughran kundër Mbretërisë së Bashkuar, 2020, § 70). Në atë rast (ibid., §§ 96-98), Gjykata theksoi se teknologjia moderne është më komplekse dhe se gjykatat vendase nuk i kushtuan vëmendje të mjaftueshme këtij aspekti kur shqyrtuan domosdoshmërinë e ndërhyrjes në të drejtën për respektimin e jetës private të kërkuesit, fotografia e të cilit u mor nga organet pas një vepre të vogël dhe u mbajt edhe pasi dënimi i tij u fshi nga regjistrat pas skadimit të afatit ligjor.

Në Breyer kundër Gjermanisë, sipas mendimit të Gjykatës, detyrimi për operatorët e telefonisë celulare për të ruajtur informacionin e pajtimtarit dhe për ta vënë atë në dispozicion të organeve sipas kërkesës është në përgjithësi një përgjigje e përshtatshme ndaj ndryshimeve në sjelljen e komunikimeve dhe në mjetet e telekomunikacionit.

Në Szabó dhe Vissy kundër Hungarisë, 2016 (§ 68), një rast në lidhje me përgjimin masiv të komunikimeve, Gjykata pranoi se është një pasojë e natyrshme e formave të marra nga terrorizmi i sotëm që qeveritë të përdorin teknologjitë më të fundit, duke përfshirë përgjimin masiv të komunikimeve, në mënyrë që të parandalojnë sulmet e afërta. Në këtë rast, Gjykata vlerësoi se legjislacioni që lejon mbikëqyrjen masive nuk ofron masat mbrojtëse të nevojshme kundër keqpërdorimit, pasi teknologjitë e reja e bëjnë më të lehtë për organet të përgjojnë sasi të mëdha të të dhënave edhe për njerëzit që nuk janë në kategorinë e synuar fillimisht nga operacioni. Përveç kësaj, ekzekutivi mund të urdhërojë masa të këtij lloji pa asnjë kontroll dhe pa asnjë vlerësim nëse ato janë rreptësisht të nevojshme dhe në mungesë të ndonjë mjeti gjyqësor efektiv ose mjeti tjetër juridik (ibid., § 73-89).

Në rastin e Roman Zakharov kundër Rusisë (GC), 2015 (§§ 302-305), Gjykata vlerësoi se rreziku i abuzimit të qenësishëm në çdo sistem të mbikëqyrjes së fshehtë ishte veçanërisht i lartë në një sistem ku shërbimet sekrete dhe policia kishin qasje të drejtpërdrejtë, me mjete teknike, në të gjitha komunikimet telefonike celulare. Gjykata gjeti shkelje të nenit 8, duke konsideruar se dispozitat ligjore ruse që lejojnë përgjimin e përgjithshëm të komunikimeve nuk ofrojnë garanci adekuate dhe efektive kundër arbitraritetit dhe rrezikut të abuzimit të qenësishëm në çdo sistem të mbikëqyrjes së fshehtë.

Në Akgün kundër Turqisë, 2021 (§§ 178-181), ku në kohën e ndalimit fillestar të kërkuesit, konstatimi se ai kishte përdorur sistemin e koduar të mesazheve ByLock ishte prova e vetme që ishte siguruar për të justifikuar dyshimin, për qëllimet e nenit 5 § 1 (c), se ai kishte kryer një vepër penale, Gjykata theksoi se përdorimi i dëshmive të tilla si baza e vetme për krijimin e dyshimit mund të ngrinte një numër pyetjesh delikate, pasi, nga natyra e saj, procedura dhe teknologjitë e aplikuara në mbledhjen e këtyre provave ishin komplekse dhe mund të zvogëlonin në mënyrë të përshtatshme aftësinë e gjykatave kombëtare për të vërtetuar vërtetësinë, saktësinë dhe integritetin e saj (shih paragrafin 373 më lart).

Në rastet Centrum för rättvisa v Sweden (GC), 2021, § 261, dhe Big Brother Watch and Others v United Kingdom (GC), 2021, §§ 322-323, Gjykata pranoi shprehimisht se përdorimi i regjimit të mbikëqyrjes masive nuk ishte në vetvete në kundërshtim me nenin 8, duke pasur parasysh përhapjen e kërcënimeve me të cilat përballen aktualisht shtetet nga rrjetet e aktorëve ndërkombëtarë, të cilët përdorin internetin për komunikim dhe ekzistencën e teknologjisë së sofistikuar që i lejoi këta aktorë të shmangnin zbulimin. Megjithatë, Gjykata theksoi se duke pasur parasysh zhvillimin e vazhdueshëm të teknologjive moderne të komunikimit, qasja e saj e zakonshme për të synuar regjimet e mbikëqyrjes do të duhej të përshtatej për të pasqyruar karakteristikat specifike të regjimit të mbikëqyrjes masive, për shkak të rrezikut të keqpërdorimit të informacioneve dhe nevojës legjitime për fshehtësi në operacione të tilla. Procesi duhet t'i nënshtrohet "masave mbrojtëse nga skaji në skaj", që do të thotë se, në nivelin e brendshëm, duhet të bëhet një vlerësim në çdo fazë të procesit të domosdoshmërisë dhe proporcionalitetit të masave që merren; që mbikëqyrja masive duhet t'i nënshtrohet autorizimit të pavarur që në fillim, kur përcaktohet lënda dhe fushëveprimi i operacionit; dhe që operacionet duhet t'i nënshtrohen mbikëqyrjes dhe auditimit të pavarur ex post facto.

