KUADRI LIGJOR PËR MBROJTJEN E TË DHËNAVE PERSONALE DHE PRIVATËSISË NË KOMUNIKIMET ELEKTRONIKE

Indrit Shtupi

Dorëzuar
Universitetit Europian të Tiranës
Shkollës Doktorale

Në përmbushje të detyrimeve të programit të Doktoratës në Shkenca Juridike, me profil në të Drejtën Publike, për marrjen e gradës shkencore “Doktor”

Udhëheqës shkencor: Prof.Asoc.Dr. Darjel Sina

Numri i fjalëve: 59.225

Vendi, muaji viti i dorëzimit

DEKLARATA E AUTORËSISË

Në përgjegjësinë time deklaroj se ky punim është shkruar prej meje siaps kërkesave të Shkollës Doktorale të Universitetit Europian të Tiranës, nuk është prezantuar para një institucioni tjetër për vlersim dhe nuk është botuar. Punimi nuk përmban material të shkruar nga ndonjë person tjeter përveç rasteve të cituara dhe referuara.

Abstrakt

Kuadri ligjor për mbrojtjen e të dhënave personale dhe privatësisë në sektorin e komunikimeve elektronike. Inkorporimi i kuadrit rregullator evropian për komunikimet elektronike në legjislacionin shqiptar. Qëllimi kryesor i këtij disertacioni është të vlerësojë Direktivën transpozitive 2002/58/KE në lidhje me përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike, amenduar nga direktivat 2006/24/KE (Direktiva e ruajtjes së të dhënave) dhe 2009/136/KE (Direktiva për shërbimin universal dhe të drejtat e përdoruesve në lidhje me rrjetet e komunikimeve elektronike dhe shërbimeve) në ligjin shqiptar.

Hulumtimi është kryer përmes prezantimit dhe analizimit të Kornizës legjislative ekzistuese për mbrojtjen e të dhënave personale në nivel ndërkombëtar dhe atë kombëtar. Fillimisht është trajtuar Shoqëria e Informacionit e cila është një shoqëri që karakterizohet nga zhvillimi paparë i rrjeteve të telekomunikacionit. Ndryshimet e vazhdueshme në teknologjitë e informacionit intensifikojnë shqetësimin se përfundimisht njerëzit do të jenë të ekspozuar vazhdimisht ndaj monitorimit të padëshiruar të privatësisë së tyre, pa mundësi të konsiderueshme për t'u mbrojtur.

Më pas është trajtuar një analizë konceptuale e privatësisë dhe të dhënave personale. Gjithashtu është tentuar të trajtohen referencat ndaj teorisë filozofike dhe ligjore, amerikane kanadeze dhe evropiane si dhe në çështje specifike ligjore. Disertacioni fillon me prezantimin e zhvillimit të përgjithshëm të Mbrojtjes së të Dhënave në Evropë nga të ashtuquajturat "gjenerata e parë", "gjenerata e dytë" dhe "gjenerata e tretë" si dhe rregulloret në iniciativat aktuale kombëtare dhe legjislative të BE. Gjithashtu është bërë një analizë krahasuese e ligjit shqiptar në krahasim me Direktivën 2002/58/KE dhe vlerësimi i shkallës së efektivitetit në mbrojtjen e të dhënave personale dhe në vijim privatësisë në Shqipëri.

Si përfundim, në disertacion theksohet nevoja në rritje për një qasje të fortë ligjore për mbrojtjen e të dhënave në dritën e teknologjive të reja duke evidentuar mangësitë e hasura në legjislacionin shqiptar.

Fjalë Kyçe: Mbrojtja e të dhënave personale, privatësia, Direktiva 2002/58/KE, legjislacioni, Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale.

Abstract

The legal framework for the protection of personal data and privacy in the electronic communications sector. Incorporation of the European regulatory framework for the Electronic Communications into the Albanian legislation. The primary goal of this thesis is to evaluate the transposition Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector as amended by directives 2006/24/EC (Data Retention Directive) and 2009/136/EC (Citizens Rights Directive) in albanian law.

The research is conducted through the presentation and analysis of the existing legislative framework on personal data protection, at national and international level.

Initially is treated the Information Society which is a society characterized by unprecedented development of telecommunications networks. The continuous changes in information technologies intensify concerns that eventually people will be constantly exposed to unwanted monitoring of their privacy, without significant opportunity to defend.

Later was treated a conceptual analysis on privacy and personal data which is attempted with references to American Canadian and European, philosophical and legal theory as well as in case law. The introduction to the subject is made with the presentation of the generational development of Data Protection in Europe from the so-called "first generation", "second generation" and "third generation"regulations to the current national and E.U legislative initiatives. A comparative analysis of the Albanian Law as opposed to Directive 2002/58/EC and the evaluation of the degree of the effectiveness on the protection of personal data and privacy in Albania follows. As a conclusion the dissertation emphasizes the growing need for a strong legal approach to data protection in the light of the emerging technologies by highlighting the identified deficiencies in the Albanian legislation.

Key Words: Personal Data Protection, privacy, Directive 2002/58/EC, Legislation, Commissioner on Information Rights and Protection of Personal Data.

MIRËNJOHJE

Finalizimi i këtij punimi është bërë i mundur falë kontributit të pamohueshëm të disa personave, të cilët meritojnë mirënjohje dhe falënderim të veçantë.

Shpreh falënderimet më të sinqerta për udhëheqësin shkencor të këtij punimi Prof. Asoc. Dr. Darjel Sina për përkushtimin, mbështetjen e tij morale dhe udhëheqjen profesionale në hartimin dhe përfundimin e temës.

Mirënjohje dhe falenderim për familjen time për përkrahjen dhe inkurajimin e tyre të vazhdueshëm gjatë shkrimit të temës. Faleminderit që keni qenë pranë meje në momentet më delikate dhe që treguat besim të palëkundur ndaj punës time.

Në mënyrë speciale ja dedikoj djalit tim të dashur, Andreas.

PËRMBAJTJA E LËNDËS

FJALOR TERMINOLOGJIK

A

Abonent ~ Çdo person fizik, person juridik, ent ose shoqatë, pjesë e një kontratë me një furnizues të shërbimeve të komunikimeve elektronike të hapura për publikun, për ofrimin e shërbimeve të tilla, ose çdo përfitues i këtyre shërbimeve përmes kartave të parapaguara.

Akses ~ Është bërja e disponueshme e lehtësirave dhe/ose shërbimeve një sipërmarrësi tjetër, sipas kushteve të përcaktuara, në baza ekskluzive ose jo ekskluzive, për sigurimin e shërbimeve të komunikimeve elektronike.

Akses në të dhënat personale ~ Nënkupton te drejtën për të hyrë në bankën e të dhënave, për tu njohur dhe për ti përdorur të dhënat, në përputhje me legjislacionin në këtë fushë.

Antivirus/Antispyware ~ Programe të cilat bëjnë të mundur kontrollimin, identifikimin, eliminimin e programeve kompjuterike të dëmshme të instaluara në kompjuterë (virus, trojan etj.).

Anti Spam ~ Program për filtrimin e e-mail "spiune" prej të cilave mund të infektohet kompjuteri.

Aparatura që ndërhyjnë në jetën private ~ Pajisje teknologjike që marrin ose regjistrojnë të dhëna për jetën private veprimet dhe lëvizjet e njerëzve.

Aprovim i subjektit të të dhënave personale ~ Çdo deklaratë me vullnet të plotë e të lirë, e dhënë shprehimisht dhe në dijeni të plotë, me të cilën subjekti i të dhënave personale pranon përpunimin e të dhënave të tij personale.

Asgjësim i korrespondencës ~ Shkatërrim përfundimtar i materialeve fizike ose elektronike të cilat përmbajnë komunikimet mes dy njerëzve ose institucioneve.

Autoritete kombëtare ~ Janë të gjitha institucionet publike që veprojnë brenda territorit të një shteti por kur përdoret në kontekstin e mbrojtjes së të dhënave personale i referohet Zyrës së Komisionerit.

Autoritet publik ~ Kuptohet çdo organ i administratës shtetërore dhe i enteve publike.

Autorizim ~ 1. Veprimi sipas kuptimeve të foljeve AUTORIZOJ, AUTORIZOHEM. Me autorizim të organeve. Kam autorizimin e dikujt. Marr autorizim prej dikujt. 2. Shkresë me të cilën i jepet e drejta dikujt të kryejë një punë në emër të atij, që e ka lëshuar këtë shkresë; dokument zyrtar që lejon dikë për të bërë një veprim a një punë. Lëshoj (jap) autorizim. Kam (marr) autorizim. Lejohet me autorizim.

B

Browser ~ Është një program nëpërmjet të cilit përdoruesit i mundësohet të kërkojë informacion në Internet. (Si psh: Internet Explorer, Mozilla, Opera, etj.)

Bllokim ~ Është ruajtja e të dhënave personale duke pezulluar përkohësisht çdo veprim tjetër përpunimi.

C

Chat ~ Mund ti referohet çdo lloji komunikimi në internet por kryesisht ka të bëjë me shkëmbimin e mesazheve tekst midis dy përdoruesve.

Cookies ~ Janë disa të dhëna që regjistrohen në kompjuter, të cilat përmbajnë informacion specifik. "cookie" lejon që çdo server mund të dijë se çfarë faqesh janë vizituar kohët e fundit, vetëm duke i lexuar ato.

D

Database ~ Janë arkiva elektronikë ku ruhen të dhëna të depozituara sipas kërkesave të përdoruesve.

Dispozitë ~ Pjesë e një norme juridike që përmban një rregull të caktuar të sjelljes; secila prej pikave të një ligji, të një urdhërese, të një rregulloreje a të një vendimi. Dispozita të përgjithshme (të veçanta). Dispozita ligjore. Dispozitat e vendimit (e marrëveshjes, e rregullores). Zbatimi i dispozitave. Shkelja e dispozitave. Në bazë të (sipas) dispozitave në fuqi.

Direktivë ~ Udhëzim që jepet nga një organ drejtues për vijën që duhet ndjekur e duhet zbatuar në një punë a veprimtari. Dha (lëshoi) direktivën. Zbatoj (vë në jetë) direktivat. Zbërthyen direktivat. Vepron sipas direktivave.

Të drejta ~ Mundësi që sigurohet me ligj a me vendime shtetërore për të gëzuar, përdorur a për të kërkuar diçka, për të vepruar në një mënyrë të caktuar, etj.

Të drejta themelore ~ Përbejnë të drejtat bazë të një individi të lidhura ngushtësisht me të dhe që janë të njohura nga kushtetuta dhe "Deklarata ndërkombëtare e të Drejtave të njeriut".

E drejte e njohjes ~ Nënkupton të drejtën për t'u njohur me një të dhënë të caktuar.

Dokument ~ Është një shkresë zyrtare që shërben për të dëshmuar ose për të vërtetuar diçka. Ai mund të jetë i printuar, dublikatë, fotografim, fotokopjim, regjistrim fonografik, regjistrim magnetikisht, regjistrim optik, etj.

DH

E dhënë personale ~ Është çdo informacion për një person fizik, i cili është i identifikuar ose i identifikueshëm. Elementet, me të cilat realizohet identifikimi i një personi, drejtpërdrejt apo tërthorazi, janë numrat e identitetit ose faktorë të tjerë të veçantë fizikë, psikologjikë, ekonomikë, socialë, kulturorë etj.

E dhënë sensitive ~ Është çdo informacion për personin fizik, që ka të bëjë me origjinën e tij racore ose etnike, mendimet politike, anëtarësimin në sindikata, besimin fetar apo filozofik, dënimin penal, si dhe të dhëna për shëndetin dhe jetën seksuale.

Të dhëna të automatizuara ~ Të dhëna të hedhura në sisteme elektronike dhe të përpunuara në to.

Të dhëna për trafikun e komunikimeve ~ Është çdo e dhënë e përpunuar për qëllime të transmetimit të komunikimeve në një rrjet të komunikimeve elektronike ose për qëllime faturimi.

Të dhëna biometrike ~ Të dhëna që lidhën më tiparet biologjike të njeriut. Janë dimensionet e matshme të trupit dhe sjelljes së individit, veçanërisht gjurmët e gishtave, struktura e kreshtave të gjurmëve, skanimi i retinës dhe irisit të syrit, analiza e formës së fytyrës dhe veshëve, karakteristikat e qëndrimit të trupit, karakteristikat fizike, psikologjike dhe të sjelljes së individit të cilat janë unike dhe të qëndrueshme.

E dhënë anonime ~ Është çdo e dhënë që në origjinë, ose gjatë përpunimit, nuk mund t`i shoqërohet një individi të identifikuar ose të identifikueshëm.

Të dhëna që lidhen me personin ~ Çdo informacion që lidhet me një person i cili është i identifikuar ose i identifikueshëm.

E

E-mail (Electronic Mail) ose Posta Elektronike ~ Konsiderohet çdo mesazh në formën e tekstit, tingullit, apo imazhit të dërguar nëpërmjet rrjetit publik të komunikimeve, i cili mund të ruhet në rrjet ose në pajisjen fundore të marrësit derisa marrësi ta marrë atë.

F

Firewall ~ Pajisje apo një program kompjuterik që është i konfiguruar për të kontrolluar trafikun që kalon nëpër rrjet, duke e lejuar apo bllokuar atë në bazë të një grupi rregullash.

Fshehtësi e korrespondencës ~ Ndalimi i hapjes së korrespondencës që mbajnë dy persona apo institucione

Fshirje e të dhënave ~ Nënkupton asgjësimin ose eliminim përfundimtar të të dhënave nëpërmjet metodave të përcaktuara paraprakisht.

Fjalët kyçe/ Key words ~ Pjesë e një treguesi të vërtetësisë që i përket një personi dhe që njihet vetëm prej tij, ndërtuar nga disa karaktere ose të dhëna të tjera në formë elektronike.

G

Grumbullim i të dhënave ~ Nënkupton marrjen dhe sistemimin e të dhënave në një formë sa më të rregullt.

Globalizim ~ i ekonomisë / Globalisation of the economy

Globalizimi i referohet fenomenit të hapjes së ekonomive dhe kufijve, çka çon në rritjen e tregtisë dhe të lëvizjes së kapitalit, lëvizjes së njerëzve dhe ideve, përhapjes së informacionit, njohurive dhe teknologjisë, nga një proces për-rregullimi. Ky proces, si gjeografik ashtu edhe sektorial, nuk ka filluar kohët e fundit, por është përshpejtuar në këtë periudhë. Ndërkohë që globalizimi është burim i shumë mundësive, mbetet një nga sfidat më të mëdha për Bashkimin Evropian sot. Në mënyrë që të shfrytëzohet plotësisht potenciali i rritjes që ofron kjo dukuri dhe për të garantuar ndarje të drejtë të përfitimeve, BE po punon për ngritjen, nëpërmjet një qeverisjeje shumëpalëshe, e një modeli për zhvillimin e qëndrueshëm, që synon të gjejë pikën e pajtimit midis rritjes ekonomike, kohezionit social dhe mbrojtjes së mjedisit.

GJ

Gjykatë ~ Evropiane e të Drejtave të Njeriut / European Court of Human Rights

Gjykata Evropiane e të Drejtave të Njeriut është një gjykatë ndërkombëtare e krijuar më 1959 në kuadër të Këshillit të Evropës. Ajo vendos për paditë e ngritura nga shtetet ose individët që kanë të bëjnë me shkeljen e të drejtave politike dhe civile të parashikuara në Konventën Evropiane të të Drejtave të Njeriut. Që nga viti 1998, ajo funksion si një gjykatë me kohë të plotë dhe individët mund t'i drejtohen asaj në mënyrë të drejtpërdrejtë. Përgjatë 50 viteve, Gjykata ka dhënë mbi 10,000 vendime. Vendimet janë të detyrueshme për shtetet të cilave ato i drejtohen dhe ato i kanë detyruar qeveritë që të ndryshojnë legjislacionin e tyre dhe praktikat e tyre administrative për një numër të madh fushash. Jurisprudenca e Gjykatës e ka kthyer Konventën për të Drejtat e Njeriut në një instrument me fuqi të madhe zbatuese për përballimin e sfidave të reja dhe për konsolidimin e demokracisë dhe shtetit të së drejtës në Evropë. Gjykata ka qendrën në Strasburg në ndërtesën e të drejtave të njeriut, projektuar nga arkitekti britanik Richard Rogers më 1994 – një ndërtesë imazhi i së cilës është bërë i njohur në mbarë botën. Nga kjo ndërtesë gjykata monitoron respektimin e të drejtave të njeriut të 800 milion evropianeve në 47 vende anëtare të Këshillit të Evropës të cilët e kanë ratifikuar Konventën.

H

Hapje e korrespondencës ~ Hapja e letrave, shkresave, komunikimeve elektronike mes dy njerëzve/institucioneve nga persona të tjerë të ndryshëm nga marrësi i destinuar.

Hacker ~ Persona të cilët modifikojnë programe kompjuterike për përdorime të jashtëligjshme.

Host ~ Është një server në të cilin mund të vendosen një apo më tepër shërbime ose website.

HTML ~ Gjuhë programimi për të ndërtuar faqe internet.

I

ICT (Information and Communication Technology) ose TIK (Teknologjitë e Informacionit dhe Komunikimeve) ~ Tërësia e pajisjeve, sistemeve dhe shërbimeve që mundësojnë përpunimin, ruajtjen dhe komunikimin elektronik.

Identitet ~ Kuptohet një kombinim unik i karakteristikave të lidhura me çdo person si p.sh. emri, mbiemri, data dhe vendi i lindjes, gjinia dhe karakteristikat fizike, kjo e gjitha duhet të jetë në përputhje me legjislacionin kombëtar apo legjislacionin ndërkombëtar të fushës duke lejuar identifikimin e personit nga autoritetet përkatëse.

Implementim ~ Vënie në zbatim të një akti.

Instant Messaging, Chat ~ Teknologji që japin mundësinë e komunikimit tekst në kohë reale midis dy apo më shumë bashkëbiseduesve ne rrjet të mbyllur apo Internet.

Internet ~ Hapësire e komunikimit në rrjet e bazuar në protokollin TCP / IP dhe e cila nuk është pronë e një shteti, kompanie apo individi.

Informacion ~ Do të thotë çdo njohuri që mund të komunikohet apo të dokumentohet, pavarësisht nga forma, për një person, fizik, juridik, dhe send.

IP (internet protocol) ~ Është protokolli i përdorur për të lejuar komunikimin e të dhënave në rrjet.

ISP (internet service provider) ~ Ofrues i shërbimit të internetit.

Instrumente elektronike ~ Janë kompjuteri, programet kompjuterike dhe çdo mjet elektronik ose automatik me të cilat bëhet përpunimi.

I interesuari ~ Nënkupton një person fizik, person juridik, organ ose shoqatë të cilit/cilës i referohen të dhënat personale.

J

Jetë private ~ Tërësia e veprimtarisë jetësore të një individi

K

Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale ~ Është autoriteti përgjegjës, që mbikëqyr dhe monitoron, në përputhje me ligjin, mbrojtjen e të dhënave personale, duke respektuar e garantuar të drejtat dhe liritë themelore të njeriut. Komisioneri është person juridik publik. Ai zgjidhet nga Kuvendi, me propozimin e Këshillit të Ministrave, për një mandat 5-vjeçar, me të drejtë rizgjedhjeje.

Kontrollues ~ Është çdo person fizik ose juridik, autoritet publik, agjenci apo njësi tjetër, të cilët, vetëm apo në bashkëpunim me të tjerë, mbajnë, përpunojnë, administrojnë, arkivojnë dhe për këtë shkak kontrollojnë të dhëna personale.

Kontroll i banesës ~ Shqyrtimi i imtësishëm i ambienteve të banimit më qëllim zbulimin e fakteve dhe provave të rëndësishme që lidhin personin që banon në të më një ngjarje a vepër të caktuar

Kontroll vetjak ~ Kontroll trupor më qëllim zbulimin e fakteve dhe provave të rëndësishme që lidhin personin me një ngjarje a vepër të caktuar.

Konventë ~ 1.Marrëveshje e lidhur ndërmjet dy a më shumë shteteve për shkëmbime në fushën tregtare, kulturore etj. Konventë ndërkombëtare. Konventë ekonomike (tregtare, doganore, kulturore). Konventë vjetore. Sipas konventës. Nënshkruan konventën. 2. Konventa është një instrument që i përket Shtyllës së tretë të Bashkimit Evropian (Drejtësia dhe Çështjet e Brendshme). Konventa miratohet nga Këshilli, i cili vepron unanimisht pas këshillimit me Parlamentin Evropian dhe hyn në fuqi pas miratimit nga të paktën gjysma e Shteteve Anëtare

Korrespondencë ~ Këmbim i vazhdueshëm letrash a shkresash ose komunikimesh elektronike ndërmjet njerëzve ose ndërmjet institucioneve; letërkëmbim.2. Lajm që merret në vendin e ngjarjes nga korrespondenti dhe që botohet në një gazetë a revistë ose jepet në radio; artikull i botuar në një gazetë, në një revistë a në një organ tjetër nga një korrespondent. Korrespondencë nga krahinat. 3. Bisedë..

Kufizim i të drejtave ~ Diçka që përcakton se deri ku e sa lejohet të gëzosh një të drejtë të caktuar ose të drejtat në përgjithësi.

Komunikim ~ Është komunikimi i të dhënave personale një ose më shumë subjekteve te caktuar te ndryshëm nga i interesuari, nga përfaqësuesi i titullarit ne territorin e vendit, nga përgjegjësit dhe te ngarkuarit, ne çdo formë, edhe përmes vënies ne dispozicion ose për konsultime.

Komunikimi elektronik ~ Çdo informacion i shkëmbyer ose i përcjellë mes një numri te caktuar subjektesh përmes një shërbimi të komunikimit elektronik të hapur për publikun. Janë të përjashtuara informacionet e dhëna për publikun nëpërmjet një rrjeti të komunikimit elektronik, si pjesë e një shërbimi të transmetimit radiofonik, përveç nëse të njëjtat informacione lidhen me një abonent ose përdorues të identifikuar ose të identifikueshëm.

Kartë, ~ae të Drejtave Themelore / Charter of Fundamental Rights

Në vijim të përvjetorit të 50-të të Deklaratës Universale të së Drejtave të Njeriut, të festuar në dhjetor 1998, Këshilli Evropian i Këlnit (3-4 qershor 1999) filloi punën për hartimin e Kartës së ë Drejtave Themelore. Qëllimi i kësaj karte ishte që Të Drejtat Themelore në nivel të Bashkimit Evropian, të bashkohen në një dokument të vetëm, për të ndërgjegjësuar më shumë mendim publik.
Karta e të Drejtave Themelore e BE-së u shpall solemnisht nga Këshilli Evropian në Nisë, më 7 dhjetor 2000. Karta bazohet në Traktatet Komunitare, konventat ndërkombëtare, si Konventa Evropiane e të Drejtave të Njeriut (1950) dhe Karta Sociale Evropiane (1989), traditat kushtetuese të përbashkëta të Shteteve Anëtare, si edhe deklarata të ndryshme të Parlamentit Evropian.
Puna për hartimin e projektit të Kartës së të Drejtave Themelore iu besua një asambleje të veçantë, Konventës, që përbëhej nga 62 anëtarë, përfshirë përfaqësuesit e institucioneve Evropiane dhe të qeverive të Shteteve Anëtare. Në 7 kapituj të ndarë në 54 nene, karta përcakton të drejtat themelore në lidhje me dinjitetin, lirinë, barazinë, solidaritetin, shtetësinë dhe drejtësinë.

L

Lexim i korrespondencës ~ Leximi i letrave, shkresave, komunikimeve elektronike mes dy njerëzve/institucioneve nga persona të tjerë të ndryshëm nga marrësi i destinuar.

Lidhje të telekomunikacionit ~ Një lidhje e themeluar për transferimin e sinjaleve elektromagnetike me kabull ose bartës optikë ose me sinjale të radios.

Link ~ lidhje.

Ligj ~ 1. Normë, rregull që vendoset nga organi më i lartë i pushtetit shtetëror dhe që është e detyrueshme për të gjithë organet shtetërore dhe për të gjithë shtetasit. Ligjet e shtetit. Ligji mbi zgjedhjet. Njohja e ligjeve. Zbatimi i ligjit. Sipas ligjeve në fuqi. Është vendosur me ligj. Është në përputhje (në pajtim) me ligjin. Është jashtë ligjit nuk është në pajtim me ligjet; nuk mbrohet nga ligjet në fuqi; nuk e lejon ligji. 2. Rregull, normë që e pranojnë dhe e zbatojnë të gjithë si diçka të përgjithshme a të detyrueshme. Ligjet e mirësjelljes. Ligje të pashkruara. i tillë ishte ligji i luftës. 3. filoz. Lidhje e brendshme, e qenësishme dhe e domosdoshme ndërmjet sendeve e dukurive të natyrës e të shoqërisë, që përcakton zhvillimin e tyre dhe e bën procesin botëror një të tërë të vetme. Ligjet e

përgjithshme (e veçanta). Ligjet e zhvillimit të natyrës e të shoqërisë. Ligji i zhvillimit objektiv. Ligjet e lëvizjes. 4. spec. Përgjithësim që nxirret duke vëzhguar e studiuar dukuritë e natyrës e të shoqërisë dhe duke zbuluar në to atë që është e përbashkët, e rregullsishme dhe qenësore. Ligji periodik. kim. Ligjet e shkencës. Ligjet e materializmit dialektik e historik. Ligjet e fizikës. Ligji i ruajtjes së energjisë. fiz. Ligji i vlerës (i mbivlerës). ek. Ligji i mohimit të mohimit. filoz. Ligjet e fonetikes. Gjuh.5. bised. E drejtë. I dha ligj atij. Ka ligj të mos e dojë. Kështu nuk ke ligj. * Bën ligjin keq. vendos çdo gjë vetë pa pyetur asnjeri dhe pa përfillur rregullat e caktuara, ç'thotë ai bëhet. E ka ligjin në teh të shpatës.

Ligj komunitar ~ Ligj i njohur dhe i zbatuar ndërkombëtarësh.

Liri themelore ~ Gëzimi i të drejtave bazike me të cilat lind njeriu, p.sh. e drejta për të jetuar; Të qenët i lirë në jetë e në punë, mungesa e shtypjes, e varësisë dhe e kufizimeve që pengojnë, vështirësojnë e ndrydhin veprimtarinë politike e shoqërore të një klase a shtrese të caktuar, të shoqërisë në tërësi ose të anëtarëve të saj.

Liri e korrespondencës ~ E drejta dhe liria e çdo personi për të këmbyer letra ose komunikime elektronike me këdo që ai dëshiron dhe për të shkruar në të çfarëdo përmbajtjeje

Login ~ Procesi nëpërmjet të cilit një përdorues fiton akses në një sistem apo rrjet kompjuterik, i cili zakonisht nënkupton futjen e një UserID-je (username) dhe një fjalëkalimi (password).

LL

Llogari anonime ~ Mjete financiare, të ruajtura ose të depozituara në bankë, të cilat përdoren për qëllime të ndryshme të cilat nuk e kanë të identifikueshëm personin që i disponon.

M

Marrës- Është çdo person fizik ose juridik, autoritet publik, agjenci apo njësi tjetër, të cilëve u jepen të dhëna personale.

Marrje e pëlqimit ~ Deklarimi i personit me shkrim apo çdo formë tjetër se është në dijeni dhe pranon t'i përpunohen të dhënat.

Mbledhje e të dhënave ~ Veprimtaria e grumbullimit të të dhënave.

Mjet komunikimi ~ 1. Tërësi pajisjesh që shërben për të mundësuar komunikimin mes dy njerëzve ose institucioneve 2. Të gjitha llojet e mjeteve në të cilat të dhënat janë të regjistruara.

Mosdorëzim i korrespondencës ~ Mosdorëzimi i materialeve që përmbajnë këmbimin e korrespondencës mes dy njerëzve/institucioneve tek marrësi i destinuar.

Mjete Përpunimi ~ Janë mjetet automatike, gjysmë automatike dhe mekanike që përpunojnë të dhëna personale.

Mbikëqyrje ~ Është ndjekja me kujdes e përpunimit të të dhënave personale, nga të gjithë kontrolluesit dhe përpunuesit nëpërmjet bashkëpunimit, kontrollit, hetimit administrativ dhe inspektimit, për parandalimin e shkeljeve dhe kur ka vend dhe vendosjen e sanksioneve administrative, për të siguruar zbatimin e urdhrave, udhëzimeve dhe rekomandimeve të Komisionerit, duke respektuar të drejtat dhe liritë themelore të njeriut.

Monitorim i të dhënave personale ~ Është puna e vazhdueshme, gjithëpërfshirëse, efikase dhe e planifikuar e institucionit në këto drejtime: udhëheqje, drejtim, organizim, ndihmë, bashkëpunim, takime sensibilizimi e njohje, orientim, raportim në Kuvend, publikim, shpjegime të ndryshme, dhënie përgjigje të ankimeve, veprimtari, seminare e leksione, aktivitete, dokumentim, hartim rregullash, marrëveshje, kontrata, udhëzime, vendime, rekomandime, kontroll i zbatimit të gjobave, krijim e hapje të regjistrave, si dhe për çështje të tjera që lidhen me ushtrimin e rregullt të veprimtarisë.

Masa minimale ~ Kompleksi i masave teknike, informatike, organizative, procedurave logjistike dhe të sigurisë që përbëjnë nivelin minimal të mbrojtjes së nevojshme në lidhje me rreziqet e përmendura në pikën 1 të nenit 27 të ligjit nr.9887, datë 10.3.2008 “Për Mbrojtjen e të Dhënave Personale”.

N

Ndreqja (korrigjimi) e të dhënave ~ Ndryshimi që i bëhet të dhënave për t’i përmirësuar, për t’i hequr gabimet e të metat.

Netiquette (Network Etiquette) ~ Etika e përdorimit të shërbimeve të rrjetit.

Normë ~ 1. Rregull e caktuar ligjore ose morale për sjelljen në jetë a në shoqëri, e detyrueshme ose e pranuar përgjithësisht; diçka e detyrueshme për t'u ndjekur; rregullat që përcaktojnë jetën e brendshme të një organizate. Normat morale (juridike). I thyen normat e egra të kanunit. Është bërë normë. 2. Masë e caktuar për diçka; sasia e përshtatshme ose e rregullt për diçka; gjendja e rregullt dhe e zakonshme për diçka. Normat e shpenzimit (e harxhimit). Norma e akumulimit. ek. Norma e mbivlerës (e fitimit). ek. Është brenda normës. Zhvillohet sipas normës. Shmanget nga norma. 3. gjuh. Tërësia e rregullave që përcaktojnë përdorimin e mjeteve të gjuhës letrare në mënyrë të njëllojtë për të gjithë pjesëtarët e një kombi; përdorimi i mjeteve gjuhësore që është ngulitur e është pranuar nga të gjithë pjesëtarët e një kombi si në ligjërimin e folur ashtu edhe në atë të shkruar.

Network ~ Është një rrjet kompjuterik.

Newsgroup ~ Quhet një sistem i cili i lejon përdoruesve të lexojnë dhe të nisin mesazhe rreth një teme të caktuar.

Nickname ~ Quhet pseudonimi i cili vendoset nga përdoruesit sipas dëshirës.

NJ

Njohje me të dhënat ~ Marrja dijeni për përpunimin e të dhënave dhe me të dhënat në fjalë.

P

Password ~ Fjalëkalim, kod sekret i një përdoruesi që nuk duhet të njihet nga përdoruesit e tjerë, dhe që i përdorur bashkë me UserID, lejon aksesimin e një sistemi.

Paprekshmëri e banesës ~ Ruajtja e mbrojtja e banesës me ligj nga çdo lloj dhunimi.

Pengesat e qarkullimit të të dhënave personale ~ Çdo rrethanë, dukuri, kriter apo kusht ligjor që pengon transmetimin dhe transferimin e të dhënave personale.

Përdorimi i të dhënave ~ Bërje e veprimeve me të dhënat, shfrytëzim i tyre për të arritur një qëllim të caktuar.

Përgjim ~ Përqendrim i vëmendjes dhe i shqisave për të hetuar çfarë ndodh me një person fizik/ juridik të caktuar; vëzhgimi organizuar i çdo veprimi, thënie ose lëvizjeje të personit.

Përhapje ~ Komunikimi i të dhënave personale ndërmjet kontrolluesve apo komunikimi i të dhënave personale tek çdo subjekt tjetër, përveç përpunuesit apo subjektit të të dhënave, përfshirë edhe publikimin.

Përpunim i të dhënave ~ Është çdo veprim që kryhet plotësisht ose jo me mjete automatike, me të dhënat personale, si grumbullimi, regjistrimi, ruajtja, renditja, përshtatja, ndreqja, këshillimi, shfrytëzimi, përdorimi, bllokimi, fshirja ose shkatërrimi apo çfarëdo veprim tjetër, si dhe transmetimi i të dhënave.

Përpunues ~ Është çdo person fizik ose juridik, autoritet publik, agjenci ose çdo njësi tjetër, përveç punonjësve të kontrolluesit, që përpunojnë të dhëna për vetë kontrolluesin.

Pëlqim ~ Është deklarata specifike, e dhënë me vullnet të lirë nga subjekti i të dhënave personale për përpunimin e të dhënave të tij.

Pëlqim i subjekteve të të dhënave ~ Është çdo deklaratë me vullnet të plotë e të lirë e dhënë shprehimisht dhe në dijeni të plotë për çfarë të dhënat do të përpunohen, me të cilën nënkupton që subjekti i të dhënave pranon që të përpunohen të dhënat e tij”.

Përafrim i ligjeve ~ Nënkupton procesin e njehsimit të legjislacionit kombëtar me atë komunitar.

Përpunimi automatik ~ Përfshin operacionet e mëposhtme, nëse kryhen plotësisht ose pjesërisht me anë të mjeteve automatike: ruajtjen e të dhënave, kryerjen e veprimeve logjike dhe/ose aritmetike mbi këto të dhëna, ndryshimin, fshirjen, marrjen ose shpërndarjen e tyre;

Privatësi ~ Do të kuptohet çdo e dhënë dhe informacion që lidhet me personin, me jetën e tij private, të drejtat, prona, mjedisi që lidhet me pronën, banesa e pjesët e saj, veprimtaria dhe interesat vetjake, e drejta e votës, shprehja e fjala, veshja, paraqitja e jashtme, fotografia, hobet, shijet, dhuntitë, cilësitë e veçanta, aftësitë, çështjet e brendshme të familjes, të dhënat sensitive (jeta e prekshme, shqisore, intime, e ngushtë, vemesa e brendshme e njeriut, origjina racore ose etnike, mendimet politike, anëtarësimi në sindikata, besimi fetar apo filozofik, dënimi penal, si dhe të dhëna për shëndetin dhe jetën seksuale), tiparet biologjike unike (vetitë, ngjyra e syve, flokëve, ngjyra e lëkurës, përmasat e format e pjesëve të trupit, zëri, ecja), të dhënat biometrike (gjurmët e gishtërinjve, imazhe të retinës, gjeometria e fytyrës ose duarve, irisit), karakteristikat gjenetike etj.

Postë elektronike ~ Është çdo mesazh në formën e tekstit, tingullit apo imazhit, të dërguar (transmetuar) nëpërmjet rrjetit publik të komunikimeve, i cili mund të ruhet në rrjet ose në aparatet terminale të marrësit derisa marrësi ta marrë.

Përdorues ~ çdo person fizik që përdor një shërbim komunikimi elektronik të hapur për publikun për qëllime private apo biznesi, pa qenë detyrimisht i abonuar.

Publikim ~ Bërja publike, e njohur botërisht e një të dhëne apo informacioni.

Palë e tretë ~ Është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër përveç subjektit të dhënave, kontrolluesit, përpunuesit dhe personat të cilët, nën autoritetin e drejtpërdrejtë të kontrolluesit apo përpunuesit, janë të autorizuar të përpunojnë të dhëna.

Përgjegjës ~ nënkupton një person fizik, person juridik, administratë publike apo ndonjë institucion tjetër, shoqatë apo organizatë që caktohet nga titullari për trajtimin e të dhënave personale.

Q

Qarkullim i të dhënave ~ Nënkupton procesin e transmetimit dhe transferimit të të dhënave personale.

Qëllime historike ~ Është përpunimi për qëllime të studimit, hetimeve, kërkimeve dhe dokumentimin e figurave, fakteve dhe rrethanave të kaluara.

Qëllime statistikore ~ Është përpunimi për qëllime të hetimeve statistikore ose rezultate statistikore, edhe me anë të sistemeve të informacionit statistikor.

Qëllime kërkimore ~ Është përpunimi për qëllime të studimit dhe hetimit sistematik në drejtim të zhvillimit të njohurive shkencore në një fushë të veçantë.

R

Regjistër i të dhënave elektronike ~ Çdo grup të dhënash që i nënshtrohet procedimit automatik.

Ruajtje e të dhënave ~ Vendosje e të dhënave personale në kushte sigurie, në përputhje me rëndësinë e tyre dhe legjislacionin në fuqi.

Riformulim, ~i i legjislacionit / Recasting of legislation

Riformulim i legjislacionit do të thotë miratim i një akti të ri ligjor, që përfshin ndryshimin që i bëhet aktit bazë, por që anulon dhe zëvendëson këtë të fundit. Ndryshe nga kodifikimi zyrtar, përfshihen edhe ndryshime thelbësore. Riformulimi i legjislacionit bën gjithashtu një përmbledhje të përgjithshme të një fushe të legjislacionit. Akti i ri ligjor botohet në Gazetën Zyrtare.

RR

Rrjet i komunikimeve elektronike ~ Janë sistemet e transmetimit dhe, nëse ekzistojnë, rrjetet e komutimit ose rrugëtimit dhe burime të tjera, të cilat lejojnë përcjelljen e sinjaleve nëpërmjet sinjaleve, radios, mjeteve optike ose mjeteve të tjera elektromagnetike, duke përfshirë rrjetet satelitore, rrjetet fikse (me komutim të qarqeve ose me komutim të paketave, përfshirë internetin), rrjetet e lëvizshme tokësore, sistemet e kabllove elektrike në raste kur ato përdoren, për transmetimin e sinjaleve, rrjetet e përdorura për transmetimet radiotelevizive, pavarësisht nga tipi i informacionit të përcjellë.

Rrjete publike të komunikimit ~ Një rrjet komunikimi elektronik i përdorur tërësisht ose kryesisht për ofrimin e shërbimeve të komunikimeve elektronike të hapura për publikun.

S

Sekret shtetëror ~ Të dhëna të fshehta që lidhen me veprimtarinë e shtetit dhe që nuk duhet të bëhen publike. Ekspozimi i paautorizuar i tyre mund të rrezikojë sigurinë kombëtare.

Sekret tregtar ~ Diçka e fshehtë që ka të bëjë me punë dhe detyra të caktuara tregtare, të cilat nuk duhet të shpallen a të njihen botërisht; që lidhet me veprimtarinë e posaçme tregtare.

Sekret vetjak ~ Diçka që lidhet me vetë personin dhe mbahet e fshehtë e nuk u tregohet të tjerëve.

Server ~ Kompjuter me parametra të larta në të cilin mund të instalohen disa shërbime të centralizuara për ti shërbyer aplikacioneve të kompjuterëve të tjerë të rrjetit. Serveri mund të përdoret si shpërndarës e-mail-i, file share, vendosje e intranetit etj.

Sigurim kombëtar ~ Do të thotë mbrojtja e pavarësisë, integritetit territorial, rendit kushtetues dhe marrëdhënieve me jashtë të Republikës së Shqipërisë.

Sistemi i telekomunikacionit ~ Është infrastruktura e telekomunikacionit e cila është përdorur si një sistem përdorues i mbyllur për kryerjen e detyrave.

Sistem arkivimi ~ Është çdo grup i strukturuar i të dhënave personale të cilat janë të aksesueshme në bazë të kritereve specifike.

Sistemi i autorizimit ~ Bashkim instrumentesh dhe procedurash që mundësojnë hyrjen në të dhënat dhe mënyrat e trajtimit të tyre, në funksion të profilit të autorizimit të kërkuesit.

Spam ~ Mesazhe elektronike, e-mail, me përmbajtje komerciale apo informuese jozyrtare.

Subjekti i të dhënave personale ~ Është çdo person fizik, të cilit i përpunohen të dhënat personale.

SH

Shërbim-i publik / Public service

Koncepti i Shërbimit Publik ka një kuptim të dyfishtë: ai përfshin si organet që sigurojnë shërbime, ashtu edhe shërbimet me interes të përgjithshëm që ato ofrojnë. Detyrimet e shërbimit publik mund të imponohen nga autoritetet publike mbi organin që siguron shërbimin (shoqëritë e linjave ajrore, transporti rrugor apo hekurudhor, prodhues energjie e kështu me radhë) në nivel kombëtar ose rajonal. Koncepti i shërbimeve publike dhe koncepti i sektorit publik (përfshirë edhe shërbimin civil) shpesh ngatërrohen gabimisht; ato ndryshojnë për sa i përket funksionit, statusit, pronësisë dhe “klientelës”.

Shërbime, ~t me interes të përgjithshëm / General interest services

“Shërbime me Interes të Përgjithshëm” janë shërbime që konsiderohen të tilla nga autoritetet publike dhe i nënshtrohen detyrimeve specifike të shërbimeve publike. Ato përfshijnë shërbime jotregtare (p.sh. arsim i detyrueshëm, mbrojtje sociale), detyrime të shtetit (p.sh. siguria dhe drejtësia) dhe shërbime me interes ekonomik të përgjithshëm (p.sh. energjia dhe komunikimet).

Shërbime, ~t me interes ekonomik të përgjithshëm / Services of general economic interest

Shërbime me interes ekonomik të përgjithshëm quhen shërbimet tregtare të interesit të përgjithshëm ekonomik, mbi të cilën autoritetet publike vënë detyrime të veçanta të shërbimit publik. Shembuj të shkëlqyer janë shërbimet e transportit, energjisë dhe komunikacionit.

Shoqëri, ~a e Informacionit / Information society

Shoqëri e Informacionit është term sinonim me "Teknologji të reja Informacioni dhe Komunikimi" (TIK). Që në fillim të viteve '90, janë zhvilluar me vrull TIK-e të reja. Përdorimi universal i shkëmbimit elektronik të informacionit, përqendrimi drejt teknologjive digjitale, rritja eksponenciale e përdorimit të internetit dhe hapja e tregjeve të telekomunikacionit, janë shenja të këtij ndryshimi.
Shoqëria e Informacionit po revolucionarizon shumë fusha të jetës së përditshme, veçanërisht mundësinë për përgatitje profesionale dhe marrje njohurish (mësimi në distancë, shërbimet e lidhura më e-learning), në organizimin e punës dhe mobilizimin e aftësive (puna nëpërmjet televizionit, kompanitë virtuale), në jetën praktike (shërbimet e-health) dhe argëtimin. Gjithashtu sigurohen mundësi të reja në lidhje me pjesëmarrjen e qytetarëve për ta bërë më të lehtë shprehjen e mendimit dhe pikëpamjeve. Megjithatë, këto ecuri pozitive shkojnë paralel me problemet e reja. Përdorimi në masë i internetit do të thotë, që janë bërë hapa kundër krimit, piraterisë, dhe çështjes së mbrojtjes të të dhënave personale dhe pronësisë intelektuale. Gjithashtu Shoqëria e Informacionit mund të kontribuojë në kufizimin e disa sektorëve të shoqërisë duke theksuar pabarazi sociale.

Shërbimi i komunikimeve elektronike ~ Shërbimet që konsistojnë tërësisht ose kryesisht në transmetimin e sinjaleve në rrjetet e komunikimeve elektronike, duke përfshirë shërbimet e telekomunikacionit dhe shërbimet e transmetimit në rrjetet e përdorura për transmetimin e rrjeteve televizive brenda kufijve të përcaktuara në nenin 2 , shkronja c) të Direktivës 2002/21/EC të Parlamentit Evropian dhe e Këshillit e 7 marsit 2002.

T

Traktat ~ Marrëveshje ose lidhje ndërmjet dy a më shumë shtetesh, palësh etj. për çështje të ndryshme politike, për marrëdhënie ekonomike etj. Traktat ushtarak. Traktat i fshehtë. Traktat famëkeq. Traktat paqeje. Traktat miqësie. Shkelja e traktatit. Denoncimi i traktatit. Lidhën një traktat.

Transmetim i të dhënave ~ është transferimi i të dhënave personale te marrësit.

Transferim ndërkombëtar ~ Është dhënia e të dhënave personale marrësve në shtetet e huaja.

Trajtimi i të dhënave ~ Janë procedurat dhe proceset e mbledhjes, përpunimit, grumbullimit, përhapjes, përdorimit dhe shkatërrimit të të dhënave.

Trajtimi kompjuterik i të dhënave ~ Është trajtimi i të dhënave me ndihmën e një kompjuteri duke përdorur memorie dhe programe të nevojshme për zbatimin efektiv të tij.

TH

Thirrje ~ Lidhje e realizuar nga një shërbim telefonik i hapur për publikun duke lejuar komunikimin nga dy drejtime në kohë reale.

U

UserID/Username ~ Varg karakteresh që identifikon ne mënyrë unike një përdorues në një sistem apo rrjet kompjuterik.

Upload ~ quhet dërgimi i të dhënave nga një sistem lokal në një sistem tjetër.

V

Virus ~ Është një program i cili infekton kompjuterin dhe mund të shkaktojë dëme në funksionimin e programeve.

W

WebSite ~ faqe interneti e cila mund të përmbajë informacione specifike.

Z

Zona sigurie ~ janë zonat ku mbahen ose ruhen, administrohen të dhëna personale dhe konfidenciale, ku hyrja i nënshtrohet një regjimi të veçantë.

A. Hipoteza/hipotezat e punimit

Hipotezat kërkimore të këtij disertacioni janë ngritur dhe formuluar për të arritur në konstatime dhe konkluzione finale në funksion të tematikës së kërkimit shkencor.

Hipoteza 1

Ligji "Për komunikimet elektronike" duhet rishikuar pasi problemet që vërehen në zbatimin e Direktivës 2006/24 të BE-së në lidhje me ruajtjen e të dhënave për qëllime të ndjekjes penale, janë të pranishme edhe në parashikimet aktuale që përmban ligji ynë.

Hipoteza 2

Në ligjin për mbrojtjen e të dhënave personale mungojnë parashikime të veçanta në lidhje me rregullimin e ndërhyrjes së autoriteteve shtetërore në të dhënat personale të qytetarëve, në rastet kur të dhënat përdoren për të garantuar sigurinë kombëtare, sigurinë publike, parandalimin dhe hetimin e kryerjes së një vepre penale, apo ndjekjen e autorëve të saj.

Hipoteza 3

Në Shqipëri, kuadri rregullator i çështjeve që lidhen me përdorimin e shërbimit të internetit dhe postës elektronike në kuadër të mbrojtjes së të dhënave personale të punëmarrësve në sektorin privat, mbetet jo i plotë.

B. Pyetjet kërkimore të punimit

1. Çfarë do të kuptojmë me të dhëna personale dhe privatësi?
2. Si kanë evoluar sot të dhënat personale dhe privatësia?
3. A është e mjaftueshme mbrojtja ligjore që i bëhet sot të dhënave personale dhe privatësisë?
4. Cili është roli i organeve përkatëse shtetërore në mbrojtjen e të dhënave personale dhe privatësisë në komunikimet elektronike?
5. A është legjislacioni Shqiptar në harmoni me standardet e Bashkimit Evropian për mbrojtjen e të dhënave personale dhe privatësisë?
6. Si e rregullon legjislacioni kombëtar mbrojtjen e të dhënave personale dhe privatësisë në komunikimet elektronike?

7. Cili është efekti i Direktivës transpozitive 2002/58/KE dhe Direktivës 2006/24/KE për mbrojtjen e të dhënave personale dhe privatësisë në Shqipëri?

C. Metodat dhe metodologjia e kërkimit

Metodat shkencore të përdorura në këtë studim janë: metoda historike, analitike, përshkruese dhe krahasuese, nëpërmjet të cilave janë trajtuar pikat kyçe të temës.

Metoda historike është përdorur për të pasqyruar zhvillimin evolutiv të fenomenit të mbrojtjes së të dhënave personale dhe privatësisë në komunikimet elektronike në nivel kombëtar dhe ndërkombëtar, si dhe proceset evoluese të përqasjes së legjislacionit të brendshëm shqiptar me instrumentat dhe aktet ndërkombëtare në fushën e të dhënave personale dhe privatësisë.

Metoda analitike bazohet kryesisht në analizën e thellë ligjore të instrumentave dhe akteve ndërkombëtare, komunitare dhe kombëtare në fushën e të dhënave personale dhe privatësisë në komunikimet elektronike.

Metoda përshkruese e përdorur në këtë punim ka pasur si qëllim përshkrimin dhe identifikimin e gjendjes aktuale të mbrojtjes së të dhënave personale dhe privatësisë në tërësi dhe në komunikimet elektronike në veçanti, në kuadër të qasjes dhe angazhimeve ndërkombëtare dhe evropiane që ka Shqipëria në fushën e mbrojtjes së të dhënave personale dhe privatësisë, duke përshkruar dhe duke bërë një trajtim të plotë dhe gjithëpërfshirës të kuadrit ligjor ndërkombëtar, evropian dhe kombëtar në lidhje me të dhënat personale dhe privatësinë, me qëllim identifikimin e problematikave që hasen në këtë fushë.

Metoda krahasuese është përdorur për të vënë përballë rregullimin e bërë nga legjislacioni ndërkombëtar dhe evropian për mbrojtjen e të dhënave personale dhe privatësisë në komunikimit elektronike, e parë kjo në raport me rregullimin e bërë nga ligjvënësi shqiptar.

Ju tashmë keni zero Privatësi – Kapërcejeni atë![1]

[1] McNeally, S., Zyrtar administrativ në Sun Microsystems në një deklaratë në vitin 2000 mbi mbrojtjen e të dhënave personale në ambientin e korporatave, i cili ka qenë riprodhuar shumë herë në literaturën botërore për çështjet e privatësisë. Siç tregohet në: http: //www .wired .com /politics/ law /news /1999 /01 /17538

Metoda e përgatitjes së tezës, predispozicioni

Ne jetojmë në epokën e zhvillimit të një modeli të ri ekonomik ku marrëdhëniet sociale dhe politike karakterizohen nga shpejtësia e ndryshimeve dhe dimensioni global. Planifikimi ekonomik, ndërhyrjet legjislative, kushtet sociale dhe kulturore kanë humbur karakteristikat e tyre kombëtare. Zhvillimet e vrullshme teknologjike kanë gjetur shprehjen e tyre më domethënëse në fushën e komunikimit dhe përhapjes së informacionit. Në botën e industrializuar, për individët, agjencitë publike, bizneset dhe organizma të tjerë privatë, përdorimi i Internetit mundëson realizimin e një pjese të konsiderueshme të komunikimeve të tyre me publikun e gjerë. Kjo përhapje në masë e komunikimeve nëpërmjet rrjeteve elektronike publike është ndikuar nga një sërë avantazhesh që ato paraqesin, të cilat kanë të bëjnë me lehtësinë, shpejtësinë e komunikimit, mundësinë për të komunikuar në kohë reale midis dy ose më shumë subjekteve që ndodhen në distanca tepër të mëdha nga njëri-tjetri etj. Krahas kësaj, pjesa më e madhe e informacionit në ditët e sotme ruhet në formë digjitale në kompjuterë pasi kjo siguron lehtësi të mëdha për ruajtjen, kopjimin dhe modifikimin e tij.

Duke marrë parasysh që sistemet kompjuterike janë të ndërlidhur ndërmjet tyre, kjo e lehtëson edhe më tej shpërndarjen e informacioneve nga një subjekt drejt një subjekti tjetër apo një numri të papërcaktuar subjektesh. Informacioni i ruajtur në këtë trajtë mund të tejçohet lehtësisht përtej kufijve të një vendi, në hapësira të mëdha gjeografike, në një kohë mjaft të shkurtër. Të gjitha këto avantazhe e bëjnë informacionin digjital formën më të përdorur të ruajtjes dhe shkëmbimit të informacionit. Evolucioni i tyre bazohet në ndërveprimin dhe marrëdhëniet me të gjitha shtetet e planetit, ajo që ne quajmë fshat global apo proces globalizimi,[2] një koncept që shpreh grupe të larmishme, procese heterogjene, karaktere ekonomike, politike dhe kulturore. Platforma mbi të cilën mbështetet ky transformim social-ekonomik nuk është

[2] Literatura mbi fenomenin e globalizimit është përhapur ndërkombëtarisht. Shih: për shembull Globalizimin nga Axford, B. (2013). "*Theories of Globalization*", fq. 74, Lechner, J. F. (2009). "*Globalization: The Making of World Society*", fq.15 dhe Bordo, M. D., Taylor, A. M., Williamson, J. G. (2007). "*Globalization in Historical Perspective*", fq. 106.

asgjë tjetër përveç teknologjive të reja të informacionit dhe komunikimit.[3] Zhvillimi i veçantë i teknologjisë të internetit bëri që në vitin 1984 shkrimtari William Gibson[4] të krijonte në librin e tij "Neuromancer",[5] rrjetin e madh digjital të informacionit të ashtuquajtur "cyber" (cyberspace).[6] Përmes rrjetit të këtyre ndërlidhjeve komplekse të epokës digjitale, burimet e reja të rrezikut të të dhënave personale, jetës publike dhe private të personit mund të ekspozohen ndaj rrezikut të shumëfishtë. Shkelja e intimitetit ka efekte të pallogaritshme në shoqëri nëpërmjet të cilave, si p.sh rreziqet e krijuara së fundi, kërcënojnë për shkak të zhvillimit të kompjuterëve dhe rrjetit të transmetimit të informacionit[7] i cili shkakton probleme të panegociueshme të mbrojtjes së të drejtave të njeriut, si dhe shkeljen e të dhënave të tyre personale dhe cenimin e të drejtës për jetë private.[8] Prandaj është e nevojshme që të eksplorohen hapësira të reja ligjore dhe të krijohen korniza të reja rregulluese të cilat mund të përgjigjen për evoluimin e vazhdueshëm të teknologjisë.[9]

Për këtë arsye, në nivel legjislativ po bëhen përpjekje për rregullat që rregullojnë mbrojtjen e të dhënave personale duke siguruar zhvillimin e qetë të teknologjive të komunikimit dhe informacionit të cilat janë një shofer kryesor i përparimit global.

Në këtë rast, dimensioni global i marrëveshjeve ligjore për mbrojtjen e jetës private dhe të dhënave personale ka një natyrë intensive ekonomike, ku lëvizja e lirë dhe të dhënat personale ndoshta kanë ndikuar në rritjen mesatare të shërbimeve ndër-

---

[3] Haftor, D. (2010). "*Information and Communication Technologies*, Society and Human Beings: Theory and Framework", fq.23.

[4] William Gibson Ford (i lindur më 17 mars 1948) është një shtetas amerikan-kanadez romancier spekulativ i cili është quajtur "profeti noir" (profeti i bardhë) e subzhanrit cyberpunk. Në https://en.wikipedia.org/wiki/William_Gibson

[5] Gibson, W. (1984). "*Neuromancer*", fq. 3 dhe (2004). "*Neuromancer - Ace Hardcove*r", fq. 8.

[6] Cyberspace është një term i përdorur vazhdimisht në literaturën botërore dhe literaturën shkencore si një koncept që mund të shprehi të gjitha marrëdhëniet komplekse që janë të bazuara rreth teknologjive digjitale. Në: http://www.techterms.com/definition/cyberspace

[7] Për këtë çështje shumë të ndjeshme të mbrojtjes së fëmijëve në internet shih: Akrivopoulou, Ch. dhe Psygkas, A., (2010). "*Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*", fq. 22.

[8] Gomien, D. (2005). "*Short Guide to the European Convention on Human Rights*", fq.89.

[9] Literatura ndërkombëtare i referohet mbikëqyrjes së re. Shih: vëllimin Marchionini, G. (1997). "*Information Seeking in Electronic Environments*", fq.174.

kufitare[10] dhe tregtisë.[11] Në të vërtetë, nismat ndërkombëtare të marrëveshjeve ligjore për mbrojtjen e privatësisë dhe të dhënave personale janë karakterizuar nga një dimension i fortë ekonomik që thekson mbrojtjen e të dhënave personale për të siguruar lëvizjen e lirë, të nevojshme për zhvillimin e shërbimeve ndërkufitare dhe komunikimin elektronik. Kjo përpjekje për të mbrojtur të dhënat personale të cilat nuk janë një qëllim në vetvete, por një parakusht i domosdoshëm për rritjen e shërbimeve ndërkufitare dhe shërbimeve të komunikimeve elektronike. Kjo mund të jetë një pikënisje për reflektim mbi qëllimet dhe mjetet e rezultateve të pritshme të ndërhyrjeve legjislative.

Me këto të dhëna, qëllimi i disertacionit është që të shqyrtojë rrezikun e të drejtës së privatësisë dhe të dhënave personale si aspekt individual i të drejtës së personit dhe rreziqet e veçanta të paraqitura nga zhvillimi i teknologjive të komunikimit elektronik si dhe paraqitjen kritike të marrëveshjeve të ngjashme mbrojtëse ligjore në nivel kombëtar dhe evropian. Për qëllimet e këtij studimi, zhvillimi teorik është kryer në monitorim të vazhdueshëm dhe dialog me jurisprudencën. Në shumë raste bëhet një analizë e gjerë e rasteve historike. Kapitujt nisin në raste të veçanta dhe të çojnë në qasje kritike të vendimit në përputhje me kuadrin ligjor ekzistues. Për më tepër, nëpërmjet analizës së vendimeve gjyqësore do të vlerësojmë opsionet e gjyqtarit në interpretimin e rregullave dhe të ligjit. Theks në këtë disertacion i jepet analizës të ligjit nr. 9918, datë 19.05.2008 të rishikuar me ligjin nr. 102/2012 "Për disa ndryshime dhe shtesa në ligjin nr. 9918", datë 19.5.2008 për "Komunikimet elektronike në Republikën e Shqipërisë", si e drejtë me ligj, i cili mbart Direktivën 2002/58/KE. Disertacioni është ndarë në 6 kapituj, që fillon me trajtimin e "Koncepteve të Privatësisë dhe të Dhënave Personale" dhe mbaron me "Konkluzionet" përmbyllëse. Në mënyrë të veçantë, ai është strukturuar si më poshtë:

Në hyrje është trajtuar Shoqëria e Informacionit e cila është një shoqëri që karakterizohet nga zhvillimi i paparë i rrjeteve të telekomunikacionit. Ndryshimet e vazhdueshme në teknologjitë e informacionit intensifikojnë shqetësimin se

[10] Pra mendimi shpjegues 5 në preambulën e Direktivës 2002/58/KE të Parlamentit Evropian dhe të Këshillit Evropian të datës 12 korrik 2002 "*Për përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike*" (Direktiva për mbrojtjen e privatësisë dhe komunikimet elektronike).

[11] Siç përmend:Cartelli, A., Palma M. (2009). "*Encyclopedia of Information Communication Technology*", fq. 653.

përfundimisht njerëzit do të jenë të ekspozuar vazhdimisht ndaj monitorimit të padëshiruar të privatësisë së tyre, me pa mundësi të konsiderueshme për t'u mbrojtur. Gjithashtu tentohet themelimi i nevojës për mbrojtjen ligjore të të dhënave personale në nivel ndërkombëtar se rrezikimi i të dhënave tona personale dhe privatësisë për shkak të mënyrës së lëvizjes së informacionit në linjë e bën të pamundur kontrollin kombëtar të këtij trafiku.

Në kapitullin e parë (I) është trajtuar koncepti i privatësisë dhe të dhënave personale në Evropën Perëndimore, SHBA dhe Kanada (ndikuar nga teoria juridike dhe filozofike), të cilat janë edhe udhëheqëse të sistemeve për mbrojtjen e të dhënave personale dhe qasjet konceptuale janë të lidhura drejtpërdrejt me qasjen legjislative, të marra në këto sisteme.

Në kapitullin e dytë (II) prezantohen mjetet teknologjike të depërtim infektimit, mjete të tilla si cookies, përgjuesit e rrjetit (web bugs), programet spiune (spyware), adresa elektronike (email), lista e komunikimit në grup (mailing list), grupet e informacionit (newsgroups), linjat e shkëmbimit ndër aktiv të mesazheve (chat), komunikimet e padëshirueshme elektronike (spamming) dhe rreziqet e shkaktuara tek të dhënat personale nga përdorimi i këtyre mjeteve teknologjike. Ky është një prezantim i nevojshëm jo vetëm për të kuptuar rreziqet për amatorët, por edhe për shkak se prezantimi dhe vlerësimi i rreziqeve dikton rregullimet e duhura ligjore.

Në kapitullin e tretë (III), normalisht është paraqitur mjedisi ndërkombëtar rregullator, pikësëpari me marrëveshjet për mbrojtjen e të dhënave personale në nivel ndërkombëtar dhe së dyti mjedisi rregullator evropian që i parapriu miratimit të Direktivës 2002/58/KE, si një kusht i të kuptuarit të evolucionit rregullator që çoi në prodhimin e kuadrit ligjor modern. Më pas janë prezantuar marrëveshjet për mbrojtjen e të dhënave personale që janë miratuar në Evropë nga ndërhyrjet e para legjislative të ashtë quajtura "gjenerata e parë", "gjenerata e dytë" dhe "gjenerata e tretë" e deri më tani me dispozitat rregullatore të së drejtës sekondare komunitare (Direktiva 2002/58/KE, 2006/24/KE dhe 2009/136/KE), gjithmonë me një theks të veçantë në komunikimet elektronike.

Në kapitullin e katërt (IV) është bërë një prezantim kritik i kuadrit të përgjithshëm ligjor në fuqi për mbrojtjen e të dhënave personale në Shqipëri. Në mënyrë të veçantë janë interpretuar dispozitat themelore të Kushtetutës dhe Kodit Penal të cilët

rregullojnë këtë mbrojtje. Kapitulli mbyllet me një prezantim të detajuar të kuadrit ligjor dhe veçanërisht ligjit nr. 9887, datë 10.03.2008[12] ndryshuar me ligjin nr. 48/2012, ndryshuar me ligjin nr.120/2014 "Për Mbrojtjen e të Dhënave Personale" i nevojshëm për analizën e mëvonshme të dispozitave të veçanta të ligjit nr. 9918, datë 19.05.2008 për "Komunikimet elektronike në Republikën e Shqipërisë",[13] ndryshuar me ligjin nr. 102/2012 për disa ndryshime dhe shtesa në ligjin nr. 9918, datë 19.5.2008 për "Komunikimet elektronike në Republikën e Shqipërisë".[14]

Në kapitullin e pestë (V) jam përpjekur të analizoj dispozitat e ligjit nr. 9918, datë 19.05.2008 ndryshuar me ligjin nr. 102/2012 "Për disa ndryshime dhe shtesa" për "Komunikimet elektronike në Republikën e Shqipërisë". Në këtë pikë, disertacioni përpiqet për të thelluar qëllimet e ligjvënësit shqiptar, duke analizuar ligjin shqiptar dhe duke specifikuar parimet klasike të përpunimit të të dhënave të cilat duhet të përmbushen nga ofruesit / kontrolluesit dhe analizon aktivitetet e autoriteteve të pavarura (Ministri, AKEP dhe AMA).

Në fund, në kapitullin e gjashtë (VI), konkluzionet e studimit theksojnë nevojën për jetën private, siç duket kjo dhe në evoluimin konceptual të shoqërive moderne. Qasja kritike është bërë gjithmonë në dritën e zhvillimeve të vazhdueshme teknologjike dhe rreziqeve të reja për të dhënat personale. Me shqyrtimin kritik të kuadrit legjislativ shqiptar, janë evidentuar mangësitë e hasura dhe janë dhënë rekomandimet e duhura për përmirësimin e tij.

[12] Ligji nr. 9887, datë 10.03.2008, ndryshuar me ligjin nr. 48/2012, ndryshuar me ligjin nr.120/2014 "*Për Mbrojtjen e të Dhënave Personale*".

[13] Ligji nr. 9918, datë 19.05.2008 "*Për Komunikimet Elektronike në Republikën e Shqipërisë*".

[14] Ligjin nr. 102/2012 për disa ndryshime dhe shtesa në ligjin nr. 9918, datë 19.5.2008 "*Për Komunikimet Elektronike në Republikën e Shqipërisë*" i ndryshuar.

Hyrje dhe bazimi teorik

Në mjedisin e ri të teknologjive të informacionit dhe komunikimit, kontrolli i informacionit dhe qasja në shërbimet specifike krijojnë një strukturë të ndryshme sociale dhe ekonomike të quajtur Shoqëri e Informacionit.[15] Shoqëria e Informacionit është një shoqëri që karakterizohet nga zhvillimi paparë i rrjeteve të telekomunikacionit. Një rrjet i telekomunikacionit është shndërruar në një rrjet digjital përmes të cilit njëkohësisht transmetohen tingujt, imazhet dhe të dhënat.[16] Këto rrjete nga ana e tyre, përmes procesit të konvergjencës me teknologjinë e informacionit, krijojnë një zhvillim të paparë në mënyrën e përpunimit, shpërndarjes dhe depozitimit të informacionit. Teknologjitë digjitale, kompjuterët dhe komunikimi me rrjetet e komunikimeve elektronike moderne janë duke ndryshuar mënyrën e informacionit të cilat përbëjnë të dhënat personale. Çdo informacion në lidhje me njerëzit nuk mund të ruhet më për një periudhë të pacaktuar kohe, në kopje të panumërta dhe me kosto minimale. Njëkohësisht informacioni ruhet lehtë dhe është i lehtë për t'u gjetur, për t'u kanalizuar e shpërndarë dhe prandaj fiton një rëndësi të madhe ekonomike dhe strategjike.[17]

Saktësia e informacionit[18] dhe personalizimi i dhënies së përparësisë së madhe për këdo që e përdor atë, mund ta përshtatë dhe ta drejtojë në një marrës të veçantë. Për këtë arsye, rëndësia e teknologjisë digjitale në shpërndarjen e informacionit është e madhe sepse ajo lejon zhvillimin e metodave të marketingut të përshtatura për grupet specifike të konsumit. Duke vepruar kështu, ai kontribuon në përmbushjen e nevojave të bizneseve për qasje në privatësi dhe informacion ku përfshihen konsumatorët dhe për t'i shërbyer qëllimeve që lidhen me shërbimet e marketingut dhe produkteve.[19]

---

[15] Manuel, C. (2001).“*The Internet Galaxy, Reflections on the Internet, Business and Society*”, Oxford University Press, Oxford, fq.39.

[16] Flichy, P. (1995). “*The history of modern communications - in the public sphere and private life*”, fq. 143.

[17] Nockelby, J. “*Privacy: Circa 2002*”, në: http//cyber.law.harvard.edu/privacy/PrivacyCirca2002.htm

[18] Për zhvillimin e konceptit të “informacionit” shih: Cappurro, R. “*The concept of information*” në dispozicion në http://www.capurro.de/infoconcept.html

[19] Shih: vlerën ekonomike të të dhënave personale në Buchmann, J. (2014). “*Internet Privacy: Options for adequate realisation*”, fq.23.

Përmes këtij procesi, informacionet bëhen autonome dhe reduktohen në burime transaksioni që janë thelbi i Shoqërisë së Informacionit, rreth së cilës strukturohet rrjeti i ekonomisë së re.[20] Ekonomia e re karakterizohet nga digjitalizimi i transaksioneve i cili ndryshon perceptimin, krijimin, reklamimin, shpërndarjen e produkteve dhe shërbimeve.[21] Hapësira dhe koha transformojnë veprimtaritë ekonomike si një gjë "reale", koha bëhet një faktor kryesor dhe hapësira zhduket.[22] Shoqëria e Informacionit nuk është asgjë tjetër, por veçse një shoqëri ku shoferi kryesor i rritjes ekonomike janë shërbimet. Zhvillimi i shërbimeve bazohet vetëm te përpunimi i informacionit lidhur me një gamë të gjerë marrëdhëniesh të të dhënave gjenetike dhe pozicionimit gjeografik të secilit prej nesh. Pra, përpunimi i lehtë dhe shpërndarja e informacioneve rrit produktivitetin dhe efikasitetin e prodhimit të shërbimeve specifike dhe nga ana tjetër çon në kosto më të ulëta për përmirësimin e shërbimeve dhe produkteve të ofruara për konsumatorin.[23]

Procesi i përshkruar vetëm ngre shumë shqetësime që lidhen me pamundësinë e një personi për të kontrolluar sasinë dhe cilësinë e informacionit në lidhje me të, duke mos ditur marrësit e informacionit dhe qëllimin për të cilin ata e përdorin këtë informacion. Përfundimisht, personi gradualisht humbet aftësinë për të përcaktuar dhe përshkruar jetën e tij private, të gëzojë atë i pa shqetësuar dhe të përcaktojë përmbajtjen e saj. Ky transformim i qytetarit në "objekt informacioni"[24] nuk është vetëm ekonomik, por edhe me rëndësi politike. Regjistrimi i lehtë i privatësisë të individëve të çon në informacion të drejtpërdrejtë ose të nënkuptuar në lidhje me bindjet politike dhe aktivitetet personale. Në këtë mënyrë, qytetarit i jepet mundësia për përdorimin e të

---

[20] Webster, F. dhe Blom, R. (2004). "*The Information Society Reader*", fq. 195.

[21] Cooke, Ph., De Laurentis, C. dhe MacNeill, S. (2010). "*Platforms of Innovation: Dynamics of New Industrial Knowledge Flows*", fq. 147.

[22] Queau, P. "*Who owns knowledge?*" në versionin elektronik Le Monde Diplomatique, në http://mondediplo.com/2000/01/14queau

[23] Bergkamp, L. (2002). "*EU data protection policy, the privacy fallacy: adverse effects of Europe's data protection policy in an information–driven economy*", Computer Law &Security Report, fq. 34.

[24] Shih: Thompson, N. (2000). "*Instilling Ethics*", fq.211 dhe Krogstie, J. (2012). "*Model-Based Development and Evolution of Information Systems: A Quality Approach*", fq.112.

dhënave të tij personale, në rastin më të mirë, duke vendosur personin në epiqendër të politikës së reklamave dhe më të keq, të shërbimeve të sigurisë të cilat në një shtet me mungesa të masave mbrojtëse demokratike dhe shqyrtimit gjyqësor të ligjshmërisë së veprimeve të tyre, kanë potencial për të bërë një shkelje të të drejtave themelore përmes përpunimit, ruajtjes dhe përdorimit të të dhënave personale me qëllim kontrollin e politikave të veprimit dhe mendimit. Ndryshimet e vazhdueshme në teknologjitë e informacionit intensifikojnë shqetësimin, se përfundimisht njerëzit do të jenë të ekspozuar vazhdimisht ndaj monitorimit të padëshiruar të privatësisë së tyre dhe pa mundësi të konsiderueshme për t'u mbrojtur.[25] Mënyra e zbatimit të masave mbrojtëse bëhet në mënyrë që privatësia e individëve të mbrohet, por dhe zhvillimi i ekonomisë së re të sigurohet, pasi ajo është bërë një objektiv i rëndësishëm i shoqërive moderne. Një seri e aplikacioneve të komunikimeve elektronike[26] e provojnë atë. Faqe të tilla si Facebook, Flickr, Twitter, Instagram përdoren nga miliona përdorues të internetit, duke ekspozuar informacione, foto dhe video të jetës së tyre personale, të cilat i ndajnë shumë herë me qindra ose mijëra njerëz që janë lejuar për të hyrë në të dhënat e tyre personale.[27] Telefonat celularë të cilët përmes teknologjisë GPS dhe Wi-Fi janë kthyer në mjete shumë përdorimëshe (Multitools) për ndjekjen e njerëzve dhe aktiviteteve. Me programin Trapster[28] zbulohen radarët e trafikut rrugor të vendosura nga Policia Rrugore. Me Inap[29] nuk ka nevojë të stresohemi ose të ndjehemi të frustruar në lidhje me atë se në çfarë stacioni do të zbresim kur udhëtojmë. Pas identifikimit të destinacionit tonë në hartë, ai më pas na zgjon në momentin e kërkuar. JOYity[30] luan

[25] Për teknologjitë e reja dhe rrezikun e të dhënave personale shih: Tene, O. (2011).*"Privacy, The New generations, International Data Privacy Law"*, fq. 15.

[26] Shih: për zhvillimin e Web dhe të dhënat personale , Peng, K. (2014). "*Anonymous Communication Networks: Protecting Privacy on the Web*", fq. 2.

[27] Të njohur si "Rrjete Sociale (Social Networks)". Shih: gjithashtu rekomandime mbi përdorimin e këtyre rrjeteve në http://www.datenschutz-berlin.de/content/europa- international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers and-common-positions-adopted-by-the-working-group dhe http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and- recommendations-for-online-social-networks

[28] http://trapster.com/

[29] http://moop.me/inap.php

[30] http://www.joyity.com/

lojën duke ndjekur dikë në hartë. Google Earth na lejon ne, që të shohim çdo cep të botës që duam përmes imazheve satelitore në vetëm disa metra larg nga sipërfaqja.[31]

Në këto rrethana për krijimin e ligjeve mbi kombëtare[32] nevojitet një përpjekje maksimale e mundshme dhe e përbashkët në nivel ndërkombëtar. Rrezikimi i të dhënave tona personale dhe privatësisë për shkak të mënyrës së lëvizjes së informacionit në rrjet (online),[33] vendos standarde të reja për rolin e rregullores së drejtë në nivel global dhe kombëtar. Për t'u ballafaquar me këtë situatë, ligjet ndërkombëtare përshtaten me teknologjitë e reja[34] duke u përpjekur që të arrihet balanca midis rrjedhjes së lirë të informacionit dhe mbrojtjes së interesit publik dhe interesave të personave.[35]

Rregullat juridike ndërkombëtare në fushën e mbrojtjes së të dhënave personale, kontribuojnë në mënyrë të barabartë lidhur me integrimin e marrëveshjeve të krijuara nga ligjet e ndryshme kombëtare, të cilat formohen nga ana e tyre duke u bazuar në traditën ligjore kombëtare, bindjet morale dhe dallimet kulturore të cilat tregojnë dallimet në prodhimin e legjislacionit përkatës dhe pasojnë me vendimet gjyqësore në mbrojtjen e privatësisë dhe të dhënave personale.

Edhe pse shpesh ndryshojnë në qasjen e tyre rregullatore, të gjitha shtetet kanë qëllim të përbashkët, sigurimin e aftësisë së subjekteve për përpunimin automatik të të dhënave personale. Të dinë informacionin që përdorin dhe përpunojnë organet përkatëse, duke përfshirë edhe mundësinë për të përcaktuar vetë subjektet se çfarë informacioni do të vihet në dispozicion për trajtim dhe tek të cilët ata dëshirojnë. Pavarësisht nga dallimet e tyre, ata e kanë kuptuar nevojën për të mbrojtur të dhënat personale dhe privatësinë nga teknologjitë moderne të komunikimeve elektronike që

---

[31] Futja e teknologjive të reja që lidhen me përdorimin e telefonave celularë në Revistën WIRED "*Inside the GPS revolution*", 12 February 2009, fq. 64.

[32] Gutwirth, S., Leenes, R. dhe de Hert, P. (2013). "*Reloading Data Protection: Multidisciplinary Insights and Contemporary*", fq.17.

[33] Sipas Berners Lee "*evolucioni më i madh dhe më i shquari teknologjik, rezultat i konvergjencës së teknologjive dhe faktorëve transformues në strukturat ekonomike dhe sjelljet sociale*", shih: Berners, L. T. (1999). "*Weaving the Web*", San Francisco, fq. 21.

[34] Për ndikimin e teknologjive të reja në të drejtën private shih: Gillies, L. (2013). "*Electronic Commerce and International Private Law: A Study of Electronic Consumer Contracts*", fq.92.

[35] Grant, R. A. dhe Bennett C. J. (1999). "*Visions of Privacy: Policy Choices for the Digital Age*", fq.193.

kanë një dimension global.[36] Krijimi i një kuadri rregullator që synon për të vënë parimet dhe rregullat rregullatore të pranuara dhe të zbatueshme në të gjitha vendet është një parakusht për mbrojtjen efektive të të dhënave personale, ku të paktën në nivel legjislativ të adresohen fenomene të tilla si p.sh Spam. Mungesa e bashkëpunimit ndërkombëtar, thjesht do të çojë në krijimin e fushave të shumta me nivele të ndryshme të mbrojtjes dhe për këtë arsye do të rezultojnë të paefektshme përpjekjet për të adresuar problemin.

[36] Shih: Bygrave, L. (2004). "*Privacy in a Global Context-A Comparative Overview*", Scandinavian Studies in Law, fq. 319 në folk.uio.no/LEE/publications/%%20inPrivacy20context.pdf 20global%

KAPITULLI I: KONCEPTET E PRIVATËSISË DHE TË DHËNAVE PERSONALE

Koncepti i privatësisë në lidhje me kërcënimet e teknologjisë moderne shqetësoi për një kohë të gjatë para teorisë juridike të ashtuquajturën botë perëndimore, sidomos SHBA-në dhe Evropën. Mbrojtja e privatësisë si një problem kompleks social dhe ligjor është subjekt kërkimor për shkencëtarët në fushat e ligjit të sociologjisë dhe filozofisë.[37] Zhvillimi i kompjuterëve dhe rrjeteve të informacionit, për arsye të rrezikut fluid dhe mjedisit të ndryshueshëm që krijoi, shkaktoi një interes të ri dhe të veçantë për jetën private.[38] Pikënisja e problematikave dhe dialogut ndërdisiplinor u bë pikërisht se jeta private ka nevojë për mbrojtje. Prandaj, konceptet e privatësisë dhe mbrojtjes së të dhënave personale u bënë një fushë e problematikave dhe analizave, si një parakusht për asistencë legjislative dhe teknike që nevojitet për mbrojtjen e tyre.[39] Qasjet teorike për konceptin e jetës private janë të shumta dhe udhëhoqën në reforma të ndryshme rregulluese. Pra, edhe mes SHBA-së dhe shteteve anëtare të Bashkimit Evropian, ekzistojnë dallime midis qasjes konceptuale për privatësinë dhe mënyrën e mbrojtjes së saj.[40]

---

[37] Clarke, R. "*What's Privacy*", në: http://www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html, Fischer-Hubner, S. (2001). "*Privacy in the Global Information Society*", IT – Security and Privacy, LNCS Springer-Verlag, Berlin - Heidelberg, fq. 5, Gavison, R. (1980). "*Privacy and the Limits of Law*", The Yale Law Journal, fq. 421, gjithashtu shih: http://www.gavison.com/a2658-privacy-and-the-limits-of-law, Solove, D. (1983). "*Understanding Privacy*", Harvard University Press, Harvard dhe Mendel, T., Puddephatt, A. dhe Wagner, B. (2012). "*Global Survey on Internet Privacy and Freedom of Expres*sion", fq.11.

[38] Siç thotë Grfinkel: "*Lufta mbi privatësinë kërkon vëmendje gjithnjë e më të madhe si në shtyp, televizion dhe internet*", siç citohet nga Leith, P. (2006). në "*The Socio-legal context of Privacy*", International Journal of Law in Context, fq.105.

[39] Dallimet mes SHBA dhe Evropë shih artikullin nga New York Times"*When American and European Ideas of Privacy Collide*", në http://www.nytimes.com /2010/02/ 28/ weekinreview /28liptak.html?_r=1, ku në përgjigje kemi rastin e dënimit të google nga gjykata italiane e shkallës së parë, e cila theksoi se mbrojtja e privatësisë në Evropë ka karakter dhe gëzon mbrojtjen e të drejtave themelore dhe në SHBA mbrohet kryesisht si e drejtë e konsumatorit.

[40] Cremer, H.J. (2010). "*Human Rights and the Protection of Privacy in Tort Law: A Comparison between English and German Law*", fq.123.

Në SHBA, në lidhje me çështjet e mbrojtjes së të dhënave personale dhe privatësisë, termi "privatësi (privacy)",[41] ose "jeta private",[42] zakonisht përkthehet me termin "Vetësi", e cila është analizuar si "gjendje e të qenit i vetmuar dhe që nuk mund të jetë në gjendje personi, për ta parë ose dëgjuar atë" dhe "gjendja i të qenit i lirë nga vëmendja e publikut",[43] pa dallim nga koncepti i të dhënave personale. Termi "personal data" i përkthyer si të dhëna personale është përdorur kryesisht në terminologjinë juridike evropiane duke krijuar kështu interpretime të ndryshme në lidhje me marrëdhëniet e dy koncepteve, pikat e identifikimit dhe diferencimin.

1.1 Dallimi midis Koncepteve "Jetë Private" dhe "Të Dhëna Personale"

Kur iu referohemi të dhënave zakonisht kuptojmë disa informacione. Të dhënat personale janë vetëm informacione "të karakterit personal" dhe veçanërisht informacione të cilat individualizohen në kohën kur lidhen me një person të veçantë, për t'u identifikuar direkt ose indirekt, ky i fundit. Informacione të tilla mund të përfaqësojnë gjithçka në lidhje me një person p.sh. veprimtari private, profesionale dhe ekonomike të tij, marrëdhëniet e tij me persona ose gjëra,[44] si marrëdhëniet ekonomike, veprimet, reagimet, qëndrimet, pavarësisht nëse ato lidhen me të tashmen ose me të kaluarën dhe se si i referohen asaj. Pra, përderisa ju lidhni me atë person një pjesë të informacionit, nuk është informacion personalisht i identifikueshëm vetëm kur të dhënat

---

[41] Për konceptin e "Privatësisë" shih: Westby, J.R. (2004). "*International Guide to Privacy*", fq.12, dhe Hall, K. (2000). "*Conscience, Expression, and Privacy*", fq.112.

[42] Grant, R. A. dhe Bennett, C.J. (1999). "*Visions of Privacy: Policy Choices for the Digital Age*", fq. 48.

[43] Teksti Anglisht thotë në shpjegimin e fjalës "*privacy*" si "*the state of being able to be alone, and not seen or heard by other people*" dhe "*the state of being free from public attention*". Shih: Longman dictionary of Contemporary English, Third Ed. (1995), fq. 1121.

[44] Tërësia e nenit 29 me Opinionin 4/2007, brenda përkufizimit të të dhënave personale duke përfshirë aktivitetet e tyre personale dhe marrëdhëniet (modelet e pjesëmarrjes së lirë, përfshirja në sjellje dhe shoqatat e konsumatorëve) si dhe marrëdhëniet dhe situata midis të drejtës private dhe asaj publike (prona, marrëdhëniet kontraktuale, lejet administrative, etj.) Opinion 4/2007 mbi "*konceptin e të dhënave personale*", në http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_el.pdf

personale të shkyçen nga personi në fjalë, domethënë kur të dhënat bëhen anonime atëherë natyrisht pushojnë të jenë të dhëna personale.[45]

Pikërisht, në këto karakteristika vihen re disa informacione si të dhëna personale, të cilat përcaktojnë marrëdhëniet e tyre me konceptin e "jetës private", sepse "mbrojtja e të dhënave personale përtej dallimit midis sferës private dhe publike, në parim nuk bën dallimin midis informacionit të thjeshtë dhe atij privat/konfidencial".[46] Në këtë kuptim koncepti i mbrojtjes së të dhënave personale është më i gjerë se privatësia. Në këtë drejtim lëviz dhe Mbikëqyrësi Evropian për Mbrojtjen e të Dhënave Personale, i cili vëren se mbrojtja e të dhënave personale "... mbulon një zonë më të madhe, pasi të dhënat personale mbrohen jo vetëm për të rritur privatësinë e subjektit. Gjithashtu ai u zotua të garantojë një tjetër të drejtë themelore, të drejtën e mos-diskriminimit".[47] Një pamje e njohur dhe e ndryshme e cila ndan nocionin e privatësisë nga ai i të dhënave personale u dorëzua në vitin 1978. Në Britaninë e Madhe, një komision i quajtur nga drejtuesi i tij "Komisioni Lindop", ndërmori një nismë për të bërë sugjerime për funksionimin e një kuadri institucional që rregullon mjedisin në të cilin funksionojnë sistemet operative kompjuterike publike dhe private.[48] Përfundimet treguan se funksionimi i legjislacionit për mbrojtjen e të dhënave personale duhet të jetë i ndryshëm nga ai i privatësisë. Në vend që të sigurojë të drejta duhet të ofrojë një kornizë për gjetjen e balancimit ndërmjet interesave të subjektit, të përdoruesit të të dhënave dhe shoqërisë si një e tërë.[49] Në përgjithësi, ne mund të trajtojmë problemin e marrëdhënieve të këtyre dy koncepteve duke pasur parasysh konceptin e të dhënave

[45] Shih: gjithashtu për konceptin e të dhënave personale Hervey, T. K. dhe McHale, J. V. (2004). "*Health Law and the European Union*", fq. 172.

[46] Hope, R. A., Savulescu, J. dhe Hendrick, J. (2008). "*Medical Ethics and Law: The Core Curriculum*", fq. 105.

[47] Dokumentet e Mbikëqyrësit Evropian për Mbrojtjen e të Dhënave Personale, në http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Papers/BackgrounddP/05-07_BP_accesstodocuments_EN.pdf. Megjithatë, vihet në dukje se Mbikëqyrësi Evropian përmend në të njëjtin tekst se "*.... Koncepti i mbrojtjes së të dhënave personale është koncept më i ngushtë se koncepti i privatësisë përderisa privatësia përfshin më shumë se të dhënat personale*".

[48] Warren, A. dhe Dearnley, J. (2005). "*Data protection legislation in the United Kingdom: from development to statute 1969-84*", fq. 238.

[49] Berkers, F., Goossenaerts, J. dhe Hammer, D. dhe Wortmann H. (2001). "*Human Models and Data in the Ubiquitous Information Infrastructure*", London-UK, fq. 9.

personale dhe konceptin e privatësisë, të cilët janë dy koncepte që në një moment ndërpriten, plotësojnë njëri-tjetrin dhe përfundimisht shumë herë në praktikë barazohen. Prandaj, pa mbrojtjen e të dhënave personale[50] nuk mund të ketë privatësi.

Për të qenë më shumë e kuptueshme se si ne arritëm në rregullimet moderne të privatësisë dhe të dhënave personale, si në nivel ndërkombëtar dhe atë kombëtar do të bëhet një diskutim i shkurtër i zhvillimit të këtyre dy koncepteve në tre sistemet kryesore të mbrojtjes së të dhënave personale dhe privatësisë, ato të SHBA-së, Kanadasë dhe Evropës.

1.2 Privatësia (Jeta Private)

1.2.1 Qasja amerikane (SHBA-së)

Në SHBA, në vendin e lulëzimit të liberalizmit ekonomik, dominoi parimi i mbrojtjes së lirive civile të individit (Liberties) i cili kërkonte të drejta nganjëherë kontradiktore të mbrojtjes së të drejtave të njeriut me ato të zhvillimit të lirë të biznesit. Ky parim u përball me një evolucion të mahnitshëm të teknologjisë nga fillimi i shekullit XIX i cili krijoi shqetësimet e para në lidhje me intimitetin (privatësinë) në shoqërinë moderne dhe formoi bazën për zhvillimin e të menduarit juridik dhe filozofik mbi të drejtën themelore të njeriut për të mbrojtur privatësinë e tij.[51]

1. Vetë-rregullimi i mbrojtjes së privatësisë

Besimi në lirinë personale[52] dhe përgjegjshmërinë individuale kishte si rezultat besimin e përhapur se të gjitha informatat në lidhje me individin mund të tregtohen në

[50] Megjithatë, kjo është një karakteristikë, se të dhënat personale si një koncept janë trajtuar në teorinë ligjore Evropiane dhe jurisprudencë në tërësi, me zhvillimin e teknologjisë së informacionit e cila kishte një rrol instrumental në përpunimin e automatizuar dhe lëvizjen e lirë të të dhënave personale.

[51] Shih: në përgjithësi kuptimin e privatësisë dhe nismave legjislative në SHBA te - Pohlman, H. L. (1993). "*Political Thought and the American Judiciary*", fq. 273 dhe Regan, P. M. (1995). "*Legislating Privacy: Technology, Social Values, and Public Policy*", fq.3.

[52] Shih: Për lirinë personale si një tipar kyç i konceptit të privatësisë në SHBA te Marcella, A. J. dhe Stucki, C. (2003). "*Privacy Handbook: Guidelines, Exposures, Policy Implementation and International Issues*", fq. 222, shih: më tepër për trajtimin e problemit të shkeljes së privatësisë në SHBA, Solove, D. (2004). "*The Digital Person-Technology and Privacy in the Information Age",* New York University Press.

qoftë se personi i njëjtë kështu dëshiron. Në lidhje se me çfarë dhe sa informacion do të zbulojë, është në dorë të personit për ta vendosur. Kjo qasje në privatësi, e njohur edhe si "arkitektura e tregut"[53] thekson privatësinë individuale përmes lidhjes së kontratave kur personi është pjesë e tyre. Pra, të gjithë duke përdorur në mënyrën e duhur të drejtën e "informacionit të vetëvendosjes"[54] mund të japin pëlqimin për transferimin dhe përdorimin e informacionit në lidhje me jetën e tyre private, ndërsa përpunimi me radhë i këtyre informacioneve i jepet organeve përgjegjëse për përdorimin e rënë dakord të informacionit të mësipërm.[55] Ndërhyrja legjislative mund të arrijë deri në sigurimin e kushteve dhe rrethanave nën të cilat shteti mund të mbledhë dhe të përdorë këto informacione.[56] Nuk është e rastësishme ndërhyrja më e rëndësishme qendrore legjislative në fushën e të dhënave personale në SHBA, e njohur si "Privacy Act" e cila rregullon mbrojtjen e të dhënave personale vetëm në organet e sektorit publik.[57] Ndërsa në nivelin e mbrojtjes kushtetuese zbatohet proporcionalisht në gjykata,[58] Amendamenti 4 i Kushtetutës së SHBA-së, që deklaron se "e drejta e shtetasve për sigurinë personale në sigurinë e shtëpive, dokumenteve dhe objekteve të tyre kundër kërkimeve të paarsyeshme dhe konfiskimeve, nuk do të shkelen dhe nuk do të lëshohen urdhra nga gjykata kompetente vetëm për shkak të një arsye serioze, shoqëruar nga një betim [ankesë në betim] apo afirmim [prova] dhe përshkrimi specifik i vendit që do të kontrollohet, personave që do të arrestohen ose sendeve që do të sekuestrohen". Në bazë të amendamentit të katërt, vendimi Olmsted kundër SHBA-së [Olmstead v. Shtetet e Bashkuara, 277 US 438 (1928)], ku gjykata vendosi se përgjimi i telefonit nga policia

[53] Shih: Artikullin nga Pöysti, T. (2009). "*Judgment in the Case of K.U. v Finland: The European Court of Human Rights requires access to communications data to identify the sender to enable effective criminal prosecution in serious violations of private life*" në http://sas-space.sas.ac.uk/5452/1/1855-2575-1-SM.pdf

[54] Shpesh i referohet konceptit "E drejta e kontrollit (Right of control)".

[55] Shkelja e këtyre detyrimeve kontraktuale krijon dhe një kërkesë kompensimi të subjektit të të dhënave.

[56] Levin, A. dhe Nicholson, M. (2005). "*Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*", University of Ottawa Law & Technology Journal, fq. 357, në http://ssrn.com/abstract=894079

[57] Shih: tekstin e ligjit mbi privatësinë (Privacy Act) në Departamentin e Drejtësisë SHBA në http://www.justice.gov/opcl/privstat.htm

[58] Përmbledhjet e vendimeve kyçe të gjykatave në http://www.fourthamendmentsummaries.com/

nuk përbën një shkelje të amendamentit 4 dhe vendimin Katz kundër SHBA-së [Katz v. Shtetet e Bashkuara, 389 US 347 (1967)] i cili e rrëzoi vendimin e mëparshëm dhe shprehu pikëpamjen se përgjimi i telefonit publik është në kundërshtim me amendamentin e katërt i cili ishte për përdoruesin një "prishje e paarsyeshme e privatësisë." Për përdoruesit, këto vendime ishin më të rëndësishmet lidhur me të drejtën e privatësisë e cila nuk mbrohet shprehimisht nga kushtetuta amerikane. Të metat e këtij sistemi janë të dukshme jo vetëm për një vëzhgues evropian, por edhe për ekspertët amerikanë.[59] Mjetet të cilat ndër veprojnë me qytetarin janë të fuqishme dhe teknologjitë e komunikimeve elektronike janë komplekse dhe të vështira për t'u kuptuar nga përdoruesit mesatarë të tyre.[60] Kushtet në të cilat tentohet një zgjidhje nga përkufizimi i paekuilibruar, mungesa e kuadrit të rreptë ligjor dhe legjislacionit kyç, krijojnë dyshime të arsyeshme në lidhje me mbrojtjen efektive të të dhënave personale dhe privatësisë.[61]

2. E drejta për izolim

Në vitin 1890 Juristët amerikanë Louis Brandeis dhe Samuel D. Warren në një nga artikujt më të njohur në literaturën botërore për problemin e privatësisë,[62] argumentuan se e drejta për t'u lënë vetëm ose e drejta për izolim "the right to be let alone"[63] është më themelore se sa të drejtat e dëshiruara prej kombeve të lira dhe se individi ka nevojë për të mbrojtur veten nga masa dhe kontrolli i pakontrollueshëm social të cilat kryhen në mënyrë që të ruhet autonomia e individit dhe identiteti i tij

[59] Shih: Artikullin e New York Times "*Strong privacy laws may explain data security in Europe*" ku edhe Joel Reidenberg profesor i Fakultetit të Drejtësisë në Universitetin Fordham si dhe udhëheqësi dhe eksperti në fushën e intimitetit Alan Westin, shprehin shqetësimet e tyre për mbrojtjen e reduktuar, ofruar për qytetarët amerikanë kundrejt atyre Evropianë.

[60] Shih: për vetë rregullimin në internet, Tambini, D., Leonardi, D. dhe Marsden, Ch. T. (2008). "*Codifying Cyberspace: Communications Self-regulation in the Age of Internet Convergence*", fq.12.

[61] Khosrowpour, M. (2001). "*Managing Information Technology in a Global Economy*", fq. 712.

[62] "*The Right to Privacy*" si ka mbizotëruar t'i referohet bibliografisë anglisht-folëse dhe "*Le droit à la vie privée*" frëngjisht-folëse.

[63] Shprehja "*right to be let alone*" është përdorur nga Gjyqtari Cooley, shih: Cooley T., "Cooley on Torts 29" (2d ed. 1888), siç thuhet në artikullin e Samuel D. Warren, Louis D. Brandeis. (shih shënimin e ardhshëm).

personal.[64] Warren e përjetoi vetë shkeljen e privatësisë nga përmbledhjet e gazetave të kohës dhe me këtë artikull kërkonte të sensibilizonte shoqërinë për rreziqet që vinin nga zhvillimi i atëhershëm i teknologjisë prej kamerave fotografike. Ai forcoi pikëpamjen e tij në drejtim të mbrojtjes së intimitetit të individit, duke argumentuar se e drejta për intimitet në fund të fundit nuk është e drejta e izolimit nga të tjerët dhe liri absolute veprimesh, por një kusht i domosdoshëm për zhvillimin e sjelljeve dhe bindjeve personale.[65]

Më vonë në harmoni me idetë e tij në vitin 1928 si një gjyqtar i Gjykatës së Lartë Federale në një vendim pikë referimi për jurisprudencën amerikane "Olmstead kundër SHBA" 277 US 438 (1928)[66] (i cili ishte pikë referimi në jurisprudencë lidhur me mbrojtjen e të dhënave personale) mbështeti fuqimisht idetë e propozuara për të drejtën e privatësisë si një vlerë themelore e jetës së Amerikës.[67]

3. Mbrojtja e privatësisë, si një problem moral

Zhvillimi i teknologjisë kompjuterike dhe përpunimit automatik të të dhënave personale shkaktoi në vitet '60 zhvillimin e teorive rreth moralit[68] dhe etikës, të lidhura me trajtimin e informacionit dhe rregullat që do të rregullojnë ato. Donn Parker president i ACM[69] ishte një nga njerëzit e parë i përfshirë në përdorimin e paligjshëm

---

[64] Warren, S. dhe Brandeis, L. (1890). "*The Right to privacy*" fillimisht u botua Harvard Law Review, V. IV, No.5, December. Riprodhuar në http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Shih: gjithashtu Gormley, K. (1992). "*One Hundred Years Of Privacy*", fq.1335, në http://cyber.law.harvard.edu/privacy/Gormley100%20Years%20of%20Privacy.htm. Shih: kritikën për teorinë e izolimit nga Rössler, B. (200). "*Privacies: Philosophical Evaluations*", fq. 17.

[65] Gallagher, S. "*A Man's Home: Rethinking the Origins of the Public/Private Dichotomy in American Law*", në http://www.historyofprivacy.net/

[66] http://caselaw.lp.findlaw.com/scripts/cases/clcc.html?court=us&vol=277&invol=438,shih: gjithashtu dhe çështjen me vendim unifikues për prishjen e privatësisë Katz v UNITED STATES, në http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=389&invol=34, shih nenin 4 të Kushtetutës Amerikane në http://www.lectlaw.com/def/f081.htm

[67] Shih: http://historyofprivacy.net/. Gjithashtu për historinë e mbrojtjes së privatësisë shih: Solove, D. "*A Brief History of Information Privacy Law*" GWU Law School Public Law Research Paper No. 215, në http://ssrn.com/abstract=914271.

[68] Konteksti historik i Etikës në IT (Informatikë) dhe literaturën relevante, shih: Stanford Encyclopedia of Philosophy, http://plato.stanford.edu/entries/ethics-computer/

[69] Shih: Association for Computing Machinery, në faqen e internetit: www.acm.org

dhe imoral të teknologjisë së re nga ekspertët e kompjuterëve. Në studimin më të famshëm të tij "Rules of Ethics in Information Processing" (Rregullat e Etikës në Përpunimin e Informacionit),[70] lidhur me nevojën për një kod sjelljeje të veçantë për specialistët e kompjuterëve, duke futur si frazë problematike, shkeljen e privatësisë si një çështje themelore morale. Ai thoshte: "Kur njerëzit depërtuan në botën e kompjuterëve lanë moralin në derë".[71] Prej atëherë e deri më tani, lidhja e nevojës për mbrojtjen e privatësisë nëpërmjet përdorimit të një etike për metodat e përpunimit të automatizuar të proceseve të të dhënave personale çoi në përdorimin e gjerë të kodeve të etikës në fushën e kompjuterëve dhe internetit, të tilla si "Netiquette",[72] i cili u bë një rregullator serioz i marrëdhënieve në rrjet (online).

4. Privatësia (Jeta private), si një dimension i personalitetit të njeriut

Gjatë të njëjtës periudhë, domethënë një vit më herët, në vitin 1967, në një kohë që zhvillimi i telekomunikacionit dhe kompjuterëve kishte filluar tashmë të ketë ndikime të dukshme në marrëdhëniet sociale-ekonomike, Alan Westin[73] në librin e tij "Privatësia dhe liria" shpjegoi konceptin e "privatësisë" përmes funksionit të saj me katër deklaratat e personalitetit të njeriut: a. pavarësinë personale, b. nevoja për çlirimin emocional të individit, c. situata e procesit të vetëvlerësimit dhe autokritikës, d. komunikimi i sigurt me palët e treta. Cahir[74] raporton veçanërisht se:

---

[70] Parker, D. (1968). "*Rules of Ethics in Information Processing*" Communications of the ACM, fq. 198.

[71] Shih: etikën e sistemeve të informacionit në faqen e internetit të Universitetit të Stannford "*Computer Ethics: Basic Concepts and Historical Overview*", në http://plato. stanford. Edu / entries/ethics-computer/

[72] "Netiquette" përshkruhet si "... një seri rregullash të pashkruara të etikës dhe moralit, shkelja e të cilave çon në dënim kolektiv dhe kritika publike, nëpërmjet pjesëmarrësve të tjerë në rrjet", shih: Strawbridge, M. (2006). "*Netiquette: Internet Etiquette in the Age of the Blog*", fq. 114.