8.1.2. Interneti dhe kërkuesit

Uebfaqet janë një mjet informacioni dhe komunikimi i dallueshëm nga mediat e shtypura, veçanërisht në aspektin e kapacitetit të ruajtjes dhe transmetimit të informacionit (M. L. dhe W. W. kundër Gjermanisë, 2018, § 91). Në dritën e disponueshmërisë së tij dhe kapacitetit të tij për të ruajtur dhe transmetuar sasi të mëdha informacioni, interneti luan një rol të rëndësishëm në përmirësimin e qasjes së publikut në lajme dhe lehtësimin e shpërndarjes së informacionit në përgjithësi [Times Newspapers Ltd kundër Mbretërisë së Bashkuar (nr. 1 dhe 2), 2009, § 27].

Rreziku i dëmit të shkaktuar nga përmbajtja dhe komunikimet në internet për ushtrimin dhe gëzimin e të drejtave dhe lirive të njeriut, veçanërisht e drejta për respektimin e jetës private, është sigurisht më e madhe se ajo që përballon shtypi, veçanërisht për shkak të rolit të rëndësishëm të motorëve të kërkimit (M. L. dhe W. W. v. Gjermani, 2018, § 91 dhe referencat e cituara në të).

Informacioni që përmban të dhëna personale të ruajtura nga media mund të gjendet lehtësisht nga përdoruesit e internetit përmes motorëve të kërkimit (ibid., § 97). Për shkak të këtij efekti intensifikues në shpërndarjen e informacionit dhe natyrën e veprimtarisë në bazë të publikimit të informacionit, detyrimet e motorëve të kërkimit ndaj subjektit individual të informacionit mund të ndryshojnë nga ato të subjektit që ka publikuar fillimisht informacionin (ibid., § 97). Prandaj, në një rast në të cilin dy persona kanë kërkuar që detajet e plota të identitetit të tyre dhe fotografitë e tyre të hiqen nga arkivat në internet të gazetave dhe radiostacioneve të caktuara pasi të kenë përfunduar vuajtjen e dënimeve të gjata me burg për vrasje (ibid., §§ 7, 12, 33), Gjykata konstaton se balancimi i interesave në fjalë mund të rezultojë në rezultate të ndryshme në varësi të faktit nëse kërkesa për fshirjen e të dhënave personale lidhet me botuesin origjinal të informacionit, veprimtaria e të cilit ishte përgjithësisht në qendër të asaj që liria e shprehjes kishte për qëllim të mbrojtur, ose një motor kërkimi, interesi kryesor i të cilit nuk ishte publikimi i informacionit fillestar në lidhje me personin në fjalë, por në veçanti lehtësimi i identifikimit të të gjithë informacionit në dispozicion në lidhje me atë person dhe krijimin e profilit të tij/saj (ibid., § 97).

Sipas mendimit të Gjykatës, arkivat e internetit kontribuojnë në ruajtjen dhe vënien në dispozicion të lajmeve dhe informacionit [Times Newspapers Ltd kundër Mbretërisë së Bashkuar (nr. 1 dhe 2), 2009, § 45]. Arkiva të tilla përfaqësojnë një burim të rëndësishëm për arsimin dhe kërkimin historik, veçanërisht sepse ato janë lehtësisht të arritshme për publikun dhe në përgjithësi janë falas.

Rasti i Biancardi kundër Italisë, 2021, §§ 67-70, i dha Gjykatës mundësinë e parë për të vendosur mbi pajtueshmërinë me nenin 10 të aktgjykimit civil kundër një gazetari për mosindeksimin e informacionit të ndjeshëm të botuar në internet. Lidhur me procedimin penal ndaj individëve privatë dhe vendimin e gazetarit për ta mbajtur informacionin lehtësisht të qasshëm, pavarësisht kundërshtimit të të interesuarve. Çështja e anonimizimit të identiteteve në artikullin online nuk u ngrit në këtë rast. Gjykata vuri në dukje se artikulli mbeti i disponueshëm në internet për tetë muaj pas kërkesës zyrtare për ta hequr atë nga personat në fjalë. Pesha e sanksionit – përgjegjësia sipas ligjit civil dhe jo penal – dhe shuma e kompensimit të dhënë nuk dukej e ekzagjeruar.

8.2. Transferimi i të dhënave dhe rrjedhat e të dhënave

Në Satakunnan Markkinapörssi Oy dhe Satamedia Oy kundër Finlandës, sipas mendimit të Gjykatës, ekzistenca e një interesi publik për të siguruar qasje dhe për të lejuar mbledhjen e sasive të mëdha të të dhënave për tatim për qëllime gazetareske nuk nënkupton domosdoshmërisht se ekziston gjithashtu një interes publik në shpërndarjen masive të të dhënave të tilla të papërpunuara në formë të pandryshuar pa ndonjë kontribut analitik. Duhet të bëhej dallim midis përpunimit të të dhënave për qëllime gazetareske dhe shpërndarjes së të dhënave të papërpunuara, në të cilat gazetarëve u është dhënë qasje e privilegjuar (ibid., § 175). Në këtë kontekst, fakti që ndalon publikimin masiv të të dhënave personale të taksimit në një mënyrë të papajtueshme me rregullat finlandeze dhe të BE-së për mbrojtjen e të dhënave nuk ishte, si e tillë, një sanksion, edhe pse, në praktikë, kufizimet e vendosura në sasinë e informacionit që do të publikohet mund të kenë bërë disa nga aktivitetet e biznesit të kompanive kërkuese më pak fitimprurëse (ibid., § 197).

Çështja Big Brother Watch dhe të tjerët kundër Mbretërisë së Bashkuar (GC), 2021, ndër të tjera, filloi çështjen e pajtueshmërisë me nenin 8 të Konventës për shkëmbimin e të dhënave të përgjuar nga shërbimet e huaja të inteligjencës, në këtë rast Agjencia e Sigurisë Kombëtare të SHBA (NSA). Gjykata deklaroi se shkëmbimi i të dhënave duhej të kornizohej nga rregulla të qarta të hollësishme që u sigurojnë qytetarëve një tregues adekuat të rrethanave dhe kushteve në të cilat organet janë të autorizuar të bëjnë kërkesa të tilla dhe të ofrojnë masa mbrojtëse efektive kundër përdorimit të kësaj kompetence për të anashkaluar ligjin vendas dhe/ose detyrimet e shteteve sipas Konventës. Pas marrjes së materialit për përgjim, vendi pritës duhet të ketë masat e duhura mbrojtëse për ekzaminimin, përdorimin dhe ruajtjen e tij; për transferimin e mëtejshëm të tij; dhe për fshirjen dhe shkatërrimin e tij. Këto masa mbrojtëse ishin po aq të zbatueshme për marrjen, nga shteti palë, të materialit të kërkuar të përgjimit nga një shërbim i huaj i inteligjencës. Nëse shtetet nuk e dinin gjithmonë nëse materiali i marrë nga shërbimet e huaja të inteligjencës ishte produkt i përgjimit, atëherë Gjykata vlerësoi se të njëjtat standarde duhet të zbatohen për të gjitha materialet e marra nga shërbimet e huaja të inteligjencës që mund të jenë produkt i përgjimit. Së fundi, çdo regjim që lejon shërbimet e inteligjencës të kërkojnë ose përgjimin ose përgjimin e materialit nga palët jokontraktuese duhet t'i nënshtrohet mbikëqyrjes së pavarur, dhe gjithashtu duhet të ekzistojë mundësia e auditimit të pavarur ex post facto (ibid., §§ 498-499).