[73] Westin, A. është profesor i të Drejtës Publike në Columbia University, ekspert në fushën e kërkimit të çështjeve të mbrojtjes së të dhënave personale të konsumatorit. Librat më të rëndësishëm të Westin "*Privacy and Freedom*" (1967) dhe "*Databanks in a Free Society*" (1972), janë më të rëndësishmit në fushën e kërkimit për mbrojtjen e privatësisë dhe të dhënave personale.

[74] Cahir, J. (2002). "*Understanding Information Laws: A Sociological Approach*", JILT në http://elj.warwick.ac.uk/jilt/02-3/cahir.html>, Westin, A. (2003). "*Contemporary perspectives on privacy: social and political dimensions of privacy*", Journal of Social Issues, fq. 431.

a) pavarësia personale është një koncept që përmbledh besimin që mbizotëron në shoqëritë demokratike, ku personi është unik dhe kështu kjo "veçanti" duhet të mbrohet nga shkeljet e autonomisë që mund të veprojnë si mjete të manipulimit dhe pengon të veprojë si një mendim autonom dhe i pavarur, veçanërisht i qytetarit të lirë në një shoqëri demokratike.

b) Nevoja për çlirimin emocional të individit. Shumë herë njeriu ndjen nevojën për t'u tërhequr dhe të përballet me mënyrën e vet brenda kornizës së momenteve personale si dhe të ndjenjave të forta të shkaktuara nga marrëdhëniet dhe situatat e tij të përditshme të cilat mund të mishëroheshin vetëm në mjedisin e mbrojtur personal, familjar apo miqësor.

c) Statusi i procesit të vetëvlerësimit dhe autokritikës. Është proces i domosdoshëm në jetën e të gjithëve në mënyrë që personi të nxjerrë mësime nga jeta dhe mund të vazhdojë të shqyrtojë progresin në lidhje me miqtë e tij. Ky proces mund të arrihet vetëm brenda mbrojtjes së sferës private, që individi të mund të përcaktojë informacionin që ka lidhje me të dhe kur ai mund të zbulohet.

d) Nevoja për komunikim të sigurt me të tjerët. E rëndësishme është veçanërisht për zhvillimin e aftësive sociale dhe të personalitetit. Mungesa e fshehtësisë së komunikimit me të tjerët me të cilën ne shprehim mendimet dhe ndjenjat tona, është një nga kërcënimet më të mëdha për zhvillimin e lirë të personalitetit të dikujt.

Nëpërmjet këtyre mendimeve Alan Westin konkludon që të bëhet e mundur mbrojtja e privatësisë duhet që individët si dhe grupet e njerëzve të përcaktojnë se kur dhe në çfarë mase informacioni rreth tyre do t'u jepet palëve të treta. Mund të themi se teoricienët e parë themelues të së drejtës për informacion personal apo informacion vetë përcaktues themeluan një koncept që nxiti zhvillimin e rregullave moderne të mbrojtjes së të dhënave personale dhe që ndikuan drejtpërdrejt në teorinë ligjore Evropiane.[75]

5. Tre aspektet e privatësisë

Përkatësisht e drejta informacionit personal ose e vetë përcaktimit u propozua dhe nga Rosenberg i cili e dalloi si një nga tre aspektet e jetës private të cilat janë:

[75] Kleve, P. dhe Mulder, R. (2008). "*Privacy protection and the right to information, In search of a new balance*", fq. 227.

a) Privatësia territoriale (territorial privacy) e cila përfshin shtëpinë, punën apo çdo vend publik që ndodhet dikush;
b) privatësia e individit (privacy of the person) që përfshin mbrojtjen e privatësisë së individëve nga pushtimet ndaj integritetit fizik dhe mendor;
c) privatësia informuese (informational privacy) që është vetëm mundësia që ka subjekti përpunues i të dhënave për të përcaktuar se kur dhe çfarë informacioni rreth tyre do t'u jepet palëve të treta.[76]

1.2.2 Qasja Kanadeze

Ligji kanadez nuk parashikon mbrojtje të veçantë të së drejtës për privatësi, mbrojtur nga dispozitat e treta që lidhen me barazinë, drejtësinë sociale, eliminimin e diskriminimit me bazë fenë, racën, gjininë, moshën apo orientimin seksual. Në mënyrë të veçantë, ligji për të drejtat e njeriut i cili u miratua nga Parlamenti Kanadez në 1976-1977 nuk përfshin një të drejtë të pavarur për privatësinë. Megjithatë, neni 5 i Kushtetutës së Quebec e njeh këtë të drejtë. Problemi i mungesës së të drejtës së privatësisë doli me miratimin e ligjit për mbrojtjen e të dhënave personale dhe ligjin për aksesin në informacion. Janë të sakta zërat në favor të njohjes të një të drejte të pavarur të privatësisë. Në ligjin kanadez kjo nevojë është e përqendruar në fjalët e profesor Dworkin (1975) i cili ndan të drejtat në abstrakte dhe konkrete. Një e drejtë abstrakte është një objektiv i përgjithshëm politik e cili nuk tregon se sa shumë rëndon në një përplasje me qëllime të tjera politike. Në të kundërt, këto të drejta përcaktohen më saktësisht dhe që në mënyrë të qartë e shprehin peshën e tyre kundër qëllimeve të tjera politike. Të drejtat abstrakte theksojnë argumente për krijimin e të drejtave të veçanta, por një pohim i bazuar në një të drejtë të veçantë është padyshim më i fuqishëm se një kërkesë e bazuar në një të drejtë abstrakte. Në bazë të këtij prezantimi është e lehtë për të kuptuar se në sistemet ligjore të së drejtës së federatës, liria e shprehjes është aq mirë institucionalizuar. Për këtë arsye sugjerohet si një zgjidhje pikëpamja e profesor Freund sipas të cilit e drejta për jetë private duhet të konsiderohet një parim i së drejtës dhe jo thjesht një normë juridike. Sot, jurisprudenca kanadeze ka formuar një pikëpamje të

[76] Rosenberg, R. (1992). "*The Social Impact of Computers*", Academic Press, New York, NY, siç referohet dhe Gritzalis, S. (2004). "*Enhancing Web privacy and anonymity in the digital era*", *Information Management & Computer Security*", fq. 255.

qëndrueshme për mbrojtjen e privatësisë. Karakteristik është fjalimi i gjyqtarit Cory në çështjen Hill të vitit 1995 i cili analizoi lidhjen midis privatësisë dhe reputacionit të individit. Ne, absolutisht pajtohemi me pikëpamjen se një shoqëri demokratike ka interes të ruajë atë që anëtarët e saj mund të fitojnë një reputacion të mirë të cilin mund ta mbrojnë në rast sulmi.[77]

1.2.3 Qasja Evropiane

Evropa në dallim nga SHBA, të cilat së bashku trajtuan mbrojtjen e privatësisë nëpërmjet konceptit të "lirisë personale", ndoqi një qasje të ndryshme teorike. Në Francë theksi ishte në mbrojtjen e privatësisë nëpërmjet konceptit të "dinjitetit të individit" dhe referuar Deklaratës së të Drejtave të Njeriut, 1789,[78] ku sipas nenit 2 të Deklaratës "Qëllimi i çdo shoqate politike është ruajtja e të drejtave natyrore dhe të patjetërsueshme të njeriut. Këto të drejta janë liria, prona, siguria dhe rezistenca ndaj dhunës". E mbrojtur në këtë mënyrë duke përfshirë të drejtën për liri, e cila sipas Gjykatës Kushtetuese franceze përbën dhe respektin për privatësinë,[79] ndërsa në Gjermani privatësia trajtohet në kuadër të mbrojtjes së "personalitetit".[80]

1.2.3.1 Shteti kujdestari i privatësisë

Periudha e gjatë e regjimeve autoritare të përjetuara nga Evropa në të cilat përpunimi i të dhënave personale të përdorura për shfarosjen e kundërshtarëve ideologjik dhe politik dhe krijimi i një gjendje frike që kishte kontroll të plotë mbi jetën e qytetarëve të saj, krijoi nevojën për rregullimin absolut dhe të rreptë të privatësisë nga

---

[77] Moore, A. D. (2011). "*Privacy Rights: Moral and Legal Foundations*", fq.13.

[78] Shih: tekstin e Deklaratës në http://www.assemblee-nationale.fr/histoire/dudh/1789.asp

[79] Vendim i Conseil constitutionnel nën/numër 2009-580 DC 10.06.2009 në lidhje me përpunimin e të dhënave personale të kryera nga organizatat e të drejtave të autorit. Koment në gazetën 2009 fq.3778. Shih: faqen e internetit të Conseil Constitutionnel , ku në paragrafin 22 të Vendimit referohet : *"Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression"; que la liberté proclamée par cet article implique le respect de la vie privée"*, në http://www.conseil-constitutionnel.fr/decision//2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html

[80] Shih: një studim të detajuar të qasjeve të ndryshme nga Whitman, J.

qeveritë kombëtare.[81] Karakteristikë e ndjeshmërisë së qytetarëve evropianë për privatësinë është një nga veprat më të rëndësishme letrare të shekullit të 20-të, libri i George Orwell, "Nineteen Eighty-Four", i cili është gjithmonë pikë referimi për diskutimet në lidhje me rolin e bazave të të dhënave dhe shtetit në shkeljen e privatësisë së qytetarëve.[82] Nën këtë prizëm nuk është e vështirë për të kuptuar theksin që i jepet në Bashkimin Evropian rregullimit të mbrojtjes së të dhënave personale përmes harmonizimit të ligjeve kombëtare dhe kontekstit të prodhimit të legjislacionit në sektorin publik dhe privat, ku në SHBA promovohet vetë-rregullimi dhe prodhimi sektorial i legjislacionit.[83]

Si shkelja e lirive personale dhe privatësisë, ashtu dhe dëmtimi i reputacionit dhe personalitetit të njeriut në Evropë, erdhi nga shteti i cili krijoi kushtet dhe detyrimin moral të qeverive evropiane të pasluftës për të siguruar pikërisht këto liri me garantimin e një shteti modern dhe demokratik. Një shtet duhet të qeveriset nga transparenca e funksionimit dhe respektimit të lirive civile nëpërmjet kuadrit të plotë ligjor që siguron të drejtën e ankimit në gjykatë.[84]

Krijimi i organeve të pavarura dhe të forta mbikëqyrëse kombëtare shpreh pikërisht atë logjikë që shpjegon nevojën për ndërhyrjen e një organi mbi kombëtar si Bashkimi Evropian. Të gjitha vendet e Evropës Perëndimore, kur filluan të bëhen të dukshme rreziqet e shfaqjes së kompjuterëve dhe përpunimit të mëvonshëm të automatizuar të të dhënave personale, ndërmorën iniciativa legjislative për të siguruar një trajtim të drejtë. Respektimi dhe mbrojtja e privatësisë u raportuan për herë të parë në nivel evropian me "Konventën e Romës për Mbrojtjen e të Drejtave të Njeriut dhe

---

[81] Cate, F. (1998). "*Privacy and Telecommunications*", Wake Forest Law Review, fq.15.

[82] Orwell, G. (2003). "*Ninteen Eighty-Four*", Penguin Books", London.

[83] Salbu, S. "*The European Data Privacy Directive and International Relations*", në http://www.wdi.umich.edu/files/Publications/WorkingPapers/wp418.pdf. Shih në lidhje me çështjen e mbledhjes dhe përpunimit të të dhënave personale në të drejtën amerikane (SHBA) Youst-Koh "*Management and discovery of Electronically Stored Information, Computer Law Review and Technology Journal*" - Summer 1997, siç thuhet në Spindler, G. dhe Börner F. (2005). "*E-Commerce Law in Europe and the USA*", fq. 128.

[84] Shih: prezantimin për klimën e terrorizmit dhe shkeljen e të drejtave të njeriut në Europë midis dy luftërave dhe pushtimin nazist të mëvonshëm në Mazower, M. (2009). "*Dark Continent: Europe's Twentieth Century*", fq. 89.

Lirive Themelore",[85] njohur dhe si "Konventa Evropiane për të Drejtat e Njeriut" (KEDNj), e cila thekson në nenin 8 paragrafi 1, se: Çdo person ka të drejtën për respektimin e jetës private dhe familjare, vendbanimit dhe korrespondencës së tij. Në tekstin e Kartës së të Drejtave Themelore të Bashkimit Evropian duke filluar me preambulën e saj ku dhe neni i parë i referohet dinjitetit të individit,[86] ndërsa në nenin 7 mbrohet e drejta e jetës private dhe familjare, në marrëveshje me dispozitën përkatëse të KEDNj-së.[87]

Sipas jurisprudencës së Gjykatës Evropiane të të Drejtave të Njeriut si dhe jurisprudencës së Gjykatës Evropiane të Drejtësisë, koncepti i privatësisë interpretohet lato sensu, duke përfshirë jo vetëm shtëpinë dhe familjen por dhe vendin e punës dhe atë të komunikimit profesional.

GJEDNj me çështjen *Niemietz kundër Gjermanisë* zgjeroi konceptin e "jetës private dhe reagimit" në çdo aspekt të marrëdhënieve industriale dhe të gjitha llojeve profesionale ose komunikimi tjetër. GJEDNj konsideroi se që t'i mohohet dikujt e drejta për mbrojtjen e privatësisë dhe banimit vetëm sepse bëhet fjalë për vendin e punës dhe komunikimin profesional, do të përbënte trajtim të padrejtë për çdo person të cilit nuk mund t'i dallohen aktivitetet profesionale ose jo profesionale.[88]

Përkatësisht, në çështjen *Amann kundër Zvicrës*, GJEDNj argumentoi përsëri mbi arsyetimin për një interpretim të gjerë të "jetës private" e cila përfshin të drejtën e individëve për të krijuar, për të zhvilluar marrëdhënie me individë të tjerë si dhe për natyrën profesionale.[89] Gjithashtu në një gjykim më të fundit në çështjen KU kundër

---

[85] U nënshkrua më 4 nëntor 1950 dhe hyri në fuqi më 3 shtator, 1953, shih: tekstin në http://www.echr.coe.int/NR/rdonlyres/E4317264-DB27-42F873E1ECCACABB045/0/English.pdf, gjithashtu shih: për nenin 8 në Kindt, E. J. (2013). "*Privacy and Data Protection Issues of Biometric Applications: A Comparative legal Analysis*", Law, Governance and Technology Series 12, fq.7.

[86] "*Dinjiteti i njeriut është i pacenueshëm. Ai duhet të respektohet dhe të mbrohet*" në http://www.europarl.europa.eu/charter/pdf/text_eng.pdf

[87] 'Neni 7 "*Respekti për jetën private dhe familjare - Gjithkush ka të drejtën për respektimin e jetës private dhe familjare, të shtëpisë dhe komunikimeve të tij*", në http://www. europarl.europa .eu/ charter /pdf /text _eng.pdf

[88] *Niemietz v. Germany*,16 E.H.R.R. 97 (ECHR 1991) pjesa 29-33, në http://hudoc.echr. coe .int /sites /eng/pages/search.aspx?i=001-57887#{%22itemid%22:[%22001-57887%22]}

[89] *Amann v. Switzerland* [GC], no. 27798/95, §§ 65-67, (ECHR 2000 II); në http://hudoc.ech.coe.int

Finlandës mbi mbrojtjen e privatësisë në hapësirën kibernetike, GJEDNj përcaktoi konceptin e privatësisë si një koncept që mbulon identitetin fizik dhe moral të njeriut.[90] Për më tepër, sipas jurisprudencës së Gjykatës Evropiane të të Drejtave të Njeriut, përcaktohet se komunikimet elektronike varen nga koncepti i intimitetit në nenin 8, paragrafi 1 i KEDNj dhe për këtë arsye u dha mbrojtje e ngjashme lidhur me disa çështje (*Klass kundër Gjermanisë*,[91] *Niemitz kundër Gjermanisë*,[92] *Copland kundër Mbretërisë së Bashkuar*,[93] *Halford kundër Mbretërisë së Bashkuar*,[94] *Malone kundër Mbretërisë së Bashkuar*,[95] *Amann kundër Zvicrës*[96]).

/sites/eng/pages/search.aspx#{%22dmdocnumber%22:[%22696374%22], %22itemid%22:[%22001-58497%22]}

[90] *K.U v. Finland*, judgment of 12 December 2008 në http://hudoc.echr.coe .int/sites/eng /pages /search. aspx#{%22dmdocnumber%22:[%22843777%22],%22itemid%22:[%22001-89964%22]}

[91] *Klass and Others v. Germany*, judgment of 6 September 1978, Series A no. 28, p. 21, § 41; në http: //hudocechr.coe.int/sites/eng/pages/search.aspx#{%22dmdocnumber%22:[%22695387%22],%22item id%22:[%22001-57510%22]}

[92] *Niemitz v.Germany*,16E.H.R.R.97(ECHR1991). GJEND në këtë rast zgjeroi konceptin e "jetës private dhe reagimit" në çdo aspekt të marrëdhënieve të punës dhe çdo lloj profesioni ose komunikimi tjetër. Shih: Markesinis, B. S. dhe Unberath H. (2002). "*The German Law of Torts: A Comparative Treatise*", fq. 79.

[93] *Copland v.United Kingdom 2007]ECHR 62617/00 (3 April 2007)*, në http:// hudoc. echr. coe.int /sites /eng/pages/search.aspx#{%22dmdocnumber%22:[%22793888%22],%22itemid%22:[%2200173049%22] }GjEDNj-ja vendosi se komunikimet elektronike të personave (ndër të cilat në mënyrë eksplicite interneti dhe e-mail) sipas konceptit të privatësisë gëzojnë mbrojtjen e nenit 8 të KEDNJ, pavarësisht nëse ndodhin në një hapësirë profesionale ose jo (Rasti *Niemitz v. Gjermnisë, Ialford v. Mbretërisë së Bashkuar dhe Amann v. Zvicrës*).

[94] *Halford v. United Kingdom Government European Court Of Human Rights (N° 20605/92), ECHR 32, June 25, 1997*, në http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58039#{%22itemid%22: [%22001-58039%22]}. GJEDNJ përcaktoi atë se telefoni i punës hyn brenda nocionit të privatësisë.

[95] *Malone v. the United Kingdom*, judgment of 2 August 1984, Series A no. 82, pp. 30-31, § 64; http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57533#{%22itemid%22:[%22001-57533% 22]}, Gjykata Evropiane e të Drejtave të Njeriut me këtë vendim piketë në Ligjin për Mbrojtjen e të Dhënave Personale vuri re se gjatë monitorimit (vëzhgimit) të kërkuesit (paditësit) është shkelur Neni 8 i Konventës Evropiane për të Drejtat e Njeriut sepse arkivat e regjistrimit përmbanin informata, numrat e telefonatave, të cilët janë sipas Gjykatës "pjesë integrale e telekomunikacionit kryer nëpërmjet telefonit".

[96] *Amann v. Switzerland* [GC], no. 27798/95, §§ 65-67, ECHR 2000 II; në http://hudoc.echr.coe.int/ sites/eng/pages/search.aspx#{%22dmdocnumber%22:[%22696374%22],%22itemid%22:[%2200158497

Nga ana tjetër dhe Gjykata Evropiane e Drejtësisë, në Rastin Österreichischer Rundfunk kundër Austrisë,[97] për t'iu përgjigjur pyetjeve të gjykatave austriake se nëse ligji kombëtar përputhet me Direktivën 95/46/KE, u përgjigj mes çështjeve të tjera shqetësuese për aplikimin ose jo të Direktivës 95/46/KE, ku pjesë të jetës profesionale mund të konsiderohen si elementë të lidhur me intimitetin individual dhe si të tilla janë të mbrojtura nga dispozitat e Direktivës Evropiane i cili nga ana e saj i referohet Nenit 8 të Konventës Evropiane për të Drejtat e Njeriut.

Në çdo rast, koncepti i privatësisë dhe kufijve të mbrojtjes ndryshon nga koha në kohë dhe nga shoqëria në shoqëri.[98] Ai që në një shoqëri është një element i mbrojtur i privatësisë, në një tjetër mund të jetë një faktor në socializimin e individit dhe publikimin si parakusht për pjesëmarrjen e tij në jetën publike. Por një gjë është fakt, se të paktën tradita morale dhe ligjore perëndimore është themeluar si përmes perspektivës së lashtë dhe filozofisë mbi vlerat e njeriut në lidhje me krijimin dhe zhvillimin e strukturave shtetërore. Mbrojtja e sferës private si një kusht për zhvillimin e lirë të personalitetit të tij do të jetë udhërrëfyes në të ardhmen për çdo referim në këtë temë.

1.3 Të Dhënat Personale

Për herë të parë legjislacioni për mbrojtjen e të dhënave personale ishte subjekt legjislativ në Konventën e Strasburgut të datës 28.01.1981 "Për mbrojtjen e individëve në lidhje me Përpunimin Automatik të të Dhënave Personale"[99] dhe është instrumenti i parë ligjor detyrues ndërkombëtar për mbrojtjen e të dhënave personale.
Në nenin e parë përcaktohet qëllimi i kësaj Konvente që është të sigurojë në territorin e secilit vend dhe për çdo individ, pavarësisht nga kombësia apo vendbanimi, respektimin e të drejtave dhe lirive themelore të njeriut dhe në veçanti të drejtën e privatësisë.[100]

%22]}

[97] GJED 20.5.2004, C-465/00,C-138/01, Osterreichischer Rundfunk (ORF), Përmbledh..2003.I-4989, paragrafët 21, 68 dhe 77, në http://eur-lex.europa.eu/legal-content /EN/TXT/ PDF/?uri =CELEX :620 12C J0342&from=EN

[98] Po aty. Whitman, J., fq. 2.

[99] http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

[100] Po aty. Teksti në faqen e internetit të Këshillit të Evropës, në http://conventions. coe.int/Treaty/ EN/Treati es/Html/108.htm

Gjithashtu në vitin 1983 Gjykata Kushtetuese Federale gjermane u pyet për të vendosur për anti kushtetutshmërinë e ligjit federal mbi regjistrimin e popullsisë dhe profesioneve në Gjermani në vitin 1982 sipas të cilit do të bëhej regjistrimi i detajuar i të dhënave të tilla emër/mbiemër, adresa e saktë, numri i telefonit, gjinia, data e lindjes, statusi martesor, bindjet fetare, lloji i punës, niveli i arsimimit, etj. Gjykata Federale vendosi se ligji kishte gabime dhe mangësi në procedurën e identifikimit në lidhje me informacionin publik. Ai minon dinjitetin dhe zhvillimin e personalitetit dhe në fund të fundit rrezikon vetë demokracinë e cila nuk mund të funksionojë nëse ekziston mungesa e mbrojtjes së privatësisë.[101] Gjykata federale argumentoi se është e pamundur të ekzistojë një shoqëri demokratike, nëse qytetari nuk e di se kush, në çfarë kohe dhe për çfarë objektivi mblidhen të dhënat e tij personale.[102]

Kështu vendosi se është e drejta e individit për të njohur, për të vendosur, për të identifikuar kur dhe në çfarë kushtesh është i mundur përpunimi e informacionit që lidhet me të. Pikërisht kjo e drejtë e "vetë përcaktimit informativ" ose "informacionit vetjak",[103] siç është e njohur zakonisht në literaturën ligjore, konsiderohet e nevojshme në mënyrë që t'i mundësojë individëve për të ndërhyrë në rrjedhën dhe përpunimin e informacionit që i përkasin , i cili shpërndahet në sferën publike.[104] Përdorimi i konceptit të të dhënave personale në jurisprudencën dhe legjislacionin evropian është i një rëndësie të veçantë si ai arrin autonominë rregullatore të së drejtës për mbrojtjen e të dhënave personale të cilat janë veçanërisht në rrezik për shkak të përparimeve teknologjike që kanë bërë të mundur përhapjen, përdorimin, shkëmbimin, dhe

[101] Poullet, Y. (2009). "*Data protection legislation*: *What is at stake for our society and democracy*?" Computer Law & Security Review, fq. 211.

[102] Conn, K. (2002). "T*he Internet and the Law: What Educators Need to Know?*", fq.16.

[103] Vendimi i 15.12.1983 BVerfGE 65,1/143, siç përshkruan Gutwirth, S. (2011). "*Computers, Privacy and Data Protection: an Element of Choice*", fq.11, Shih: gjithashtu Gutwirth, S., Poullet, Y. dhe de Hert P. (2010). "*Data Protection in a Profiled World*", fq.25. Gjithashtu prezantimi i vendimit Hornung G, Schnabel Ch. "*Data protection in Germany I: The population census decision and the right to informationalself-determination*"CLSR,200984, në http://www.datenschutz.rlp.de/downloads/bve rfg _65 _1 _ -_ vo lks za ehlung .pdf.

[104] Wright, D. dhe de Hert, P. (2011). "*Privacy Impact Assessment*", fq.512., siç përshkruhet në Mendel, T, Puddephatt, A. dhe Wagner, B. (2012). "*Global Survey on Internet Privacy and Freedom of Expression*", fq.106.

korrelacionin e të dhënave të mbledhura dhe të përpunuara.[105] Pra, të dhënat personale[106] duhet gjithmonë të konsiderohen në kontekstin e përpunimit të automatizuar dhe mbrojtja e tyre është vetëm një mjet për të arritur mbrojtjen e privatësisë. Në zonën evropiane kuptimi i të dhënave personale u përdor veçanërisht në nenin 286 të "Traktatit të Komunitetit Evropian" (TEC), "Marrëveshjen Shengen" në "Kartën e të Drejtave Themelore të Bashkimit Evropian", në Direktivën 95/46/KE, në "Rekomandimin Nr. R (99) 5 të Komitetit të Ministrave të Shteteve Anëtare për mbrojtjen e privatësisë në internet", në Direktivën 2002/58/KE dhe Direktivën 2006/24/KE. Në Shqipëri legjislacioni kombëtar transferoi Direktivën 95/46/KE në Ligjin nr. 9887, datë 10.03.2008 "Për Mbrojtjen e të Dhënave Personale" ndryshuar me Ligjin nr. 120/2014 "Për disa ndryshime dhe shtesa në ligjin nr. 9887". Në mënyrë të veçantë, Ligji nr. 9887[107] përcakton se "të dhëna të karakterit personal do të thotë çdo informacion në lidhje me një person fizik, të identifikuar ose të identifikueshëm, direkt ose indirekt, në veçanti duke iu referuar një numri identifikimi ose një a më shumë faktorëve të veçantë për identitetin e tij fizik, fiziologjik, mendor, ekonomik, kulturor apo social. Nuk llogariten si të dhëna personale të dhënat e grumbulluara, të cilat nuk mund të identifikojnë subjektet e të dhënave". Respektivisht Direktiva 95/46/KE jep përkufizimin e të dhënave të karakterit personal duke deklaruar se ai është " ... çdo informacion në lidhje me një individ, identiteti i të cilit është i njohur apo mund të konstatohet ose të përcaktohet drejtpërdrejtë ose tërthorazi me një numër të caktuar identifikues ose me një ose më shumë faktorë të veçantë të tij fizik, fiziologjik, mendor, ekonomik, identitet kulturor ose social"[108] që të pasqyrojë qëllimin e ligjvënësit Evropian për të dhënë një kuptim të gjerë të termit të "të dhënave të karakterit

[105] Morgan, R. dhe Boardman, R. (2012). "*Data Protection Strategy: Implementing Data Protection Compliance*", fq.149.

[106] Termi të dhëna personale është bërë më i përhapur se termi "të dhëna të karakterit personal" që është gjetur në shumë pjesë të legjislacionit, të tilla si Direktivën 95/46/KE, Ligjin 9887/2008 dhe Konventa 108.

[107] Ligji nr. 9887, datë 10.03.2008, "*Për Mbrojtjen e të Dhënave Personale*" i ndryshuar me Ligjin nr. 120/2014 "*Për disa ndryshime dhe shtesa në ligjin nr. 9887*".

[108] Neni 2, pika b), Direktiva 95/46/KE e Parlamentit Evropian dhe e Këshillit të datës 24.10. 1995 "*Për mbrojtjen e individëve në lidhje me përpunimin e të dhënave personale dhe mbi lëvizjen e lirë të këtyre të dhënave*", OJ L 281, 23.11 0.1995, fq.31.

personal", i cili është mbajtur në të gjithë procesin legjislativ.[109] Të dhëna personale janë konsideruar gjithashtu dhe gjykimet me karakter vlerësues në masën që marrëdhëniet ndaj personave apo pronës të projektohen në një deklaratë informative për personin të cilit i përket informacioni. Një gjykim me vlera të tilla si p.sh "Klienti i Mirë" edhe nëse nuk përmban të dhëna mbi të cilat mbështetet "vlerësimi", tregon diçka në lidhje me marrëdhëniet e personit për të cilin flitet. Në vitin 2003 u lëshua vendimi i parë i Gjykatës Evropiane të Drejtësisë (GJED) mbi Direktivën 95/46/KE duke interpretuar konceptin e të dhënave personale. Bëhet fjalë për çështjen Lindqvist[110] që përbën tashmë çështjen rrethanore më të vendosur në literaturën ligjore, lidhur me Direktivën 95/46/KE. Kjo ishte hera e parë që GJED përcaktoi fushëveprimin e Direktivës për mbrojtjen e të dhënave, të karakterit personal dhe qarkullimin e lirë të tyre në internet që ka të bëjë me përdorimin nga Lindqvist, në faqen e internetit të kishës protestante Suedeze për publikimin e të dhënave personale të anëtarëve të kishës pa pëlqimin e tyre. Gjatë pyetjeve paraprake të gjykatës suedeze në të cilën B. Lindqvist kishte apeluar kundër vendimit të shkallës së parë, e cila e dënoi atë me një gjobë prej 4000 korona suedeze (rreth 450 euro), GJED vendosi se të dhëna të tilla si emri, telefoni, adresa, anëtarësimi, shëndeti dhe statusi[111] përbëjnë të dhëna personale dhe për publikimin e tyre në faqen e internetit të Kishës protestante suedeze thjesht nevojitej pëlqimi i individëve në fjalë.[112]

Kjo shumëllojshmëri e aspekteve shpjegon se pse në fund të fundit mbrojtja e të dhënave personale është reduktuar në një të drejtë themelore, e cila është projektuar për

---

[109] Opinion 4/2007 "*Për Kuptimin e të Dhënave Personale*" - Neni 29 Ekipi i Punës në Mbrojtjen e të Dhënave Personale", në faqen: http://ec. europa. eu/justice/ policies/ privacy /docs/ wpdocs / 2007 / wp 13 6_en.pdf

[110] GJED 6.11.2003, C-101/01, Linqvist, Përmbledh. 2003.I-12971, në http://eur- lex.europa.eu/ Lex UriServ/LexUriServ.do?uri=CELEX:62001J0101:EL:HTML dhe vendimi i dt. 06.11.2003.

[111] Ai tha se një koleg kishte lënduar këmbën e tij dhe ishte me pushim të pjesshëm (raport mjekësor) për shkak se ishte i sëmurë.

[112] Shih: komentet mbi çështjen Garcia, F. (2005). "*Bodil Lindqvist*: *A Swedish Churchgoer's, Violation of the European Union's Data,Protection Directive Should Be a Warning to U.S. Legislators*", Fordham Intellectual Property, Media & Entertainment Law Journal, fq. 1204, në http://law. fordham.edu/publications/articles/200flspub6132. pdf. (BodilLindqvist,C-101/01).

të siguruar mbrojtje në një shoqëri ku përpunimi i të dhënave personale është i një rëndësie në rritje në fusha të ndryshme, qofshin ato të natyrës personale apo publike.[113]

Në kuadër të analizës së konceptit të të dhënave personale është e nevojshme për të bërë dallimin mes: të thjeshta dhe të ndjeshme për shkak se ai është një dallim i sanksionuar me ligj që synon mbrojtjen e rreptë e të dhënave të ndjeshme personale.

1.3.1 Dallimi në mes të dhënave të thjeshta dhe të ndjeshme personale

Termi "të dhëna të ndjeshme personale" na shqetëson si kategori e veçantë e të dhënave personale. Ligji nr.9887, datë 10.03.2008 ndryshuar me ligjin nr. 120/2014 "Për disa ndryshime dhe shtesa në ligjin nr. 9887"[114] përcakton si informacione të ndjeshme personale të dhënat në lidhje me:

1. origjinën racore ose etnike,[115]
2. mendimet politike,[116]
3. besimin fetar apo filozofik,
4. anëtarësimin në organizatat sindikale,[117]
5. dënimin penal,[118]
6. shëndetin,[119]
7. jetën seksuale.[120]

E njëjtë është dhe dispozita përkatëse e Direktivës së transpozuar i cili thotë se "... të dhënat që lidhen me origjinën racore ose etnike, mendimet politike, fetare ose filozofike, anëtarësitë në organizatat sindikale, shëndetin, mirëqenien sociale dhe jetën

[113] Po aty. Shih konceptin e të dhënave personale Akrivopoulou, Ch. dhe Psygkas, A. (2010)., fq. 9, si dhe në Gutwirth, S., Leenes, R. dhe de Hert, P. (2013). "*Reloading Data Protection: Multidisciplinary Insights and Contemporary*", fq.12.

[114] Ligji nr. 9887, datë 10.03.2008 "*Për Mbrojtjen e të Dhënave Personale*" ndryshuar me Ligjin nr. 120/2014 "*Për disa ndryshime dhe shtesa në ligjin nr. 9887*".

[115] I referohet përkatësisë etnike sesa kombësisë e cila nuk është e dhënë personale.

[116] Kur këto zbulohen drejtpërdrejt ose tërthorazi, por në mënyrë të sigurtë.

[117] Pjesëmarrja në sindikatat e punëtorëve.

[118] Vendimi i formës së prerë nga një Gjykatë Penale.

[119] Informacioni në lidhje me gjendjen fizike, mendore apo shpirtërore dhe të përdorimit të ilaçeve, me barkode, etj.

[120] Në shumë raste kjo është e mundur për të përcaktuar preferencën seksuale duke parë faqet e lidhura online apo pjesëmarrja në organizatat e homoseksualëve.

seksuale, në akuzat penale apo dënimet, si dhe pjesëmarrja në shoqatat e mësipërme të individëve”.[121]

Në këtë pikë vlen të përmendet se me këtë dispozitë, si legjislacioni evropian dhe ai kombëtar kufizuan rrethin e të dhënave sensitive dhe të informacionit, ku përfshin një vlerë shtesë dhe të veçantë në mbrojtjen e privatësisë që karakterizojnë statusin e veçantë të individit dhe formojnë thelbin e privatësisë. Nga dispozitat ligjore, vijon se ndryshe nga pjesëmarrja në ndonjë grupim, shoqatë apo organizatë tjetër, të tilla si pjesëmarrja në klube shkencore ose sportive, nuk përbën të dhëna personale të ndjeshme për shkak se ajo u gjykua se publikimi i tyre nuk përbën rrezik të veçantë për të drejtat individuale.

[121] Neni 8 i Direktivës 95/46/KE.

KAPITULLI II: RREZIQET NDAJ TË DHËNAVE PERSONALE NË KOMUNIKIMET ELEKTRONIKE

2.1 Hyrje

Siç pamë më lart, Shoqëria e Informacionit bazohet në teknologjitë e reja të avancuara digjitale dhe rrjetet publike të komunikimit, të cilat transformojnë vazhdimisht të dhënat, duke krijuar sfida të reja për mbrojtjen e privatësisë dhe të dhënave personale të përdoruesit.[122] Në veçanti, zhvillimi i Internetit i cili është një vend ku në momentin e parë të krijimit të tij u konsiderua si një vend i mahnitshëm i lirisë të ideve dhe informacionit, një vend ku specifika e karakteristikave të tij teknike, të tilla si natyra globale dhe decentralizimi, do t'i japi një shtysë zhvillimit të shoqërisë së informacionit. Në vazhdim u pranua se gjërat ishin shumë më të komplikuara dhe se interneti ishte një vend ku zhvillohen aktivitete të tilla si përhapja e informacioneve të rreme dhe shpifëse, mbështetja e terrorizmit, vjedhjet e pronësisë intelektuale dhe përpunimit të paligjshëm të të dhënave personale nga organet qeveritare apo joqeveritare që kanë përdorur gjithmonë teknologjitë moderne të komunikimit për aktivitetet e mbikëqyrjes së ligjshme apo të paligjshme të aktiviteteve dhe komunikimit të individëve. Por në vitet e fundit pas sulmeve terroriste në Nju Jork dhe Londër u rritën rrezikshëm dhe në mënyrë shqetësuese përpjekjet për të monitoruar (përgjuar) teknologjikisht komunikimet e bëra nga bisedat telefonike dhe elektronike (email). Një shembull përbën sistemi satelitor i vëzhgimit "Echelon",[123] i cili është gjithëpërfshirës në botën e telekomunikacioneve. Ai mund të dallojë dhe të identifikojë të dyshuarit për veprimet kriminale dhe terroriste duke përdorur NSA (National Security Agency) dhe GCHQ (Government Communications Head Quarters)[124] duke lejuar bashkëpunëtorët e largët të shërbimeve të inteligjencës për të komunikuar me kompjuterët në çdo vend qëndrimi dhe të marrin automatikisht rezultatet e kërkuara.[125] Pastaj "Carnivore" i cili

[122] Portela, I. M. (2010). "*Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues*", fq 189.

[123] Informacion më të zgjeruar në lidhje me sistemin e vëzhgimit "Echelon", shih: në http://en.wikipedia.org/wiki/ECHELON

[124] Agjencia Kombëtare e Sigurisë e SHBA-së dhe agjensia korresponduese në Britaninë e Madhe.

[125] Shih: liritë dhe të drejtat në fushën e Drejtësi dhe Punëve të Brendshme të Parlamentit Evropian, në http ://w w w . europarl.eu.int/committees/en/default.htm dhe Rezoluta e Parlamentit Evropian mbi ekzistencën e

sipas informatave të lëshuara nga EPIC,[126] është një program (software) me të cilin FBI-ja vëzhgon trafikun në ambientet e ISP-ve për të kontrolluar informatat që gjenden në e-mail-et e të dyshuarve për veprime kriminale.[127] EPIC raporton se në të ashtuquajturën "Carnivore"[128] mund të spastrojë miliona mesazhe elektronike (e -mail) në sekondë dhe është i aftë për të lejuar autoritetet e zbatimit të ligjit që të monitorojnë të gjitha komunikimet digjitale të një ofruesi të shërbimit të internetit, mjafton që përdoruesi të përdorë një nga fjalët kyç të cilat sistemi automatikisht i njeh dhe implikon të dyshuarin edhe në qoftë se përdorimi i fjalës është krejtësisht i rastësishëm.[129] Problemet që zhvillohen për madhësinë dhe pasojat e rrezikut të të drejtave të njeriut brenda mjedisit të zhvillimit spektakolar, së ashtuquajturës "Teknologjia e Informacionit dhe Komunikimit" (Information and Communication Technologies, ICTs), si dhe përpjekjet për të menaxhuar ato në nivel rregullues, janë kuptuar lehtësisht nga prezantimi dhe analiza e këtyre teknologjive të reja.

Teknologjitë tradicionale të telekomunikacionit d.m.th. komunikimet telefonike janë ndërthurur me monitorimin politik dhe shkeljet e privatësisë Si telekomunikacion nënkuptohet bartja e sinjaleve ndërmjet pikave fundore me përdorimin e kabullit, radiovalëve, ose mjeteve të tjera elektromagnetike dhe optike.[130] Në hapësirën e telekomunikacionit tradicional, rreziqet që lindin nga zhvillimet e teknologjisë edhe pse

---

një sistemi global, përgjimin e komunikimeve private dhe komerciale (Sistemi i vëzhgimit Echelon), në http://www.europarl.europa.eu/

[126] Shih: Electronic Privacy Information Center (EPIC) është një qendër kërkimore me seli në Uashington me qëllim ndërgjegjësimin e publikut për çështjet e lirive civile dhe vlerat kushtetuese për mbrojtjen e privatësisë, në http://epic.org/epic/about.html

[127] Dunham, G. (2002). "*Carnivore, surveillance system of E-mail by the FBI: Neutralizing of Offenders, no to privacy*", Federal legal papers communications [Vol. 54], në http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1311&context=fclj

[128] http://epic.org/privacy/carnivore/ 8_02_release.html

[129] Edhe pse FBI thirri jurisprudencën e Gjykatës së Lartë Federale të justifikojë veprimin e saj, kritikat nga organizatat e të drejtave të njeriut kanë qenë të vazhdueshme dhe këmbëngulëse. Kanali Fox News zbuloi se më 18.01.2005 FBI zëvendësoi "Carnivore" me një teknologji të re për përdorim komercial pa specifikuar nëse ajo është në përputhje me jurisprudencën dhe legjislacionin e mbrojtjes së të dhënave personale.

[130] Neni 2, paragrafi c i Direktivës 97/66/KE i Parlamentit Evropian dhe Këshillit të datës 15 dhjetor 1997 në lidhje me përpunimin e të dhënave personale dhe privatësisë në telekomunikacion.

në fakt është një version i ri i metodave tradicionale të monitorimit dhe përgjimeve telefonike të cilat ndikojnë shumë më tepër në nivelet e sigurisë dhe konfidencialitetin e telekomunikacionit si dhe regjistrimin e bisedave personale. "Zënia në kurth" e bisedave telefonike nga agjencitë qeveritare apo subjektet private, edhe nëse bëhet për qëllime ligjore dhe legjitime, ose thjesht për të regjistruar apo sistematizuar bindjet politike, fetare dhe zakonet e konsumit madje edhe për çdo lloj realizimi të interesave private është bërë një praktikë e zakonshme dhe e rrezikshme.[131] Rrjetet moderne digjitale të komunikimit mundësojnë mbledhjen e komunikimeve të të dhënave në telefoninë fikse (p.sh., numrat e telefonit të përdoruesve, kohën e saktë të thirrjes dhe kohëzgjatjen e saj).[132] Respektivisht dhe në telefoninë e lëvizshme (mobile) për shkak se për të funksionuar sistemi i komunikimit duhet të bëhet identifikimi i aparatit nga stacioni bazë, kështu që shënohet vendndodhja e saktë e përdoruesit.[133] Në këtë mënyrë, telefoni celular është në thelb një pajisje personale komunikimi që identifikohet me një përdorues të veçantë[134] në krahasim me telefoninë fikse në të cilën numri i referohet një parapaguesi (abonenti), ku përdoruesit janë zakonisht më shumë se një. Pra, përdorimi i telefonit celular dhe regjistrimi i të dhënave të lëvizjes dhe vendndodhjes kanë pasoja të drejtpërdrejtë në identifikimin dhe personalizimin e abonentit përdorues, i cili ka në thelb një "spiun në xhepin e tij".[135]

---

[131] Shih: Choo, A. L. T. (2008). "*Abuse of Process and Judicial Stays of Criminal Proceedings*", fq. 42.

[132] Zureik, E. dhe Salter, M. (2013). "*Global Surveillance Policing*", fq. 93, gjithashtu shih dhe në Digital Footprints an Internet Society Reference Framework (2014). fq.5, në http:/ /www. Internetsociety .org/ doc/digital-footprints-internet-society-reference-framework

[133] Froomkin, M. (2000). "*The Death of Privacy*", Stanford Law Review, fq. 1479, dhe shih: artikullin nga Chen, B. "*Why and How Apple is Collecting your Iphone Location Data*", Revista Wired (Wired Magazine) rreth zbulimeve të fundit nga iPhone i kompanisë Apple, i cili përfshin në sistemin funksional iOS 4, një skedar i quajtur "*consolidated.db*" dhe në të cilin përfshihen koordinatat e vendndodhjes së bashku me kohën korresponduese dhe më e rëndësishmja pa kriptim (i pakoduar, i lirë), me pasojë që çdokush të mund të shohë në cilët vende ndodhet përdoruesi i celularit. http:/ /www. wired.com /gadgetlab / 20 11 /04/apple-iphone-tracking/

[134] Kjo në rastin kur ka abonim, pasi tek abonentët me parapagim (prepaid) nuk mund të identifikohet pajtimtari dhe përdoruesi.

[135] Sipas shprehjes së Green, N. dhe Sean, S. (2004). "*A Spy in your Pocket? The Regulation of Mobile Data in the UK*". *Surveillance & Society*, fq..573, gjithashtu shih: http://www.surveillance-and-society.org.

Por sistemet tradicionale të telekomunikacionit kanë fituar aplikime dhe një formë të re. Si një rezultat i procesit të konvergjencës së komunikimit dhe përdorimit të mëvonshëm të internetit si një lëvizje e vetme e platformës së informacionit, sjell rreziqe të qenësishme në funksionim dhe kërkon prezantim të posaçëm dhe analiza.[136][137]

Interneti nisi si një përpjekje për të krijuar një rrjet kompjuterik universitar të quajtur "ARPANET" në vitin 1969.[138] Origjina e Luftës së Ftohtë vinte nga ideja për të krijuar një rrjet kompjuterik që kompjuterët mund të komunikonin me njëri-tjetrin edhe pas një lufte bërthamore. Kjo gjë bëri që studiuesit të zhvillojnë idenë e tyre të komunikimit në mes dy pikave në rrjet (p.sh., A dhe B) edhe nëse ndërpritet lidhja direkt mes tyre, lidhja kanalizohet nëpërmjet pjesëve të tjera të rrjetit, i cili do të përcjellë informacion në Seksionet A dhe B.

---

[136] Për historinë e internetit shih: Castells, M. (2000). "*The Internet Galaxy, - Reflections on the Internet, Business and Society*", Oxford University Press 1 dhe në Leiner, B. dhe Cerf, V. (1997). "*The Past and Future History of the INTERNET*", Vol. 40, No. 2 Communications of the acm, në http://cs.ucla.edu/~lk/LK/Bib/PS/paper204.pdf, Internet Society, "*A Brief History of the Internet*", në http :// www .isoc.org/ internet /history /brief.sh tml#Introduction

[137] Karakteristike, është paraqitja e pikave të dobëta të rrjeteve të telefonave mobile GSM nga gazetari Anthony Bosnakoudi i revistës "*Mbrojtja dhe Diplomacia*", ku ai shpjegon se si bëhen përgjimet e bisedave në telefonat celularë. Ai thekson në mënyrë të veçantë se komunikimi midis një telefoni celular dhe kullës qelizore të Stacionit Bazë (Base Station), në të cilën ndodhet përdoruesi i telefonit, kryhet ndërmjet sistemit encryption. Megjithatë ekziston një mënyrë për të ndërhyrë sepse përgjuesi mund të ketë një pajisje që punon në njërën anë si një telefon celular dhe në tjetrën si një stacion bazë. "Stacioni Bazë" operon pranë objektivit - telefon celular dhe brenda zonës së mbulimit të stacionit real bazë, i cili funksionon si një telefon celular normal, kështu që Stacioni aktual Bazë të "mendojë" se ai është objektivi – celular i përgjimit. Objektivi komunikon me Stacionin e rremë Bazë, i cili çorienton celularin dhe se nuk është e mundur komunikimi i koduar (encryption), derisa objektivi telefon celular të detyrohet të komunikojë pa kodim(lirshëm) me stacionin e rremë bazë. Për të mos kuptuar rrjeti që nuk ekziston asnjë anomali, pjesa tjetër e aparatit të përgjimit komunikon Stacionin real Bazë dhe pretendon se është objektivi telefon celular. Në të vërtetë, kodon komunikimin e marrë nga objektivi, në mënyrë që as përdoruesi i telefonit celular dhe rrjeti të kuptojnë që vepron si një ndërmjetës i cili promovon përgjimin e telefononatës në Stacionin Bazë.

Shih: Bosnakoudi, A. "*Defence and Diplomacy*" Teksti siç është paraqitur në faqen e internetit http://news.in.eng/science-technology/article/?aid=681425

[138] ARPA, (Advanced Research Projects Agency). Agjensi kërkimore që u themelua në vitin 1958 gjatë Luftës së Ftohtë, si një përgjigje ndaj nisjes në hapësirë të satelitit artificial Sputnik nga Bashkimi Sovjetik.

Në vitin 1978 u zhvillua protokolli komunikimit TCP / IP i cili lejon komunikimet kompjuterike përmes rrjeteve të ndryshme pa pasur nevojë njëri rrjet për informacione teknike rreth rrjetit tjetër. Pastaj në vitin 1983, Ministria e Mbrojtjes së SHBA-ve për arsye sigurie vendosi të krijojë një rrjet të veçantë kompjuterik MILNET[139] duke lënë ARPANET të evoluojë në ARPA-internet dhe të pasojë një rrjet universitar dedikuar kërkimeve.[140] Në vazhdim përmes zhvillimit teknologjik dhe liberalizimit të shërbimeve të telekomunikacionit doli një rrjet i aksesueshëm globalisht nga të gjithë me lidhje telekomunikacioni kabllore ose me valë. Interneti u zhvillua përfundimisht në gjithë botën si një rrjet i kompjuterëve që komunikojnë me njëri-tjetrin dhe të transferojnë informacione. Identiteti i secilit kompjuter është identifikuar nga një adresë unike, numerike IP e formës xxx.xxx.xxx.xxx ku xxx janë numra prej 0 deri 255 (p.sh. 194.178.86.66), i quajtur IPv4 që mund të krijojë deri në 4.294.967.296 adresa. Këta numra në vazhdim i përkasin një emri fushe apo emri hapësire siç quhet, emri Domain (Domain name) liria e zgjedhjes për përdoruesit e kompjuterit korrespondues dhe kështu krijon atë që quhet Sektori Emrave të Sistemit (DNS)[141] një lloj direktorie që përkthehet Domain name në adresat IP.[142] Nga ana tjetër këto adresa janë të ndara në adresa (IP) të qëndrueshme dhe dinamike në varësi të faktit nëse ato janë të lidhura përherë me një kompjuter ose të ndryshojnë çdo herë kur një kompjuter lidhet në internet.[143] Ndërsa tashmë duke krijuar IPv6 ky numër shumëzohet në mënyrë

---

[139] Milnet (military network).

[140] Po aty. Castells, M. I., fq.11.

[141] Domain names funksionojë si adresat e faqeve dhe kanë dy ose më shumë nivele, p.sh. edu.al ku "al" është konsideruar emërtimi i rajonit ndërsa EDU është emri i internetit.

[142] http://www.webopedia.com/TERM/D/DNS.html (20-12-2008)

[143] Shih: Bezzi, M., Duquenoy, P. dhe Fischer-Hübner S. (2010). "*Privacy and Identity Management for Life*", 5th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/Prime Life International, Summer School, Nice, France, September 9-12, 2009, Revised Selected Paper, fq. 21, ku analizohet funksionimi i adresave IP dhe mbështet pikëpamjen që të dy adresat e qëndrueshme dhe dinamike janë të dhëna të lëvizshme dhe për këtë arsye hyjnë brenda sferës së të dhënave personale që duhen mbrojtur.

Tërësia e nenit 29 konsideron adresat IP si të dhëna që i referohen një personi i cili mund të identifikohet. Si "ofruesit e qasjes në Internet dhe administratorët e rrjeteve lokale mund të përdorin mjete të arsyeshme për të verifikuar identitetin e përdoruesve të internetit të cilët kanë si zakonisht një adresë IP" pasi zakonisht "rakordohet" sistematikisht në një data file, ora, kohëzgjatja dhe adresa dinamike IP që ofrohet për përdoruesit e internetit. E njëjta gjë mund të thuhet edhe për ofruesit e shërbimeve të internetit të cilët

konsistente që çdo përdorues i internetit të ketë mundësi të marrë adresë unike IP.[144] Pra, sa herë që një përdorues viziton një fotografi ose shkarkon arkiva nga interneti në kompjuter, adresa IP automatikisht shkon tek ofruesi i shërbimeve të internetit (ofrues interneti, ose Internet Service Provider (ISP),[145] i cili si ndërmjetës do të dërgojë informatat e përshtatshme për përdoruesit që kanë kërkuar ato. Këto informacione, çdo herë që ndjekin rrugën nga një kompjuter në një tjetër ndahen në copëza shumë të vogla të ashtuquajtura paketa që përfshijnë adresën IP të dërguesit dhe marrësit. Secila paketë udhëton në internet, e pavarur nga tjetra dhe kur ajo arrin destinacionin e saj bashkohet me paketat e tjera. Ky proces është bërë nëpërmjet Protokollit të Kontrollit të Transmetimit/Protokollit të Internetit (Transport Control Protocol/Internet Protocol - TCP/IP). Protokolli i Kontrollit të Transmetimit përdoret për të transmetuar të dhënat në internet dhe është projektuar të instalohet shumë lehtë dhe nuk varet në një kompjuter të veçantë ose në sistemin operativ. Protokolli shumë thjeshtë, është gjuha që përdorin kompjuterët për të komunikuar.

Në vitin 1990 u zhvillua nga Tim Berners Lee "World Wide Web" (Webi Gjërësisht në Botë) ose thjesht Web.[146] Termi "www" cili u zhvillua në Zvicër në laboratorët e CERN[147] në vitin 1993 dhe është një instrument që lehtëson qasjen, kërkimin dhe gjetjen e informacionit në internet. Interneti në ditët e sotme nga shumë është konsideruar dhe identifikuar si "www", pasi me "www" ne mund të lundrojmë në internet, por kjo është diçka krejtësisht e ndryshme.[148] Termi "www" është në fakt një koleksion i madh i faqeve të informacionit elektronik duke përfshirë tekste, audio, video dhe foto,[149] d.m.th. "www" ndërlidh informatat e tilla të depozituara në kompjuterët e

---

mbajnë një regjistër mbi HTTP server. Në këto raste nuk ka dyshim se bëhet fjalë për të dhënat personale brenda kuptimit të Nenit 2) të Direktivës [...]) (Neni 29, 5063/00/ENG.END OE 37. Dokument pune. "*Mbrojtja e privatësisë në internet -. Një qasje e integruar e BE-së për mbrojtjen e të dhënave në internet*", në www.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37el.pdf).

[144] Shih: Për funksionimin e IP në http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf.

[145] Të tillë janë p.sh Albtelekom, Primo, Abisnet, Abcom, Tring e të tjerë.

[146] Shih: Berners - Lee T. (1989)."Weaving the Web" dhe Berners-Lee, T., Fischetti, M. (2008). "*Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*". fq.54.

[147] Qendra Evropiane për Grimcat Fizike.

[148] "*Lundrojmë ose shfletojmë*" është terminologjia e zakonshme e përdoruesve të internetit.

[149] Stuckey, K. D. (1996). "*Internet and Online Law*", Law Journal Press, fq.36.

lidhur me internetin. Përdoruesit e internetit mund të jenë të lidhur për të përdorur një browser (program shfletues).[150] Këto informacione janë organizuar në faqe elektronike të quajtura faqet Web (Pages Web) të cilat përmbajnë tekste, informacione në lidhje me strukturën e faqes dhe hiperlidhjet (hyperlinks)[151] në arkiva grafike të tjera. Shumë faqe Web janë ruajtur në një vend të veçantë në internet e cili është në dispozicion të publikut dhe quhet Website. P.sh. të gjitha faqet janë të depozituara në www.uet.edu.al është Website i Universitetit Evropian të Tiranës. Vendosja e një hyperlinku të padukshëm kundrejt kompanive të marketingut në Hapësirën kibernetike(Cyberspace) në faqet e tyre, faqet e internetit të përbashkëta (sidomos motorët e kërkimit)[152] udhëzojnë softuerët shoqërues, (Internet Explorer), të krijojnë një lidhje të pavarur me serverin e marketingut të kompanisë në cyberspace. Siç u përmend më lart, softuerët shoqërues transferojnë automatikisht të dhëna të ndryshme d.m.th. adresa IP, faqe referuese (nëse motori i kërkimit mund të përfshijnë fjalë kyçe të shtypura nga përdoruesi që kryen kërkimin), kompani, versionin dhe gjuhën e përdorur softuerin e kërkimit (p.sh. Internet Explorer 11, anglisht, lloji dhe sistemi i përdorur operativ: Windows 2014, Linux 17, Mac OS X 10.10, etj) dhe në fund "cookie" që janë përcaktuesit e autentifikimit të përdoruesit (p.sh. UserId=342ER432), të cilat mund të kenë qenë të vendosura nga promovimi i kompanisë komerciale.[153][154]

[150] Quhet shfletuesi i internetit.

[151] (Hiper)lidhjet (hyperlinks) janë simbolet joaktive të përfshira në një faqe HTML të cilat nëse i aktivizojmë, na drejtojnë në faqe interneti të tjera me përmbajtje të ngjashme ose të ndryshme, të cilat i ka krijuar / ose menaxhohen nga një person apo organizatë tjetër. Kështu për shembull, në Faqen zyrtare në internet të Universitetit Europian të Tiranës, përveç informatave të ndryshme rreth Universitetit, Fakulteteve, Departamenteve etj, të cilat i ka krijuar, ruajtur dhe informon publikun dhe studentët për organizimin dhe shërbimet e kërkuara në Universitet, janë të përfshira edhe hyperlinks në faqet e universitetit si biblioteka të universitetit dhe ato kombëtare apo rajonale, autoritetet publike etj.

[152] Motorët e kërkimit kanë zënë tërësinë e Nenit 29, i cili vendosi se ata nuk ndërhyjnë në konceptin e "komunikimeve elektronike", por paraqesin rreziqe për privatësinë e përdoruesve të tyre. Shih: Opinion 1/2008 për çështjet e mbrojtjes së të dhënave në lidhje me motorët e kërkimit, në http://ec.europa.eu/ justice _ home/fsj/privacy/docs/wpdocs/2008/wp148_eng.pdf. Si dhe përgjigjia e Google në http : // 209 .85 .139 .110/blog_resources/Google_response_Working_Party_06_2007.pdf.

[153] Working Paper 37 "Protection of privacy on the Internet. - An integrated approach of EU data protection online".

Në paragrafët e mëposhtëm do të bëhet një prezantim më specifik i këtyre teknologjive që krijojnë rrezikun për mjedisin e të dhënave personale dhe privatësisë, në mënyrë që të lehtësohet thellimi i metodave dhe qëllimet e trajtimit legjislativ të këtyre rreziqeve.

2.2 "Cookies"

"Cookies"[155] janë pjesët e të dhënave që mund të ruhen në arkivat e tekstit që janë vendosur në hard diskun e përdoruesit të internetit, ndërsa website mban një kopje të tyre.[156] Ato janë pjesë e trafikut të HTTP,[157] dhe si të tilla mund të transportohet pa u

---

[154] Sipas Gauthoronet, S. dhe Frédéric, N. "*Duke kombinuar "përpëlitjen*"e softuerit shëtitës me hyperlinks të padukshëm, një kompani marketingu në Cyberspace, me parazgjedhje, mund të njohi të gjitha fjalët kyçe të shtypura nga përdoruesit e internetit në motorin e kërkimit në të cilin kompania reklamon, kompjuterin, sistemin operativ, kompaninë software të shëtitësit dhe përdoruesit të internetit, adresën IP të përdoruesit, kohën dhe kohëzgjatjen e seancave në HTTP. Nëse të dhënat janë trajtuar në kombinim me të dhëna të tjera në dispozicion të kompanisë rezultojnë të dhëna të reja të tilla si: 1. Vendi i banimit i përdoruesit të Internetit, 2. Sektori i internetit në të cilën i takon përdoruesi, 3. Aktivitetet në terren të kompanisë që ka kontraktuar përdoruesin e internetit, 4. Cikli i punimeve dhe madhësia e kompanisë që ka kontraktuar përdoruesin, 5. Përgjegjësitë dhe pozicioni i përdoruesit në lundrim (shfletim) në kontekstin e shoqërisë, 6. Ofruesi i shërbimeve të aksesit në Internet, 7. Llojet dhe faqet e vizituara nga një përdorues." Shih: Gauthoronet, S., Frédéric N. "*On-line services and data protection and the protection of privacy*", Study for the Commission of the European Community (DG XV) në http ://ec .europa. eu / justice _ home / fsj/privacy/docs/studies/online-serv.pdf

[155] Louis J. Montulli II (i njohur më mirë si Lou Montulli) është një programues i cili është i njohur mirë për punën e tij në prodhimin shfletues të web. Cookies u shpikën nga Lou Montulli në vitin 1994, kur ai punonte në kompaninë Netscape, në http://en.wikipedia.org/wiki/Lou_Montulli

[156] King, I. (2003). "*On – line Privacy in Europe-new regulation for cookies*", Information & Communication Technology Law, fq. 228 dhe Bailey, M. (2011). "*Complete Guide to Internet Privacy, Anonymity & Security*", fq. 291 dhe po aty Mendel, T, Puddephatt, A. dhe Wagner, B. (2012). fq.45.

[157] Protokolli i Transferimit të Teksteve të gjata(të mëdha) (HyperText Transfer Protocol) është një protokoll për transferimin e teksteve të gjata (HyperText). Protokolli i Transferimit të Teksteve të gjata (HTTP) nuk punon me lidhje të vazhdueshme, por çdo herë që dikush pyet për një faqe, lidhet me serverin, merr të dhënat dhe më pas shkëputet. Pra, ajo nuk mund të mbajë "direkt" porosinë e konsumatorit duke shkuar nga faqja në faqe dhe nuk mund të njohë identitetin e tij. Zgjidhjen e japin "cookies" ky arkiv teksti që ruhet në hard disk, ndihmon çdo herë që ju vizitoni një faqe web dhe të vërtetojnë se jemi ne dhe jo dikush tjetër.

penguar nga trafiku IP.[158] "Cookies" instalohen në hard diskun e kompjuterit të përdoruesit, të cilat përmbajnë informacion në lidhje me individin i cili e vendosi atë që mund të lexohet nga faqja e internetit apo nga kushdo që është në gjendje të njohë formatin, të dhënat e kësaj faqe interneti. Ata përmbajnë çdo informacion që website dëshiron që të përfshijë në to: faqet e shikuara nga përdoruesit, reklamat që ka zgjedhur për të lexuar, numrin e identifikimit të përdoruesit për sa kohë qëndron dhe cilat faqe të internetit frekuenton etj.

Në disa raste, shërbejnë për qëllime të përkryera legjitime, të tilla si për të siguruar një shërbim përmes internetit, ose për të lehtësuar shfletimin e përdoruesit në internet. Faqet e internetit përdorin "cookies" për të njohur identitetin e përdoruesit çdo herë që ata do të vizitojnë faqen e internetit, në mënyrë që përdoruesit të mos jenë të detyruar të sigurojnë të dhënat e tyre në çdo vizitë në faqet e internetit.[159] Në këtë mënyrë çdo herë që dikush viziton një faqe interneti, bëhet njohja e lëvizjeve të tij të fundit dhe frekuentimeve të faqeve on-line për shkak të "cookies" që janë instaluar në kompjuterin e përdoruesit. Sigurisht kjo ndihmon kompanitë për të krijuar profilin e veçantë të përdoruesit, i cili përveç të dhënave të tilla si zakonet e konsumit, zakonet politike dhe interesat kulturore apo të tjera, mund të përmbajë informacione që lëvizin në fushën e të dhënave të ndjeshme personale, të tilla si orientimi seksual, aktiviteti politik apo fetar. Sigurisht nuk mund të jetë e rrezikshme për përdoruesin e internetit nëse nuk mund të bëhet identifikimi i tij me një person të veçantë. Në këtë rast një faqe interneti, pasi kërkon nga një përdorues të plotësojë një formular me të dhënat personale të përdoruesit ka potencialin për të bërë pastaj vendosjen e një "cookie" kështu që mund të identifikojë adresën IP të përdoruesit me të dhënat aktuale të adresës dhe kështu mundëson njohjen dhe shpalosjen e të dhënave të vërteta të përdoruesit i cili pushon së qeni një lundërtar anonim në internet, me pasoja të ekzistojë rreziku për të zbuluar të dhëna të ndjeshme personale që zbulojnë origjinën racore ose etnike, mendimet politike,

[158] Protokolli Internetit (IP) është protokoll komunikimi kryesor në kompletin e protokollit të internetit për transmetimin e të dhënave gramore nëpër kufijtë e rrjetit. Matthews, J. (2005). "*Computer Networking: Internet Protocols (IP) in Action*", fq. 3.

[159] Protokolli për transaksione të sigurta elektronike – "cookie" (SET-Cookie) gjendet në krye të përgjigjes HTTP, në superlidhës të padukshëm. Nëse kohëzgjatja është specifikuar, "cookie" është ruajtur në hard diskun e përdoruesit të internetit për atë periudhë të caktuar dhe pastaj të kthehet në faqen e internetit nga e cila erdhi.

fetare ose bindjet filozofike, pjesëmarrjen në unione, organizimin dhe anëtarësimin në sindikata, shëndetin e personit, orientimin seksual, etj.[160]

2.3 "Përgjuesit (Çimkat) e Web" (Web Bugs)

Një "Web Bug" është një komandë në drejtim të shfletuesit që lidhet me një server të tretë dhe të japi disa informacione. A është dhe "Web Bug" si "cookies" që identifikon adresën IP të përdoruesit dhe regjistron trafikun e të dhënave të përdoruesit, ndërsa lundron në web? Problemi është se Web Bug është i padukshëm për përdoruesit, sepse ai është i vendosur brenda një imazhi, ku për shkak të madhësisë së tij, nuk është i dukshëm me sy të lirë. Ata janë zakonisht vetëm imazhe me madhësi 1x1 pixel. Kur ne shikojmë një faqe web me një baner reklamash, mund të kuptojmë se një palë e tretë mbledh informacion në lidhje me ne, apo vendos një cookie në kompjuterin tonë. Por në rastin e një Web Bug, nuk mund të dimë për lidhjen e kompjuterit tonë me një server të një pale të tretë. Kështu nuk i jepet mundësia përdoruesit ta çaktivizojë, refuzojë apo heqë, si mundësia që ka për të bërë me cookies. Kjo natyrisht shkakton probleme të mëdha për shkak se web bugs janë përdorur nga një palë e tretë për të monitoruar cilat faqe vizitohen nga përdoruesit.[161] Një aktivitet tjetër i Web Bugs lidhet me aftësinë që ata kanë për të verifikuar adresat e email-it të përdoruesve të internetit.

Web Bugs mund të identifikojnë se kush dhe kur lexoi dikush një e-mail dhe madje të dihet adresa IP e marrësit të e-mail-it. Pra kur përdoruesit hapin mesazhe të pa dëshiruara (spamm) atëherë të ashtuquajturat spammers marrin mesazhe se këto adresat e-mail janë të vlefshme.[162] Kjo është e arsyeshme si dhe është shumë e dobishme për ata

---

[160] Shih: Fuchs, Ch., Boersma, K. dhe Albrechtslund, A. (2012). "*Internet and Surveillance: The Challenges of Web 2.0 and Social Media*", fq.138 si dhe Hyatt, M. (2001). "*Invasion of privacy: how to protect yourself in the digital age*", fq.11. dhe Smith, G. J. H. (2007). "*Internet Law and Regulation*", fq. 687.

[161] Shih: Sharon N. (2002). "*Internet privacy — regulating cookies and web bugs*" Privacy Law and Policy Reporter në http://www.austlii.edu.au/au/journals/PLPR/2002/26.html, gjithashtu dhe Chung, W. dhe Paynter, J. "*Privacy Issues on the Internet*", në http :// www .hicss .hawaii .edu /HICS S_35/ HICSS papers /PDF documents/INISC02.pdf

[162] http://www.ecomputerlaw.com/articles/show_article.php?article=2002_web_bugs

që dërgojnë e-mail-le të padëshirueshme sepse duke e ditur që kush i lexojnë, ata organizojnë mesazhe të tjera për të dërguar ose fshirë ato që nuk i lexojnë.[163]

2.4 "Programi Spiun" (Spyware)

"Spyware" është një lloj programi kompjuterik që instalohet në hard diskun e një kompjuteri pa ndonjë njohuri të përdoruesit dhe pa qenë në gjendje të ç'instalohet ose të trajtohet me përdorimin e antiviruseve dhe firewalls.[164] Zakonisht instalohet kur përdoruesi përdor shërbime falas në instalimin e programit kompjuterik të ashtuquajtur "freeware" pa e kuptuar atë.[165] Ky program pasi është instaluar një herë në kompjuterin e përdoruesit fillon mbledhjen e informacionit lidhur me lëvizjen që kryen në internet përdoruesi, faqet e internetit që ai viziton, blerjet që bën në internet madje edhe numrat e kartës së kreditit dhe llogarive bankare.[166]

2.5 Posta Elektronike (E-mail)

Rreziqet që rrjedhin nga përdorimi i e-mail-it mund të krahasohen me rreziqet dhe shkeljen e fshehtësisë së letrave postare. Funksionet specifike të mesazheve në postën elektronike, të tilla si dërgimi i email-ve ka shpesh marrës të shumtë dhe se mund të marrin dijeni për përmbajtjen e tyre, si dhe të gjitha misioneve të përdoruesit, duke krijuar një mjedis të rrezikshëm.[167] Funksioni i postës elektronike (e-mail-it) është si vijon: Fillimisht një përdorues shkruan një mesazh në programin e tij "klient i postës

---

[163] Shih: Informacion për web bugs në faqen e internetit të Electronic Frontier Foundation http://w2.eff.org/Privacy/Marketing/web_bug.html

[164] Për "*Spyware*" shih në Center for democracy and technology (cdt), "Ghosts in our machines: background and policy proposals on the "spyware" problem", 2003, në http:// www. cdt. Org /privacy /031100 spyware.pdf.

[165] P.sh instalimi i programeve për "shkarkimin" e filmave dhe muzikës.

[166] Schrijver, S. Schraeyen, J. (2005). "*Spyware: Inoccent espionage in cyberspace?*" Communications Law, fq. 17.

[167] Në letrën e Mbrojtjes së privatësisë në internet. - Një qasje e integruar e BE-së për mbrojtjen e të dhënave në internet. Neni 29, përshkruan në mënyrë të analizuar procedurën e funksionimit të e-mail dhe rastet e rrezikimit të privatësisë. Neni 29, 5063/00/OE.37. Letër pune. Mbrojtja e privatësisë në internet.-Një qasje e integruar të BE-së për mbrojtjen e të dhënave në internet në http://.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37eng.pdf

elektronike" dhe kompleton fushën e adresës së marrësit me adresën e duhur e-mail.[168] Duke klikuar pliktrën (opsionin) "Dërgoj" (Send) në postën elektronike të klientit, e-mail-i dërgohet me të ashtuquajturin "Protokolli i Thjeshtë i Dërgimit të Postës" (Simple Mail Transport Protovol - SMTP)[169] në serverin e postës elektronike të marrësit (zakonisht organizatë) ose në kutinë postare të disponueshme në llogarinë e përdoruesit të internetit nëpërmjet një ofruesi të shërbimit të internetit.[170] Nëse e-mail-i dorëzohet në serverin e postës elektronike të organizatës,serveri e kalon mesazhin e postës elektronike (e-mail-in) direkt te marrësi ose te një server transmetues[171] i postës elektronike ("transmetim i ardhur nga jashtë").[172] Marrësi ose është lidhur direkt me serverin transmetues të postës elektronike (p.sh. në një rrjet lokal LAN), ose është i lidhur në mënyrë që të kërkojë mesazhet e postës elektronike përmes protokollit të postës (protokolli POP) për të mundësuar marrësin që të lidhet me serverin e postës elektronike dhe të kontrollojë nëse ai ka mesazhe.[173] Përmbajtja e mesazhit të postës elektronike ruhet në serverin e postës elektronike derisa klienti i "postës elektronike" (e-mail) të përdoruesit të kërkojë dorëzimin e tij. Në disa raste përdoruesi nuk e fshin e-mail-in, por e lë të ruajtur në serverin e postës elektronike edhe në qoftë se ai ka marrë një kopje të tij. Problemi për të dhënat personale krijohet, kur mblidhen adresat elektronike për të dërguar mesazhe promocionale dhe kur monitorohet trafiku mesazheve. Mbledhja e adresave elektronike (e-mail) mund të ndodhi:

1. Kur një ofrues i programit(software) të postës elektronike që është blerë ose nga përdoruesi ose është dhënë dhuratë, kërkon nga përdoruesi të dhënat e tij personale që ta regjistrojë atë.

---

[168] Një adresë e-mail p.sh. i.shtupi@yahoo.com në pjesën e djathtë identifikon identitetin e kompjuterit host ku marrësi i mesazhit tonë mban një llogari, e cila i referohet adresës IP të serverit postës elektronike. Pjesa e majtë përshkruan të dhënat e personalizimit të marrësit të mesazhit. Mund t'i referohet emrit aktual, por mund të jetë një pseudonim ose kod i përzgjedhur nga marrësi ose një kod i rastit që është dhënë nga serveri i e-mail-it.

[169] Shih: përshkrimin e teknikës të SMTP në http://www.vanemery.com/Protocols/SMTP/smtp.html

[170] Po aty. Dokumenti 37 OE, fq.22.

[171] Mesazhi i postës elektronike mund të kalojnë nëpër disa servera transmetues të postës elektronike deri se të arrijë serverin e postës elektronike të marrësit.

[172] Po aty. Dokumenti OE 37. fq. 38.

[173] Po aty. fq. 37.

2. Kur një ofrues i programit(software) të postës elektronike përdor programe (software) për të lexuar adresën e tij.

3. Nëse ekzistojnë të meta të sigurisë, që lejojnë një faqe interneti të informohet për adresat elektronike të personave që e vizitojnë atë.

4. Në shumë raste, faqet e internetit mund të kërkojnë adresën tuaj të e-mail (p.sh. faqet komerciale në mënyrën e blerjes, për regjistrimin para se të hyjnë në një dhomë bashkëbisedimi (chat room), etj.).

Të dhënat e trafikut[174] që kanë nevojë protokollet për kryerjen e transmetimit të mesazhit nga dërguesi te marrësi, i siguron vetë dërguesi dhe mund të jenë p.sh. adresa e postës elektronike të marrësit dhe pjesë nga informacionet teknike të gjeneruara automatikisht gjatë përpunimit të mesazhit të postës elektronike, si datën dhe kohën e dërgimit, llojin dhe versionin e programit të "klientit të postës elektronike".

Në vazhdim të dhënat e komunikacionit vendosen në kokë (pjesën kryesore), transmetohen tek marrësit bashkë me vetë mesazhin. Informacione përcjellëse të të dhënave të trafikut, përdoren nga serveri i postës elektronike dhe "klienti i postës elektronike (e-mail)" të marrësit, për menaxhimin e duhur të mesazheve hyrëse. Marrësi mund të përdori të dhënat e transmetuara të trafikut (personat privatë të adresës së postës elektronike) për qëllime analitike (p.sh., për të kontrolluar kursin (rrugën) e mesazhit të postës elektronike nëpërmjet internetit).[175]

Sipas ligjit "Për Komunikimet Elektronike në Republikën e Shqipërisë" me postë elektronike do të kuptojmë çdo mesazh në formën e tekstit, tingullit apo imazhit, të dërguar nëpërmjet rrjetit publik të komunikimeve, i cili mund të ruhet në rrjet ose në pajisjen fundore të marrësit derisa marrësi ta marrë atë.[176] Në doktrinë, shfaqet mendimi se një përkufizim i tillë synon të jetë neutral nga pikëpamja teknologjike dhe të përfshijë

[174] Të dhënat e lëvizjes (motion) në dërgimin e e-mail-ve janë: a) adresa e postës elektronike dhe adresa IP e dërguesit, b) lloji, versioni dhe gjuha e agjentit të klientit, c) adresa e postës elektronike (e-mail) i marrësit, d) data dhe koha e dërgimit të e-mail-it, e) madhësia e e-mail me shumën e karaktereve (shkronja dhe numra) të përdorura, f) subjekt i mesazhit (kjo gjithashtu përmban informacione mbi përmbajtjen e komunikimit), g) emri, madhësia dhe tipi i ndonjë dokumenti të bashkangjitur, një listë e transportuesve SMTP të përdorur për transmetimin.

[175] Po aty. Dokumenti OE 37, fq. 38-39.

[176] Neni 3, pika 34 e ligjit nr. 9918, datë 19.5.2008 "*Për Komunikimet Elektronike në Republikën e Shqipërisë*" (I ndryshuar).

çdo mesazh të transmetuar nëpërmjet komunikimeve elektronike, ku pjesëmarrja e njëkohshme në komunikim e dërguesit dhe e marrësit të mesazhit nuk është e nevojshme. Koncepti i postës elektronike është shumë më i gjerë se sa koncepti i e-mail-it. Në këtë koncept do të përfshihen gjithashtu shërbimet e mesazheve të shkurtra (SMS), të mesazheve multimediale (MMS), shërbimet e postës zanore etj.[177]

2.6 Lista e Komunikimit në Grup (Mailing List)

Mailing Lists janë sisteme komunikimi në grup të bazuara në postën elektronike.[178] Në praktikë, me mjete të tilla, një grup përdoruesish kanë mundësinë të shkëmbejnë mesazhe mbi një argument specifik duke përdorur postën elektronike. Qëllimi i Mailing Lists është ai i organizimit dhe i administrimit të forumeve mbi argumente të veçanta: të gjithë përdoruesit e interesuar mbi një argument të përcaktuar mund të regjistrohen në listë (duke i dërguar një mesazh të posaçëm server-it administrues të listës (listserver) dhe që nga ky moment të marrin pjesë në marrjen dhe transmetimin reciprok të mesazheve.

Në praktikën gjyqësore të huaj, komunikimet e zhvilluara në një mailing list, janë njohur si komunikim privat. Këto komunikime do të konsiderohen se kanë natyrë private për sa kohë që shkëmbimi i mesazheve, i cili në një rast të tillë nuk përfshin dy subjekte, por shumë persona, ose më mirë një "komunitet virtual", nuk drejtohet nga subjekte të papërcaktuar, por midis subjekteve që bëjnë pjesë në një komunitet të "mbyllur", që përjashton të tjerë të cilët nuk bëjnë pjesë në të.

2.7 Grupet i Informacionit (Newsgroups)

Newsgroup-i është një grup diskutimi që mbështetet në një temë të caktuar paraprakisht.[179] Ka funksion të njëjtë me mailing list, por ndryshon nga kjo e fundit sepse mesazhet nuk dërgohen në kutinë postare të përdoruesit të veçantë të regjistruar në listë, por në një lloj "tabele elektronike" në të cilën përdoruesi mund të seleksionojë mesazhet që i interesojnë dhe të marrë pjesë në diskutim. Newsgroup-et mund të jenë me hyrje/akses të lirë ose të kushtëzuar në rast se parashikohet një

[177] Büllesbach, A. (2010). *"Concise European IT Law"*, Kluwer Law International, fq. 182-183.

[178] Shih: Në mënyrë të detajuar në http://en.wikipedia.org/wiki/Mailing_list

[179] Shih: Për më tepër informacion në http://www.newsgroups.com/

fjalëkalim aksesi me të cilin janë pajisur një shumicë subjektesh të përcaktuar. Në këto raste newsgroup-et do të rezultonin të ishin komunitete të mbyllura të ngjashme me mailing list.

2.8 Linjat e Shkëmbimit Interaktiv të Mesazheve (Chat)

Chat-i është një mekanizëm i shkëmbimit ndëraktiv dhe në kohë reale të mesazheve midis përdoruesve që ndodhen prezentë në të njëjtën kohë në një chat-line. Në varësi të opsionit të zgjedhur të bisedës, komunikimi i zhvilluar në një linjë chat-i, mund të jetë publik ose privat midis dy personave. Shërbimi i chat-it, bëhet i mundur në sajë të rezervimit të një hapësire të caktuar posaçërisht për këtë qëllim në një rrjet të komunikimeve elektronike publike.[180]

2.9 Komunikimet e Padëshiruara Elektronike (Spamming)

Direktiva 97/66/KE, si në të vërtetë dhe Direktiva 2002/58/KE parashikonte përdorimin e sistemeve të thirrjeve automatike pa ndërhyrjen e njeriut (makinat automatike të thirrjes) ose faksit (fax) për qëllime të marketingut të drejtpërdrejtë duke lejuar vetëm në rastet kur abonentët kanë dhënë pëlqimin e tyre paraprak.[181] Nuk ishte parashikuar në Direktivën 97/66/KE përdorimi i e-mail për qëllime të marketingut të drejtpërdrejtë, i cili rezultoi përfundimisht në krijimin e problemeve të mëdha të ashtuquajtura mesazhe "Spam".

Koncepti i "Spam" përafrohet ndryshe nga legjislacionet kombëtare dhe aktorët e ndryshëm.[182] Në Francë për shembull Komisioni Kombëtar i të Dhënave Personale dhe Lirive (Komisioni Nationale de l'informatique et des Libertés) i referohet

---

[180] Për më shumë lidhur me metodat e komunikimit në chat dhe mënyrën e funksionimit të tyre shih: Schneider, G., Evans, J., dhe Pinard, K. (2009). "*The Internet: Illustrated Series*". Boston: Course Technology Cengage Learning. fq.144-147.

[181] Neni 12 i Direktivës 97/66/KE.

[182] Në prill të vitit 1994 një avokat nga shteti i Arizonës filloi operacionin e reklamimit të një programi kompjuterik (software) në internet të firmës ligjore Cantor & Siegel. Reagimet ishin të ashpra dhe të menjëhershme duke dërguar mesazhe se reklamat e pa kërkuara nuk do të tolerohen në internet, ndërkohë që ishin në fillimet e tyre. Mijëra ishin reagimet për përdoruesit me apelimin tipik të përdoruesit të internetit drejt përdoruesve të tjerë për të dërguar arra dhe kanaçe ("Dërgo arra dhe kanoçe të Spamit për Cantor & CO").

"spamming" ose "spam" si praktikë që të dërgojë dikush mesazhe të padëshiruara në numër të madh dhe në mënyrë të përsëritur për individë me të cilët dërguesi nuk kishte asnjë kontakt të mëparshëm dhe adresat elektronike u mblodhën në mënyrë jo të drejtë.[183] Mesazhet e dhëna të karakterit komercial nëpërmjet postës elektronike, të cilat janë të njohura si "spam", paraqesin një rrezik të madh për zhvillimin e internetit, se ata janë tashmë 70% e mesazheve të postës elektronike.[184] Në komunikatën e Komisionit Evropian për mesazhet e dhëna të karakterit tregtar ose "spam" në Parlamentin Evropian, Këshillin, Komitetin Ekonomik dhe Social Evropian dhe Komitetin e Rajoneve në të cilin bëhet referimi si për fenomenin e "postës së pavlerë"(spam) dhe për mënyrat e trajtimit të tij. Vihet re se "spami" ka marrë përmasa të tilla alarmante dhe për t'i bërë të ditur menjëherë rrezikun përdoruesve të e-mail-ve ose SMS-ve, se duhet të ndalojnë përdorimin e këtyre shërbimeve të Internetit ose të komunikimeve të lëvizshme (celulare), apo edhe për të reduktuar ato në një të shkallë të madhe.[185]

Sipas raportit të Organizatës për Bashkëpunim Ekonomik dhe Zhvillim (OECD) rritja e mesazheve spam ka një ndikim negativ jo vetëm sa i përket trajtimit të konsumatorëve të mesazheve komerciale nëpërmjet internetit, por dhe në zhvillimin e tregtisë elektronike që pranon uljen e besimit në transaksionet e konsumatorit nëpërmjet internetit, besim që përbën çelësin për rritjen dhe suksesin e tij.[186] Ndërsa sipas ish

---

[183] Shih: Për Spam, analizën e Butler, M. (2003). "*Spam - the meat of the problem*", në Computer Law & Security Report, f.q 388, gjithashtu shih dhe përkufizimin që i jep Agjencia Kombëtare e Shoqërisë së Informacionit në Shqipëri, nëpërmjet Rregullores për Faqet Zyrtare të Internetit në Administratën Publike, e cila përkufizon si spamm (Mesazhet elektronike (e-mail) të padëshiruara, kryesisht komerciale, që përfshijnë një numër të madh marrësish. Njihen ndryshe si bulk-email ose junk-email), fq.3 në http://www.akshi.gov.al/Rregullore/rregullore_për_faqet_zyrtare_te_internetit_te_administrates_publike. pdf dhe shih studimin mbi shkallën e suksesit të mesazheve elektronike të padëshiruara dhe marzhin e fitimit që lejon ky aktivitet në dërgimin e mesazheve të tilla. Përfundimet e tyre janë botuar në studimin: "*Spamalytics: An Empirical Analysis of Spam Marketing Conversion*". http :// www .icsi. berkeley . edu /gfx/nav/logo.gif

[184] http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/3746023.stm (21-11-05)

[185] Komunikimi nga Komisioni për Parlamentin Evropian, Këshillin, Komitetit Evropian Ekonomik dhe Social dhe Komitetin e Rajoneve, në http :// europa .eu .int /eurlex /lex/ lexuriserv /site /el/ com/ 2004/ com2004_0028el01.doc. Nuk mbulohen mesazhet e dhëna me përjashtim të komunikimeve elektronike p.sh posta (konvencionale) e dhënë.

[186] Background paper for the OECD workshop on spam, në www.oecd.org

Komisionerit Evropian për çështjet e biznesit Errki Liikanen "tashmë Spam përfshin kosto më të larta për bizneset. Vetëm me kushtet e humbjes së produktivitetit, kostoja është vlerësuar në miliarda euro në Evropë. Komunikimet për qëllime të ligjshme komerciale dhe promovuese nuk publikohen më."[187] Kjo është arsyeja pse preambula e Direktivës 2002/58/KE nënvizon këtë nevojë për të ofruar garanci për abonentët në mbrojtjen e privatësisë nga komunikimet e pa kërkuara me qëllim marketingu të drejtpërdrejtë dhe dërgimi i komunikime të tilla tregtare të pa kërkuara, jo vetëm që shkel të drejtat e privatësisë personale, por ka të ngjarë të shkaktojë vështirësi në rrjete dhe pajisjet fundore të komunikimeve elektronike.[188] Këto zhvillime teknologjike i rregulloi Direktiva e re për komunikimet elektronike.[189] Në veçanti në Nenin 13 të Direktivës 2002/58/KE, rregullohen çështjet që dalin nga të ashtuquajturat komunikime të padëshirueshme me qëllim promovimin e drejtpërdrejtë të produkteve, shërbimeve ose reklamave. Nga prezantimi i shkurtër i teknologjive të internetit, kuptohet jo vetëm se anonimiteti i internetit është një mit, por dhe se qytetari mesatar është në një pozitë mjaft të vështirë për të përballuar i vetëm rreziqet e mundshme që mund të rrezikojnë të dhënat e tij personale, nga depërtimi i teknologjive të cilat ndryshojnë vazhdimisht dhe bëjnë që rregullat ligjore moderne, të vjetruara dhe të dobëta të ndjekin zhvillimet teknologjike. Ndër risitë më të fundit telematike do të veçonim realizimin e shërbimeve të telefonisë nëpërmjet Internetit si dhe dërgimin/marrjen nëpërmjet Internetit të SMS-ve drejt një numri telefoni dhe anasjelltas. Përdorimi i këtyre shërbimeve bëhet i mundur në sajë të aplikacioneve të posaçme për këtë qëllim, të vendosura në telefonat inteligjentë të njohur gjerësisht me emërtimin smartphones.[190]

[187] Liikanen, E. (2nd February 2004). "*Opening remarks at the OECD workshop on spam, OECD Workshop on Spam Brussels*", në http ://europa .eu.int/rapid/ pressReleasesAction. do? Reference = SPEECH /04/55 &format =HTML &aged= 0&language = EN & g uiLanguage=en 23-9-2005.

[188] Opinion shpjegues 40 i Direktivës 2002/58/KE.

[189] Po aty. Shih prezantimin e masave në Smith, G. J. H. (2007), fq. 687

[190] Standage, T. (2005). "*The Future of Technology*", fq. 152.

KAPITULLI III: MARRËVESHJET PËR MBROJTJEN E TË DHËNAVE PERSONALE NË NIVEL NDËRKOMBËTAR

Ligji për mbrojtjen e personit nga përpunimi i të dhënave personale si brenda kornizës së mbrojtjes së të drejtave të njeriut dhe rregullores autonome, ndoqi një rrugë të gjatë në nivel ndërkombëtar dhe evropian. Në nenin 12 të Deklaratës Universale të të Drejtave të Njeriut të OKB-së, të datës 10 Dhjetor të vitit 1948, Nenin 17 të Paktit Ndërkombëtar mbi të Drejtat Civile dhe Politike që hyri në fuqi 23 Mars 1976, si dhe themelimin e Agjencisë për Bashkëpunim dhe Zhvillim Ekonomik në vitin 1980 mbi "Parimet për mbrojtjen e sferës personale të njeriut dhe të rrjedhave tej kufitare të të dhënave personale", mbrojtja e privatësisë ishte një parakusht për gëzimin e të drejtave themelore të njeriut. Në Evropë, në të cilën Lufta e Dytë Botërore kishte krijuar një ndjeshmëri të veçantë në popuj dhe qeveri, për nevojën në mbrojtjen e të drejtave të njeriut dhe privatësisë, u hartua dhe u nënshkrua nga shtetet evropiane në 1950 "Konventa e Romës për mbrojtjen e të drejtave dhe lirive themelore të njeriut" ose siç njihet ajo zakonisht "Konventa Evropiane për të Drejtat e Njeriut", e cila është teksti i parimeve që formojnë bazat për evolucionin e ligjit të mbrojtjes së të dhënave personale. Megjithatë, në vazhdim, nevoja për mbrojtje më të madhe të të dhënave personale krijoi një shqetësim të vazhdueshëm për shkak të zhvillimit të teknologjive të monitorimit të privatësisë dhe përpunimit automatik të të dhënave personale dhe çoi vendet evropiane në prodhimin e legjislacionit si në nivel kombëtar ashtu dhe në nivel të Komunitetit Evropian. Kështu ndoqën së pari të ashtuquajturat Legjislacionet Evropiane të "gjeneratës së parë", si ai gjerman "Ligji i Hesse" dhe ai Francez "Ligji 78-17", në vazhdim pastaj vazhdoi Legjislacioni Evropian i "gjeneratës së dytë", me "Konventën 108" dhe "Marrëveshjen Shengen" dhe Legjislacioni Evropian i "gjeneratës së tretë",[191] të tilla si Karta e të Drejtave Themelore të Bashkimit Evropian, Direktiva 95/46/KE, "Rekomandimi nr. R (99) 5", Direktiva 97/66/KE, Direktiva 2002/58/ KE amenduar nga Direktiva 2006/24/KE dhe Direktivën 2009/136/KE.

[191] Koncepti i "*brezit të tretë*", siç thuhet në: Gutwirth, S., Leenes, R. dhe de Hert, P. (2014). "*Reforming European Data Protection Law*", fq. 312.

3.1 Rregullimet në Kuadër të OKB-së

3.1.1 Deklarata Universale e të Drejtave të Njeriut të OKB-së

Përvojat e hidhura të fituara gjatë Luftës së Dytë Botërore, që përveç humbjes së jetëve njerëzore ishte gjithashtu dhe një periudhë e shkeljeve të plota të të drejtave të njeriut, të cilat udhëhoqën bashkësinë globale në kërkim të parimeve të përbashkëta për mbrojtjen e dinjitetit dhe vlerën e qenieve njerëzore, të afta për të krijuar kushte më të mira të jetese. Nevoja për mbrojtjen e privatësisë, e cila kishte qenë e shkelur nga regjimet totalitare në kontinentin evropian, u pa si një objektiv kyç dhe referimi i parë i madh për të drejtën e privatësisë gjendet në Nenin 12 të Deklaratës Universale të të Drejtave të Njeriut të OKB-së, ku dhe thekson se askush nuk duhet t'i nënshtrohet ndërhyrjes arbitrare në jetën e tij private, familje, banesën ose korrespondencën vetjake, si dhe sulmeve kundër nderit dhe prestigjit personal.[192] Kjo rregullore, e cila u miratua nga Asambleja e Përgjithshme e OKB-së më 10 dhjetor, 1948 është e ndikuar veçanërisht nga Deklarata Franceze e të Drejtave të Njeriut dhe të Qytetarit e vitit 1789,[193] e cila ishte atëherë baza mbi të cilën ka evoluar kuadri ligjor modern për mbrojtjen e të dhënave personale dhe privatësisë.

3.1.2 Konventa Ndërkombëtare mbi të Drejtat Civile dhe Politike[194]

Orientimi fiks në këto parime i bashkësisë ndërkombëtare, konfirmohet nga dispozita që gjendet në nenin 17[195] të Paktit Ndërkombëtar mbi të Drejtat Civile dhe

---

[192] Teksti i Deklaratës është faqen e internetit të OKB-së në http://www.unhchr.ch/udhr/lang/eng.htm, ku deklarohet: "Askush nuk duhet t'i nënshtrohet ndërhyrjes arbitrare në jetën private, familje, banesën ose korrespondencën vetjake si dhe sulmeve kundër nderit dhe prestigjit personal. Gjithkush ka të drejtën të mbrohet nga ligji kundër ndërhyrjeve ose sulmeve të llojit të tillë".

[193] Kombet e Bashkuara, Asambleja e Përgjithshme, Sesioni 3. "*Vendimi 217A i Deklaratës Universale të të Drejtave të Njeriut*", 1948. Teksti i Paktit është respektivisht në faqen e internetit të OKB-së, në http://www.unhchr.ch/html/menu3/b/a_ccpr.htm, shih: për të në Stratford, J. (1998). "*Data Protection and Privacy in the United States and Europe*" IASSIST Quarterly, pg. 17 dhe Geronta, A. (2002). *"Protecting citizens from electronic processing of personal data*", pg.79.

[194] International Covenant on Civil and Political Rights. Teksti gjendet në faqen zyrtate të internetit të OKB-së, në http://www2.ohchr.org/english/law/ccpr.htm

Politike të miratuara nga Mbledhja e Përgjithshme e OKB-së në vitin 1966.[196] Ky pakt në nenin 17 si dhe në një dispozitë të ngjashme me Nenin 12 të Deklaratës Universale të të Drejtave të Njeriut të OKB-së thotë se askush nuk do t'i nënshtrohet ndërhyrjeve arbitrare ose të paligjshme në jetën e tij private, familje, banesë ose korrespondencën vetjake dhe as sulmeve të paligjshme ndaj nderit dhe prestigjit personal. Rreth Paktit, Komiteti i OKB-së për të Drejtat e Njeriut[197] botoi një tekst "Komente të Përgjithshme" për zbatimin e Paktit, i cili ka lidhje të drejtpërdrejtë dhe thekson parimet themelore që kemi gjetur në të gjitha instrumentet ndërkombëtare për mbrojtjen e të dhënave personale. Për sa i përket Neni 17, shpreh që kjo e drejtë zbatohet kundër të gjitha sulmeve kundër privatësisë qoftë nga autoritetet shtetërore ose nga persona fizikë ose juridikë dhe në këtë mënyrë ta detyrojë shtetin për të marrë masat e duhura legjislative për mbrojtjen e kësaj të drejte.[198]

Në të njëjtën kohë vërehen se këto masa të jenë të efektshme dhe se çdo person duhet të jetë në gjendje të dijë nëse depozitohen të dhënat e tij personale, me metodat e automatizuara, nga kush dhe për çfarë qëllimesh dhe të ndërhyjë për të ndryshuar apo fshirë të dhënat.[199] Pra, për herë të parë mishërohet në instrumentet ndërkombëtare zgjerimi i mbrojtjes së të drejtave të njeriut kundër çdo shkelje dhe në qoftë se ajo është burim sulmi (organ shtetëror ose person fizik ose juridik) dhe në përputhje me zgjerimin e të drejtës së ankimit në gjykatë për të siguruar mbrojtje gjyqësore.

---

[195] 1. Askush nuk duhet t'i nënshtrohet ndërhyrjes arbitrare ose të paligjshme në jetën e tij private, familje, banesë ose korrespondencën vetjake si dhe sulmeve të paligjshme ndaj nderit dhe prestigjit personal.

2. Gjithkush ka të drejtën të mbrohet nga ligji kundër ndërhyrjeve ose sulmeve të tilla.

[196] "*Konventa mbi të Drejtat Civile dhe Politike*" e cila u miratua nga Asambleja e Përgjithshme e Kombeve të Bashkuara me Vendimin 2200 (XXI) të 16 dhjetorit 1966.

[197] I cili përbëhet nga një trup i pavarur ekspertësh për të mbikëqyrur zbatimin e Paktit nga Shtetet Anëtare. Shih: faqen e internetit http://www2.ohchr.org/english/bodies/hrc/index.htm

[198] Komenti i përgjithshëm 16, parag. 1.

[199] Po aty. parag. 10.

3.2 Teksti i Parimeve të O.B.E.ZH (O.E.C.D)[200]

Në vitin 1980 u miratua nga Organizata për Bashkëpunim Ekonomik dhe Zhvillim (O.E.C.D) një tekst jo-detyrues, por në fund të fundit me shumë ndikim në zhvillimin e së drejtës për mbrojtjen e të dhënave personale, që përmban udhëzime në formën e parimeve të përgjithshme.[201] Në fund të viteve 1980 O.E.C.D konsideroi se dallimet që ekzistojnë ndërmjet ligjeve kombëtare mund të pengojnë lëvizjen e lirë të të dhënave personale, me implikime serioze në fusha të tilla si sigurimet dhe bankat. Qëllimi themelor i O.E.C.D natyrisht nuk ishte mbrojtja e të dhënave personale, por krijimi i një kodi ndërkombëtar që do të harmonizonte masat kombëtare për të lehtësuar lëvizjen e dhënave personale.[202] Pra komisioni i ekspertëve rezultoi në një tekst që kishte karakteristika: a. të teknologjisë neutrale, b. jo-detyruese, c. të mos kufizimit të sektorit privat apo publik, d. të njohjes së vlerës që kishte rrjedha e të dhënave ndër-kufitare brenda parimeve të O.E.C.D për zhvillimin e një tregu të lirë, e. prevalenca e parimit të Përgjegjësisë së kontrolluesit, g. të direktivës për Shtetet Anëtare të O.E.C.D, për zbatimin uniform të rregullave dhe parimeve të thjeshta konceptuale gjuhësore.[203] Elementë të cilët në total kanë kontribuar në ndikimin afatgjatë mbi instrumentet e mëvonshme kombëtarë dhe ndërkombëtarë për mbrojtjen e të dhënave personale, që sollën risi në këtë fushë.

Teksti u quajt "Parimet që rregullojnë mbrojtjen e sferës personale të njeriut dhe të rrjedhave tej kufitare të të dhënave personale"[204] dhe përmban 8 parime:

---

[200] Organizata për Bashkëpunim dhe Zhvillim Ekonomik (Organization for Economic Cooperation and Development).

[201] Po aty. Bygrave, L. ,shih: Kabera Karanja, S. (2008). "*Transparency and Proportionality in the Schengen Information System and Border Control Cooperation*", fq.138., pg. 78, gjithashtu dhe González Fuster G. (2014). "*The Emergence of Personal Data Protection as a Fundamental Right of the EU*", fq. 174.

[202] Clarke, R. "*Beyond the OECD Guidelines: Privacy Protection for the 21st Century*", në www .anu.edu.au/people/Roger.Clarke/DV/PP21C.html.

[203] Kirby, M. (2011). "*The history, achievement and future of the 1980 OECD guidelines on privacy*" International Data Privacy Law, fq. 6.