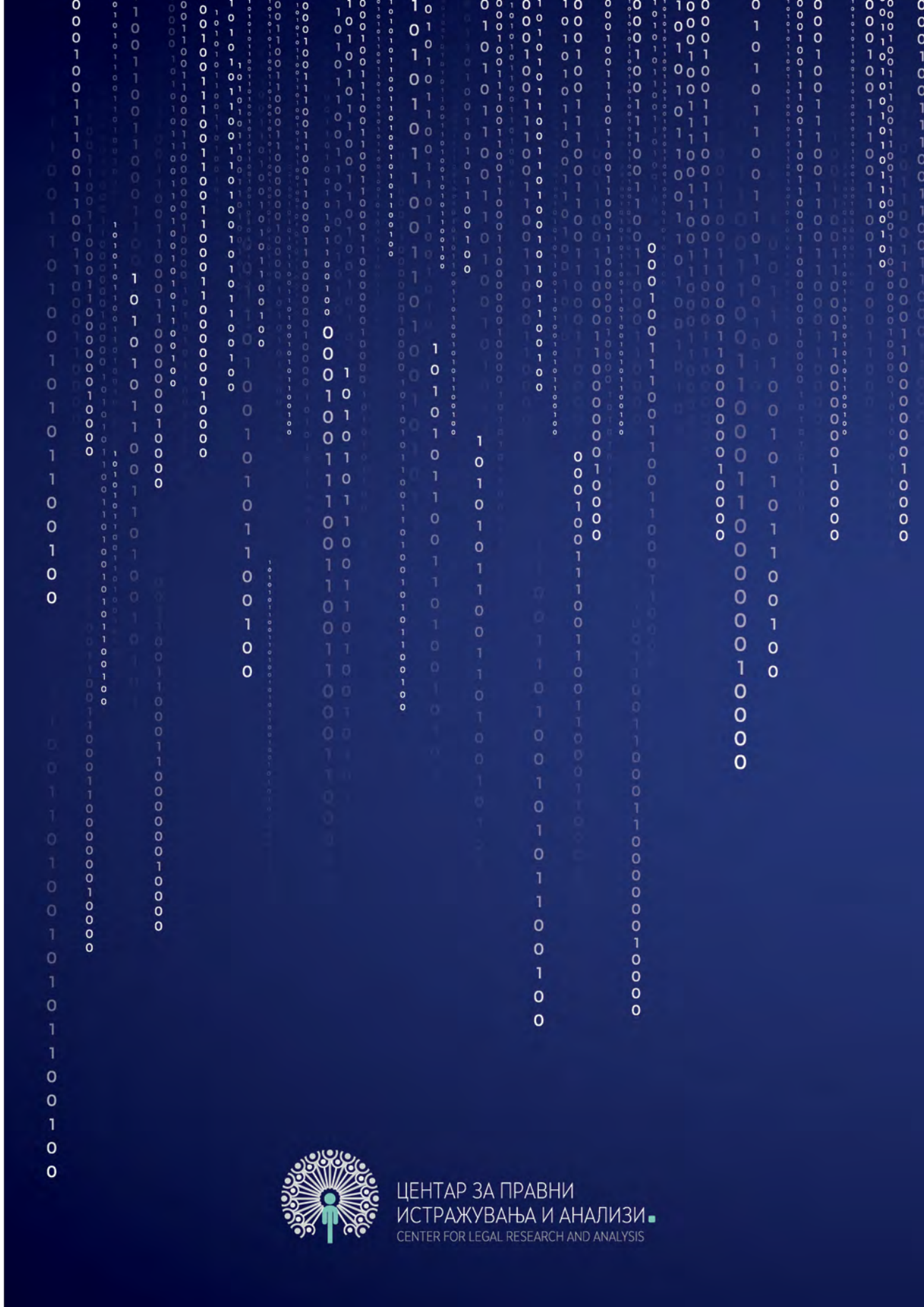
VIII.

8.3. Trajnimi i aktorëve dhe organeve në kuadër të gjyqësorit

Për shkak se privatësia dhe mbrojtja e të dhënave është një çështje komplekse, gjyqësori duhet të marrë trajnime specifike në këtë fushë. Sigurisht, ky trajnim do të përfshijë Ligjin për mbrojtjen e të dhënave, por edhe të gjitha rregulloret dhe aktet e tjera të përmendura në këtë udhërrëfyes, me theks në GJEDNJ dhe praktikën e GJEDNJ-së. Sigurisht, është gjithashtu e nevojshme të merren njohuri pak më të avancuara të njohurive themelore në shkencat kompjuterike, internet, etj. Në kohën në të cilën jetojmë, duhet të ketë gjithashtu një fokus specifik në teknologjitë e reja, siç është inteligjenca artificiale.

8.4. Fushatat për ngritjen e vetëdijes publike

Duhet të zhvillohen fushata ndërgjegjësimi për të informuar njerëzit në lidhje me mbrojtjen e të dhënave, rreziqet e përpunimit të të dhënave personale në mjedisin online dhe të drejtat e tyre, duke përfshirë mundësinë e mjeteve juridike efektive dhe çfarë duhet të përfshijnë këto mjete. Kjo gjithashtu do të ndihmojë aktorët e përfshirë të marrin informacion në lidhje me të drejtat, detyrimet, përgjegjësitë dhe mjetet juridike dhe mjetet juridike në mbrojtjen e të drejtave të tyre të privatësisë dhe të dhënave të tyre personale.


ЦЕНТАР ЗА ПРАВНИ
ИСТРАЖУВАЊА И АНАЛИЗИ
CENTER FOR LEGAL RESEARCH AND ANALYSIS