[204] O.E.C.D Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, në http://www.oecd.org/document/18/0,2340,es_2649_34255_1815186_1_1_1_1,00.html

1. Parimi i kohëzgjatjes së kufizuar të mbledhjes së të dhënave personale, duke deklaruar se mbledhja e të dhënave personale duhet të jetë e përpunuar në mënyrë të drejtë dhe të ligjshme, d.m.th. subjektet e përpunimi të jenë në gjendje të japin pëlqimin paraprak, pasi t'i jetë njoftuar shkaku ligjor i përpunimit të të dhënave të tyre.[205]

2. Parimi i cilësisë së të dhënave në mënyrë që të dhënat personale të mbledhura duhet të jenë adekuate, relevante me qëllimet për të cilat ato janë mbledhur, në mënyrë që të kufizojnë sasinë e të dhënave.[206]

3. Parimi i kufizimit të qëllimit sipas të cilit të dhënat personale do të mblidhen për qëllime të caktuara, të qarta dhe legjitime dhe të përpunohen më tej në një mënyrë të përputhshme me këto qëllime. Kjo do të thotë se çdo ndryshim në qëllimin e mbledhjes së të dhënave duhet të shoqërohet nga procedura të ligjshme dhe arsyetimin e këtij ndryshimi, me informimin e njëkohshëm të subjektit të përpunuar dhe shkatërrimin e të dhënave në qoftë se konsiderohet se nuk do të përdoren në të ardhmen.[207]

4. Parimi i kufizimit të përdorimit të të dhënave në mënyrë që të dhënat personale të mos zbulohen apo publikohen për qëllime të tjera përveç atyre të përshkruara në paragrafin e mësipërm. Në këtë rast bëhet futja e dy përjashtimeve, kështu që të ekzistojë mundësia, nëse bëhet me pëlqimin e subjektit ose autorizohet nga ligji.[208]

5. Parimi i marrjes së masave mbrojtëse ku përgjegjësi i përpunimit duhet të marri masat e përshtatshme organizative[209] dhe teknike, si masa për sigurinë e të dhënave dhe mbrojtjen kundër shkatërrimit aksidental ose të paligjshëm të të dhënave.[210]

6. Parimi i transparencës, i cili duhet të udhëheqë politikën dhe praktikat e mbrojtjes së të dhënave personale nga bërja publike e aktiviteteve të përfshira në përpunimin e të dhënave personale.[211]

---

[205] Pargrafi 7 i Tekstit.

[206] Po aty. Pargrafi 8.

[207] Po aty. Pargrafi 9.

[208] Po aty. Pargrafi 10.

[209] Si memorandumi shpjegues që shoqëron tekstin e udhëzimeve. Masa të tilla mund të jenë në sigurinë e ndërtimeve, sigurinë e objekteve, dhe niveleve të autorizimit në hyrje dhe si masa rigoroze teknike që lidhen me sigurinë e sistemit kompjuterik.

[210] Po aty. Pargrafi 11.

[211] Po aty. Pargrafi 12.

7. Parimi i pjesëmarrjes individuale si e drejtë për qasje të subjektit. Ky është ndoshta më i rëndësishmi i këtyre parimeve dhe që siguron ligjshmërinë për përpunimin e të dhënave personale. Pra, personi duhet a) të di nëse procesuesi i të dhënave ka të dhëna në lidhje me të, b) të komunikojë me ta në një kohë të arsyeshme, mënyrë të lirë dhe të kuptueshme, c) t'i jepen shpjegime kur i mohohen pretendimet në përputhje me paragrafët e mësipërm d) të kontestojë nëpërmjet procesit gjyqësor dhe autoriteteve administrative në lidhje me të dhënat e tij dhe të kërkojë fshirjen ose ndryshimin e tyre.[212]

8. Parimi i përgjegjësisë së kontrolluesit sipas të cilit kontrolluesi duhet të bëhet i përgjegjshëm për korrigjimin ose mos zbatimin e rregullave të mëparshme.[213]

Megjithëse ishte përmendur si një tekst jo-ligjërisht detyrues , udhëzimet e bënin një tekst referencë me ndikim të madh në të ardhmen e prodhimit të instrumenteve, që janë projektuar për të mbrojtur të dhënat personale. Ky tekst u bë pikë referimi për zhvillimi dhe për gjeneratën e dytë të legjislacionit evropian, domethënë e ashtuquajtura konventa "108" dhe instrumentet ligjorë të gjeneratës së tretë të tilla si Direktiva 95/46/KE dhe tekste veçanërisht të tilla si Direktiva 2002/58/KE, të cilat përfshijnë të gjitha ose disa nga këto 8 parime në ligjin kombëtar të shteteve anëtare të Bashkimit Evropian. Sidoqoftë, zhvillimet e teknologjisë janë të papërmbajtura. Një tekst i krijuar më shumë se 30 vjet më parë, nuk mund të na japi përgjigje për problemet, siç janë motorët e kërkimit, rrjetet sociale, telefonat e "zgjuar" (smart phones).

Si do të zbatohen parime të tilla si kufizimi i përdorimit të të dhënave, kohëzgjatja e kufizuar e mbledhjes së të dhënave personale në mjedisin e ri teknologjik dhe ekonomik, të ekonomisë së globalizuar dhe ekonomive në zhvillim?[214]

---

[212] Po aty. Pargrafi 13.

[213] Po aty. Pargrafi 11.

[214] Micheal Kirby Kryetari i komisionit të ekspertëve, të cilët hartuan tekstin e "*Parimeve*", ngre një sërë çështjesh në lidhje me fuqinë e primeve të OECD-së, jo vetëm në lidhje me teknologjitë e reja dhe shfaqjen e vendeve të ekonomisë globale që nuk mund të ketë perceptime të njëjta në lidhje me mbrojtjen e të dhënave personale në flukset ndërkufitare. Shih: Kirby, M. (1979). "*O.E.C.D. Guidelines on Privacy*", Law Reform Commission, fq.6.

3.3 Rregullimet në Rendin Juridik Evropian

3.3.1 Konventa Evropiane për të Drejtat e Njeriut

Konventa e Romës për "Mbrojtjen e të drejtave dhe lirive themelore të njeriut", synonte forcimin e të drejtave të përmendura gjithashtu dhe në "Deklaratën Universale të të Drejtave të Njeriut të OKB-së".[215] Ajo u nënshkrua më 4 nëntor të vitit 1950 dhe hyri në fuqi më 3 shtator të vitit 1953.

U ratifikua nga shteti shqiptar me ligjin nr. 8137/31.07.1996 dhe shpallur me dekretin nr. 1573, datë 02.08.1996 të Presidentit të Republikës së Shqipërisë.

Në lidhje me jetën private në nenin 8 paragrafi 1, theksohet se çdo person ka të drejtë për respektimin e jetës private dhe familjare, shtëpisë dhe korrespondencës së tij. Këtë mbrojtje e plotëson paragrafi i dytë, ku ai redukton mbrojtjen në detyrim të shtetit. Ai thekson se nuk do të ketë asnjë ndërhyrje nga një autoritet publik për të ushtruar atë të drejtë, vetëm nëse ndërhyrja parashikohet me ligj dhe është një masë që në një shoqëri demokratike është e nevojshme për sigurinë kombëtare, sigurinë publike, sigurimin e prosperitetit ekonomik të vendit, për mirëmbajtjen e rendit publik, parandalimin e veprave penale, mbrojtjen e shëndetit ose të moralit, ose për mbrojtjen e të drejtave dhe lirive të të tjerëve.[216]

KEDNj është një nga tekstet kryesore referues për mbrojtjen e të drejtave të njeriut në nivelin mbarë evropian[217] dhe u bë një model i mbrojtjes së të drejtave mbi kombëtare të njeriut, që çoi në nënshkrimin e Konventës Amerikane për të Drejtat e

---

[215] Kombet e Bashkuara, Asambleja e Përgjithshme, Sesioni 3. "*Vendimi 217A i Deklaratës Universale të të Drejtave të Njeriut*", 1948, po aty http://www.unhchr.ch/html/menu3/b/a_ccpr.htm

[216] Neni 8 i Konventës ndryshuar nga Protokolli 11, Romë 04. 11. 1959. Teksti gjendet në faqen e internetit të Këshillit të Evropës, në http://conventions.coe.int, si dhe shih: Sarat, A. (2014). "*A World without Privacy*", fq. 242.

[217] Shih: Renucci J.F. (2005). "*Introduction to the European Convention on Human Rights: The Rights Guaranteed and the Protection Mechanism*", Volume 88, fq. 19, gjithashtu shih në lidhje me historinë e Konventës në Roca, J. G. dhe Santolaya, P. (2012). "*Europe of Rights: A Compendium on the European Convention of Human Rights*", fq.17, gjithashtu efekti mbi ligjin e brendshëm, respektivisht shih: në Craig, P. P. dhe Burke, G. (2011). "*The Evolution of EU Law*", fq. 324.

Njeriut në 1969,[218] i Kartës Afrikane të të Drejtave të Njeriut dhe të Drejtave të Popujve 1981[219] dhe Kartën Arabe të të Drejtave të Njeriut në vitin 1994.[220] KEDNj substancionoi këtë mbrojtje duke krijuar mekanizmin e duhur gjyqësor,[221] Gjykatën Evropiane të të Drejtave të Njeriut.[222] Siç vihet në dukje, zbatimi nga Konventa është jo vetëm i të drejtave substanciale, por dhe të drejtës së individit për të apeluar tek mekanizmi gjyqësor, "e cila është një masë e vërtetë revolucionare në shoqërinë ndërkombëtare të pasluftës, një sfidë për një ri negocim sipas realiteteve të reja politike dhe sociale të pozicionit të individit si subjekt i së drejtës ndërkombëtare".[223] Lidhur me të drejtën për jetë private (intimitet), e cila u konsiderua si veprim vetëm drejt shkeljeve të pushtetit shtetëror, por madje edhe në krijimin e "detyrimit pozitiv" të shtetit për të marrë masat e nevojshme për mbrojtjen e privatësisë.[224] Shumë shpejt u njoh që të veprojë dhe mes individëve, ku shtetet kanë përgjegjësinë për shkeljen e të drejtave të njeriut në territorin e tyre.[225] Gjykata Evropiane e të Drejtave të Njeriut (GJEDNj) me një sistem ligjesh (jurisprudencë) konstant, amplifikon fuqinë e Nenit 8, paragrafi 1 i KEDNj-së, zgjeron konceptin e privatësisë dhe specifikon kushtet për heqjen e fshehtësisë te të dhënat e telekomunikacionit në kohët e mjedisit fluid, rrezikues i privatësisë.

---

[218] Konventa gjithashtu e njohur si Pakti i San José është një nga instrumentet ndërkombëtare të të drejtave të njeriut i cili u miratua në vitin 1969, por hyri në fuqi në vitin 1978. Shih: në http:// www .cidh. org/Basicos/English/Basic3.American%20Convention.html, sidomos mbi privatësinë shih nenin 11

[219] http://www.achpr.org/english/_info/charter_en.html

[220] U miratua në Maj 2004 dhe hyri në fuqi në vitin 2008, në http:/ /www 1.umn.edu/ humanrts / instree /loas2005.html?msource=UNWDEC19001&tr=y&auid=3337655 neni 21

[221] Neuwahl, N. A. dhe Rosas, A. (1995). "*The European Union and Human Rights*", fq. 25.

[222] Neni 19 i Konventës, i cili thotë se: "*Për të arritur të sigurohet respektimi i detyrimeve që rrjedhin për Palët e Larta Kontraktuese me anë të kësaj Konvente dhe protokolleve të saj, rekomandohet Gjykata Evropiane e të Drejtave të Njeriut, e emërtuar "Gjykata". Gjykata funksionon me bazë të caktuar*".

[223] Lawson, E. H. dhe Bertucci, M. L. (1996). "*Encyclopedia of Human Rights*", fq. 35.

[224] Bygrave, L. (1998). "*Data Protection Pursuant to the Right of Privacy in Human Rights Treaties*", International Journal Of Law and Information Technology, fq..247.

[225] Bignami, F. (2008). "*The Case for Tolerant Constitiuonal Patriotism: The right to Privacy Before the European Courts*", Cornell International Law Journal, fq. 219, ku përmend çështjen e *Hannover v. Germany* App.No59320/00.

Në mënyrë specifike theksohet se të jetë e ligjshme ndërhyrja në privatësinë e individëve duhet të përmbushen tre kushte:

a. Trajtimi që bëhet nga një autoritet publik duhet të bëhet me autorizim legjislativ dhe t'i bëhet e ditur qytetarit.[226]
b. Qëllimi i intervenimit (ndërhyrjes) të jetë legjitim, pra të jetë në përputhje me rastet e përmendura në nenin 8, par. 2.[227]
c. Të jenë në proporcion me qëllimin që ndiqet d.m.th., nëse do të arrijë objektivat qeveria me këtë ndërhyrje dhe në qoftë se nuk mund të arrijë këtë qëllim me mjete të tjera, si dhe në qoftë se në fund shkalla e rrezikimit të së drejtës për privatësi nuk është e tillë që të imponojë dominimin e së drejtës sipas ligjit.[228]

Nga jurisprudenca e qëndrueshme e GJEDNj-së dhe GJED-së të paharrueshëm janë çështjet e mëposhtme:

Në çështjen Halford kundër Mbretërisë së Bashkuar,[229] një ish police, Allison Halford u ankua se pas ankesave të saj kundër policisë se ka pasur diskriminim në aspektin e ngritjes në detyrë për shkak të seksit të saj, ku dhe telefoni në zyrën e saj ishte përgjuar. Me gjithë kundërshtimet e Qeverisë Britanike se është e drejta e punëdhënësit të monitorojë telefonat e punëmarrësve, GJEDNj-ja konsideroi se kjo është një shkelje e dispozitave të KEDNj-së për privatësinë dhe më veçanërisht paragrafi 1 i nenit 8 të KEDNj-së.

Në çështjen Niemitz kundër Gjermanisë,[230] avokati gjerman u ankimua në GJEDNj për shkak se u urdhërua një hetim për zyrën e tij dhe u konfiskuan dokumente në të. GJEDNj-ja zgjeroi konceptin e "jetës private (privatësisë) dhe reagimit" në çdo aspekt të marrëdhënieve të punës dhe në çdo lloj profesioni apo komunikimi tjetër. Në mënyrë të veçantë u vendos se mohimi i të drejtës për mbrojtjen e privatësisë dhe

---

[226] Bignami, F. (2007). "*Privacy and Law Enforcementin the European Union:The Data Retention Directive*", Chi. J. Int.l Law, fq. 233, gjithashtu shih: Po aty. *Amann v. Switzerland.*

[227] Po aty.

[228] Po aty.

[229] Shih: *Halford v. United Kingdom*.

[230] Shih: *Niemitz v.Germany*.

vendbanimit në hapësirë profesionale do të përbënte trajtim të padrejtë për ata që ushtrojnë në të njëjtën hapësirë aktivitet, i cili nuk mund të klasifikohet lehtësisht si aktivitet shtëpiak apo profesional. Pra GJEDNj-ja vendosi, që jo vetëm pati shkelje të Nenit 8, par. 1 të KEDNj dhe paragrafit të dytë të të njëjtit nen, por duke gjykuar se ndërhyrja e autoritetit publik nuk ishte një operacion që justifikohet nga kushtet dhe parimi i proporcionalitetit sipas nenit 8, par. 2 të KEDNj.

Në çështjen Copland kundër Mbretërisë së Bashkuar,[231] nëpunësja e administratës së një Kolegji, bëri një ankimim në Gjykatën Evropiane të të Drejtave të Njeriut, sepse administrata e Kolegjit kishte bërë përgjimin e komunikimeve elektronike (telefon, internet dhe e-mail) të saj, në vendin e punës, d.m.th. në Kolegj. Në këtë rast, Mbretëria e Bashkuar, duke përfaqësuar Kolegjin, argumentoi se përgjimi është bërë për të përcaktuar nëse ankuesja, përdori të mirat e Kolegjit, për përfitime të saja personale apo për përmbushjen e detyrave të punës. GJEDNj-ja u shpreh mbi natyrën e monitorimit dhe argumentoi se ky përfshinte analizimin e llogarive ekzistuese telefonike të Kolegjit dhe jo përmbajtjen e bisedave telefonike ose analizimin e përmbajtjes së faqeve Web të vizituara nga ankuesja. GJEDNj pasi deklaroi se Mbretëria e Bashkuar është përgjegjëse për operacionet e Kolegjit, si një autoritet publik sipas nenit 8 të KEDNj ku rezulton se në këtë shtet kolegji është subjekt administrativ. Në fund vendosi që komunikimet elektronike të individëve (ndër të cilat në mënyrë eksplicite interneti dhe e-mail) sipas konceptit të privatësisë, gëzojnë mbrojtjen e nenit 8 të KEDNj, pavarësisht nëse ndodhin në një ambient profesional ose jo-profesional (Vendimet Niemitz v. Gjermanisë, Halford v. Mbretërisë së Bashkuar dhe nga Amann v. Zvicrës). Në mënyrë të veçantë, GJEDNj hodhi poshtë pretendimet e qeverisë britanike, duke pranuar njërën anë, se koncepti i mbrojtjes së ofruar nga neni 8 i KEDNj, përtej përmbajtjes të komunikimit, rrjedhin dhe elementët e jashtëm të saj, të cilët në fakt janë "një element integral i komunikimit telefonik" (Çështja Malone kundër Mbretërisë së Bashkuar). Ndërsa në anën tjetër, edhe pse përvetësimi i këtyre të dhënave u bë ligjërisht përmes listave të detajuara të thirrjeve telefonike, kjo nuk ishte arsye për të mos zbatuar nenin 8 të KEDNj. Së fundi, GJEDNj vuri në dukje se ruajtja e të dhënave personale në lidhje me jetën private të individit, edhe nën mbrojtjen e nenit 8 të KEDNj,

[231] Shih: *Copland v. United Kingdom.*

duhet zbatuar, pavarësisht edhe nëse ato u shpallën (u publikuan) për palët e treta ose u përdorën kundër ankimueses në procedurat disiplinore apo procedura të tjera.

Çështja Malone kundër Mbretërisë së Bashkuar,[232] u bë një piketë për Ligjin e mbrojtjes së të dhënave personale, GJEDNj konsideroi se gjatë mbikëqyrjes së bisedave telefonike të ankuesit nga ana e policisë, është shkelur nenin 8 i Konventës Evropiane për të Drejtat e Njeriut, sepse arkivat e regjistrimit përmbanin informacion, veçanërisht numrat e thirrjeve elektronike, të cilët janë në përputhje me gjykatën "elementi integral i telekomunikimeve të kryera me telefon" Kështu, Gjykata qartazi deklaroi se "elementet e jashtëm" të komunikimit janë pjesë e konceptit dhe sferës mbrojtëse të konfidencialitetit.

Çështja Lindquist kundër Suedisë,[233] çështja Bodil Lindquist e Gjykatës Evropiane të Drejtësisë nuk jep përgjigje të qarta duke i lënë liri veprimi çdo shteti për balancimin e të drejtave në konflikt. Veçanërisht në këtë çështje, GJED duhet t'iu ishte përgjigjur dy pyetjeve. Së pari, nëse referenca për persona në faqet e internetit, me informacion në lidhje me punën e tyre dhe zakonet e tyre janë përpunim i të dhënat personale sipas nenit 3 të Direktivës dhe së dyti, nëse përpunimi në faqet e internetit përbën transferim në vendet e treta si akt i paautorizuar në përputhje me nenin 25.

Në Suedi znj. Lindquist, krijoi një faqe personale në internet që përmbante informacion për jetën e kolegëve të saj, si emrat dhe profesionet e tyre madje edhe të dhënat e tyre mjekësore. Megjithatë, ajo nuk arriti të informojë ata për veprimet e mësipërme dhe gjithashtu të informojë autoritetin kombëtar për mbrojtjen e të dhënave personale në Suedi. Kur kolegët e saj deklaruan pakënaqësinë e tyre, ajo hoqi të dhënat nga interneti. Prokurori e akuzoi për shkelje të ligjit për mbrojtjen e të dhënave personale sepse përpunoi të dhëna personale me mjete automatike, pa njoftim paraprak, përpunoi të dhëna të ndjeshme personale dhe të dhënat personale të transferuan në një vend të tretë pa pëlqimin e dhënë. Dispozitat e zbatueshme ishin nenet 1,2,3,8,9 dhe 25 të Direktivës 95/46/KE. Në mënyrë të veçantë, neni 1 përkufizon Qëllimin e Direktivës, i cili është mbrojtja e qytetarëve kundër shkeljes së të dhënave të tyre personale, neni 2

---

[232] Në çështjen *Malone v. United Kingdom*, judgment of 2 August 1984, Series A no. 82, pg. 30-31, par. 64; në http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=695410&portal = hbkm & sour ce=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649

[233] *Lindquist v. Sweden.*

përmban definicionet, neni 3 përcakton fushëveprimin e Direktivës, neni 8 i referohet të dhënave personale në lidhje me shëndetin, neni 9 përcakton përjashtimet, dhe më në fund neni 25 i referohet transferimit të të dhënave tek të tretët. Së fundi, legjislacioni kombëtar për mbrojtjen e të dhënave personale është më i rreptë se regjimi i mbrojtjes së të dhënave të BE-së: Direktiva parashikon harmonizimin e plotë, kështu Shtetet anëtare duhet të miratojnë legjislacionin kombëtar konform regjimit të Direktivës. Megjithatë, dispozita të caktuara të Direktivës, në mënyrë eksplicite mund të autorizojnë Shtetet Anëtare, të miratojnë regjime më të kufizuara të mbrojtjes. Kjo duhet të bëhet në përputhje me objektivin e ruajtjes së një ekuilibri ndërmjet lëvizjes së lirë të të dhënave personale dhe mbrojtjes së jetës private. Përveç kësaj, shtetet anëtare duhet të mbeten të lira për të rregulluar fushat, përjashtuar nga qëllimi i zbatimit të Direktivës në mënyrën e vet, me kusht që asnjë dispozitë tjetër e ligjit të BE të përjashtojë atë.

Në vendimin K.U kundër Finlandës, GJEDNj trajtoi mundësinë e mbrojtjes së privatësisë së individëve në hapësirën kibernetike (cyberspace).[234] Në mënyrë të veçantë, prindërit e të miturit të cilit informacioni personal, i ishte postuar në një faqe interneti për takime erotike, pa pëlqimin e tij, apeluan duke përfaqësuar atë në GJEDNj pas mohimit të shërbimit server për të zbuluar kush i vendosi të dhënat personale të të miturit në këtë faqe interneti dhe përligjjen e mëvonshme të tij nga drejtësia finlandeze për shkak të legjislacionit finlandez për mbrojtjen e konfidencialitetit, i cili ndalon zbulimin e të dhënave të kryerësit të shkeljes. GJEDNj në këtë rast vendosi që "jeta private" është një çështje që mbulon identitetin "fizik dhe moral" të individit, të cilën shteti është i obliguar që ta mbrojë atë, kur nuk është duke u respektuar dhe arriti në përfundimin se ka pasur shkelje të Neni 8 të KEDNj, për shkak të mungesës së legjislacionit në Finlandë, i cili i jep prioritet mbrojtjes së privatësisë në lidhje me konfidencialitetin e komunikimit.[235]

Në vendimin më të fundit Agjencia e Mbrojtjes së të dhënave Personale, Mario Gonzales kundër "Google" Spanjë, Gjykata Evropiane e Drejtësisë, me vendimin e

---

[234] *K.U. v. Finland* (Application no. 2872/02), 2 December 2008. Shih: vendimin në http://www.garanteprivacy.it/garante/document?ID=1620370 dhe shih përmbledhjen e vendimit në http://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/KU%20v%20Finland%20en%20presse.pdf

[235] Po aty. *K.U. v. Finland para. 46- 50*

marrë së fundmi, detyron gjigantin e internetit “Google” të ndryshojë disa prej rezultateve të kërkimit me kërkesë të individëve të prekur prej tyre, që ndryshe quhet “e drejta për t’u harruar”.

Vendimi i GJED ishte në përputhje me interpretimin që i bëri Agjencia e Mbrojtjes së të Dhënave Personale Direktivës 95/46. Në shqyrtimin nëse Google ishte subjekt i Direktivës si kontrollues i të dhënave, gjykata konstatoi se aktivitetet e një motori kërkimi, përbëjnë përpunim e të dhënave.[236] Sipas gjykatës, të gjitha linqet e parëndësishme e të pa rifreskuara duhet të fshihen, sipas kërkesës së vetë qytetarëve. Fillimisht çështja u publikua nga një qytetar spanjoll Mario Gonzales, i cili ankohej se një njoftim ankandi për shtëpinë e tij, që vazhdon ende të shfaqet sot pas 16 vjetësh në “Google” shkelte privatësinë e tij.[237] Mbështetësit e së drejtës për t’u harruar” e konsiderojnë një fitore këtë vendim, që “Google”-n vet e ka lënë të zhgënjyer. Gjykata për dhënien e këtij vendimi u bazua në Direktivën 95/46 “Për mbrojtjen e individëve nga përpunimi automatik i të dhënave personale.

Komisioni Evropian propozoi një ligj duke i dhënë të drejtë përdoruesve të drejtën për t’u harruar në 2012-ën, por vetëm sot Gjykata theksoi se tashmë, njerëzit kanë të drejtën të kërkojnë që informacioni i tyre të zhvendoset e të fshihet përfundimisht.

A mundet vërtet kushdo, që nuk e pëlqen një histori të vjetër, thjesht të bëjë kërkesë, dhe ajo të zhduket? Rasti duhet të jetë pikërisht ky: vendimi i Gjykatës Evropiane të Drejtësisë tregon se të drejtat e individit vijnë në plan të parë, kur vjen puna te kontrolli i të dhënave të tyre personale.

3.3.2 Më të rejat nga Legjislacioni Evropian

Në vazhdim të KEDNj, shtetet evropiane të përballura me zhvillimet teknologjike që çuan në rritjen e mbështetjes për përpunimin automatik të të dhënave

[236] Direktiva përcakton përpunimin e të dhënave si "çdo veprim ose një sërë veprimesh të cilat kryhen në të dhënat personale, nëse janë apo jo më mjete automatike, të tilla si mbledhja, regjistrimi, organizimi, ruajtja, adaptimi apo ndryshimi, rikthimi, konsultimi, shfrytëzimi, zbulimi i transmetuar, përhapja ose vënia në dispozicion, shtrirja ose kombinimi, bllokimi, fshirja ose shkatërrimi. "Direktiva e Këshillit 95/46, shënim 1, arti. 2 (b), në 38 (theksi i shtuar).

[237] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, në http://curia.europa.eu/juris/liste.jsf?num=C-131/12

personale, filluan të krijojnë legjislacione, të cilët bazohen në parimet e mbrojtjes së të drejtave të njeriut. Ata përballen ende me problemin brenda rregulloreve të specializuara. Pra, në vitet 1970, vende të ndryshme evropiane si Gjermania, Suedia dhe Franca bënë krijimin e legjislacioneve të ashtuquajtura "gjenerata e parë", të cilat ishin rregulloret e para për mbrojtjen e të dhënave personale.[238] Gjatë dekadës së viteve 1980, u krijuan legjislacionet e para të ashtuquajtura "gjenerata e dytë", në mënyrë që t'i përgjigjen zhvillimeve të vazhdueshme të teknologjisë, të cilat krijuan një fushë të re në rrezikimin e të dhënave personale.[239] Kështu u krijuan dy nisma të mëdha legjislative, të tilla si Konventa e Strasburgut 28.01.1981, "Për Mbrojtjen e Individëve në Lidhje me Përpunimin Automatik të të Dhënave Personale që quhet "Konventa 108" dhe "Marrëveshja Shengen" për heqjen e kontrolleve në kufijtë e brendshëm ndërmjet vendeve që e kishin nënshkruar atë.

Por transformimi i teknologjisë dhe konvergjenca e teknologjive të informacionit dhe të telekomunikimit vështirësoi akoma dhe më shumë kontrollin e ligjshëm dhe të drejtën e përpunimit të të dhënave personale. Pra kështu u krijua legjislacioni i "gjeneratës së tretë", ku përmes një qasjeje të gjerë konceptuale, teknologjikisht neutrale, u përpoq dhe u përball me problemet aktuale dhe të ardhshme të mbrojtjes së të dhënave personale dhe privatësisë, duke i vendosur ato në legjislacionin komunitar (acquis) dhe në këtë mënyrë zhvilloi mbrojtjen, si detyrim komunitar i Shteteve Anëtare të BE-së.

3.3.2.1 Legjislacionet Evropiane të "Gjeneratës së parë"

Përpjekja e parë legjislative në nivel shtetëror në Evropë për mbrojtjen e të dhënave personale u mbajt në Gjermani në vitin 1970, ligji për mbrojtjen e të dhënave personale i Landit të Hesenit. Ky ligj ishte pionier në krijimin e një autoriteti të pavarur rregullator dhe shprehu logjikën rregullatore që ekzistonte në Gjermani, ku ndërhyrja rregullatore e një shteti i cili synon të rregullojë sjelljet, duhet të mbështetet nga parimet rregullatore për të mbrojtur të drejtat e individëve kundrejt shtetit.[240] Në vazhdim Suedia

[238] Rule, J. B. dhe Greenleaf, G. W. (2010). "*Global Privacy Protection: The First Generation*". fq. 19.

[239] Po aty. fq.41.

[240] Hessisisches Datenschutzgeset, Gesetz und Verordungsblatt I. (1970), fq. 625, siç raportohet dhe në Burkert, H. "*Privacy and Data Protection- A German/European Perspective*", në http://www.mpp-rdg .mpg . de/pdf_dat/burkert.pdf

ishte ndër të parat shtete në krijimin e legjislacionit, ku në vitin 1973 miratoi Ligjin për mbrojtjen e të dhënave personale (Datalag) dhe krijimit të një autoriteti mbikëqyrës për të mbikëqyrur përpunimin e automatizuar të të dhënave, bërë ose nga shteti apo një subjekt privat.[241] Ndërhyrjet legjislative sigurisht që kishin karakteristikë të përbashkët se nuk u përpoqën të blindojnë mbrojtjen e të drejtës themelore të privatësisë dhe mbrojtjes së të dhënave personale, aq sa të ndërhyjnë në funksionimin e duhur, të sigurt dhe të saktë "të bazave të të dhënave", që ishin shpërndarë në zona të ndryshme administrative të shteteve, pa qenë e lehtë për qeveritë qendrore, që të kontrollojnë organizimin e duhur të përpunimit të të dhënave.[242] Në gjysmën e dytë të viteve 1970 ka pasur ndërhyrje të tjera legjislative nga Franca, Austria dhe Norvegjia. Në Francë në vitin 1978 u miratua Ligji nr. 78-17 në lidhje me të dhënat, arkivat dhe liritë e njeriut dhe themeloi një Komision Kombëtar i cili është një organ kolektiv shumë anëtarësh i përbërë nga zyrtarë të lartë qeveritarë. Ky komitet, i njohur si "Commission Nationale de l'information et des libertes", kishte pavarësi organizative dhe funksionale nga ekzekutivi dhe ishte standard ndërkombëtar i autoritetit të pavarur publik, përgjegjës për ruajtjen e të drejtave individuale nga ana e përpunimit të të dhënave personale.[243] Nismave të tjera të ndërmarra ishin nga Austria me "Datenschutzgesetz BGBl. 565/1978" dhe Norvegjia me "Lov om personregistre av 9 juni 1978 nr. 48". Karakteristikë e këtyre nismave legjislative ishte se shkuan një hap më tej se reformat legjislative gjermane dhe suedeze pasi njohën të drejtën e individit në menaxhimin e informatave personale dhe të drejtën për të refuzuar përpunimin e të dhënave personale për qëllime specifike.[244]

---

[241] Soren O. "*Protection of Personal data –But How?*", në http ://www. Itkommissionen .se/dynamaster /file_archive/030121/991899fe86e3aecaa92d4e5730148f50/5.1%20%20Security%20and%20Vulnerability%20-%20S%F6ren%20%D6man.pdf

[242] Mayer-Schönberger V.(1997).*"Generational Development of Data Protection in Europe*" in Philip Agre dhe Marc Rotenberg (eds), "*Technology and Privacy: The New Landscape*", MIT Press, Cambridge, fq.219.

[243] Noorda, C., Noorda, C. W. dhe Hanloser, S. (2011). "*E-discovery and Data Privacy: A Practical Guide*". fq.105.

[244] Lindsay, D. (2005). "*An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law*" 29 Melbourne University Law Review, fq. 179.

3.3.2.2 Legjislacionet Evropiane të "Gjeneratës së dytë"

3.3.2.2.1 Konventa 108

Brenda kushteve të zhvillimeve të shpejta në teknologjitë e informacionit dhe të komunikimit u bë gjithnjë e më e kuptueshme se Neni 8 i KEDNj nuk mjaftonte për të mbrojtur të dhënat personale dhe të privatësisë, të cilat ishin në mjedisin e rrezikut.[245] Dëshira për një instrument modern që i përgjigjet nevojës për specifikimin e parimeve për përpunimin e të dhënave personale dhe të drejtave të subjekteve të këtij trajtimi, çoi në miratimin e Konventës së Strasburgut. Konventa e Strasburgut 01.28.1981 "Për mbrojtjen e individëve në lidhje me përpunimin automatik të të dhënave personale" është instrumenti i parë ligjor ndërkombëtar dhe detyrues ndërkombëtarisht për mbrojtjen e të dhënave personale.[246] Në nenin e parë përcaktohet qëllimi i kësaj Konvente, që është të sigurojë në territorin e secilës palë dhe për çdo individ, pavarësisht nga kombësia apo vendbanimi, respektimin e të drejtave dhe lirive të tij themelore dhe në veçanti të drejtën për privatësi, në lidhje me përpunimin automatik të të dhënave personale që lidhen me të ("mbrojtja e të dhënave").[247] Konventa themeloi parimet e përgjithshme të cilat duhet të drejtojnë përpunimin automatik të të dhënave personale dhe që u bënë Udhërrëfyes për legjislacionin pasues sekondar në nivel kombëtar dhe të BE-së, të tilla si parimi i ligjshëm i mbledhjes dhe përpunimit, parimi i specifikimit dhe i qëllimit të drejtë të përpunimit, parimi i domosdoshmërisë së përpunimit, parimit të saktësisë së të dhënave, parimi i kohës së caktuar të ruajtjes së të dhënave.[248] Në veçanti, Neni 5 i Konventës 108 thekson që të dhënat duhet të jenë:

a) Fituar dhe të bëhet përpunimi i tyre në një mënyrë të ligjshme dhe të drejtë,[249] që do të thotë se, ose subjektet e të drejtave të tilla duhet të japin pëlqimin për këtë

---

[245] Shih: Preambulën e Konventës 108.

[246] Shqipëria e firmosi Konventën e Strasburgut të datës 01.28.1981, në 9/6/2004, e ratifikoi në 14/2/2005 dhe hyri në fuqi në 1/6/2005.

[247] : "..... *është të sigurojë në territorin e secilës palë dhe për çdo individ, pavarësisht nga kombësia apo vendbanimi, respektimin e të drejtave dhe lirive të tij themelore dhe në veçanti të drejtën e tyre për privatësi, në lidhje me përpunimin automatik të të dhënave personale që lidhen me të"*. ("mbrojtja e të dhënave") Teksti në faqen e internetit të Këshillit të Evropës, http ://convention s. coe. int/ Treaty / EN /Treaties/Html/108.htm

[248] http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm

[249] Neni 5, para.1 Konventës 108.

përpunim, ose legjislacioni duhet të përcaktojë kushtet dhe qëllimet e mbledhjes dhe përpunimit.[250]

b) Të ruhen dhe të mbahen vetëm për qëllime të specifikuara dhe legjitime dhe të mos përdoren në asnjë mënyrë të papërputhshme me ato qëllime,[251] në mënyrë që të kufizohet sasia dhe llojet e informacioneve të përpunuara.
c) Të jenë adekuate, relevante dhe jo të tepërta nga ç'është e nevojshme në dritën e objektivave të kërkuara për të cilat ruhen.[252]
d) Të jenë të sakta dhe në çdo rast që është e nevojshme, të përditësohen.[253]
e) Në fund të dhënat jo vetëm duhet të jenë të nevojshme për të arritur qëllimet për të cilat përpunohen, por do të mbahen vetëm për kohën e nevojshme të kërkuar, kështu përtej kësaj nuk duhet të jetë e mundur përcaktimi i subjektit të cilit i takon.

Gjithashtu për shkak të përpunimit të të dhënave personale, mund të zbulojnë origjinën racore, bindjet politike dhe fetare, informacion mbi shëndetin, jetën seksuale dhe bindjet kriminale, gjithashtu të merren masa mbrojtëse përkatëse.[254] Vetë konventa në nenin 8 parashikon një seri të të drejtave themelore të subjektit të përpunimit, të tilla si të drejtën e informimit për qëllimet e mbajtjes së arkivave të të dhënave, e drejta e ndreqjes ose fshirjes së të dhënave të tilla. Në vazhdim, pasi Konventa 108 u inkorporua në ligjet kombëtare të shteteve anëtare, u paraqit nevoja për harmonizimin e ligjeve kombëtare, sepse përfundimisht u bë e qartë se ka pasur dallime në Shtetet Anëtare për sa i përket nivelit të mbrojtjes së të drejtave dhe lirive të individëve, sidomos të drejtën për privatësi lidhur me përpunimin e të dhënave të karakterit personal. Problemi ishte se ato dallime pengonin transmetimin e të dhënave të tilla nga territori i njërit në territorin e një Shteti tjetër Anëtar dhe për këtë arsye u krijuan pengesa për aktivitetet e shumta ekonomike në nivel Komunitar.[255] Nevoja për krijimin

[250] Chalmers, D., Davies, G. dhe Monti, G. (2010). "*European Union Law: Cases and Materials*", fq 133.

[251] Po aty. Neni 5, para.2.

[252] Po aty. Neni 5, para.3.

[253] Po aty. Neni 5, para.4.

[254] Po aty. Neni 6.

[255] Campbell, D. (2007). "*The Internet 2007: Laws and Regulatory Regimes*", fq. 98, shih dhe Janssen, K. dhe Crompvoets, J. (2013). "*Geographic Data and the Law: Defining New Challenges*", fq. 98, shih dhe

e ligjit primar komunitar çoi në miratimin e Direktivës së parë komunitare për mbrojtjen e harmonizuar të të dhënave personale, Direktiva 95/46/KE.

3.3.2.2.2 Marrëveshja Shengen

Në kuadër të kërkimit të mënyrave për realizimin e parimit komunitar të lëvizjes së lirë të personave brenda Komunitetit Evropian, në vitin 1985, Franca, Gjermania, Belgjika, Luksemburgu dhe Holanda vendosën krijimin e zonës "Shengen".[256] Me Traktatin e "Shengenit", Shtetet Anëtare duhet të shfuqizojnë kontrollet e brendshme kufitare ndërmjet vendeve që kanë nënshkruar atë. U krijua një kufi i vetëm i jashtëm, ku realizohen kontrollet e hyrjeve në zonën Shengen.[257] Në të njëjtën kohë u përcaktuan rregullat e përbashkëta për vizat, azilin dhe kontrollin në kufijtë e jashtëm për të lejuar lëvizjen e lirë të personave brenda vendeve që kanë nënshkruar marrëveshjen.[258] Për të kompensuar mungesën e sigurisë që do të rezultonte nga qarkullimi i lirë, ai krijoi Sistemin Elektronik të Informacionit Shengen SIS (Schengen Information System).[259] SIS është një bazë të dhënash komplekse që u lejon autoriteteve kompetente të Shteteve

---

Karanja, S. K. (2008). "*Transparency and Proportionality in the Schengen Information System and Border Control Cooperation*", fq. 142.

[256] Emri i qytetit në Luksemburg ku janë nënshkruar marrëveshjet e para.

[257] Zona Shengen u zgjerua ngadalë me të gjitha Shtetet Anëtare. Italia nënshkroi marrëveshjet në 27 nëntor të vitit 1990, Spanja dhe Portugalia në 25 qershor 1991, Greqia në 6 nëntor 1992, Austria më 28 prill 1995, Danimarka, Finlanda dhe Suedia në 19 dhjetor 1996. Estonia, Republika Çeke, Lituania, Hungaria, Letonia, Malta, Polonia, Sllovakia dhe Sllovenia hynë në zonën Shengen në 21 dhjetor 2007. Më 28 shkurt 2008, u nënshkrua një protokoll për pjesëmarrjen e Lihtenshtajnit në hapësirë dhe më në fund u bashkuan Zvicra në 12 dhjetor, 2008. Gjithashtu në përputhje me Protokollin aneksuar Traktatit të Amsterdamit, Irlanda dhe Mbretëria e Bashkuar mund të marrin pjesë në të gjitha ose një pjesë e dispozitave të acquis Shengen. Pra, Mbretëria e Bashkuar bashkëpunon në aspekte që lidhen me policinë, bashkëpunimin gjyqësor në çështjet kriminale, luftën kundër drogës dhe Sistemin e Informacionit Shengen (SIS). Në vitin 2011 u bë dhe pranimi i Bullgarisë dhe Rumanisë në Traktat.

[258] Po aty. Karanja, S. K. (2008). fq. 132, gjithashtu shih: Brouwer, E. R. (2008). "*Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*", fq. 186 dhe Boehm, F. (2012). "*Information Sharing and Data Protection In the Area of Freedom, Security and Justice-Towards Harmonised Data Protection Principles for Information Exchange at EU-level*", fq. 260.

[259] Colvin, M. (2000). "*The Schengen Information System: A Human Rights Audit : a Justice Repor*t", fq 68.

Shengen shkëmbimin e të dhënave për kategori të caktuara të personave dhe mallrave.[260] Në veçanti, baza e të dhënave përmban informacion mbi personat e kërkuar, të huajt e padëshiruar, personat që kanë nevojë për mbrojtje gjyqësore, automjetet e vjedhura, etj., në mënyrë që të jetë i përshtatshëm koordinimi mes policisë, doganave dhe autoriteteve gjyqësore në trajtimin dhe luftimin e krimit të organizuar dhe terrorizmit.

Për sa i përket mbrojtjes së të dhënave personale të personave të cilat lëvizin, u parashikua detyrimi i Shteteve Anëtare për të nxjerrë ligje për mbrojtjen e të dhënave personale, duke siguruar një nivel të mbrojtjes ekuivalente me atë që rezulton nga "Konventa 108" dhe krijimin e autoritetit mbikëqyrës përkatës i cili duhet ta sigurojë. Shqipëria pas miratimit të ligjit nr. 9887, datë 10.03.2008, ndryshuar me ligjin nr. 48/2012 "Për mbrojtjen e të dhënave personale" (në pajtim me Direktivën 95/46/EK), vazhdoi më tej me iniciativa për të krijuar kuadrin e nevojshëm ligjor për mbrojtjen e të dhënave personale të qytetarëve dhe për krijimin e kushteve në përfshirjen e vendit tonë në sistemin e mirëkuptimit Shengen pas liberalizimit të vizave me BE.

3.3.2.3 Legjislacionet Evropiane të "Gjeneratës së tretë"

3.3.2.3.1 Direktiva 95/46/KE[261]

Mbrojtja e të dhënave personale në Komunitetin Evropian gjeti shprehjen e vet me ndërhyrjen e ligjit në fushën e së drejtës sekondare Komunitare.[262] Në vitin 1995 u miratua Direktiva 95/46/KE, si një kuadër i përgjithshëm për mbrojtjen e të dhënave

---

[260] Carrera, S. Wiesbrock, A. (2009) "*Civic Integration of Third-Country Nationals Nationalism versus Europeanisation in the Common EU Immigration Policy*", fq. 16, në http: //www.google.al/ url?sa=t&rct=j&q=& esrc= s&source=web &cd=2&ved=0CC0QFjAB& url=http%3A%2F%2Faei. Pitt .edu% 2F15100 %2F0 1%2FENACT_report_on_integrating_TCNs_e-version _final.pdf&e i= Jq3 dUeK qHcTasga ZyYGY Ag&u sg=AFQjCNGLgNgR_8HrWtN-4Auxsr89B12mTw&bvm =bv .4870 5608 ,d .Yms

[261] Bergkamp, L. dhe Dhont, J. (2002). "*Data Protection in Europe and the Internet: An Analysis of the European Community's Privacy Legislation in the Context of the World Wide Web*", fq. 34, gjithashtu Elgesem, D. (1999). "*The structure of rights in Directive 95/46EC on the protection of individuals with regard to the processing of personal data and the free movement of such data*", Ethics and Information Technology, fq. 283.

[262] Kaczorowska, A. (2013). "*European Union Law*", fq. 215.

personale të bazuara në kodifikimin e Konventës së Strasburgut 28.1.1981 "Për mbrojtjen e individëve nga përpunimi automatik i të dhënave personale".[263]

Baza ligjore e saj ishte Neni 100a (tani Neni 95) i Traktatit të Bashkimit Evropian, por shpallja e Kartës së të Drejtave Themelore të Bashkimit Evropian[264] nga Parlamenti Evropian, Këshilli dhe Komisioni në dhjetor të vitit 2000 dhe në veçanti Neni 8 i Kartës i cili parashikon të drejtën për mbrojtjen e të dhënave, që vendos theksin më shumë në dimensionin e "mbrojtjes së të drejtave themelore" të Direktivës. Me Direktivën 95/46/KE të Parlamentit Evropian dhe Këshillit, Bashkimi Evropian ka fituar njërin prej teksteve më të qëndrueshëm dhe të detajuar, që ndikuan dhe ndikojnë në botën ndërkombëtare të prodhimit rregullator mbi mbrojtjen e privatësisë.[265] Qëllimi i Direktivës ishte për të mbrojtur të drejtat dhe liritë e individëve në lidhje me përpunimin e të dhënave personale,[266] si një parakusht për funksionimin normal të tregut të brendshëm,[267] nga i cili kërkohet jo vetëm mundësia e lëvizjes së të dhënave personale në mes të Shteteve Anëtare, por dhe mbrojtja e të drejtave themelore të individit në mënyrë uniforme në të gjitha Shtetet Anëtare.[268] Kjo mbrojtje mund të arrihet vetëm duke përcaktuar parimet udhëzuese që përcaktojnë ligjshmërinë e përpunimit të të dhënave personale. Neni 32 i Direktivës u dha Shteteve Anëtare një periudhë prej tre vitesh për t'u përshtatur me këto rregulla, të cilat në bazë të nenit 249 (ish 189) i TEK, obligoheshin për zbatimin e menjëhershëm dhe të plotë.[269] Direktiva në përputhje me "Konventën 108" përmban parimet udhëzuese për përpunimin e të dhënave personale.

---

[263] Direktiva 95/46/KE e Parlamentit Evropian dhe e Këshillit e 24 .10.1995 "*Për mbrojtjen e individëve në lidhje me përpunimin e të dhënave personale dhe mbi lëvizjen e lirë të këtyre të dhënave*", EUR Lex 281, 23.11.1995, fq.31.

[264] Shih: në http://europa.eu.int/comm/justice_home/unit/charte/index_en.html

[265] Direktiva 95/46/KE e Parlamentit Evropian dhe e Këshillit e 24 .10.1995 për mbrojtjen e individëve në lidhje me përpunimin e të dhënave personale dhe mbi lëvizjen e lirë të këtyre të dhënave, EUR Lex 281, 23.11.1995, fq.31.

[266] Po aty. Neni 1, paragrafi 1.

[267] Sipas nenit 7 të Traktatit, sigurohet lëvizja e lirë e mallrave, personave, shërbimeve dhe kapitalit.

[268] Opinion shpjegues 3 i Direktivës 95/46/KE.

[269] Loukeri, G. (1997)."*Harmonization of law on the protection of individuals against the processing of personal data in the European Union*", fq. 547.

Këto parime udhëzuese lidhen me:

1. Cilësinë e të dhënave, d.m.th. të dhënat e karakterit personal duhet specifikisht të jenë subjekt i përpunimit të drejtë dhe të mblidhen për qëllime specifike, të qarta dhe legjitime. Ato gjithashtu duhet të jenë të sakta dhe kur është e nevojshme, të përditësuara.[270]
2. Përpunimin e ligjshëm e të dhënave, pra përpunimi i të dhënave personale nuk mund të bëhet vetëm nëse personi i cili zotëron të dhënat ka dhënë shprehimisht pëlqimin e tij[271] ose nëse përpunimi është i nevojshëm në veçanti në rastet e pretenduara.

Veçanërisht rregullimi i miratimit të mëparshëm ndoshta ishte ndërhyrja më e rëndësishme legjislative dhe rregullimi i një rëndësie të veçantë për ruajtjen dhe rritjen e ndikimit të mbrojtjes së të dhënave me ndikim global, në kontrast me kuadrin rregullator amerikan për mbrojtjen e të dhënave personale, ku parimi i opt - out, gjatë të cilit subjektet e trajtimit të kenë mundësi të refuzojnë përdorimin e të dhënave personale të tyre nëse ata dëshirojnë.[272] Direktiva gjithashtu prezanton konceptin e të dhënave personale të ndjeshme duke përshtatur kategoritë specifike për të cilat në parim ndalohet përpunimi i të dhënave personale të tilla si origjina racore ose etnike, mendimet politike, fetare ose filozofike, anëtarësimi në sindikata, shëndeti dhe jeta seksuale.[273]

Më pas parimi i vetëvendosjes informative është realizuar me dhënien e së drejtës për qasje në të dhëna të këtyre individëve[274] dhe futjen e të drejtës për korrigjim, fshirjen ose bllokimin e të dhënave të të tretëve,[275]gjithashtu të drejtën për të

---

[270] Po aty. Neni 6 paragrafi 1.

[271] Pëlqimi konsiderohet në përcaktim të nenit 2 të Direktivës si "*çdo dekleratë e qëllimtë, e lirshme, specifike dhe e informuar, me të cilin personi për të cilin kanë të bëjnë të dhënat pranon përpunimin e të dhënave personale lidhur me të*".

272 Bouckaert, J.M.C. dhe Degryse, H.A. (2006). "*Opt In versus Opt Out: A Free-Entry Analysis of Privacy Policies*", Discussion Paper 2006-96, Tilburg University, Center for Economic Research, në http://weis2006.econinfosec.org/docs/34.pdf. E shohim si një mundësi që me siguri është ajo që kompanitë duan që në studimet e kryera në SHBA, vetëm një përqindje e vogël që kanë marrëdhënie, përfundimisht refuzojnë përdorimin e të dhënave të tyre personale pasi ata tashmë kanë bërë përdorimin e një tjetër shërbimi që ofrohet tashmë.

[273] Neni 8 paragrafi 1 i Direktivës 95/46/KE.

[274] Po aty. Neni 12.

[275] Po aty. Neni 10.

kundërshtuar përpunimin e të dhënave.[276] Në Direktivë zhvillohen dispozita shumë të rëndësishme ku parashikojnë se lejohen transferimet e të dhënave personale nga Shteti Anëtar te një vend i tretë,[277] me kusht që vendi i tretë të ketë një nivel të përshtatshëm të mbrojtjes.[278] Kjo vendosje është karakterizuar si veçanërisht e rëndësishme për shkak të rëndësisë së veçantë që i jepet rrjedhjes ndërkufitare të të dhënave personale, si një mjet për zhvillimin e tregtisë ndërkombëtare.[279] Mjaftueshmëria e një mbrojtje të tillë dhënë nga vendi i tretë duhet të vlerësohet duke marrë parasysh të gjitha rrethanat që rrethojnë një operacion të transferimit të të dhënave ose grupin e transferimit të të dhënave. Në veçanti, studiohet natyra e të dhënave, qëllimi dhe kohëzgjatja e veprimit të përpunimit të propozuar, ose vendi i origjinës dhe destinacioni përfundimtar, rregullat e përgjithshme dhe sektoriale të së drejtës, rregullat profesionale dhe masave të sigurisë që janë në fuqi në atë vend (vendi i tretë).[280] Njëkohësisht parashikohet dhe zhvillimi i një sistemi të një informacioni të ndërsjellët ndërmjet Shteteve Anëtare, ku ata konsiderojnë se një vend i tretë siguron një nivel të përshtatshëm të mbrojtjes, në mënyrë që të marrin masat e nevojshme për të parandaluar çdo transferim të të dhënave në atë vend të tretë. Në rastin e këtyre rregullimeve gjithashtu ishte e nevojshme për të formuar një kornizë ligjore që merr parasysh perceptimet e SHBA, partnerit më të madh politiko-ekonomik të Bashkimit Evropian në lidhje me transferimin e të dhënave personale nga vendet e BE- në SHBA, pasi SHBA sipas parimeve dhe kritereve të Direktivës nuk ofron nivel mbrojtje të kënaqshëm, pasi si filozofia ashtu dhe korrigjimi

[276] Po aty. Neni 14 paragrafi 1.

[277] Kjo duhet të theksohet ndoshta kuptohet pa thënë se koncepti i vendit të tretë përfshin çdo vend jashtë Bashkimit Evropian.Në çështjen tashmë të famshme C-101/01 Rasti i Procedimit penal kundër Bogil Lindqvist, Gjykata vendosi se nuk kishte asnjë transferim të të dhënave në një vend të tretë brenda kuptimit të nenit 25 të Direktivës 95/46, kur një person i cili është brenda shtetit anëtar regjistrohet në faqen e Internetit, e cila është ruajtur në sitin e ofruesit të internetit, që është krijuar në atë shtet ose në një shtet tjetër anëtar, duke lejuar kështu një qasje në këto të dhëna për këdo që lidhet me internetin, duke përfshirë personat në një vend të tretë, në http://eur- lex. europa. eu/ LexUriS/LexUriServ. Do? Uri = CE LE X: 62 0 0 1J0101:EL:HTML

[278] Po aty. Neni 22.

[279] Siç u përmend në opinionin shpjegues 57 të Direktivës 95/46/KE "*.. rrjedha ndërkufitare e të dhënave personale është e nevojshme për zhvillimin e tregtisë ndërkombëtare ..*".

[280] Neni 25 paragrafi 2 i Direktivës 95/46/KE.

i rregullatorit të mbrojtjes së të dhënave personale, janë krejtësisht të ndryshme.[281] Kështu, për transferimin e të dhënave personale në SHBA, u zbatua në tetor të vitit 2000, marrëveshja mbi sistemin e mbrojtjes që bazohet në "parimet e portit të sigurtë" (Safe Harbor).[282]

Çështje të rëndësishme për rrjedhjen e të dhënave ndërkufitare okupuan dhe okupojnë akoma Bashkimin Evropian, ku janë rastet e arkivave të të dhënave që krijojnë linjat ajrore të pasagjerëve në rezervimin dhe fluturim për ku, nga ku, ose nëpërmjet

---

[281] Shafer, G. (1999). "*The Power of EU Collective Action: The Impact of EU Data Privacy Regulation on US Business Practice*", European Law Journal, fq. 419.

[282] Safe Harbor është një sistem i vetë-rregullimit, sipas të cilit marrësi i të dhënave të futura në një listë të veçantë të Komisionit Federal të Tregtisë të Shteteve të Bashkuara (Komisioni Federal i Tregtisë), angazhohet në përputhje me parimet e mësipërme, ku në çdo rast përpunohen të dhënat personale që janë transmetuar nga një vend i BE-së.

"*Shkurtimisht mund të përshkruante dikush sistemin e parimeve të Safe Harbor si vijon: Parimet e Safe Harbor përbëhen nga njoftimet e hershme (që korrespondon me të drejtën e informacionit), përzgjedhëse (e cila i referohet aftësisë së përpunimit të informacionit për qëllime të ndryshme nga ato të mbledhjes së tij), për transferimin e mëtejshëm, sigurinë, integritetin e të dhënave, qasjen dhe zbatimin...*".

"*Sipas sistemit të mësipërm çdo organ pranon sistemin e vetë-rregullimit në përputhje me parimet e mësipërme të mbrojtjes së të dhënave, regjistrohet me iniciativën e tij në një regjistër të veçantë që mbahet në Departamentin amerikan të Tregtisë. Kjo do të thotë që organizatat e regjistruara mund të marrin të dhënat personale nga Bashkimi Evropian. Vihet në dukje se Komisioni i Tregtisë nuk do të kontrollojë nëse vërtet organizmi paraqet garancitë apo ka ndërmarrë hapat e duhura për të ruajtur autoritetin. Agjencia merr përsipër përgjegjësinë duke deklaruar se dhe pse merr pjesë në programe të veçanta për të mbrojtur privatësinë (privacy), gjithashtu përputhet me direktivat e autoriteteve relevante evropiane për mbrojtjen e të dhënave ...*".

"*Për çështjen e sanksioneve në rast të shkeljes së parimeve nga ana e Komisionit Federal të Tregtisë është angazhuar për të lëvizur kundër shkelësve sipas dispozitave të përgjithshme për shtrembërim dhe mashtrim.*"

Shih: informacion mbi "*parimet e portit të sigurtë*" (Safe Harbor). Në faqen e internetit të Departamentit amerikan të Tregtisë http://www.export.gov/safeharbor/SH_Overview.asp

Gjithashtu në Salbu, S. (2002)."*The European Data Privacy Directive and International Relations*", në http://law.vanderbilt.edu/journals/journal/35-02/Salbu10.pdf dhe Long, W. dhe Quek, P. "*Personal Data privacy protection in an age of globalization: the US-EU safe harbor compromise*", Journal of European Public Policy fq. 325 , Memorandum, Baker & Mackenzie, "*Implementing the US-EU Data Privacy* "*Safe Harbor*", në http://www.bakernet.com/ecommerce/Safe%20Harbor%20Alert%20--% 20N ov% 20 2001.docbodil

Shteteve të Bashkuara të Amerikës, të ashtuquajtura PNR (Passenger Name Record),[283] të cilat transferohen tek zyra Doganore dhe Mbrojtjes Kufitare të SHBA CBP (Customs and Border Protection) ku arkivat me të dhënat elektronike të transferimit të parave online të ashtuquajtura Swift (Society for Worldwide Interbank Financial Telecommunication) janë transmetuar tek autoritetet amerikane, në kundërshtim me legjislacionin evropian për transmetimin e këtyre të dhënave në vendet jashtë BE-së.

Konkretisht vendimi 2004/496/KE[284] i Këshillit i dha dritën e gjelbër përfundimit të një marrëveshjeje midis BE-së dhe SHBA-së për përpunimin dhe transferimin e emrave dhe të dhënave personale të udhëtarëve dhe vazhdoi me Vendimin 2004/535/KE[285] të Komisionit, ku vlerësojë kënaqshëm mbrojtjen e të dhënave personale të ruajtura në dosjet e udhëtarëve, tek të cilët kishte akses CBP. Parlamenti Evropian reagoi dhe i kërkoi GJED për të anuluar këto marrëveshje. Gjykata Evropiane e Drejtësisë në gjykimin e saj të datës 30 maj 2006, plus çështjet e gjykuara C-317/04 dhe C-318/04 anuloi Vendimin 2004/496/KE të datës 17 maj 2004 mbi përfundimin e Marrëveshjes ndërmjet Komuniteti Evropian dhe SHBA-së dhe detyruan institucionet t'i japin fund marrëveshjes me Shtetet e Bashkuara jo më vonë se 30 shtator 2006. [286]

---

[283] Brenda dosjes së pasagjerit (Passenger Name Record ose PNR) përfshihen 34 "*fusha*" të dhënash ndërmjet të cilave është kodi për gjetjen e dosjes, datat e rezervimit të vendit, informacion në lidhje me jetën e një pasagjeri, data e pritshme e ikjes dhe e kthimit. Kështu, transferohen të dhënat personale të personave të cilët anuluan ose ndryshuan fluturimin, emrin e tyre, adresën aktuale, adresën ku ata kanë banuar, adresën e-mail apo dhe fusha nga të cilat mund të përfitojnë të dhëna të ndjeshme.

[284] 2004/496/EC:Council Decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection Official Journal L 183, 20/05/2004, fq. 0083.

[285] 2004/535/EC:Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection (notified under document number C (2004) 1914) Official Journal L 235, 06/07/2004 P. 0011 – 0022.

[286] Plus çështjet e gjykuara C-317/04 dhe C-318/04: Vendim i Gjykatës (Dhoma me përbërje të madhe) i datës 30 Maj 2006 - Parlamenti Evropian kundër Këshillit të Bashkimit Evropian (Mbrojtja e individëve në lidhje me përpunimin e të dhënave personale - Transporti Ajror - Vendimi 2004/496/KE - Marrëveshja ndërmjet Komunitetit Evropian dhe Shteteve të Bashkuara të Amerikës - Transferimi i deklaratave me

Më 21 shtator 2010, Komisioni Evropian miratoi një paketë propozimesh për shkëmbimin e të dhënave në ruajtjen e emrave të pasagjerëve (Passenger Name Record - PNR) me vendet e treta, për përcaktimin e parimeve të përgjithshme, ku duhet të jenë të bazuara në të gjitha marrëveshjet me vendet e treta në lidhje me të dhënat e PNR, siç është propozuar nga Komisioni, që të përdoren për qëllimin e vetëm për të luftuar terrorizmin dhe format e krimit serioz ndërkombëtar. Duhet të kufizohet në të dhënat e nevojshme për të arritur qëllimin e mësipërm, ndërkohë që pasagjerët do të duhet të informohen në mënyrë të qartë në lidhje me shkëmbimin e të dhënave PNR, për sa i përket atyre, të kenë të drejtë për të shqyrtuar këto të dhëna, si dhe të kenë të drejta në mjetet juridike efektive administrative dhe gjyqësore, ofruese të mbrojtjes juridike.[287] Reagimet vazhdojnë në emër të luftës kundër terrorizmit dhe duket që amplifikohet një organizëm shumë dimensional, monitorues, regjistrues dhe përpunues i jetës sonë private. Megjithatë, Mbikëqyrësi Evropian për Mbrojtjen e të Dhënave Personale me një opinion mbi propozimin e Komisionit shprehu shqetësimin e tij se Komisioni deklaroi se të dhënat PNR "do të përdoren për të parandaluar një krim, me anë të një hetimi ose arrestimi të personave para se të kryet një krim" bazuar në "treguesit e rrezikut të paracaktuar, të bazuara në të dhëna objektive",[288] si çështje shumë serioze që janë: pajtueshmëria me parimet themelore të privatësisë dhe mbrojtjen e të dhënave, duke përfshirë edhe ato të përcaktuara në nenin 8 të KEDNJ-së, nenet 7 dhe 8 të Kartës dhe Neni 16 i TFEU (Traktati i Bashkëpunimit të BE-së).

---

emrat e pasagjerëve në Byronë e Doganave dhe të Mbrojtjes Kufitare të Shteteve të Bashkuara të Amerikës - Direktiva 95/46/KE - Neni 25 - vendet e treta - Vendim 2004/535/KE - nivel të mjaftueshëm të mbrojtjes) EEC 178, 29. 07.2006, fq.1-2, në http://eurlex.europa.eu/LexUriServ/ LexUriServ.do?uri=CE LEX:C2006/178/02:EL:NOT

[287] Komunikatë për shtyp "*Komisioni Evropian miraton strategjinë e jashtme të BE për të dhënat nga PNR (PNR)*", Bruksel, 21 shtator 2010, në http ://europ a.eu/rapid /press Releases Action.do?reference =IP/10/11 50&format=HTML&aged=1&lan guage=EL&guiLanguage=el. Shih: Komunikatën nga Komisioni, "*në lidhje me qasjen globale për transfertat e shtetit pas emrave të pasagjerëve (PNR) në vendet e treta*", në http://eur lex .europa .eu/Lex UriServ /Lex UriSer v.do ? uri = COM :20 10 :0 49 2: F IN :EL:PDF

[288] Mendimi i Mbikëqyrësit Evropian për Mbrojtjen e të Dhënave në Komunikatën e Komisionit për qasje globale ndaj transferimeve të situatave me emrat e pasagjerëve (PNR) në vendet e treta (2010 / C357/02), në http://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:357:0007:0011:EL:PDF, pjesa 18.

Brenda këtyre kornizave funksionon dhe sistemi SWIFT (Society for the Worldwide Interbank Financial Telecommunication) i cili është një rrjet përmes së cilit informacioni lidhet me 80% të transfertave elektronike financiare në mbi 200 vende dhe është një mjet i shkëlqyer i depërtimit në privatësinë e individëve sidomos pas vitit 2006, kur SHBA e përdori atë për të identifikuar terroristët e dyshuar dhe financuesit e tyre.[289] Struktura e SWIFT ndryshoi të gjitha informatat në lidhje me transaksionet financiare në kuadër të Zonës Ekonomike Evropiane dhe Zvicra nëpërmjet SWIFT do të mbetet brenda zonës evropiane. Këshilli vazhdoi më tej me përfundimin e marrëveshjes[290] me SHBA mbi përpunimin dhe transferimin e të dhënave të mesazheve financiare nga Bashkimi Evropian në Shtetet e Bashkuara për qëllimet e programit të monitorimit, të financimit të terrorizmit (Terrorist Finance Tracking Programme) i njohur si TFTP.[291] Reagimet qenë të shumta dhe në Parlamentin Evropian, ku u dëgjuan tashmë akuza ndaj Komisionit dhe Këshillit për marrëveshjen që do të rrezikonte jetën private të qytetarëve evropianë,[292] sidomos pas Raportit të Europol i publikuar në 02.03.2011 në zbatim të marrëveshjes TFTP, e cila thotë se kushtet për mbrojtjen e të dhënave personale nuk u respektuan dhe se përkundër faktit, aplikimet e autoriteteve të SHBA ishin shpesh të përgjithshme dhe të paqarta. Europol miratoi të gjitha aplikimet për transferimin e të dhënave.[293]

Një ndryshim i rëndësishëm në rregulloret në fuqi në nivel global dhe evropian ishte themelimi i një grupi mbrojtje të individëve në lidhje me përpunimin e të dhënave personale, në të cilin përfshiheshin përfaqësues të autoriteteve kombëtare mbikëqyrëse, si të Mbikëqyrësit Evropian të Mbrojtjes së të Dhënave dhe Komisionit, të cilat do të

---

[289] EU-US Agreement on SWIFT bank data transfer, në http://europeonthestrand.ideasoneurope.eu/2010/07/07/eu-us-agreement-on-swift-bank-data-transfer/

[290] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, OJ L 195 of 27/07/2010, në http://eur- lex.europa .eu /Lex Uri Serv/ L exUriServ.do?uri=OJ:L:2010:195:0005:0014:EN:PDF.

[291] Shih: në lidhje me TFTP në http://www.edri.org/files/SWIFT-FAQ-2010-02-09.pdf

[292] Pop V. *"Court only option against Swift agreement, says MEP"*, në http :// eurobserver. com/22/32010.

[293] "SWIFT agreement implementation not respecting data protection safeguards", në http://www.edri.org/edrigram/number9.5/swift-agreementdatprotection-safeguards

kontribuojnë për zbatimin e njëllojshëm të rregullave kombëtare të miratuara në zbatim të Direktivës 95/46/KE,[294] përmes koordinimit të këtyre komisioneve. Me Nenin 29 të Direktivës u themelua grupi për mbrojtjen e individëve në lidhje me përpunimin e të dhënave personale.[295] Ky grup i cili ka status këshillimor dhe vepron në mënyrë të pavarur, përbëhet nga një përfaqësues i autoritetit ose autoriteteve të kontrollit të caktuar nga çdo Shtet Anëtar, një përfaqësues i autoritetit ose autoriteteve të themeluara për institucionet, organet e Komunitetit gjithashtu dhe një përfaqësues i Komisionit.

Në veçanti, përgjegjësitë e grupit janë:

a) Të shqyrtojë çdo temë që mbulon zbatimin e dispozitave kombëtare të miratuara në zbatim të Direktivës 95/46/KE, në mënyrë që të kontribuojë në zbatimin e njëllojshëm të tyre.
b) T'i sigurojë Komisionit një opinion mbi nivelin e mbrojtjes në Komunitet dhe në vendet e treta.
c) Të këshillojë Komisionin mbi çdo amendament të propozuar të kësaj Direktive, për çfarëdo mase shtesë ose specifike që duhet të ndërmerret për të mbrojtur të drejtat dhe liritë e individëve në lidhje me përpunimin e të dhënave personale dhe çdo propozim tjetër masash të Komunitetit që ndikojnë në këto të drejta dhe liri
d) Të japë një opinion mbi kodet e sjelljes, përpiluar në nivel Komunitar.[296] Për më tepër, tërësia e Nenit 29, mund të nxjerrë me nismën e vet, rekomandime për çdo çështje që lidhet me mbrojtjen e individëve në lidhje me përpunimin e të dhënave personale në Komunitet,[297] si dhe të përgatisë për këtë qëllim një raport që përcillet gjithashtu në Parlamentin Evropian dhe Këshill.

3.3.2.3.2 Karta e të Drejtave Themelore të Bashkimit Evropian

Me rastin e 50-vjetorit të Deklaratës Universale të të Drejtave të Njeriut në dhjetor të vitit 1948, Këshilli Evropian në 3-4 qershor 1999, në Këln vendosi të

[294] Opinion shpjegues 65 i Direktivës 95/46/KE.

[295] I ashtuquajturi "Grupi i Punës, Neni 29".

[296] Po aty. Neni 30 paragrafi 1.

[297] Po aty. Neni 30 paragrafi 3.

ndërmarrë punën për zhvillimin e Kartës së të Drejtave Themelore të Njeriut.[298] Qëllimi ishte mbledhja e të drejtave themelore të zbatueshme në nivel të BE-së në një tekst të vetëm për t'i bërë ato më të qarta. Karta e të Drejtave Themelore të BE-së, zyrtarisht u shpall në takimin e Këshillit Evropian në Nisë në 7 dhjetor 2000.[299] Karta është e bazuar në Traktatet e Komunitetit të konventave ndërkombëtare, duke përfshirë Konventën Evropiane të të Drejtave të Njeriut të vitit 1950, në traditat e përbashkëta kushtetuese të shteteve anëtare dhe deklaratave të ndryshme të Parlamentit Evropian.[300] Përmban të drejta, por që nuk garantohen nga Konventa Evropiane për të Drejtat e Njeriut (KEDNJ), e cila është e kufizuar në mbrojtjen e të drejtave civile dhe politike. Këto janë të drejtat që burojnë nga kushtet moderne sociale[301] dhe në veçanti të drejtat sociale të punëtorëve, mbrojtjen e të dhënave, bioetikën ose e drejta për administrim të mirë.[302] Edhe pse nuk u bë ligjërisht detyruese, mbështeti pikëpamjen se Karta është rezultat i "traditave të përbashkëta kushtetuese" dhe është bërë tashmë pjesë e legjislacionit komunitar (acquis communautaire) pavarësisht mos inkorporimit të saj në Traktate.[303] Veçanërisht nenet 7 dhe 8, i referohen respektimit të jetës private dhe familjare dhe mbrojtjes së të dhënave personale, si të dallueshme në mes të të drejtave të tyre

[298] Karta e të Drejtave Themelore të Bashkimit Evropian, Gazeta Zyrtare 364, 18.12.2000. fq. 0001-0022, në http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000X1218(01):EL:HTML, shih: Di Federico , G. (2011). "*The EU Charter of Fundamental Rights: From Declaration to Binding Instrument*", fq.79, si dhe Torres Pérez, A. (2009). "*Conflicts of Rights in the European Union: A Theory of Supranational Adjudication*", fq14, si dhe Alston, Ph. dhe De Schutter, O. (2005). "*Monitoring Fundamental Rights In The EU: The Contribution Of The Fundamental Agency*", fq.65 dhe Peers, S. dhe Ward, A. (2004). "*The European Union Charter of Fundamental Rights*", fq. 190.

[299] http://europa.eu/legislation_summaries/glossary/index_e_en.htm

[300] Catannaci, J. dhe Misfud-Bonnici, J. (2005). "*Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty*", Information & Communications Technology Law, fq. 5.

[301] Po aty. Bignami, F. (2008). fq.224.

[302] http://europa.eu/scadplus/glossary/charter_fundamental_rights_el.htm

[303] Lenaerts, K. dhe De Smijter, E. (2001). "*A Bill of Rights for the European Union*", fq. 299, gjithashtu ky rezultat ishte i njohur për tri arsye kryesore: së pari për shkak të konsensusit të tre institucioneve, së dyti për shkak të përbërjes dhe funksionimit të Konventës që e hartoi atë dhe së treti për shkak të "*interpretimit tërësor*" të termit traditat e përbashkëta kushtetuese nga GJED. Ky interpretim bazohet mbi njohjen nga ana e Shteteve Anëtare të të drejtave themelore, ku Gjykata thirret të mbrojë. Në www .fd. uc. pt/ igc /pdf / papers/john_morjin.pdf

themelore. Në nenin 7, mbrohet e drejta e jetës private dhe familjare, në pajtim me dispozitat përkatëse të KEDNJ.[304] Neni 8 përmbledh legjislacionin evropian për mbrojtjen e të dhënave personale duke dhënë elementet thelbësore të vetëvendosjes informative, të cilat janë pëlqimi, aksesi, korrigjimi, parimi i qëllimit të përpunimit të të dhënave personale dhe kontrolli i këtyre rregullave nga një autoritet i pavarur.[305] Karakteristike është dhe mungesa e ndonjë referencë për lëvizjen e lirë të këtyre të dhënave, që "shkëput" mbrojtjen e të dhënave personale nga funksionimi i tregut të brendshëm, duke e bërë mbrojtjen e të dhënave personale një të drejtë universale.[306]

3.3.2.3.3. Rekomandimi Nr. R (99) 5

Rekomandimi Nr. R (99) 5 i Komitetit të Ministrave të Këshillit të Evropës për mbrojtjen e privatësisë në internet, përfshin udhëzime ku përshkruajnë parimet e praktikës së mirë, për sa i përket privatësisë për përdoruesit[307] dhe ofruesit e shërbimeve të internetit (ISP).[308]

Komiteti i Ministrave vuri në dukje se për shkak të zhvillimit teknologjik dhe përgjithësimit të mbledhjes e përpunimit të të dhënave personale në rrugët e

---

[304] Neni 7 "*Respekti për jetën private dhe familjare-Gjithkush ka të drejtën për respektimin e jetës private dhe familjare, vendbanimin dhe komunikimeve të tij*".

[305] Neni 8 Mbrojtja e të dhënave personale:

"1. Gjithkush ka të drejtën e mbrojtjes së të dhënave personale në lidhje me të.

2. Përpunimi i këtyre të dhënave duhet të bëhet i përpunuar në mënyrë të drejtë për qëllimet e specifikuara dhe në bazë të pëlqimit të personit në fjalë, apo në një tjetër bazë legjitime të parashikuar nga ligji. Çdo person ka të drejtë për qasje në të dhënat e mbledhura që kanë të bëjnë me të dhe t'i korrigjojë.

3. Respektimi i këtyre rregullave duhet t'i nënshtrohet kontrollit nga një autoritet i pavarur".

[306] Gibbs, A. H. (2011). "*Constitutional Life and Europe's Area of Freedom, Security and Justice*", fq. 98, Shih: Deklaratën e Monteux nën kornizën e konferencës së Komisionerëve për Mbrojtjen e të Dhënave Personale dhe Privatësisë duke deklaruar: "*The protection of personal data and privacy in a globalised world: a universal right respecting diversities*", në http //www. edps. eu.int /legislation/05-09-16_ Montreux _declaration_EN.pdf

[307] Frackman, A., Martin, R. C. dhe Ray, C. (2002). "*Internet and Online Privacy: A Legal and Business Guide*", fq. 121.

[308] Shih: Tekstin e Rekomandimit në https:// wcd.coe.int/com.instranet. InstraServlet?command =com. instranet.CmdBlobGet&InstranetImage=276580&SecMode=1&DocId=396826&Usage=2, si dhe gjithashtu Boehm, F. (2012). "*Information Sharing and Data Protection In the Area of Freedom, Security and Justice*", fq.92.

komunikimit, paraqet rreziqe për të mbrojtur dhe për të ruajtur privatësinë e individëve, gjithashtu është e nevojshme për t'u siguruar se komunikimet janë kryer me ndihmën e teknologjive të reja, të respektojnë të drejtat e njeriut dhe liritë themelore të njeriut, sidomos të drejtën e privatësisë dhe fshehtësisë së korrespondencës, të garantuara në nenin 8 të KEDNJ-së. Më tej rekomandon dhe shpërndarjen e gjerë të udhëzimeve, si për përdoruesit dhe për ofruesit e shërbimit të internetit (ISP).

Rekomandimi nuk është ligjërisht i detyrueshëm, por është i një rëndësie të veçantë pasi kjo iniciativë u ndërmor në kontekstin e nevojës për krijimin e parimeve themelore të mbrojtjes së të dhënave në internet si një qasje e parë për këtë çështje.[309]

3.3.2.3.4 Rregullorja (KE) Nr. 45/2001

Kuadri Komunitar për mbrojtjen e të dhënave personale u plotësua nga neni 286 TEC (Traktati themelues i Komunitetit Evropian) ku zgjeron mbrojtjen e veprimeve Komunitare dhe kundër trajtimeve tek të cilat veprojnë institucionet dhe shërbimet komunitare, si dhe parashikon krijimin e një Autoriteti të pavarur mbikëqyrës.

Kështu, Neni 286 thekson që nga 1 Janari 1999, aktet Komunitare në mbrojtjen e individëve në lidhje me përpunimin dhe lëvizjen e lirë të të dhënave personale do të zbatohen për institucionet dhe organet e përcaktuara nga Traktati ose në bazë të tij.[310] Këshilli do të vendosë një trup të pavarur mbikëqyrës përgjegjës për monitorimin e zbatimit të akteve të Komunitetit për institucionet dhe organet e Komunitetit, gjithashtu do të miratojë dispozitat e tjera përkatëse sipas nevojës.[311] Së fundi, zbatimi i kërkesave

---

[309] Në përputhje me dispozitat e nenit 15 të Statutit të Kartës së Këshillit të Evropës paragrafi b, duke marrë parasysh se qëllimi i Këshillit të Evropës është arritja e një konvergjence më të madhe ndërmjet anëtarëve të tij.

[310] Shih Opinionin 5/2001 mbi Raportin Special nga ana e Avokatit të Popullit Evropian në Parlamentin Evropian në vzhdim të draft rekomandimit që u dorëzua në Komisionin Evropian në kuadër të ankesës 713/98/IJH, (On the European Ombudsman Special Report to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH), në http://ec. europa .eu/ justice_home/fsj/privacy/docs/wpdocs/2001/wp44el.pdf

[311] "1. Nga 1 janar 1999, aktet Komunitare veprojnë në mbrojtjen e individëve në lidhje me përpunimin dhe lëvizjen e lirë të të dhënave personale në fuqi për institucionet dhe agjencitë e themeluara nga ky Traktat ose në bazë të tij.

2. Para datës që përmendet në paragrafin 1, Këshilli, duke vepruar në përputhje me procedurën e parashikuar në nenin 251, rekomandon një organ të pavarur mbikëqyrës, përgjegjës për monitorimin e

të nenit 286 u bë me miratimin e Rregullores 45/2001[312] "Për mbrojtjen e individëve në lidhje me përpunimin e të dhënave personale nga institucionet dhe organet e Komunitetit për lëvizjen e lirë të këtyre të dhënave.[313] Ajo kishte për qëllim, të krijonte një kuadër të të drejtave të mbrojtura, si dhe përcaktimin e detyrimeve të kontrolluesit të të dhënave brenda institucioneve dhe organeve të Komunitetit, krijimin i një Autoriteti mbikëqyrës të pavarur,[314] përgjegjës për mbikëqyrjen dhe përpunimin e të dhënave personale nga institucionet dhe organet e Komunitetit.[315]

3.3.2.3.5 Direktiva 2002/58/KE

Zhvillimi i teknologjive në fushën e telekomunikacionit evidentoi se ishin burimi kryesor i rrezikut të të dhënave personale dhe gjeti një nevojë urgjente për rregullim ligjor sektorial, që të plotësojë dhe ta detajojë Direktivën 95/46/KE. Kështu u miratua Direktiva 97/66/KE[316] e cila specializoi Direktivën 95/46/KE në lidhje me përpunimin e të dhënave personale në sektorin e telekomunikimeve. Direktiva 97/66/KE kishte një qëllim të dyfishtë: konfrontimin e teknologjive të reja të telekomunikacionit që ishin burim i rrezikut të së drejtës vetë përcaktuese të informimit të individit[317] dhe

---

zbatimit të akteve të tilla Komunitare në institucionet dhe organet e Komunitetit dhe miraton dispozita të tjera të përshtatshme". Teksti i Traktatit në http://eur lex. Europa .eu/el/treaties /dat/12002E/htm /C_ 2002325EL.003301.html/

[312] Rregullorja (KE) Nr. 45/2001 e Parlamentit Evropian dhe e Këshillit të datës 18 Dhjetor 2000 "*Për mbrojtjen e individëve në lidhje me përpunimin e të dhënave personale nga institucionet dhe organet e Komunitetit dhe mbi lëvizjen e lirë të këtyre të dhënave*", Gazeta Zyrtare L 008, 2001/12/01 fq 0001-0022.

[313] Neni 3 i Rregullores 45/2001.

[314] Mbikëqyrësi Evropiane për Mbrojtjen e të Dhënave Personale. Në http://www.edps.europa.eu, shih: dhe Kosta, E. (2013). "*Consent in European Data Protection Law*", fq. 428, gjithashtu shih dhe Vendimin nr. 1247/2002/KE të Parlamentit Evropian, Këshillit dhe Komisionit të datës 1 Korrik 2002 "*Për rregullat dhe kushtet e përgjithshme që rregullojnë punën e Mbikëqyrësit Evropian për Mbrojtjen e të Dhënave*", E.E L183 12/07/2002 fq. 0001-0002.

[315] Neni 1 i Rregullores 45/2001.

[316] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, në http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML.

[317] Direktiva 97/66/KE e Parlamentit Evropian dhe e Këshillit e datës 15 Dhjetor 1997 "*Për përpunimin e të dhënave personale dhe privatësisë në sektorin e telekomunikacioneve*", në http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML.

harmonizimin e ligjeve të Shteteve Anëtare për të siguruar zhvillimin e qëndrueshëm të tregut të telekomunikacioneve në Komunitet.[318] Objektivi kryesor ishte harmonizimi më i madh i mundur i dispozitave rregulluese në Shtetet Anëtare, me anë të veprimit rregullator në nivel të BE-së dhe kombëtar, për të siguruar një nivel ekuivalent të mbrojtjes së të drejtave dhe lirive themelore, sidomos të drejtës së privatësisë, në lidhje me përpunimin e të dhënave personale në sektorin e telekomunikacionit dhe lëvizjen e lirë të këtyre të dhënave dhe të pajisjeve të telekomunikacioneve dhe shërbimeve në komunitet.[319] Por zhvillimet e shpejta në teknologjitë e informacionit dhe të komunikimit, e kanë bërë të domosdoshme nevojën për të përmbushur kërkesat e reja dhe specifike të shkaktuara nga teknologjitë e avancuara digjitale në rrjetet publike të komunikimit, në lidhje me mbrojtjen e të dhënave personale dhe privatësisë së përdoruesit. Kjo krijoi nevojën për zëvendësimin e menjëhershëm të kuadrit ligjor ekzistues për telekomunikacionet.[320] Direktiva 97/66/KE duhet t'i përshtatet zhvillimeve të tregjeve dhe teknologjive për shërbimet e komunikimeve elektronike, në mënyrë që të ofrojnë të njëjtin nivel të mbrojtjes së të dhënave personale dhe privatësisë për përdoruesit e shërbimeve të komunikimeve elektronike të disponueshme për publikun, pavarësisht nga teknologjitë e përdorura. Tashmë në fund të viteve 80 dhe në fillim të viteve 90, ndryshime themelore ndodhin në peizazhin ndërkombëtar të telekomunikacionit me përparimet në teknologji për të transformuar tregun e telekomunikacioneve, duke e bërë atë një nga industritë më të mëdha në mbarë botën. Aktivizimi në këtë fushë i kompanive të mëdha, e bën nevojën për liberalizimin dhe mbizotërimin e kushteve të konkurrencës së lirë, direkt në këtë treg. Ata që kanë pasur tradicionalisht monopolin e sektorit, Organizmat Kombëtarë të Telekomunikacionit u detyruan për të lejuar furnizimin e shërbimeve të telekomunikacionit tek operatorët

[318] Nenova, M. B. (2007). "*European Community Electronic Communications and Competition Law*", fq. 191.

[319] Neni 1, paragrafi 1 të Direktivës 97/66/KE.

[320] The Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation. Results of the Public Consultation on the Green Paper [COM (97) 623]. COM (99) 108 final, 9 March 1999, në http://aei.pitt.edu/ 983/01/telecom _convergence_gp _follow_COM _99_ 108.pdf.

privatë, pavarësisht vendit të tyre të origjinës.[321] Këto zhvillime, me teknologji digjitale të reja dhe të përparuara, futen në rrjetet publike të telekomunikacioneve dhe sollën probleme të reja që kërkojnë trajtim të ndryshëm për sa i përket mbrojtjes së të dhënave personale dhe privatësisë së individit. Ndërkohë këto zhvillime në fushën e teknologjisë së telekomunikacionit dhe nevojën pasuese për furnizim më të mirë të shërbimeve përkatëse me çmime më të ulëta, që të përmirësojnë cilësinë duke krijuar nevojën për formimin e një kuadri modern të fortë rregullator, i cili mund të mbështes këto zhvillime.[322] Objektivi kryesor ishte harmonizimi më i madh i mundur i dispozitave rregulluese në Shtetet Anëtare përmes veprimit rregullator në nivel të BE-së dhe në nivel kombëtar. Për këtë qëllim në vitin 2002 u hartuan katër direktivat, bazuar në nenin 95 të Traktatit dhe një Kuadër – Direktivë, të miratuara nga Komisioni Evropian, si Direktiva 2002/19/KE,[323] Direktiva 2002/20/KE,[324] Direktiva 2002/21/KE,[325] Direktiva 2002/22/KE[326] dhe Direktiva 2002/58/KE.

Nga këto rëndësi më të madhe ka Direktiva 2002/58/KE "Për përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve

---

[321] Kirkman, G. dhe Cornelius, P. K. (2002) "*The Global Information Technology Report 2001-2002: Readiness for the Networked World*", Oxford University Press, USA, fq. 157.

[322] Shih: në lidhje me kuadrin i ri për shërbime të komunikimeve elektronike në http://europa.eu/ scadplus /leg/el/lvb/l24216.htm si dhe Kiessling, T. dhe Blondeel, Y. (1996)."*The EU Regulatory Framework in Telecommunications-A Critical Analysis, Telecommunications Policy in the EU*" dhe Weinstein, S. (2003)."*The New European Commission Regulatory Framework for Electronic Communications*", Hertfordshire Law Journal, fq. 43, gjithashtu dhe Varney, E. (2013). "*Disability and Information Technology: A Comparative Study in Media Regulation*", fq147.

[323] Direktiva 2002/19/KE e Parlamentit Evropian dhe e Këshillit të datës 7 Mars 2002 "*Për aksesin ndaj rrjeteve të komunikimeve elektronike, faciliteteve shoqëruese, si dhe interkoneksionin e tyre*" (Access Directive) EE L 108 e datës 24.04.2002, fq. 7 - 20.

[324] Direktiva 2002/20/KE e Parlamentit Evropian dhe e Këshillit të datës 7 mars 2002 "*Për autorizimin e rrjeteve dhe shërbimeve të komunikimeve elektronike*" (Direktiva e Autorizimit). EE L 108 e datës 24.4. 2002, fq. 21 - 32.

[325] Direktiva 2002/21/KE e Parlamentit Evropian dhe e Këshillit të datës 7 mars 2002 "*Për një kuadër të përbashkët rregullator për rrjetet e komunikimit elektronik dhe shërbimeve*" (Kuadër Direktiva). EE L 108 e datës 24.4.2002, fq. 33 – 50.

[326] Direktiva 2002/22/KE e Parlamentit Evropian dhe e Këshillit të datës 7 mars 2002 "*Për shërbimin universal dhe të drejtat e përdoruesve në lidhje me rrjetet dhe shërbimet e komunikimeve elektronike*" (Direktiva e Shërbimit Universal). EE L 108 e datës 24.4.2002, fq. 51 – 77.

elektronike",[327] e cila erdhi si pasojë e domosdoshme e veçantisë së "plakjes" së parakohshme të rregullave të së drejtës lidhur me teknologjitë e reja.[328] Direktiva 2002/58/KE konfirmon përpjekjet e bëra në Bashkimin Evropian, që të mbizotërojë ndërhyrja legjislative në kundërshtim me filozofinë amerikane të vetë rregullimit.[329] Është Direktiva 2002/58/KE, siç është paraardhësja 97/66/KE, një rregullim vertikal sektorial si plotësues i teksteve ndërkombëtare dhe Kuadër Direktivës 95/46/KE. Vetë-rregullimi për ligjvënësit Evropian natyrisht nuk refuzon, por në të kundërt inkurajon iniciativa të lidhura me kodet e sjelljes të shoqatave profesionale dhe organizatave për përpunimin e të dhënave dhe raportimin tek autoritetet kombëtare. Zëvendësoi për këtë arsye, Direktivën 97/66/KE, për të cilën është argumentuar se ajo mund të mbulojë të gjitha mjetet moderne të komunikimit me interpretimin e saj të gjerë. Në lidhje me Direktivën 2002/58/KE, objektivi kryesor i ligjvënësit Komunitar ishte formulimi i rregullave teknologjikisht neutrale, brenda mjedisit të vazhdueshëm të zhvillimeve teknologjike.[330] Nuk ka asnjë referencë për "fushë telekomunikacioni", por për "komunikime elektronike".

Deri tani "Rrjeti i komunikimeve elektronike" nënkupton sistemet e transmetimit dhe sipas rastit, pajisjen e kalimit ose kursit dhe resurset e tjera të cilat lejojnë bartjen e sinjaleve me përdorimin e kabullit (telegraf), radio valëve, optike ose mjeteve të tjera elektromagnetike, duke përfshirë rrjetet satelitore, rrjetet fikse (transferimi i të dhënave nëpërmjet qarqeve dhe paketave të transmetimit duke përfshirë internetin) dhe të lëvizshme tokësore, sistemet e kabllove elektrike, kur përdoren për transmetimin e sinjaleve, rrjetet e përdorura për radion dhe televizionin, dhe rrjetet e televizionit

[327] Shih ndryshimin e mëtejshëm të saj, me anë të Direktivës 2009/136/KE.

[328] Guagnin, D., Hempel, L. dhe Oxygen, C. (2012). "*Managing Privacy Through Accountability*", fq. 281 dhe Berglund, S. (2009). "*Putting Politics Into Perspective: A Study of the Implementation of the EU Utilities Directives*", fq.51, si dhe Westby, JR. (2004). "*International Guide to Privacy*", fq. 102.

[329] Po aty. Nenova, M. B. (2007), fq. 101.

[330] Kështu, Neni 6 i Direktivës 97/66/KE i cili referohet vetëm "*Telefonatave*" ishte i paefektshëm pasi ai mbron p.sh. vetëm të dhënat e gjeneruara nga trafiku i thirrjeve telefonike tradicionale por jo të dhënat të ngjashme të trafikut të gjeneruara gjatë transmetimit të komunikimit në internet. Pra, kur flasim për "*të bërë një telefonatë*" në nenin 6 do të zëvendësohet nga "*transmetim të një komunikimi*" për të mbuluar të gjitha të dhënat e trafikut në një mënyrë të asnjanësisë teknologjike.

kabllor, pavarësisht nga lloji informacionit që përcjellin.[331] D.m.th. fjala "Komunikim" nënkupton çdo shkëmbim ose bartje informacioni ndërmjet numrave të caktuar të palëve me anë të vënies publikisht në dispozicion të shërbimit të komunikimeve elektronike. Nuk përfshin ndonjë informatë të bartur si pjesë e një shërbimi transmetues për publikun nga ana e rrjetit të komunikimit elektronik, përveçse kur informacioni mund të jetë i lidhur me abonentin e identifikueshëm ose përdoruesin që merr informacionin.[332] Përafrimi i legjislacionit nëpërmjet rregulloreve teknologjikisht neutrale është për të siguruar kapacitetet rregullues të sundimit të ligjit në një mjedis teknologjikisht fluid, i cili është një nga qëllimet kryesore të ligjvënësit Komunitar. Qëllimi i Direktivës është të sigurojë të drejtën e privatësisë në lidhje me përpunimin e të dhënave personale në komunikimet elektronike, me ndjekjen paralele për të siguruar lëvizjen e lirë të këtyre të dhënave, pajisjeve dhe shërbimeve të komunikimeve elektronike në Komunitet. Duke përsëritur thelbin e qëllimit të dyfishtë të hartimit të saj dhe të Kuadër Direktivës së parë 95/46/KE për mbrojtjen e të dhënave personale, ku nevoja për realizimin e objektivave kryesore të Komunitetit Evropian, ishte krijimi i një zone të vetme të transaksioneve financiare. Kjo çoi në ndjekjen e reformave rregullatorë, që do të lehtësonin lëvizjen ndërkufitare të të dhënave personale, mes të Shteteve Anëtare, të domosdoshme për të siguruar lëvizjen e lirë të mallrave, personave, shërbimeve dhe kapitalit, duke mbrojtur paralelisht të dhënat personale.[333]

Direktiva 2002/58/KE nuk zbatohet për aktivitetet e mbuluara nga Tituj V[334]dhe VI[335] të Traktatit mbi Bashkimin Evropian, në çështje të përbashkëta të politikës së jashtme të sigurisë, policisë dhe bashkëpunimit gjyqësor, në çështjet që lidhen me krimin[336] dhe në çdo rast në aktivitetet që kanë të bëjnë me sigurinë publike, mbrojtjen,

---

[331] Neni 2, pika a. e Direktivës 2002/21/KE.

[332] Neni 2 i Direktivës 2002/58/KE.

[333] Neni 2 i Traktatit të Romës përcaktoi qëllimin e mëposhtëm për Komunitetin Ekonomik Evropian (EEC), "*për të promovuar zhvillimin harmonik të aktiviteteve ekonomike në të gjithë Komunitetin, një zgjerim të vazhdueshëm dhe të balancuar, një rritje stabël, një ngritje të shpejtë të standardit të jetesës dhe marrëdhëniet e ngushta mes Shteteve që bashkon atë*".

[334] Nenet 11-28 të Traktati mbi Bashkimin Evropian.

[335] Po aty. Nenet 29-42.

[336] Consolidated versionof the Treaty on European Union Official Journal of the European Union C 321/E5 E/5 në http://eurlex. europa.eu/LexUriServ/ Lex UriServ .do ?uri =OJ :C : 2 00 6: 3 2 1 E : 0 0

sigurinë shtetërorë (duke përfshirë mirëqenien ekonomike të shtetit, përderisa aktivitetet kanë të bëjnë me çështjet e sigurisë së shtetit) si dhe aktivitetet e shtetit në fushat e ligjit penal.

Në Direktivën 2002/58/KE në nenin 2 janë dhënë përkufizime themelore të tilla si:

a) "Komunikimi", që është çdo informacion që shkëmbehet ose transferohet ndërmjet një numri të caktuar të palëve, nëpërmjet një shërbimi të komunikimeve elektronike në dispozicion të publikut;
b) "Trafiku i të dhënave",[337] që janë të dhënat që vihen në përpunim për qëllime të transmetimit të komunikimit, përmes një rrjeti të komunikimeve elektronike ose për qëllim të faturimit të tyre;
c) "Të dhënat mbi vendndodhjen", të cilat vihen në përpunim në një rrjet të komunikimeve elektronike ose shërbimit të komunikimeve elektronike, që tregon pozicionin gjeografik të pajisjes fundore të një përdoruesi, të një shërbimi në dispozicion të publikut të komunikimeve elektronike";[338]
d) Posta elektronike (e-mail) e cila është definuar si çdo mesazh me tekst, me zë, me tingull ose imazh, të dërguar nëpërmjet një rrjeti të komunikimit publik ku mund të ruhet në rrjet ose në pajisjen e fundme të marrësit deri në momentin kur merret nga pranuesi.[339]

Për shkak të rreziqeve të veçanta që ekzistojnë për shkeljen e sigurisë së rrjeteve të komunikimit, theksohet veçanërisht nevoja e ofrimit të sigurisë dhe informacionit përkatës[340] për përdoruesit/abonentët rreth rreziqeve dhe masave teknike dhe organizative për funksionimin e rrjeteve të komunikimeve elektronike që duhet të

01:0331:EN:PDF.

[337] Në Direktivën 2002/58/KE bëhet një hap i madh në krahasim me Direktivën 97/66/KE, e cila rregullon vetëm transmetimin e përmbajtjes.

[338] Si u zëvendësua në bazë të Direktivës 2009/136/KE së Parlamentit Evropian dhe e Këshillit të datës 25 nëntor 2009.

[339] Neni 2, paragrafi I i Direktivës 2002/58/KE.

[340] Opinion shpjegues 20 i Direktivës 2002/58/KE, i cili thekson se "*Kërkesa për të informuar abonentët për rreziqet e veçanta të sigurisë nuk çliron ofruesit e shërbimeve nga detyrimi që të marrin me shpenzimet e veta masat e duhura dhe të menjëhershme për të korrigjuar ndonjë të re, apo të parashikojnë rreziqet e sigurisë dhe të rivendosin nivelin normal të sigurisë së shërbimit*".

marrin ofruesit e shërbimeve dhe rrjeteve të komunikimeve elektronike.[341] Më tej në lidhje me të dhënat e trafikut në lidhje me abonentët dhe përdoruesit, të cilat përpunohen dhe ruhen nga ofruesi i rrjetit publik, apo vënien publikisht në dispozicion të shërbimeve të komunikimeve elektronike, duhet të fshihen ose të bëhen anonime kur nuk është më e nevojshme për qëllimin e transmetimit të një komunikimi pa cenuar paragrafët 2, 3 dhe 5 të nenit 6 të Direktivës dhe Neni 15 paragrafi 1.[342] Përjashtime për ndalimin e përgjithshëm mbi ruajtjen dhe përpunimin e trafikut të të dhënave për përdorim, kur është fjala për promovim të shërbimeve të marketingut të komunikimeve elektronike si dhe për ofrimin e shërbimeve me vlerë të shtuar, vetëm me pëlqimin e abonentit / përdoruesit, pasi përdoruesi është njoftuar (këshilluar) për natyrën e të dhënave të përpunuara.[343] Është vërejtur gjithashtu se rasti i vetëm ku lejohet heqja e kësaj mbrojtjeje, pa asnjë kufizim është kur bëhet fjalë për hetime të karakterit penal, apo për të mbrojtur sigurinë kombëtare, mbrojtjen kombëtare si dhe sigurinë publike. Direktiva 2002/58/KE bën dallimin e brendshëm të të dhënave të vendndodhjes, në mënyrë, që kur të dhënat e vendndodhjes përdoren për shërbime me vlerë të shtuar, të sigurojnë mbrojtje më të madhe për përdoruesit. Ajo thekson se për shkak të rreziqeve të mëdha për privatësinë, ku përfshihet përpunimi i të dhënave të vendndodhjes, lejohet përpunimi i tyre, duke i paraprirë anonimitetit të tyre dhe:

A. Ka marrë më parë pëlqimin e qartë të përdoruesit/abonent për ofrimin e shërbimeve me vlerë të shtuar.
B. ka qenë i njoftuar paraprakisht përdoruesi/abonent për gjatësinë, llojin dhe qëllimin e përpunimit.[344]

Teknologjitë e reja të telekomunikacionit kanë sjellë ndryshime dramatike në mënyrën e ofrimit të këtyre shërbimeve të telekomunikacionit. Situata ka ndryshuar, ku shqetësimet dhe frika që u zhvilluan për ekspozimin në rritje të rrezikut të të dhënave personale, solli gjithashtu ndryshim në mënyrën e trajtimit të çështjeve të listave

[341] Neni 4 i Direktivës 2002/58/KE.

[342] Neni 6.

[343] Po aty.

[344] Neni 9 .

telefonike. Kjo është arsyeja pse përdoruesit e shërbimeve të telekomunikacionit mund të kenë elementë të shumtë në kuadër të komunikimit jashtë shërbimeve të telefonisë fikse, të tilla si telefonia e lëvizshme (mobile) dhe adresa e-mail. Çështja trajtohet nga Direktiva në nenin 12. Ky nen kërkon nga Shtetet Anëtare informacionin e mëparshëm dhe pa pagesë të abonentëve për qëllime dhe mundësisht listat e përdorshmërisë, aftësitë e abonentëve për të përcaktuar nëse dhe çfarë të dhënash personale të tyre do të përfshihen në lista, e drejta abonentëve për regjistrim pa pagesë, për verifikimin e regjistrimit, korrigjimin dhe tërheqjen e të dhënave personale, mundësinë për të qenë i nevojshëm pëlqimi i abonentëve për të përdorur për qëllime të tjera përtej kërkimit të të dhënave të kontaktit.[345] Një nga çështjet kyçe që shqetësonte ekspertët për mbrojtjen e dhënave personale, ishte koncepti i marketingut të drejtpërdrejtë. Parimi bazë i vendosur nga Direktiva ishte se përdorimi i sistemeve të automatizuara të thirrjes (fax, e-mail) lejohet vetëm me pëlqimin paraprak (opt-in) të abonentit siç përcaktohet në Nenin 13 të Direktivës 2002/58/KE. Gjithashtu në lidhje me mbrojtjen e konfidencialitetit paraqitet një përjashtim i rëndësishëm në nenin 15 par. 1. i Direktivës, me të cilin renditet parimi i përgjithshëm i mbrojtjes së privatësisë së trafikut të të dhënave dhe informacionit të vendndodhjes.[346] Parashikon mundësinë për Shtetet Anëtare, që të kufizojnë të drejtat dhe detyrimet e parashikuara në nenet 5 dhe 6, nenin 8, paragrafët 1-4 dhe të nenin 9 të Direktivës dhe të marrin masa legjislative për ruajtjen e të dhënave për një kohë të caktuar. Ndër të tjera është e mundur që Shtetet Anëtare të miratojnë masa legjislative për të siguruar mbajtjen e të dhënave për një periudhë të caktuar kohe, për të lehtësuar objektivat e dispozitës. Me nenin 11 të Direktivës 2006/24/KE shtohet paragrafi 1a dhe ndryshohet paragrafi 1 i nenit 15 të Direktivës 2002/58/KE, e cili nuk është më i vlefshëm për të dhëna të cilat, i ruan në mënyrë eksplicite Direktiva 2006/24/KE.[347]

[345] Neni 12.

[346] Neni 15.

[347] "1a. *Paragrafi 1 nuk është i vlefshëm për të dhëna të cilat mbahen për ruajtje, e shpreh në mënyrë eksplicite Direktiva 2006/24/KE e Parlamentit Evropian dhe e Këshillit e datës 15 Mars 2006, "Për ruajtjen e të dhënave që krijohen ose të përpunohen në lidhje me vënien në dispozicion të publikut të shërbimeve të komunikimeve elektronike ose të rrjeteve të komunikimeve publike", për sa i përket qëllimeve të nenit 1, paragrafi 1 të Direktivës*".

3.3.3 Ndryshimet e fundit në Direktivën 2002/58/KE me Direktivat 2006/24/KE dhe 2009/136/KE

3.3.3.1 Direktiva 2006/24/KE[348]

Me vërshimin e sulmeve terroriste (në Madrid në vitin 2004 dhe në Londër në vitin 2005) u krijua një klimë e frikës që çoi në koshiencë se nevojitet miratimi i masave të përbashkëta për ruajtjen e të dhënave të telekomunikacionit për arsye të rëndësisë të trafikut të të dhënave të vendndodhjes për hetimin, zbulimin dhe ndjekjen e veprave të rënda penale si dhe veprat penale që lidhen me përhapjen e terrorizmit. Në mars të vitit 2006, Parlamenti Evropian dhe Këshilli miratoi direktivën për ruajtjen e të dhënave të krijuara ose të përpunuara në lidhje me vënien në dispozicion të publikut të shërbimeve të komunikimeve elektronike ose të rrjeteve të komunikimeve publike dhe për ndryshimin e Direktivës 2002/58/KE. Direktiva ka për qëllim të harmonizojë dispozitat e Shteteve Anëtare në lidhje me detyrimet për ofruesit e shërbimeve të komunikimeve elektronike për sa i përket ruajtjes së të dhënave.[349] Sipas logjikës së përcaktuar në preambulën e Direktivës, "ruajtja e të dhënave ka provuar të jetë një mjet i nevojshëm dhe efektiv për institucionet e zbatimit të ligjit, në shumë shtete anëtare, veçanërisht në çështjet serioze siç është krimi i organizuar dhe terrorizmi."[350]

Direktiva thekson se qëllimi i kësaj ndërhyrjeje është për të siguruar që të dhënat do të jenë në dispozicion për qëllimet e zbulimit, hetimit dhe ndjekjes penale të krimeve të rënda, siç është përcaktuar në bazë të ligjit kombëtar të Shteteve Anëtare,[351] për një periudhë jo më pak se gjashtë muaj dhe deri dy vjet nga data e komunikimit.[352] Prandaj duhet ti referohemi legjislacionit të Shteteve Anëtare për të parë saktësisht se në çfarë

---

[348] Direktiva është transpozuar në ligjin tonë kombëtar nga ligji nr. 9918, datë 19.05.2008 "*Për Komunikimet Elektronike në Republikën e Shqipërisë*" (Fletore Zyrtare nr.84, 10.06.2008) "*Ruajtja e të dhënave të krijuara ose të përpunuara në lidhje me vënien në dispozicion të publikut, shërbimet e komunikimeve elektronike ose e rrjeteve publike të komunikimit, të përdorin sistemet e mbikëqyrjes, me marrjen apo regjistrimin audio ose video në vende publike dhe dispozitat e lidhura*".

[349] Maras. M.H. (2012). "*Counterterrorism*", fq. 136, gjithashtu dhe Mordini, E. dhe De Hert P. (2010). "*Ageing and Invisibility*", fq.. 129.

[350] Opinion shpjegues 6 i Direktivës 2006/24/KE.

[351] Neni 1 i Direktivës 2006/24/KE.

[352] Neni 6.

termash dhe kushtesh do të bëhet zbatimi i Direktivës.[353] Veçanërisht Direktiva 2006/24/KE[354] parashikon, në derogim të neneve 5, 6 dhe 9 të Direktivës 2002/58/KE,[355] detyrimin e Shteteve Anëtare të miratojnë masa për të siguruar që të dhënat e përcaktuara në nenin 5 të Direktivës të mbahen në përputhje me dispozitat e tij, madje edhe kur të dhënat janë thirrje të humbura. Vetëm kur nuk arrihet lidhja, Direktiva nuk kërkon ruajtjen e të dhënave në lidhje me këto thirrje.[356] Sigurisht specifikohet me Direktivën, dispozitat që lidhen me trafikun e të dhënave dhe vendndodhjen (lokacionit) e të dhënave dhe jo përmbajtjen e komunikimit.[357] Në mënyrë të veçantë Direktiva 2006/24/KE përcakton në nenin 5, që mund të mbahen në përputhje me kushtet dhe qëllimet e Direktivës, të dhëna specifike për të cilat bëhet numërimi përfundimtar, ndërmjet të cilave janë:

a. të dhënat e nevojshme për të gjetur dhe identifikuar burimin e komunikimit,
b. të dhënat e nevojshme për identifikimin e destinacionit të komunikimit,[358]

---

[353] Në Shqipëri procedura dhe kriteret ligjore për qasje në të dhëna dhe heqjen e këtyre kushteve parashikohen në implementimin e neneve 6 dhe 7 të ligjit nr. 9918, datë 19.05.2008 "*Për komunikimet Elektronike në Republikën e Shqipërisë*". Për probleme në zbatimin e ardhshëm të Direktivës dhe zbatimin e saj në ligjin e brendshëm shih dhe Anne, C. dhe Meuwese M. (2008). "*Impact Assessment in European Union Lawmaking*", fq. 248.

[354] Për prezantimin dhe analizimin e dispozitave të Direktivës shih Gutwirth, S., Leenes, R. dhe De Hert, P. (2012). "*European Data Protection: In Good Health?*" fq. 218, gjithashtu Weber, R. H. dhe Heinrich, U. I. (2012). "*Anonymization*", fq. 41 si dhe Koenig, Ch. dhe Bartosch A. (2009). "*EC Competition and Telecommunications Law*", 2nd Edition, fq. 523.

[355] Nenet 5, 6 dhe 9 të Direktivës 2002/58/KE, përcaktojnë rregullat që zbatohen për përpunimin, ofruesit e shërbimit të rrjetit dhe shërbime të trafikut si dhe vendndodhjes së të dhënave të gjeneruara nga përdorimi i komunikimeve elektronike. Këto të dhëna duhet të fshihen ose bëhen anonime kur nuk është më e nevojshme për qëllimin e përhapjes së një komunikimi, përveç të dhënave të nevojshme për faturim dhe pagesat e interkoneksionit. Me kushtin e pëlqimit, të dhëna të caktuara gjithashtu mund të jenë të përpunuara për qëllime marketingu, si dhe për dhënien e vlerës së shtuar të shërbimeve.

[356] Neni 3 i 13 i Direktivës 2006/24/KE.

[357] Neni 2, paragrafi 2 a) dhe neni 5 paragrafi 2 dhe opinioni shpjegues 13 i Direktivës 2006/24/KE.

[358] Për rrjetin e telefonisë fikse dhe telefonisë celulare: Numri i quajtur ose numrat (numri ose numrat e thirrur), në rastet që përfshijnë shërbime suplementare të tilla si transferimi / devijimi i thirrjes, numri ose numrat e telefononit drejt të cilëve u bë thirrja telefonike, emrër/mbiemri dhe adresat e abonentëve ose të përdoruesve të regjistruar; në lidhje me adresën elektronike (e-mail) dhe telefonisë nëpërmjet internetit:

c. të dhënat e nevojshme për të identifikuar datën, kohën dhe zgjatjen e komunikimit,[359]
d. të dhënat e nevojshme për identifikimin e llojit të komunikimit,[360]
e. të dhënat e nevojshme për të identifikuar pajisjet e përdoruesve të komunikimit apo të supozuara si pajisje të tyre të komunikimit,[361]
f. të dhënat e nevojshme për të identifikuar vendndodhjen e pajisjeve të komunikimit të lëvizshëm (mobil)[362] si në telefoninë e rrjetit fiks dhe telefoninë e lëvizshme (celulare), si dhe qasjen në internet dhe postën elektronike (e-mail), si dhe telefoninë nëpërmjet internetit.[363]

---

numri i kartës së identitetit të përdoruesit ose numri telefonik i thirrjes së marrësit të parashikuar të thirrjes telefonike, emër/mbiemër dhe adresën e abonentit ose përdoruesit të regjistruar dhe numri i kartës së identitetit të përdoruesit të marrësit të parashikuar të komunikimit.

[359] Lidhur me rrjetet e telefoninë fikse dhe të telefonisë së lëvizshme (mobile), data dhe koha e fillimit dhe mbarimit të komunikimit; në lidhje me qasjen në internet dhe e-mail dhe telefonisë nëpërmjet internetit: data dhe koha e hyrjes dhe daljes nga interneti në një zonë të caktuar kohe,si dhe në adresën e protokollit të internetit (IP), qoftë dinamike apo statike që dha në komunikim ofruesi i shërbimit të komunikimit të aksesit në Internet, numri i kartës së identitetit të përdoruesit, të abonentit ose përdoruesit të regjistruar, data dhe koha e hyrjes dhe e daljes në shërbimin e postës elektronike (e-mail) ose të shërbimit të internetit, bazuar në një zonë të caktuar kohore.

[360] Lidhur me rrjetet e telefoninë fikse dhe të telefonisë së lëvizshme: shërbimi i përdorur telefonik ; në lidhje me postën elektronike (e-mail) dhe telefoninë nëpërmjet internetit: shërbimi i përdorur telefonik.

[361] Për sa i përket rrjetit të telefonisë fikse, numrat e telefonit të thirrësit dhe të thërriturit; lidhur me telefoninë e lëvizshme (mobile): numrat e telefonit të thirrësit dhtë thërriturit duke e quajtur dhe quhet Identiteti Ndërkombëtar i Abonentit (Pajtimtarit) të Telefonisë së Lëvizshme (International Mobile Subscriber Identity) (IMSI) e thirrësit, Identiteti Ndërkombëtar i Pajisjes së Telefonisë së Lëvizshme (International Mobile Equipment Identity) (IMEI) të thirrjes, ose IMSI i të thërriturit, ose IMEI i të thërriturit, ndërsa në rastin e shërbimeve të para-paguara anonime, nevojitet data dhe koha e aktivizimit fillestar të shërbimit dhe kodi i vendndodhjes (ID Cell) nga i cili u aktivizua shërbimi, për sa i përket lidhjes me internetin dhe adresën elektronike (e-mail) dhe Telefoninë nëpërmjet Internetit: numri telefonik i thirrjeve për hyrje (dial-up) nëpërmjet telefonit qasje, linjë digjitale e pajtimtarit (Digital Subscriber Line) (DSL) ose pikë tjetër në fund të burimit të komunikimit;

[362] Në mënyrë të veçantë këto janë kode të vendodhjes (ID Cell) në fillim të komunikimit; të dhënat me cilat identifikohet vendndodhja gjeografike e qelizave duke iu referuar kodeve të vendodhjes së tyre (ID Cell) gjatë periudhës për të cilën mbahen të dhënat e komunikimit.

[363] Si me rrjetet e telefonisë fikse dhe të telefonisë celulare: numri i telefonit të thirrësit, emri dhe adresa e pajtimtarit ose përdoruesit të regjistruar; në lidhje me qasjen në internet dhe adresën elektronike (e-mail)

Direktiva kërkon nga Shtetet Anëtare të sigurojnë që kategoritë e të dhënave të përcaktuara në nenin 5, të mbahen për periudha jo më pak se gjashtë muaj dhe jo më shumë se dy vjet nga data e komunikimit[364] duke problematizuar se si të sigurohen objektivat e Direktivës, d.m.th. hetimin, zbulimin dhe ndjekjen e veprave të rënda penale, ku kryerja e krimeve nuk mund të mos jetë zbuluar në kohën e ruajtjes së detyrueshme të këtyre të dhënave.[365] Gjithashtu parashikohet në nenin 12 të kësaj Direktive, se nëse një Shtet Anëtar përballet me rrethanat e veçanta që kërkojnë një shtrirje të kufizuar të periudhës së mbajtjes maksimale të përmendur në nenin 6 mund të marrë masat e nevojshme. Mjafton të njoftojë menjëherë Komisionin dhe të informojë shtetet e tjera anëtare mbi masat e marra dhe arsyet për të cilat i mori.[366] Direktiva parashikon gjithashtu, se për ruajtjen e të dhënave duhet të përmbushë disa parime të sigurisë nga ana e ofruesve të shërbimeve të komunikimeve elektronike. Prandaj është e nevojshme, që të dhënat e ruajtura të jenë të së njëjtës cilësi, të trajtohen me siguri dhe mbrojtje për të dhënat në dispozicion të publikut ose të një rrjeti publik të komunikimeve elektronike. Referimi është bërë gjithashtu edhe për nevojën për masa teknike dhe organizative për të mbrojtur të dhënat kundër shkatërrimit aksidental ose të paligjshëm, humbjes aksidentale, ndryshimit, ruajtjes së paautorizuar ose të paligjshme, përpunimit, aksesit ose përhapjes dhe për të siguruar që të dhënat mund të arrihen vetëm nga personeli i autorizuar special, që të dhënat të shkatërrohen në fund të periudhës së mbajtjes, përveç atyre që u është lejuar aksesi, të cilat janë ruajtur.[367]

Në çdo rast, të dhënat e ruajtura dhe çfarëdo informate tjetër në lidhje me to, duhet të transferohet sipas kërkesës së autoriteteve kompetente, pa vonesa të tepruara.[368]

---

si dhe telefonisë nëpërmjet Internetit: kodi që i jepet identitetit të përdoruesit, identiteti i përdoruesit dhe numri i telefonit që jepet për çdo komunikim që hyn dhe del në rrjetin publik telefonik, emrin dhe adresën e pajtimtarit ose përdoruesit të regjistruar që i atribuohet gjatë kohës së komunikimit adresa e internetit (Internet Protocol), numri i kartës së identitetit të përdoruesit ose numri i telefonit.

[364] Neni 6 i Direktivës 2006/24/KE.

[365] Po aty. Gutwirth, S., Leenes, R. dhe De Hert, P. (2012). fq.176.

[366] Neni 12.

[367] Neni 7.

[368] Neni 8.

Një pikë që është e rëndësishme, por që edhe të shqetëson, lidhet me paqartësinë e afatit "autoritetet kompetente", ku saktësisht do të thotë "pa vonesë të tepruar".[369]

Direktiva 2006/24/KE ka shkaktuar shumë reagime[370] dhe është konsideruar në kundërshtim me Konventën Evropiane për të Drejtat e Njeriut si dhe jurisprudencën e Gjykatës Evropiane të të Drejtave të Njeriut,[371] ku ka diskutime në lidhje me pajtueshmërinë e saj me kushtetutat kombëtare.[372] Ruajtja e detyrueshme e të dhënave dhe të gjithë atyre që janë përfshirë në një komunikim, edhe pse nuk ka asnjë provë për vepër penale, konsiderohet shkelje e parimeve të mbrojtjes së të dhënave personale, të tilla si parimi i ligjshmërisë së qëllimit dhe mënyrës së procesimit, si dhe parimin e proporcionalitetit, pasi të dhënat mblidhen në emër të objektivave të përgjithshme dhe të paqarta.[373] Tërësia e nenit të 29 si në opinionin e tij të parë,[374] ashtu dhe në opinionin e lëshuar pas miratimit të Direktivës 2006/24/KE, shpreh rrezikun që paraqet për të drejtat themelore të Direktivës,[375] ndërkohë që Direktiva mund të kontribuojë për cenimet e jetës së përditshme të qytetarëve që mund të vendosi në rrezik vlerat themelore dhe liritë që gëzojnë dhe çmojnë të gjithë qytetarët evropianë.

---

[369] Po aty. Taylor, M. fq. 311.Taylor beson se nuk do të ketë probleme teknike në transmetimin e të dhënave, mes përfituesve dhe autoriteteve kombëtare.

[370] Shih: informacion në lidhje me Grupin Punës (Arveitskreises Vorratsdatenspeicherung) të ngritur në Gjermani për të parandaluar aplikimin e Direktivës përkatëse në ligjin gjerman, në http://www.vorratsdatenspeicherung.de/content/view/16/39/lang,en/

[371] Rowland, D. (2004). "*Data Retention and the War Against Terrorism – A Considered and Proportionate Response?*", Journal of Information Law&Technology (JILT) në http://www2.warwick. ac.uk/fac/soc/law2/elj/jilt/2004_3/rowland/

[372] Buckland, J. A. (1992). "*Combating computer crime: prevention, detection, investigation*", fq. 308.

[373] Gutwirth, S., Poullet, Y., De Hert, P. dhe Leenes, R. (2011). "*Computers, Privacy and Data Protection: An Element of Choice*", fq. 403.

[374] Opinioni 2005 mbi propozimin e Direktivës së Parlamentit Evropian dhe Këshillit për ruajtjen e të dhënave të përpunuara, në funksion për të siguruar shërbimet publike të komunikimeve elektronike dhe amendimin e Direktivës 2002/58/KE [COM (2005) i datës 21.09 .2005, dalë më 21 tetor, 2005].

[375] Opinioni 3/2006 mbi Direktivën 2006/24/KE të Parlamentit Europian dhe Këshillit për ruajtjen e të dhënave të krijuara ose të përpunuara në lidhje me ofrimin e shërbimeve të komunikimeve elektronike të ;disponueshme për publikun ose të rrjeteve të komunikimeve publike dhe për ndryshimin e Direktivës 2002/58/KE.

Gjithashtu, plotëson opinionin e vet mbi propozimet për transpozimin e Direktivës, në një mënyrë uniforme dhe në përputhje me kërkesat e nenit 8 të Konventës Evropiane për të Drejtat e Njeriut. Për të arritur këtë objektiv propozon që Shtetet Anëtare të zbatojnë masa mbrojtëse të përshtatshme dhe specifike. Në mënyrë të veçantë, tërësia e nenit 29 thekson se, Direktivës i mungon mbrojtje adekuate dhe specifike për sa i përket përpunimit të të dhënave të komunikimit duke lënë hapësirë për interpretime të ndryshme dhe zbatimin e saj nga shtetet anëtare. Masat mbrojtëse të përshtatshme dhe të veçanta janë të nevojshme për të mbrojtur interesat jetike të individëve, siç referohet në Direktivën 2002/58/KE, në veçanti të drejtën për garantimin e konfidencialitetit kundër vendosjes në dispozicion të publikut shërbimet e komunikimeve elektronike, duke propozuar një sërë masash të nevojshme për të mbrojtur të dhënat personale, sipas dispozitave të Direktivës.[376] Ndërsa për transpozimin e Direktivës në një mënyrë uniforme dhe në përputhje me kërkesat e nenit 8 të Konventës Evropiane për të Drejtat e Njeriut, Neni 29 u bën thirrje Shteteve Anëtare për të zbatuar masat e duhura dhe specifike mbrojtëse të mëposhtme:

1) "Respektimi i të dhënave justifikohet vetëm për qëllime të veçanta. Prandaj, termi "krim i rëndë" duhet të përcaktohet qartë dhe të përshkruhet në mënyrë të qartë;
2) Të dhënat duhet të jenë në dispozicion vetëm të autoriteteve të caktuara posaçërisht në zbatim të ligjit;
3) Të dhënat e mbajtura nën ruajtje duhet të ruhen në minimum;
4) Hetimi, zbulimi dhe ndjekja e veprave penale të përmendura në Direktivë nuk duhet të interpretohet në shkallë të gjerë të të dhënave, bazuar në të dhënat e ruajtura në lidhje me zakonet e udhëtimit dhe komunikimit të qytetarëve, të cilët nuk dyshohen nga Autoritetet në zbatimit të ligjit;
5) Qasja në të dhënat duhet të autorizohet nga autoritetet gjyqësore, me rezervat e vendeve ku qasja specifike lejohet nga ligji dhe i nënshtrohet mbikëqyrjes së pavarur;
6) Ofruesit e shërbimeve publike ose rrjeteve të komunikimeve elektronike të mos kenë të drejtë të procesojnë për qëllime të tjera, sidomos të dhënat e tyre që

[376] Po aty. fq. 1.

mbahen ekskluzivisht për qëllime të rendit publik në përputhje me Direktivën përkatëse."[377]

Kohët e fundit Gjykata Federale Kushtetuese e Gjermanisë, hodhi poshtë legjislacionin e debatueshëm, që i imponon kompanive të telekomunikacionit të ruajnë të dhënat e thirrjeve telefonike dhe trafikut të internetit për 6 muaj, me qëllim që të jenë në dispozicion të Autoriteteve në konfrontimin e terrorizmit dhe krimit. Vendimi i Gjykatës së Lartë Gjermane përcakton, se këto të dhëna duhet të fshihen menjëherë, ndërkohë që ky ligj të jetë përsëri i zbatueshëm, kërkohen rreptësishtë ndryshime. Gjykata vendosi që ruajtja e të dhënave, nuk ishte mjaftueshmërisht e sigurt dhe se nuk ishte i qartë përdorimi i mundshëm i tyre. Kështu vuri në dukje se ligji i ka tejkaluar kërkesat e Direktivës Evropiane. Ligji nuk u hodh poshtë në tërësinë e tij, por u pezullua zbatimi i tij, deri sa të bëheshin ndryshimet e nevojshme që kufizojnë fushëveprimin. Gjykata u shpreh se kërkohet përfshirje e Autoritetit të Pavarur për Mbrojtjen e të Dhënave, për të verifikuar përdorimin e të dhënave të ruajtura personale. Gjithashtu përcaktoi se përdorimi i kësaj baze të dhënash, duhet të bëhet sipas urdhrit të gjykatës.[378]

Disa nga paditësit shpresuan që vendimi do të gjykojë antikushtetues ruajtjen e të dhënave dhe se do të kundërshtonte ligjin në tërësi, gjë që nuk ndodhi. Çështjen e sollën para Gjykatës Supreme 35.000 qytetarë, duke përfshirë Ministren e Drejtësisë Gjermane Sabine Leutheusser-Schnarrenberger. Vendimi u parapri nga paralajmërimet e qeverisë për kompanitë si Google, Facebook e Microsoft me qëllim që këto të fundit të zbatojnë një politikë më transparente të ruajtjes së të dhënave të përdoruesve të internetit.[379] Më datë 18 Prill 2011, Komisioni Evropian miratoi një raport të vlerësimit të Direktivës për mbajtjen e të dhënave e cila rezulton në një grup konkluzionesh mbi zbatimin e Direktivës së zbatuar që nga viti 2006 deri më sot.[380] Konkluzionet e raportit

[377] Po aty. fq. 2-3.

[378] http://www.spiegel.de/international/germany/0,1518,681251,00.html (02.03.2010) gjithashtu shih: përmbledhjen e tekstit të vendimit në gjuhën angleze në http: //www. datatilsynet.no /upload/ dokumenter/dommer/pressrelease_dataretention_bundesverfassu ngsgericht.pdf

[379] Po aty.

[380] Report from the Commission to the Council and the European Parliament "Evaluation report on the Data Retention Directive (Directive 2006/24/EC) http ://ec.europa. eu/commission _20102014/ malmstrom/archive/20110418_data_retention_evaluati on_en.pdf

të vlerësimit janë përmbledhur në deklaratën për shtyp të Komisionit Evropian si më poshtë:[381]

- Shumica e shteteve anëtare bien dakord mbi domosdoshmërinë e ruajtjes së të dhënave për zbatimin e ligjit, mbrojtjen e viktimave dhe sistemet e drejtësisë penale.
- Ekzistojnë dallime të mëdha në inkorporimin e Direktivës përkatëse 2006/24/KE, për shembull, periudhat e ruajtjes të ndryshojnë midis 6 muajve dhe 2 vjetëve, qëllimet për të cilat ajo mund të fitojë qasje në të dhëna, përdorimin e të dhënave, si dhe procedurat ligjore për t'u futur në të dhëna që ndryshojnë në mënyrë të konsiderueshme.
- Vështirësitë e harmonizimit të Direktivës me ligjet kombëtare mund të krijojnë vështirësi për ofruesit e shërbimeve të telekomunikacionit, veçanërisht për ofruesit e vegjël. Dëmshpërblimi i ofruesve në BE, ndryshon në shpenzimet për të ruajtur dhe të siguruar qasje në të dhëna.
- Njihet se ruajtja e të dhënave është një kufizim i të drejtës së privatësisë. Prandaj dhe Komisioni do të konsiderojë një rregullim më të rreptë të ruajtjes, qasjes, dhe përdorimit të të dhënave të ruajtura

Publikimi i raportit ka pasur si qëllim të nxjerrë në pah rëndësinë e rregulloreve përkatëse për të luftuar krimin dhe terrorizmin, si një përgjigje ndaj kritikave intensive që ende vazhdojnë mbi efektet e shkeljes së të dhënave personale dhe privatësisë, ndërsa, siç është përmendur nga Komisioneri i BE për Çështjet e Brendshme Cecilia Malmstrom, tashmë shqyrtohet amendimi i saj në lidhje me të cilën, lejohet futja në të dhënat e ruajtura në burim, si dhe qëllimi dhe procedurat e hyrjes në to.[382]

---

[381] Komisioni vlerëson Direktivën mbi ruajtjen e të dhënave të telekomunikacionit, në http://europa. eu/ rapid/pressReleasesAction.do?reference=IP/11/484format=HTML&aged=0&lang uage =EL&g ui Langu age=fr

[382] Shih: Konferencën për shtyp të Komisioneres Cecilia Malmstrom për Punët e Brendshme "*Data Retention Directive – a valuable tool in fighting serious crime and terrorism, but in need of improvement*", Press conference on the Evaluation report on the Data Retention Directive Brussels, 18 April 2011, në http://europa.eu/rapid/pressReleasesAction. do?reference =SPEECH/ 11/ 280 & format=HTML&aged=0&language=EN&guiLanguage=en

3.3.3.2 Direktiva 2009/136/KE

Brenda prizmit të zhvillimeve teknologjike në treg, Komisioni nisi planin e tij për rishikimin[383] e kuadrit rregullator të BE-së në lidhje me rrjetet dhe shërbimet e komunikimeve elektronike. Në mënyrë të veçantë, Komisioni ka shqyrtuar funksionimin e pesë Direktivave që përbëjnë kuadrin ekzistues rregullator për rrjetet dhe shërbimet e komunikimeve (Direktiva 2002/19/KE, Direktiva 2002/20/KE, Direktiva 2002/21/KE, Direktiva 2002/22/KE dhe Direktiva 2002/58/KE) së bashku të referuara si "Direktiva Kuadër dhe Direktiva specifike" dhe në veçanti për të përcaktuar nëse ekziston nevoja për modifikim në prizmin e zhvillimeve teknologjike në treg.[384] Përfundimisht përmes procedurës së nenit 251 të Traktatit të KE-së,[385] që themeloi Direktivën 2009/136/KE,[386]

---

[383] Rishikimi i kuadrit rregullator të BE-së për rrjetet e komunikimeve elektronike dhe shërbimeve është një hap i rëndësishëm drejt arritjes së Hapësirës së Vetme Evropiane Informative dhe në të njëjtën kohë të shoqërisë së informacionit pa përjashtime, të cilat përbëjnë objektiva që përfshihen në kuadrin strategjik për zhvillimin e shoqërisë së informacionit, "*i2010 - Një shoqërie Evropiane e informacionit për zhvillim dhe punësim*". Shih: Komunikatën e Komisionit për Këshillin, Parlamentin Evropian, Komitetin Ekonomik dhe Social Evropian dhe Komitetin e Rajoneve – "*Strategjia i2010 - Një shoqërie Evropiane e informacionit për zhvillim dhe punësim*" {SEC(2005) 717}/* COM/2005/0229, në http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0229:EL:NOT.

[384] Shih: gjithashtu: Opinionin-2/2008 për rishikimin e Direktivës 2002/58/KE për mbrojtjen e privatësisë në sektorin e komunikimeve elektronike (Direktiva "*Për mbrojtjen e privatësisë në komunikimet elektronike*"), në http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/ 2008/wp150 _ eng.pdf, Opinioni 1/2009 mbi propozimin për ndryshimin e Direktivës 2002/58/KE për mbrojtjen e privatësisë në sektorin e komunikimeve elektronike (Direktiva "*Për mbrojtjen e privatësisë në komunikimet elektronike*"), në http://ec.europa.eu/justice_home/fsj /privacy/docs/wpdocs/2009 /wp159 _eng.pdf dhe Opinioni i dytë i Mbikëqyrësit Evropian për Mbrojtjen e të Dhënave mbi rishikimin e Direktivës 2002/58/KE në lidhje me përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike (Direktiva për privatësinë dhe BE (2009 / C128/04).

[385] Komisioni do të paraqesë një propozim për Parlamentin Evropian dhe Këshillin. Këshilli, duke vepruar me shumicë të cilësuar, pas konsultimit me Parlamentin Evropian do të miratojë aktin e propozuar, ose të miratojë një qëndrim të përbashkët dhe t'ia komunikojë atë Parlamentit Evropian, i cili nga ana e tij ose miraton këtë pozicion të përbashkët ose refuzon apo propozon amendamente. Këshilli, me shumicë të cilësuar, miraton ose jo, me procedurën e pajtimit të palëve, të vazhdojë në botimin e aktit mbi tekstin e përbashkët, të rënë dakord.

[386] Direktiva 2009/136/KE e Parlamentit Evropian dhe e Këshillit e datës 25 nëntor 2009 amendon Direktivën 2002/22/KE mbi shërbimin universal dhe të drejtat e përdoruesve në lidhje me rrjetet e

e cila merret me ndryshimet në Direktivat 2002/22/KE[387] dhe 2002/58/KE[388] ku rregullon çështjet lidhur me bërjen publike të shkeljeve të dispozitave mbi të dhënat personale të përfshira në Direktivën 2002/58/KE. Kërkon dhënien e informacionit mbi masat e marra nga ofruesi për adresimin e shkeljes, si dhe rekomandimet për pajtimtarët (abonentët) ose individët në fjalë. Inkurajon përdoruesit e fundit të marrin hapat e nevojshme për të mbrojtur pajisjet e tyre fundore kundër viruseve dhe "programeve spiune" (spyware). Thekson se metodat për ofrimin e informacioneve dhe ofrimin e të drejtës së refuzimit, duhet të jenë mundësisht sa më të qarta dhe të realizueshme. Ofruesve të postës elektronike dhe shërbimeve të tjera, duke pasur parasysh fundin, i jepet mundësia e rekursit ligjor kundër mesazheve elektronike bllokues (spammers) të karakterit komercial dhe për këtë arsye të mbrojnë interesat e klientëve të tyre, si pjesë e interesave të ligjshme të biznesit të tyre. Veçanërisht në Nenin 2 të Direktivës 2009/136/KE ose Direktivën 2002/58/KE (Direktiva për privatësinë në komunikimet elektronike) ndryshohet si vijon:

Në nenin 1 të Direktivës 2002/58/KE në të cilin përcaktohet fushëveprimi dhe qëllimi Direktivës, paragrafi 1 është zëvendësuar nga i riu i cili ndryshon nga i mëparshmi vetëm në shtimin e të drejtës së konfidencialitetit përveç asaj të privatësisë.[389] Nevoja për shtimin e afatit të termit të konfidencialitetit, nuk është shpjeguar në preambulën e Direktivës së re. Ne mund të konsiderojmë se përdorimi i termit në Nenin 1 shërben për të përfunduar qëllimin e Direktivës, në mënyrë që ajo të pajtohet me pjesën tjetër të tekstit, ku termi "Confidentialité" dhe "Confidentiality" në versionin francez dhe anglez të Direktivës 2002/58/KE, shfaqet në preambul dhe titullin

komunikimeve elektronike dhe shërbimeve, të Direktivës 2002/58 / KE në lidhje me përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike dhe Rregulloren (EC) Nr. 2006/2004, për bashkëpunimin ndërmjet autoriteteve kombëtare përgjegjëse për zbatimin e mbrojtjes së konsumatorit. Gazeta Zyrtare e Bashkimit Evropian L 337/11.

[387] Direktiva për shërbimin universal.

[388] Direktiva për mbrojtjen e privatësisë në komunikimet elektronike.

[389] Neni 2 paragrafi 1 i Direktivës 2009/136/KE: "*Kjo Direktivë parashikon harmonizimin e dispozitave kombëtare të kërkuara për të siguruar një nivel ekuivalent të mbrojtjes së të drejtave dhe lirive themelore, veçanërisht të drejtën për privatësi, konfidencialitetit në lidhje me përpunimin e të dhënave personale në sektorin e komunikimeve elektronike dhe për të siguruar lëvizjen e lirë të këtyre të dhënave dhe të pajisjeve të shërbimeve elektronike të komunikimit në Komunitet*".

e nenit 5.[390] Direktiva e re përparon dhe në një seri ndryshimesh të përkufizimeve të Direktivës 2002/58/KE, me rishikimin e përkufizimit të të dhënave të vendndodhjes, me heqjen e përkufizimit "Thirrje"[391] dhe shtimin e përkufizimit të "shkeljes së të dhënave personale". Koncepti i të dhënave të vendndodhjes modifikohet. "Të dhënat e vendndodhjes" nuk janë vetëm të dhënat që i parashtrohen përpunimit në një rrjet të komunikimeve elektronike, por që tregojnë pozicionin gjeografik të pajisjes fundore në dispozicion të një përdoruesi të shërbimeve të komunikimeve elektronike të disponueshme për publikun dhe të dhënave të përpunuara nga një shërbim i komunikimeve elektronike.[392]

Shtimi i termit "shërbim i komunikimeve elektronike" është në përputhje me frymën dhe letrën e Direktivës dhe kontribuon në përmirësimin dhe të kuptuarin e Direktivës, pasi përpunimi i të dhënave të vendodhjes, ndodh kur i ofrohet shërbimi para paguesit/përdoruesit. Analizohet si "shkelje e të dhënave personale", shkelja e sigurisë që çon në shkatërrimin aksidental apo të paligjshëm, humbjen, ndryshimin, zbulimin e paautorizuar apo në qasje në të dhënat personale të cilat transmetohen, ruhen ose janë përpunuar në një mënyrë tjetër në lidhje me ofrimin e shërbimeve të komunikimeve elektronike në dispozicion të publikut në Komunitet.[393] Nevoja për implementimin e konceptit të shkeljes së të dhënave personale çoi në hartimin përfundimtar të një përkufizimi, qëllimi i të cilit do të jetë i mjaftueshëm "për të përfshirë shumicën e shkeljeve të mundshme të tilla, si rastet e qasjes së paautorizuar të palës së tretë në të dhënat personale, ndërhyrjes së padrejtë në server që përmban të dhëna personale dhe korrigjimin e të dhënave të tilla".[394] Përkufizimi do të përfshijë edhe rastet kur të dhënat personale janë humbur ose janë publikuar, edhe pse nuk është provuar ende se ka pasur

[390] Në përkthimin shqip të Direktivës 2002/58/KE termi "*Confidentialité*" dhe "*Confidentiality*" në frëngjisht dhe anglisht kontribuohet si fshehtësi, por këtë herë në Direktivën 2009/136/KE ofrohet si "*konfidencialitet*", duke krijuar pyetje në lidhje nëse kjo është vetëm një qasje e ndryshme ose përkthim që shpreh një ndryshim thelbësor konceptual.

[391] Siç tregohet në Direktivën 2002/58/KE "*Thirrje*" është lidhja e bërë përmes një shërbimi telefonik në dispozicion të publikut duke lejuar komunikimin e dyanshëm në kohë reale. Në nenin 2, paragrafi 2, pika B të Direktivës 2009/136/KE thuhet në mënyrë eksplicite se elementi d) fshihet.

[392] Neni 2, paragrafi 2, pika A, i Direktivës 2009/136/KE

[393] Po aty. Paragrafi 2, pika I.

[394] Pika 20 e Opinionit të dytë të Mbikëqyrësit Evropian për Mbrojtjen e të Dhënave Personale.

akses të paautorizuar. Kjo do të përfshijë rastet kur të dhënat personale mund të jenë humbur (p.sh. për shkak të ruajtjes në CD ROM , USB ose pajisje të tjera portative), ose publikuar nga përdoruesit e rregullt (dosje me të dhënat e punonjësve që vihen në dispozicion të publikut aksidentalisht dhe shkurtimisht nëpërmjet internetit). Për shkak se nganjëherë nuk mund të vërtetohet se të tretët e paautorizuar në një kohë të caktuar, mund të kenë akses ose jo në të dhënat, por është padyshim e qëllimshme të kualifikohen në kuadër të përkufizimit menjëherë mbi rastet e lartpërmendura.[395] Direktiva 2009/136/KE është zëvendësuar me nenin 3 të Direktivës 2002/58/KE, nëse ai zbatohet përveç në përpunimin e të dhënave personale në lidhje me ofrimin e shërbimeve të komunikimeve elektronike, në dispozicion të publikut, në rrjetet e komunikimit publik në Komunitet dhe në rastet e rrjeteve publike të komunikimit që mbështesin pajisje të mbledhjeve të të dhënave dhe identifikimit.[396] Pika më e rëndësishme dhe thelbësore për rishikimin e Direktivës 2002/58/KE është rishikimi i nenit 4, në lidhje me sigurinë e rrjetit të komunikimeve elektronike.[397] Duke zëvendësuar titullin e parë (të cilit i shtohet termi i përpunimit), i cili vendoset në nenin e deritanishëm dhe paragrafin e parë, ku thekson se masat në paragrafin 1[398] duhet të paktën:

a. të sigurojnë që të dhënat personale mund të arrihen vetëm nga personeli i autorizuar për qëllime të autorizuara ligjërisht,[399]

b. të mbrojnë të dhënat personale të ruajtura ose të transmetuara nga shkatërrimi aksidental ose i paligjshëm, nga humbja aksidentale apo ndryshimi dhe ruajtja e paautorizuar ose e paligjshme, nga përpunimi, aksesi ose përhapja.

c. të sigurojnë zbatimin e sigurisë në lidhje me përpunimin e të dhënave personale.

---

[395] Pika 21 e Opinionit të dytë.

[396] Neni 2, paragrafi 3 i Direktivës.

[397] Po aty. Paragrafi 4.

[398] "*Ofruesi i shërbimit të komunikimeve elektronike në dispozicion të publikut duhet të marrë, nëse është e nevojshme bashkërisht me ofruesin e rrjetit të komunikimit publik në lidhje me sigurinë e rrjetit, masa të përshtatshme teknike dhe organizative për të mbrojtur sigurinë e shërbimeve të tij. Duke marrë parasysh aftësitë e fundit teknike dhe koston e zbatimit të tyre, këto masa duhet të sigurojnë një nivel të duhur të sigurisë, të ngjashëm me rrezikun ekzistues*".

[399] Shih: gjithashtu Arsyetimin shpjegues 57 par. b të Direktivës 2009/136/KE.

Gjithashtu siguron që masat e marra nga ofruesit e shërbimeve të komunikimeve elektronike të disponueshme për publikun, do të inspektohen nga autoritetet kompetente kombëtare, të cilat do të nxjerrin rekomandime për praktikat më të mira në lidhje me nivelin e sigurisë që duhet të arrihet me këto masa. Në vazhdim u shtua paragrafi 3 në nenin 4 të Direktivës 2002/58/KE,[400] i cili parashikon që në rast të shkeljes së të dhënave personale:

a. personi ofrues i shërbimit të komunikimeve elektronike në dispozicion të publikut duhet të zbulojë dhe të njoftojë pa vonesë, shkeljen e të dhënave personale tek autoritetet kompetente kombëtare.[401]

b. ofruesi duhet të japë gjithashtu informacion shpjegues për shkeljen e bërë ndaj abonentit para pagues ose individit të interesuar, pa vonesa të panevojshme kur shkelja e të dhënave personale ka të ngjarë të ndikojë negativisht në të dhënat personale të një abonenti para pagues apo një personi në privatësinë e tyre.[402]

c. njoftimi i shkeljes së të dhënave personale të një abonenti (pajtimtari) ose personi të interesuar, nuk ka nevojë të ndodhë nëse ofruesi ka demonstruar në mënyrë të pranueshme ndaj autoritetit kompetent që i ka zbatuar masat e përshtatshme teknologjike mbrojtëse dhe se këto masa janë zbatuar për të dhënat në lidhje me shkeljen e sigurisë. Për më tepër theksohet se këto masa të mbrojtjes teknologjike duhet t'i bëjnë të dhënat e pakuptueshme për çdo person, i cili nuk është i autorizuar të ketë qasje në këto të dhëna.

d. nëse ofruesi nuk e ka njoftuar tashmë abonentin ose individin e interesuar për shkeljen e të dhënave personale, e bën autoriteti kompetent kombëtar, duke marrë në konsideratë ndikimin e mundshëm të shkeljes, pra mund t'i kërkojë ofruesit që ai të bëjë këtë njoftim të domosdoshëm ndaj abonentit.[403]

e. njoftimi duhet:

1. Të përmbajë të paktën natyrën e shkeljes së të dhënave personale dhe pikat e kontaktit ku ata mund të marrin informacion shtesë.

---

[400] Neni 2, paragrafi 4, pika c) e Direktivës 2009/136/KE.

[401] Po aty. Paragrafi 4, pika c).

[402] Risia e futur në këtë pikë është përdorimi i fjalës "*persona të interesuar*" e cila zgjeron kategorinë e përfituesve, të cilëve u njoftohet shkelja e sigurisë, në mënyrë që të përfshijë të gjithë personat e ineresuar dhe jo vetëm "*abonentët*".

[403] Pa cenuar detyrimin e ofruesit për të njoftuar abonentët e interesuar dhe individët në fjalë.

2. Të rekomandojë masa për të zbutur efektet e mundshme negative të shkeljes së të dhënave personale.
3. Ndërsa, në njoftimin tek autoriteti kompetent kombëtar duhet të përshkruhen pasojat e shkeljes dhe masat e propozuara ose të ndërmarra nga ofruesi, për të konfrontuar shkeljen e privatësisë.

Vihet në dukje se neni 4 i Direktivës 2009/136/KE, ishte fillimisht fusha e konsultimeve mes palëve të përfshira në procesin e rishikimit të Direktivës 2002/58/KE. Fillimisht objekt i mosmarrëveshjeve të diskutueshme ishte gama e subjekteve që do të mbulohen në kërkesën e njoftimit. U argumentua se këto detyrime duhet të shtrihen dhe tek ofruesit e shërbimeve të shoqërisë së informacionit, si në bankat on-line (në linjë), në aktivitetet on-line të sipërmarrjeve, ofruesit e shërbimeve shëndetësore on-line, etj.,[404] sepse zgjerimi i fushës së zbatimit do të ndihmojë për të rritur vetëdijen publike dhe do të reduktoheshin rreziqet në fushën e sigurisë.[405] Mbikëqyrësi Evropian për Mbrojtjen e të Dhënave vë në dukje në opinionin e tij të dytë, se shkeljet e sigurisë kanë për qëllim jo vetëm kompanitë e telekomunikimit por dhe llojet e tjera të kompanive/ofruese, të tilla si kompanitë e shitjes me pakicë on-line, bankat on-line, farmacitë on-line,[406] duke rezultuar se shkelja e llojeve të ndryshme të të dhënave personale mund të ketë ndikim serioz në jetën private të një personi.[407] Edhe pse në dispozitat e Direktivës 2009/136/KE nuk është theksuar se këto dispozita zbatohen jo vetëm për ofruesit e shërbimeve të komunikimeve elektronike, por dhe për ofruesit e shërbimeve të shoqërisë së informacionit. Në preambul thuhet në mënyrë eksplicite se

[404] Opinion 2/2008 për rishikimin e Direktivës 2002/58/KE mbi mbrojtjen e privatësisë në sektorin e komunikimeve elektronike (Direktiva "*Për mbrojtjen e privatësinë në komunikimet elektronike*") fq. 3, në http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_el.pdf (14.01.2010)

[405] Shih: Clarke R. A. dhe Knake K. (2012). "*Cyber War: The Next Threat to National Security and What to Do About It*", fq.127.

[406] Shih: pikën 23 të opinionit të dytë të Mbikëqyrësit Evropian për Mbrojtjen e të Dhënave për rishikimin e Direktivës 2002/58/KE, në lidhje me përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike. (Direktiva mbi privatësinë e BE-së (2009/ C 128/04).

[407] Bankat dhe institucionet e tjera financiare mund të jetë në posedim të informacionit tepër konfidencial (p.sh. të dhënat e llogarive bankare), zbulimi i të cilave mund të mundësojë përdorimin për vjedhjet e identitetit, ndërsa përpunimi dhe shkelja e të dhënave të ndjeshme personale të shërbimeve shëndetësore on-line në lidhje me shëndetin, mund të jetë veçanërisht e dëmshme për individët.

“..... nevoja për kërkesë të qartë dhe njoftim të detyrueshëm në të gjitha fushat, si dhe te ofruesit e shërbimeve të shoqërisë së informacionit, duhet të konsiderohet si një prioritet në nivel të BE-së”.[408] Kështu, inkurajohen legjislacionet kombëtare që të ndërmarrin hapa të menjëhershëm dhe të përshtatshme për zbatimin e parimeve që rregullojnë rregullat për shkeljen e të dhënave në Direktivën 2002/58/ KE, pavarësisht nga sektori apo lloji i të dhënave.[409]

Paragraf i ri 4 i cili i shtohet nenit 4 të Direktivës 2002/58/EK[410] parashikon që autoritetet kompetente kombëtare mund të:

a) miratojnë udhëzime,

b) nxjerrin udhëzime në lidhje me rrethanat në të cilat kërkohet nga ofruesi, njoftimin e shkeljeve të të dhënave personale, zbulimin e shkeljeve të të dhënave personale, formatin e njoftimit të tillë, si dhe mënyrën në të cilën duhet të bëhet njoftimi,
c) të jenë në gjendje për të monitoruar nëse ofruesit kanë përmbushur detyrimet e tyre në lidhje me zbulimin e shkeljes së të dhënave personale dhe
d) imponojnë masat e duhura ndëshkimore në rast pakujdesie të ofruesve për ta bërë këtë.

Për të ndihmuar autoritetet kompetente kombëtare, ofruesit duhet të mbajnë regjistrime të shkeljeve të të dhënave personale që përbëjnë përshkrimin e fakteve relevante, rezultatet e tyre, efektet dhe masat që janë marrë, në një nivel që lejon autoritetet kompetente kombëtare për të verifikuar përputhjen me dispozitat e paragrafit 3.

Neni 4 plotësohet me paragrafin e fundit, në të cilën thuhet se Komisioni mund të miratojë masa teknike të zbatimit lidhur me rrethanat, format dhe procedurat që zbatohen në kërkesat e informimit dhe njoftimit për të siguruar qëndrueshmërinë e masave të propozuara, gjithmonë në bashkëpunim dhe në përfshirjen e palëve të interesuara. Lidhur me çështjen e pëlqimit paraprak neni 5,[411] i paragrafit 3 të Direktivës

[408] Opinion shpjegues 59 i Direktivës 2009/136 /KE.

[409] Po aty.

[410] Neni 2, paragrafi 4, c) të Direktivës 2009/136/KE.

[411] 1. Shtetet Anëtare do të sigurojnë, me anë të legjislacionit kombëtar, konfidencialitetin e komunikimeve me anë të rrjetit të komunikimit publik dhe shërbimeve të komunikimeve elektronike të

2002/58/KE është zëvendësuar nga neni 2, paragrafi 5 i Direktivës 2009/136/KE. Në veçanti, në nenin 5, paragrafi 3 të Direktivës 2002/58/KE, parashikohej që kontrolluesi i të dhënave fillimisht i jepte përdoruesit / pajtimtar informacione të qarta dhe të plota në përputhje me Direktivën 95/46/KE, ndër të tjera në lidhje me qëllimet e përpunimit, në vazhdim i jep atij të drejtën të refuzojë ruajtjen e informacionit apo për të fituar qasje në informacionin e ruajtur në pajisjet e tij fundore. Dispozita e re e nenit 2, paragrafi 5 e Direktivës 2009/136 5/KE kërkon në çdo rast miratimin e mëparshëm paraprak duke i dhënë prioritet sistemit opt-in. Kjo është një dispozitë e nevojshme të rishikohet, për të qenë në përputhje me të gjithë Direktivën 2002/58/KE, e cila karakterizohet nga dominimi i sistemit të pëlqimit paraprak për përpunimin e të dhënave personale.[412] Në fjalinë e dytë të të njëjtit paragraf, Direktiva 2002/58/KE është rishikuar në hapësirën e dhënë që të lejojë çfarëdo ruajtje apo qasje (aksesi) teknike, ose kur qëllimi i vetëm i së cilës është kryerja e një transmetimi komunikimi,[413] përmes rrjetit të komunikimeve elektronike, ose kur është absolutisht e nevojshme për të mundësuar ofruesin e shërbimit të shoqërisë së informacionit, që është kërkuar në mënyrë të qartë nga para paguesi ose

---

disponueshme për publikun si dhe të dhënat lidhur me trafikun. Në veçanti, ata do të ndalojnë të dëgjuarit, përgjimin, magazinimin ose lloje të tjera të përgjimit apo vëzhgimin e komunikimeve dhe të dhënave të lidhura me trafikun nga persona të tjerë, me përjashtim të përdoruesve, pa pëlqimin e përdoruesve të interesuar (në fjalë), përveç kur autorizohet me ligj, në përputhje me nenin 15 paragrafi 1. Ky paragraf nuk parandalon ruajtjen teknike e cila është e domosdoshme për bartjen e komunikimit pa paragjykuar parimin e konfidencialitetit.

2. Paragrafi 1 nuk do të ndikojë në asnjë autorizim ligjor për regjistrimin e komunikimeve dhe të dhënave lidhur me trafikun, kur kjo kryhet në rrjedhën e praktikës ligjore të biznesit për qëllimin e ofrimit të dëshmisë së transaksioneve komerciale ose për ndonjë komunikim tjetër biznesi.

3. Shtetet Anëtare sigurojnë që përdorimi i rrjeteve të komunikimeve elektronike për të ruajtur informacion apo për të fituar qasje në informacionin e ruajtur në pajisjet terminale të një para paguesi ose shfrytëzuesi i lejohet vetëm nëse i ofrohen një para paguesi ose shfrytëzuesi të veçantë ,informacion i qartë dhe i plotë, në përputhje me Direktivën 95/46/KE. Ndër të tjera në lidhje me qëllimet e procesimit, dhe përgjegjësia për kontrollin e të dhënave të tij, përdoruesi ka të drejtë të refuzojë një procesim të tillë. Kjo nuk parandalon ndonjë ruajtje teknike ose aksesin, për të vetmin qëllim të së cilës është kryerja ose lehtësimi i transmetimit të komunikimit përmes një rrjeti të komunikimeve elektronike, apo kur është e domosdoshme vetëm për ofrimin e shërbimit për shoqërinë e informacionit, e cila është kërkuar shprehimisht nga përdoruesi ose para paguesi.

[412] Kosta. E (2013). "*Consent in European Data Protection Law*", fq.85.

[413] Fjalia e dytë, paragrafi 3, Direktiva 2002/58/KE.

shfrytëzuesi për të ofruar këtë shërbim. Shtimi i ndajfoljes "absolutisht", ende duket se reflekton një shtrëngim të kushteve në një nivel simbolik pasi ajo nuk është shoqëruar me analiza të mëtejshme. Gjithashtu paragrafi 3 i nenit 6 u zëvendësua me shtimin në vend të dukshëm të mbiemrit "i mëparshëm" me pëlqimin që kërkohet të jepet nga parapaguesi ose shfrytëzuesi për përpunimin e të dhënave të tyre personale për qëllime të marketingut të shërbimeve dhe komunikimeve elektronike, ose për sigurimin e shërbimeve me vlerë të shtuar.[414] Natyrisht organi ligjvënës nuk ka dashur të ketë ndonjë dyshim se kur duhet të jepet pëlqimi, i cili nga objekti i të gjitha rregullimeve tregon në mënyrë të qartë se ai duhet të jepet përpara se të bëhet përpunimi.

Në lidhje me "Thirrjet e Pa kërkuara"[415] vihen re ndryshimet e mëposhtme në nenin 13 të Direktivës 2002/58/KE. Në paragrafin 1 në pikën ku referohet, se lejohet përdorimi i sistemeve të thirrjeve automatike, shtohet fjala "komunikim" dhe "mund të lejohet", duke i lënë legjislacioneve kombëtare për të vendosur nëse do të lejojnë apo jo përdorimin e tyre në lidhje me abonentët ose përdoruesit, të cilët kanë dhënë pëlqimin e tyre paraprak. Në vazhdim në paragrafin 2, theksohet se përdorimi i të dhënave të kontaktit të postës elektronike të klientit, nëpërmjet shitjes së një produkti apo shërbimi nga një person fizik ose juridik për marketing të drejtpërdrejtë të produkteve të tyre të ngjashme ose të shërbimeve, mund të jenë të lejueshme me kusht që klientëve të tyre, t'u jepet qartë dhe dukshëm mundësia të kundërshtojnë pa para dhe lehtësisht këtë mbledhje. Gjithashtu të mundësojë përdorimin e hollësive të kontakteve elektronike, duke i shtuar kërkesën e tyre, që të jetë e mundur për klientët të kundërshtojnë atë në kohën e mbledhjes së të dhënave të mësipërme.[416] Në paragrafin e tretë për të përfunduar mbrojtjen e dhënë për ndalimin e thirrjeve të pa kërkuara, kur mungon pëlqimi i të interesuarve, i shtohet atyre përveç abonentit dhe përdoruesi, i cili për arsye të panjohura ishte lënë jashtë Direktivës fillestare 2002/58 KE.[417]

Lidhur me ndalimin e zbulimit të identitetit të dërguesit ose personit në emër të të cilit është dërguar mesazhi pa një adresë të vlefshme të dërguesit, i shtohet një arsye e

[414] Neni 6, i Direktivës 2009/136/ KE.

[415] Neni 7.

[416] Rregullimi i mëparshëm parashikonte ".... dhe kjo me çdo mesazh ...." .

[417] Rregullimi i mëparshëm parashikonte "Opsioni përkatës përcaktohet nga legjislacioni kombëtar".

dytë ndalimi, pikërisht kur shkelet neni 6 i Direktivës 2000/31KE,[418] ndërkohë që bëhet pjesë e dispozitës mbrojtëse dhe inkurajimi i klikimit të faqeve të veçanta të internetit, si një mënyrë promovimi i marketingut. Në fund, i rëndësishëm është shtimi i paragrafit të gjashtë në nenin 13, i cili parashikon mbrojtjen gjyqësore të personave fizik dhe juridik nga shkeljet e dispozitave kombëtare për mbrojtjen e të dhënave personale dhe privatësisë, në mënyrë që ofruesit e shërbimeve të postës elektronike dhe ofruesit e shërbimeve të tjera të kenë të drejtë ti drejtohen organeve të drejtësisë kundër mesazheve bllokues (spammers) të karakterit komercial dhe në këtë mënyrë të mbrojnë interesat e klientëve të tyre, si pjesë e interesave të tyre të ligjshme të biznesit.[419]

[418] Në mënyrë të veçantë, neni 6 i Direktivës 2000/31/KE thotë se "*Përveç kërkesave të tjera të informacionit të përcaktuara nga ligji Komunitar, Shtetet Anëtare duhet të sigurojnë që komunikimet tregtare të cilat janë pjesë e shërbimit të shoqërisë së informacionit ose janë të paktën pjesë e përmbushjes së kushteve të mëposhtme: a) komunikimi komercial duhet të jenë qartësisht i identifikueshëm, b) personi fizik ose juridik në emër të të cilit bëhet komunikimit komercial duhet të jetë qartësisht i identifikueshëm, c) oferta promovuese, të tilla si uljet e çmimeve, primet dhe dhuratat, ku lejohen nga Shteti Anëtar në të cilin është vendosur ofruesi i shërbimit, duhet të jenë qartë të identifikueshme, qasja në kushtet ku mund të përfitojnë nga ofertat duhet të jenë lehtësisht të arritshme dhe të paraqiten në mënyrë të qartë dhe të saktë, d) konkurrenca reklamuese ose lojërat, nëse lejohen në Shtetin Anëtar ku është vendosur ofruesi i shërbimit, kanë detyrimin të identifikohen qartë, qasja në kushtet për pjesëmarrje duhet të jetë lehtësisht e arritshme dhe kushtet të paraqiten në mënyrë të qartë dhe të saktë*".

[419] Opinion shpjegues 68 i Direktivës 2009/136/KE, pika e tretë.

KAPITULLI IV: KUADRI LIGJOR SHQIPTAR PËR MBROJTJEN E TË DHËNAVE PERSONALE DHE PRIVATËSISË

4.1 Sanksionimi i Garancive Kushtetuese në Kushtetutën Shqiptare

Pas ratifikimit të Konventës Evropiane të të Drejtave të Njeriut, në Shqipëri ndodhën ndryshime pozitive në rendin kushtetues dhe ato hapën rrugën drejt forcimit të shtetit ligjor. Më parë dispozitat kryesore kushtetuese dhe më pas Kushtetuta e vitit 1998, sanksionuan të drejtat dhe liritë themelore të individit dhe krijuan mjetet e nevojshme për të garantuar ushtrimin efektiv të tyre. Dispozitat e neneve 3 (1) në lidhje me dinjitetin njerëzor,[420] 35 (1) për mbrojtjen e të dhënave personale, 35(2) për mbledhjen, përdorimin dhe bërjen publike të të dhënave rreth personit, të cilat bëhen me pëlqimin e tij, me përjashtim të rasteve të parashikuara me ligj[421] dhe nenit 36 për mbrojtjen e privatësisë së komunikimit dhe korrespondencës ose e çdo mjeti tjetër të komunikimit. Këto janë të garantuara në Kushtetutë[422] dhe janë kuadri kryesor kushtetues i mbrojtjes së të dhënave personale, i cili garanton, mbrojtjen e privatësisë duke siguruar në mënyrë të veçantë "të drejtën për vetëvendosje informuese" të individit, pra të drejtën e individit për të vendosur vetë për sigurimin dhe përdorimin e informacionit personal. Mjedisi i ri i rrezikut të të dhënave personale në lidhje me iniciativat ndërkombëtare për të forcuar mbrojtjen e të dhënave personale, udhëhiqet ekskluzivisht nga ligjvënësi kushtetues në Kushtetutën e vendit tonë. Në këtë mënyrë, mbrojtja e të dhënave personale është e sanksionuar shprehimisht në pjesën e dytë tek të "drejtat dhe liritë themelore të njeriut" dhe në formën e "lirive dhe të drejtave vetjake" tek kreu i II (pjesa e dytë) i Kushtetutës, veprimtaria e të cilave varet mbi të drejtën e qytetarit për informim dhe pjesëmarrje në shoqërinë e informacionit.[423]

4.1.1 Të drejtat dhe liritë themelore, neni 15, paragrafi 1 dhe 2

Neni 15, paragrafi 1 i referohet të drejtave dhe lirive themelore të njeriut dhe parashikon se ato "..... janë të pandashme, të patjetërsueshme e të padhunueshme dhe

[420] Neni 3, paragrafi 1 i Kushtetutës të Republikës së Shqipërisë.

[421] Neni 35.

[422] Neni 36.

[423] Neni 23.

qëndrojnë në themel të të gjithë rendit juridik".[424] Ndërsa paragrafi 2 i referohet mbrojtjes së të drejtave dhe lirive themelore të njeriut, ku parashikon se "Organet e pushtetit publik, në përmbushje të detyrave të tyre, duhet të respektojnë të drejtat dhe liritë themelore të njeriut, si dhe të kontribuojnë në realizimin e tyre."[425] Në këtë mënyrë, ligjvënësi kushtetues jo vetëm që përcakton parimin e përgjithshëm të përgjegjësisë së shtetit dhe institucioneve të tij për të respektuar vlerën e qenieve njerëzore dhe për të siguruar parandalimin e sulmit ndaj saj, por dhe përcakton detyrimin për të mbrojtur njeriun kundër çdo përpjekje për ta bërë objekt që t'i shërbejë çdo qëllimi që është në kundërshtim me Kushtetutën. E kundërta vjen në nenin 2 paragrafi 1 të Kushtetutës së vitit 1976, i cili përcaktohet si shtet i diktaturës së proletariatit[426] ku shprehet në një kontekst të caktuar historik dëshira e qeverisjes diktatoriale për të identifikuar dhe të institucionalizuar detyrimin e përgjithshëm të shtetit për të mos hequr dorë nga sulmi në dëm të njeriut, dinjitetit të personave dhe kjo vjen nga institucionet shtetërore. Kjo periudhë historike është karakterizuar dhe përjetuar si një periudhë traumatike dhe denigruese e të drejtave dhe lirive themelore të njeriut në Shqipëri.

4.1.2 Liritë dhe të drejtat ekonomike, sociale dhe kulturore, kreu IV

Kreu IV, përcakton dhe personalitetin e mbrojtur mirë të individëve, në formën e lirive dhe të drejtave ekonomike, sociale dhe kulturore[427] duke i dhënë dimensionin e parë pozitiv mbrojtjes së personalitetit, duke siguruar që të gjithë të kenë të drejtën për të zhvilluar lirisht personalitetin e tyre i cili kuptohet si një grup atributesh, aftësish dhe situatash që lindin nga ekzistenca e njeriut si qenie racionale dhe e vetëdijshme. Ky zhvillim i personalitetit realizohet me pjesëmarrjen e individit në jetën sociale, ekonomike dhe politike të vendit, duke krijuar një detyrim pozitiv të Shtetit[428] për të siguruar ushtrimin e papenguar dhe efektiv të të drejtave themelore të cilat janë të

[424] Neni 15, paragrafi 1 i Kushtetutës së Republikës së Shqipërisë.

[425] Po aty. Paragrafi 2.

[426] Neni 2, paragrafi 1 i Kushtetutës së Republikës Popullore Socialiste të Shqipërisë e vitit 1976.

[427] Kreu i IV i Kushtetutës së Republikës së Shqipërisë.

[428] Nenet 51,52,53,54,55,56,57,58 dhe 59 të Kushtetutës së Shqipërisë.

garantuara nga ai, me futjen e rregullave që parandalojnë rrezikun e sulmeve[429] ndaj të drejtave civile me krijimin e procedurave administrative dhe gjyqësore.

Kreu IV në tërësinë e neneve të tij siguron zhvillimin e personalitetit të njeriut përmes pjesëmarrjes në jetën shoqërore, ekonomike dhe politike të vendit. Në thelb përcakton detyrimin e shtetit që të përmbahet nga veprimet (status negativus),[430] që mund të kufizojnë ose të privojnë këtë të drejtë dhe diçka që mund të ndodhë në qoftë se shteti nuk respekton dhe mbron vlerat njerëzore. Personaliteti është një rrjet pasurish që përbën njeriun në thelb, me të cilin është i pandashëm dhe që përmban çdo element të tij si individualitetin fizik, mendor, social dhe shpirtëror të njeriut. Koncepti i personalitetit është qartësisht më i gjerë se koncepti i të dhënave personale, i cili përfshin aspekte të jetës individuale dhe sferës së privatësisë.

4.1.3 Mbrojtja e të dhënave personale, neni 35

Mbrojtja e të dhënave personale është një e drejtë themelore në Shqipëri e cila është sanksionuar me Kushtetutë. Pra, neni 35 paragrafi 1 parashikon se: "Askush nuk mund të detyrohet, përveçse kur e kërkon ligji, të bëjë publike të dhëna që lidhen me personin e tij" dhe paragrafi 2: "Kushdo ka të drejtën e mbrojtjes nga mbledhja, përpunimi, përdorimi dhe bërja publike e të dhënave personale, me përjashtim të rasteve parashikuara me ligj.

Respektimi i jetës private kërkon në parim mosndërhyrjen në vendimet që merr vetë individi rreth mënyrës së bërjes së jetës së tij. Mbrojtja e jetës private dhe familjare, në Kushtetutën tonë, bëhet përmes disa dispozitave, veçanërisht nga neni 35 (mbrojtja e të dhënave personale), neni 36 (liria dhe fshehtësia e korrespondencës), neni 37 (paprekshmëria e banesës), neni 53 (mbrojtja e martesës dhe familjes), etj. Për çështjen në gjykim,[431] Gjykata Kushtetuese vlerëson se është e nevojshme të analizohet neni 35 i Kushtetutës, në të cilin, që në paragrafin e parë, deklarohet se "Askush nuk mund të detyrohet, përveçse kur e kërkon ligji, të bëjë publike të dhëna që lidhen me personin e

[429] Ekzistenca e një sulmi apo rreziku përkatës vendosin ekzistencën ose jo të detyrimit përkatës të shtetit.

[430] Stolleis M. (2001). *"Public Law in Germany"*, 1800-1914", fq 350 si dhe Ehlers D. (2007). *"European Fundamental Rights and Freedoms"*, fq. 33.

[431] Vendim i Gjykatës Kushtetuese të Republikës së Shqipërisë nr.16/2004.

tij". Padyshim që edhe në këtë rast, në parim, qëllimi i hartuesve të Kushtetutës ka qenë pikërisht garantimi i asaj hapësire të nevojshme brenda së cilës, individi, do të mund të zhvillonte në mënyrë të pavarur personalitetin e tij.

Zhvillimi i teknologjisë moderne dhe zhvillimi i teknologjive të reja për të automatizuar grumbullimin, përpunimin dhe përdorimin e informacionit personal, siç u diskutua tashmë, çoi në nivel ndërkombëtar në një seri rregullimesh ligjore të mbrojtjes së të dhënave personale. Ligjvënësi shqiptar pasoi këto rregullime ligjore me ligje të ngjashme.[432] Subjekte të së drejtës të nenit 35 janë të gjithë në Shqipëri, si shqiptarët ashtu dhe të huajt dhe personat pa shtetësi. Aq sa vetëm përmendja e përpunimit të paligjshëm të të dhënave të subjektit pa u nevojitur dhe mbështetja e të drejtave të tjera kushtetuese. Pranues i të drejtës është shteti si tërësi me subjektet juridike të së drejtës publike dhe të së drejtës private, kur ato ushtrojnë autoritet publik.

Gjithashtu, Gjykata Kushtetuese e Republikës së Shqipërisë është shprehur se ekziston një lidhje e drejtpërdrejtë ndërmjet çështjes objekt gjykimi dhe kushtetutshmërisë së dispozitave ligjore, për të cilat kërkohet të ushtrohet kontrolli kushtetues.[433] Gjykatat referuese kanë konstatuar se palët ankuese, duke u bazuar tek ligji për gjendjen civile, si objekt shqyrtimi, kanë kërkuar ndryshimin e përbërësit "kombësi" në regjistrat e gjendjes civile. Nisur nga ky konstatim, gjykatat referuese kanë çmuar se dispozitat ligjore përkatëse, të zbatueshme për zgjidhjen e çështjeve konkrete, bien ndesh me parimin kushtetues të mos detyrimit për të shprehur përkatësinë etnike, të sanksionuar në nenin 20 të Kushtetutës dhe parimin e mos detyrimit për të bërë publike të dhëna personale, të parashikuar në nenin 35 të Kushtetutës.

Në vendimin më të fundit, Gjykata Kushtetuese në lidhje me kërkesën e një grupi deputetësh të Kuvendit të Shqipërisë për shfuqizimin, si të papajtueshëm me Kushtetutën e Republikës së Shqipërisë, të vendimit nr.354, datë 04.06.2014 të Këshillit të Ministrave "Për ngritjen e bazës së të dhënave IMEI për regjistrimin e numrave IMEI të aparateve celulare, që përdoren në rrjetet e shërbimeve të komunikimeve të lëvizshme" dhe pezullimin e tij,[434] vendosi pushimin e gjykimit të çështjes për

[432] Integrimin e Direktivës së BE 95/46/KE me miratimin e ligjit Nr.9887, datë 10.3.2008 për "*Mbrojtjen e të dhënave personale*".

[433] Vendim i Gjykatës Kushtetuese të Republikës së Shqipërisë nr.52 datë 01.12.2011.

[434] Vendim i Gjykatës Kushtetuese të Republikës së Shqipërisë nr.57 datë 01.12.2014.

kontrollin e pajtueshmërisë me Kushtetutën, të VKM nr. 354 i cili u shfuqizua nga VKM nr. 642/2014.

Interesant është mendimi i pakicës së Gjykatës Kushtuese që mjetin e përdorur nga shumica e gjejnë të sforcuar dhe mendojnë se nuk është i përshtatshëm për çështje të kësaj natyre dhe si objekt kundërshtimi, cënon parimin e shtetit të së drejtës më konkretisht: parimin e hierarkisë së akteve normative dhe kriteret kushtetuese për nxjerrjen e akteve nënligjore, referuar neneve 4/1, 116 dhe 118 të Kushtetutës si dhe disa nga të drejtat dhe liritë themelore kushtetuese, si, për shembull, të drejtën e mbrojtjes së të dhënave personale, të sanksionuar nga neni 35 i Kushtetutës dhe neni 8 i KEDNJ dhe të fshehtësisë së komunikimit (neni 36 i Kushtetutës). Gjithashtu, kërkuesi parashtron se nëse për arsye të mbrojtjes së interesit publik apo të të drejtave të të tjerëve, është i nevojshëm kufizimi i këtyre të drejtave, që mund të vendoset vetëm me ligj. Fakti që në rastin konkret ky kufizim është parashikuar me vendim të Këshillit të Ministrave, përbën tejkalim të kritereve të përcaktuara në nenin 17 të Kushtetutës.[435]

Mendimi i pakicës vlerëson se përcaktimi, rast pas rasti, i parimeve kushtetuese në fusha të rëndësishme në drejtim të respektimit të të drejtave dhe lirive themelore të individit (si ajo e mbrojtjes së jetës private), i shërbejnë stabilitetit juridik të vendit si një kusht i rëndësishëm për funksionimin e shtetit të së drejtës, në mënyrë që të evitohen ndryshimet e shpeshta në legjislacion, të cilat mund të çojnë në cenim të parimit të sigurisë juridike.

Në këtë këndvështrim, në ndryshim nga shumica, në rastin konkret jemi të mendimit se Gjykata duhet të analizonte në themel dhe t'u jepte përgjigje pretendimeve të palëve pjesëmarrëse në gjykim vetëm në lidhje me kontrollin e pajtueshmërisë me Kushtetutën të aktit të kundërshtuar.

4.1.4 Liria dhe fshehtësia e korrespondencës ose e çdo mjeti tjetër të komunikimit, neni 36

Neni 36 i Kushtetutës[436] parashikon lirinë dhe fshehtësinë e korrespondencës ose të çdo mjeti tjetër të komunikimit. Neni i referohet në mënyrës të veçantë sigurimit të fshehtësisë së letrave dhe korrespondencës së lirë ose komunikimit si një zgjerim i të

[435] Po aty, fq.8.

[436] "*Liria dhe fshehtësia e korrespondencës ose e çdo mjeti tjetër të komunikimit janë të garantuara.*"

drejtës së lirisë personale. Dy komponentët e kësaj të drejte janë liria e korrespondencës ose komunikimit dhe konfidencialiteti i të gjitha formave të komunikimit që duhet të konsiderohen në rrethana dhe në bazë të tij, nëse palët e interesuara synojnë të ruajnë komunikimin e tyre si të fshehtë. Me liri të korrespondencës do të kuptohet liria për të komunikuar me të tjerët nëpërmjet letrave ose me anë të çdo mjeti tjetër komunikimi si dhe e drejta që ka çdo person për të zgjedhur lirisht subjektet me të cilët dëshiron të komunikojë. Ndërkohë, fshehtësia e korrespondencës lidhet me të drejtën për të mbajtur të fshehtë prej të gjithë atyre që nuk janë shkëmbyesit e korrespondencës ose bashkë komunikuesit, përmbajtjen e komunikimit pavarësisht faktit nëse kjo e fundit ka apo jo karakter sekret. "Liria" dhe "fshehtësia " e korrespondencës janë dy aspekte që karakterizojnë mënyrën e vendosjes së marrëdhënieve të individit, të komunikimit të tij me botën e jashtme dhe shfaqjen e tij në shoqëri".[437] Natyra e fshehtë e korrespondencës duhet parë në këndvështrimin pasiv dhe atë aktiv. Në kuptimin e tij pasiv, ky parim nënkupton detyrimin e personave të paautorizuar për të mos marrë dijeni, shpërndarë apo përdorur informacionet e lidhura me subjekte të përcaktuara, ndërkohë në kuptimin e tij aktiv, parimi shprehet në të drejtën që gëzojnë palët në një komunikim për të përjashtuar të tretët nga marrja dijeni apo transmetimi i komunikimit të realizuar prej tyre.[438] E drejta e respektimit të korrespondencës së personit ka për qëllim mbrojtjen e konfidencialitetit të komunikimeve private dhe është interpretuar si garanci e të drejtës së komunikimeve të pandërprera dhe të pa censuruara me të tjerët. Niveli i mbrojtjes është i lartë, pasi nuk ekziston parimi *de minimis* që të konstatohet se ka pasur ndërhyrje: hapja e një letre ose hapja e një e-maili si komunikim elektronik mjafton.[439]

E drejta për të kryer komunikimin e lirë është sigurisht një parakusht për mbrojtjen e konfidencialitetit. Megjithatë, nuk mund të ketë informacion sekret në qoftë se e drejta nuk e ka garantuar paraprakisht më parë të drejtën në komunikimin e lirë d.m.th. e drejta e njeriut "të zgjedhë llojin e instrumentit, si dhe mënyrën e

[437] Morsink, J. (2011) "*The Universal Declaration of Human Rights: Origins, Drafting, and Intent*", fq.135.

[438] Akrivopoulou, Ch. M. (2012). "*Human Rights and Risks in the Digital Era: Globalization and the Effects of Information Technologies*", fq.54.

[439] Çështja *Narinen Kundër Finlandës*.

komunikimit”[440] pa penguar pushtetin privat apo operatorët private. Megjithatë, në qoftë se palët nuk duan privatësinë, atëherë do të mund të konsideronim se mbrojtja e shprehjes së lirë bëhet e pavarur nga e drejta për intimitet. Por a është e mundur të mos pengojë lirinë e komunikimit, nëse komunikimi kontrollohet?

Parimi i fshehtësisë së korrespondencës ka ardhur duke u shtrirë natyrshëm mbi format e reja të komunikimeve, duke përfshirë bisedat telefonike dhe komunikimet elektronike nëpërmjet Internet-it. Zbatimi i parimit të fshehtësisë së korrespondencës mbi komunikimet elektronike, nënkupton jo vetëm mbrojtjen e përmbajtjes së komunikimit, por gjithashtu edhe të informacioneve në lidhje me kohën e dërgimit të mesazhit, gjithashtu personin të cilit i është dërguar mesazhi, si dhe në rastin e komunikimeve të realizuara me anë të telefonave celularë, por dhe të informacionit në lidhje me vendndodhjen e pajisjes fundore të përdorur gjatë komunikimeve.[441]

Kushtetuta garanton fshehtësinë e komunikimit në çdo mënyrë dhe në qoftë se kjo bëhet duke marrë parasysh në të ardhmen të gjithë evolucionin teknologjik të mundshëm dhe për këtë arsye informacioni që lidhet me komunikimin, si dhe informacionet e tjera që lidhen me komponentët e jashtëm rrjedhin nga intimiteti i garantuar në Kushtetutë.[442]

4.1.5 Paprekshmëria e jetës private dhe familjare, duke mbrojtur banesën, neni 37

Në Kushtetutën e Republikës së Shqipërisë mbrojtja e lirisë dhe të drejtave të personit, jetës private dhe familjare, sanksionohen përmes disa dispozitave, veçanërisht në nenin 18 (të gjithë janë të barabartë përpara ligjit), nenin 20 (personat që u përkasin pakicave kombëtare ushtrojnë në barazi të plotë para ligjit te drejtat dhe liritë e tyre), nenet 22, 23 dhe 24 (lirinë e shprehjes, lirinë e informimit, lirinë e ndërgjegjes dhe fesë), nenet 27-33 (liritë dhe të drejtat në procesin penal), nenin 36 (liria dhe fshehtësia e korrespondencës), nenin 37 (paprekshmëria e banesës), nenin 53 (mbrojtja e martesës dhe familjes) etj..

[440] Spiro, O. (2013). “*E Drejta e Internetit*”, fq. 52.

[441] Direktiva 97/66/ K E, pika 19.

[442] Zaganjori, Xh., Anastasi, A., Çani, E. “*Shteti i së Drejtës në Kushtetutën e Republikës së Shqipërisë*”, fq.23.

Ballafaqimi i rreziqeve të krijuara nga përdorimi i teknologjive të reja monitoruese dhe përgjuese[443] i udhëhequr nga ligjvënësi kushtetues shqiptar në miratimin e Kushtetutës të vitit 1998, Neni 37 paragrafi 1 dhe 2,[444] garanton lirinë personale dhe përcakton paprekshmërinë e jetës private dhe familjare, duke mbrojtur banesën (e cila konsiderohet e paprekshme) nga sulmet e pushtetit shtetëror (non facere), [445] i cili kryesisht ka në dispozicion të tij teknologjitë e reja të vëzhgimit. Dispozita e mësipërme në mënyrë eksplicite thotë se banesa e çdo kujt është e paprekshme dhe se jeta private dhe familja e individit është e pacenueshme.

Themeli i kësaj të drejte individuale është çdo individ. Kjo është një e drejtë ligjore e mbështetur në nenin 35 paragrafi 1, i cili identifikon paprekshmërinë e të drejtës së mbrojtjes në mbrojtjen e të dhënave personale. Pra, "banesa" nuk shikohet fjalë për fjalë si domicilium[446] por si çdo akomodim-hapësirë që nuk është i arritshëm për të gjithë, ndërsa jeta private apo hapësira private interpretohet në konceptin e informacionit personal që lidhet me jetën private të individit. Paragrafi i tretë i nenit 37, paraqet se "askujt nuk mund t'i bëhet kontroll personal jashtë procesit penal" dhe mund të bëhet vetëm në rastet dhe në mënyrat e parashikuara me ligj. Autoriteti gjyqësor nuk do të jetë i varur nga sekreti kur ekzistojnë arsyet e sigurisë kombëtare ose nëse ajo duhet bërë për zbulimin e veprave penale veçanërisht të rënda.

4.2 Ligji Nr. 9887, datë 10.03.2008 "Për mbrojtjen e të dhënave personale" i ndryshuar

Ligji i parë, miratuar në Shqipëri për mbrojtjen e të dhënave personale është ai i vitit 1999, ligji nr. 8517, datë 22.07.1999 "Për mbrojtjen e të dhënave personale", i cili u

[443] Së fundmi skandali "*Watergate*" i "*pothuajse*" përgjimeve telefonike që tronditën opinionin botëror dhe demonstroi nevojën për mbrojtje kushtetuese dhe penale të intimitetit privat dhe konfidencialitetit të komunikimeve, shih në lidhje me "Watergate" në http://www.washingtonpost.com/wp-srv/politics/special/watergate/#chapters (20-5-2009)

[444] Ku thuhet: "1. *Paprekshmëria e banesës është e garantuar*. 2. *Kontrollet e banesës, si dhe të mjediseve që njësohen me të, mund të bëhen vetëm në rastet dhe në mënyrat e parashikuara me ligj*."

[445] Shih: Berger, A. (1968). "*Encyclopedic Dictionary of Roman Law - Volume 43*", fq. 603.

[446] Po aty. Berger, A. (1968). fq. 441.

revokua nga ligji nr. 9887, datë 10.03.2008[447] "Për Mbrojtjen e të Dhënave Personale" ndryshuar me ligjin nr. 48/2012 dhe me ligjin nr.120/2014. Ky i fundit është hartuar në harmonizim edhe me Direktivat dhe rekomandimet e BE dhe të KE-së, si Direktivat 2002/58/KE dhe 95/46/KE të Parlamentit Evropian dhe Këshillit Evropian apo edhe Konventën e Këshillit të Evropës "Për mbrojtjen e individëve nga Përpunimi Automatik i të Dhënave Personale", ratifikuar nga Republika e Shqipërisë me ligjin nr. 9288, datë 07.10.2004.

Me miratimin e këtij ligji u themelua për herë të parë Autoritetit mbikëqyrës për mbrojtjen e të dhënave personale.

Këto janë ngjarje të rëndësishme që do të japin një kontribut thelbësor në përmbushjen e qëllimeve, objektivave dhe strategjive të vendit tonë në respektim të të drejtave e lirive të njeriut, në përputhje me standardet e Bashkimit Evropian. Një aspekt i rëndësishëm për funksionimin e këtij autoriteti mbikëqyrës që garanton mbrojtjen e të dhënave personale duke respektuar të drejtat dhe liritë themelore të njeriut është lidhja dhe bashkëpunimi me institucionet publike dhe private, që ligji i quan Kontrollues e Përpunues për respektimin e këtyre të drejtave kushtetuese të personave për t'u rreshtuar kështu përkrah vendeve më të zhvilluara të Evropës.

Ligji i veçantë është i ndarë në dhjetë kapituj dhe 44 nene më të rëndësishmet e të cilave do të paraqiten si udhëzues thelbësor për të kuptuar rregullat sektoriale si dhe të përpunimit të të dhënave personale në sektorin e komunikimeve elektronike.

4.2.1 Fushë zbatimi dhe përkufizimet

Në kapitullin e I të ligjit përcaktohet objekti, parimi i përgjithshëm, përkufizimet dhe fusha e zbatimit të tij. Specifikohet se objekti dhe parimi i përgjithshëm i këtij ligji është të krijojë kushtet për përpunimin e të dhënave personale për të mbrojtur të drejtat dhe liritë themelore të personave fizikë dhe në mënyrë të veçantë privatësinë[448] dhe jo mbrojtjen e personave juridikë. Përcaktimi i rregullave për mbrojtjen e të dhënave personale është bërë mbi eksperiencën e vendeve të zhvilluara të Evropës dhe mbështetur në akte e dokumente të rëndësishme kombëtare e ndërkombëtare. Në radhën

[447] Ligji nr. 9887, datë 10.03.2008, ndryshuar me ligjin Nr. 48/2012, ndryshuar me ligjin nr.120/2014 "*Për Mbrojtjen e të Dhënave Personale*".

[448] Neni 1 dhe 2 i ligjit nr. 9887 i ndryshuar.

e akteve normative me fuqi në të gjithë territorin e Republikës së Shqipërisë, menjëherë pas Kushtetutës, rreshtohen marrëveshjet ndërkombëtare të ratifikuara. Çdo akt ndërkombëtar i ratifikuar bëhet pjesë e sistemit të brendshëm juridik. Lidhja që ekziston midis Kushtetutës së Shqipërisë dhe akteve ndërkombëtare është pasqyrim i procesit të pranimit të standardeve ndërkombëtare në fushën e të drejtave të njeriut në tërësi e në veçanti në fushën e mbrojtjes së privatësisë dhe të dhënave personale.

Në ligjin "Për mbrojtjen e të dhënave personale" nuk është përcaktuar se ç'kuptojmë me privatësi. Kjo del nga legjislacioni ynë i fushës së mbrojtjes së të drejtave themelore të njeriut si dhe legjislacioni ndërkombëtar i kësaj fushe dhe mbrojtjes së të dhënave personale.[449] Sipas nenit 3 të ligjit "Për mbrojtjen e të dhënave personale", e dhënë personale është informacioni që mundëson identifikimin e një personi të caktuar.[450] Pra, si element të të dhënave personale në privatësi përfshihen: emri, mbiemri, datëlindja, adresa postare ose e e-mail, numri i telefonit, numri identifikues i taksave, numri i patentës, shenjat e gishtërinjve, ADN-ja, fotografitë, numri i sigurimeve shoqërore, të dhëna këto që identifikojë individët, qoftë direkt ose indirekt.

Të dhënat sensitive kanë të bëjnë me jetën e prekshme, shqisore, intime, të ngushtë, vemesa e brendshme e njeriut, origjinën racore ose etnike, mendimet politike, anëtarësimi në sindikata, besimi fetar apo filozofik, dënimi penal si dhe të dhëna për shëndetin dhe jetën seksuale.

Ajo që duhet thënë është se në amendamentet e mëtejshme të këtij ligji do të ishte e domosdoshme zgjerimi i përkufizimit të shumë termave të fushës së mbrojtjes së të dhënave personale, pasi është fushë e re e pa lëvruar asnjëherë më parë. Më poshtë, përcaktohet fusha e zbatimit të ligjit[451] që përkufizon si "tërësisht ose pjesërisht" përpunimin e të dhënave personale, nëpërmjet mjeteve automatike si dhe për përpunimin me mjete të tjera të të dhënave personale që mbahen në një sistem arkivimi apo kanë për qëllim të formojnë pjesë të sistemit të arkivimit. Më tej sqarohet se këto dispozita ligjore zbatohen për përpunimin e të dhënave personale të

[449] Çabej (Pogaçe), F., Gjoleka, A. dhe Shala, A. (2010). *"Komentar i ligjit për mbrojtjen e të dhënave personale", Tiranë*, fq.6.

[450] Neni 3 i ligjit nr. 9887 i ndryshuar.

[451] Neni 4.

kryera nga:

a) kontrollues të vendosur në Republikën e Shqipërisë;

b) misionet diplomatike ose zyrat konsullore të shtetit shqiptar;

c) kontrollues, të cilët nuk janë të vendosur në Republikën e Shqipërisë por që e ushtrojnë veprimtarinë nëpërmjet përdorimit të çdo mjeti që ndodhet në Republikën e Shqipërisë.

Në rastet e parashikuara në shkronjën "c" të pikës 2 të këtij neni, kontrolluesi cakton një përfaqësues i cili duhet të jetë i vendosur në Republikën e Shqipërisë. Parashikimet e këtij ligji që zbatohen nga kontrolluesit, zbatohen edhe për përfaqësuesit e tyre. Ky ligj nuk zbatohet për përpunimin e të dhënave:

a) për persona fizikë, për qëllime thjesht familjare ose personale;

b) vetëm për rastet kur jepet informacion për persona publikë zyrtarë ose punonjës të administratës publike (shtetërore), nëpërmjet të cilave pasqyrohet aktiviteti publik, administrativ ose çështje lidhur me detyrën e tyre.

Ligji për mbrojtjen e të dhënave personale, gjen zbatim për të gjithë veprimet që kryhen me të dhënat personale. Ai mbulon gjithçka, që nga grumbullimi i të dhënave personale e deri tek shkatërrimi i tyre dhe përfshin gjithashtu edhe thjeshtë mbajtjen e të dhënave personale. Fusha e mbulimit të ligjit është shumë e gjerë. Ai gjen zbatim tek të gjitha institucionet publike e private si edhe tek individët, në rastet kur ata përpunojnë të dhëna personale.

4.2.2 Përpunimi i të dhënave personale dhe kriteret ligjore të përpunimit të të dhënave personale

Në kapitullin e II të ligjit përcaktohen bazat dhe parimet e mbrojtjes së të dhënave personale që duhet të drejtojnë përpunimin e të dhënave personale të tilla si: a. parimi i ligjshmërisë së qëllimit të përpunimit;[452] b. kërkon mbledhjen e të dhënave personale për qëllime specifike, të përcaktuara qartë, e legjitime;[453] c) në mjaftueshmërinë e të dhënave, të cilat duhet të lidhen me qëllimin e përpunimit dhe të mos e tejkalojnë këtë qëllim; ç) në saktësinë që të dhënat duhet të kenë dhe, kur është e nevojshme, duhet të përditësohen; duhet ndërmarrë çdo hap i arsyeshëm për të fshirë

[452] Neni 5, paragrafi 1, shkronja (a).

[453] Po aty. Paragrafi 1, shkronja (b).

apo korrigjuar të dhëna të pasakta apo të paplota, në lidhje me qëllimin për të cilin janë mbledhur apo për të cilin përpunohen më tej; d) në mbajtjen në atë formë, që të lejojë identifikimin e subjekteve të të dhënave për një kohë, por jo më tepër sesa është e nevojshme për qëllimin, për të cilin ato janë grumbulluar ose përpunuar më tej. Kontrolluesi është përgjegjës për zbatimin e këtyre kërkesave në të gjitha përpunimet automatike ose me mjete të tjera të të dhënave.[454]

Kontrolluesit e përmendur më sipër, gjatë marrjes në punë ose për ushtrimin e kompetencave të tyre të ngarkuara me ligj, përpunojnë të dhëna si emri, mbiemri, gjendja civile, arsimi etj., (çdo informacion për një person fizik, i cili është i identifikuar ose i identifikueshëm) që mund të jenë të dhënë personale të zakonshme, por ndërmjet tyre ose kryesisht marrin të dhëna si gjendja shëndetësore (raporti mjekësor), dëshminë e penalitetit, gjurmë të gishtërinjve etj., që janë të dhëna sensitive.

Nuk ka ndarje tek Kontrolluesit dhe Përpunuesit për përpunimin e të dhënave. Çdo njëri prej tyre mund të përpunojë njëkohësisht të dhëna të zakonshme dhe të dhëna sensitive. Kështu, Kontrolluesit gjatë marrjes në punë përpunojnë të dhëna si emri, mbiemri, gjendja civile, arsimi etj., që janë të dhënë personale të zakonshme, por ndërmjet tyre marrin dhe të dhëna si gjendja shëndetësore (raporti mjekësor), dëshminë e penalitetit etj., që janë të dhëna sensitive.

Përveç parimeve themelore të parashikuara të trajtimit, ligjvënësi parashikon ligjshmërinë procedurale d.m.th kriteret ligjore të kushteve të përpunimit.[455] Në mënyrë eksplicite theksohet se përpunimi i të dhënave personale është i lejuar vetëm nëse subjekti i të dhënave ka dhënë pëlqimin[456] si dhe kur përpunimi është i nevojshëm për përmbushjen e një kontrate[457] ose kur është e nevojshme për të mbrojtur interesat jetike të subjektit të të dhënave,[458] për përmbushjen e një detyrimi ligjor të kontrolluesit[459] ose kur është nevojshme për kryerjen e një detyre ligjore me interes publik ose ushtrimin e një kompetence të kontrolluesit ose të një pale të tretë, së cilës i janë përhapur të

[454] Po aty. Paragrafi 2.

[455] Po aty. Neni 6.

[456] Neni 6, paragrafi 1, shkronja (a).

[457] Po aty. Paragrafi 1, shkronja (b).

[458] Po aty. Paragrafi 1, shkronja (c).

[459] Po aty. Paragrafi 1, shkronja (ç).

dhënat[460] dhe kur tarifa e përpunimit është absolutisht e nevojshme për mbrojtjen e të drejtave dhe interesave legjitime të kontrolluesit, marrësit apo personave të tjerë të interesuar.

Por, në çdo rast, përpunimi i të dhënave personale nuk mund të jetë në kundërshtim të hapur me të drejtën e subjektit të të dhënave për mbrojtjen e jetës personale dhe private.[461] Ligji për mbrojtjen e të dhënave nuk e shpjegon pëlqimin ose nuk e përcakton se si ai duhet të jepet. Metoda e marrjes së pëlqimit do të ndryshojë nga rasti në rast. Në disa raste, organi do t`u kërkojë individëve të firmosin një dokument ose të cekojnë në kuti on-line. Në raste të tjera, duhet të jetë e nevojshme për individët të informohen rreth asaj se çfarë do të ndodhë me të dhënat e tyre. Në qoftë se ata vazhdojnë veprimtarinë ata duhet të demonstrojnë që e kanë marrë pëlqimin. Por shpesh mund të ketë arsye që pëlqimi mund të mos merret, prandaj ligji parashikon pesë mënyra alternative për të bërë përpunimin të ligjshëm, ekzistenca e njërit është e mjaftueshme për përpunimin e të dhënave personale. Kërkohet që kontrolluesit gjatë përpunimit të të dhënave personale të balancojnë interesat e tyre kundrejt të drejtave dhe interesave të individëve të interesuar. Kontrolluesit ose personat të cilëve u janë zbuluar të dhënat mund t`i përpunojnë ato për qëllimet e tyre të ligjshme, me kusht që këta individë të mos kenë të drejta dhe interesa më të forta që të thonë se të dhënat nuk duhet të përpunohen. Ligji referon se "të dhënat sensitive" janë të dhëna personale që përmbajnë informacion për individin që kanë të bëjnë me: origjinën e tij racore ose etnike, mendimet politike, anëtarësimin në sindikata, besimin fetar apo filozofik, dënimin penal, si dhe të dhëna për shëndetin dhe jetën seksuale.[462] Përpunimi i të dhënave sensitive bëhet vetëm nëse[463] subjekti i të dhënave ka dhënë pëlqimin. Pëlqimi "i dhënë" ka kuptimin e një pëlqimi që është dhënë aktivisht nga person i interesuar në përgjigje të pyetjes "jam dakord". Pëlqimi i shprehur nuk ka pse të jepet me shkrim, ai mund të jepet me gojë. Por nëse ky pëlqim jepet me shkrim, atëherë kjo është një provë e qartë e pëlqimit. Ky pëlqim i dhënë, mund të revokohet në çdo çast dhe e bën të paligjshëm përpunimin e mëtejshëm të të dhënave kur është në interesin jetik të

[460] Po aty. Paragrafi 1, shkronja (d).

[461] Po aty. Paragrafi 1, shkronja (e).

[462] Neni 7, paragrafi 1.

[463] Po aty. Paragrafi 2.

subjektit të të dhënave ose të një personi tjetër dhe subjekti i të dhënave është fizikisht ose mendërisht i paaftë për të dhënë pëlqimin e vet, kur autorizohet nga autoriteti përgjegjës për një interes të rëndësishëm publik nën masa të përshtatshme mbrojtëse, kur lidhet me të dhëna që janë bërë haptazi publike nga subjekti i të dhënave ose është i nevojshëm për ushtrimin apo mbrojtjen e një të drejte ligjore kur të dhënat përpunohen për qëllime historike, shkencore ose statistikore, nën masa të përshtatshme mbrojtëse, të dhënat kërkohen për qëllime të mjekësisë parandaluese, diagnostikimit mjekësor, sigurimit të kujdesit shëndetësor, kurimit, menaxhimit të shërbimeve të kujdesit shëndetësor dhe përdorimi i tyre kryhet nga personeli mjekësor ose persona të tjerë, që kanë detyrimin për ruajtjen e fshehtësisë, kur të dhënat përpunohen nga organizatat jofitimprurëse politike, filozofike, fetare ose sindikaliste, për qëllime të veprimtarisë të tyre të ligjshme, vetëm për anëtarët, sponsorizuesit ose personat e tjerë, që kanë lidhje me veprimtarinë e tyre. Këto të dhëna nuk u bëhen të ditura një pale të tretë, pa pëlqimin e subjektit të të dhënave, përveç kur parashikohet ndryshe në ligj dhe kur përpunimi është i nevojshëm për përmbushjen e detyrimit ligjor dhe të të drejtave specifike të kontrolluesit në fushën e punësimit, në përputhje me Kodin e Punës.[464] Përpunimi i të dhënave sensitive autorizohet nga autoriteti përgjegjës për një interes të rëndësishëm publik. Kjo mund të ndodhë kur kontrolluesit konstatojnë se nuk kanë asnjë nga kushtet ligjore të përpunimit të të dhënave dhe i drejtohen Komisionerit. Atëherë Komisioneri mund të autorizojë përpunimin e të dhënave personale për arsye të interesit të rëndësishëm publik. Një tjetër formë e trajtimit është transferimi ndërkombëtar i të dhënave personale[465] i cili kryhet me marrës nga shtete me një nivel të mjaftueshëm të mbrojtjes së të dhënave personale. Niveli i mbrojtjes së të dhënave personale për një shtet përcaktohet duke vlerësuar të gjitha rrethanat lidhur me përpunimin, natyrën, qëllimin dhe kohëzgjatjen e tij, shtetin e origjinës dhe destinacionin përfundimtar, aktet ligjore dhe standardet e sigurisë në fuqi në shtetin marrës. Shtetet që kanë nivel të mjaftueshëm të mbrojtjes së të dhënave përcaktohen me vendim të Komisionerit.[466] Si shtete me nivel të mjaftueshëm, ekspertët e KE konsiderojnë 27 shtetet anëtare të BE dhe shtetet e tjera që Komisionin Evropian i ka përfshirë (Zvicra, Kanada, SHBA, etj.),

[464] Po aty. Paragrafi 2, shkronjat (a,b,c,ç,d,dh,i,e dhe ë).

[465] Neni 8 i ligjit.

[466] Neni 8, paragrafi 1.

vendet që kanë ratifikuar Konventën si dhe vende të tjera jashtë Evropës (Australi, Japoni, Honkong etj.). Çfarë ndodh nëse transferimi ndërkombëtar i të dhënave personale bëhet me një shtet që nuk ka nivel të mjaftueshëm të mbrojtjes së të dhënave personale?

Lidhur me kriteret për Transferimin ndërkombëtar të të dhënave personale me një shtet që nuk ka nivel të mjaftueshëm të mbrojtjes së të dhënave personale që përshkruhet në pikën 2,[467] mund të themi se pëlqimi i subjektit të të dhënave është një nga rastet më të shpeshta. Pëlqimi do të përdoret vetëm kur nuk ka mundësi të tjera për të legjitimuar transferimin e të dhënave. Pëlqimi do të jepet i lirë, duhet të jetë i informuar, i ligjshëm dhe me mirëbesim. Kur bëhet fjalë për të dhëna sensitive, pëlqimi duhet të jetë gjithashtu "i shprehur". Pëlqimi i subjektit përkatës të të dhënave është i nevojshëm vetëm në qoftë se nuk siguron një nivel të mjaftueshëm të mbrojtjes së të dhënave në shtetin marrës (që nuk është anëtar i BE-së). Në përputhje me ligjin, pëlqimi mund të jetë i nënkuptuar, veçse kur transferohen të dhëna sensitive, pëlqimi duhet të jetë i shprehur dhe i qartë. Pëlqimi mund të jetë i nënkuptuar, pra nëpërmjet plotësimit të formularit të aplikimit ose me deklaratë me shkrim, e cila është një provë e qartë dhe e shprehur e pëlqimit. Pëlqimi duhet të jepet i lirë, i ligjshëm, me mirëbesim dhe subjekti i të dhënave të jetë i mirë informuar. Përjashtimi i përcaktuar në shkronjën "c", zbatohet kur transferimi është i nevojshëm për të përfunduar ose plotësuar një kontratë të lidhur me një individ ose palë të tretë me kërkesë të individit. Por, kjo duhet të kuptohet se një transferim i tillë mund të realizohet vetëm kur është i "nevojshëm" dhe ekzistenca e kontratës nuk është e barasvlershme me autorizimin në përgjithësi për transferimin e të dhënave. Si shembull, është transferimi i të dhënave personale ndërmjet bankës në mënyrë për të realizuar transfertën e parave kur klienti e kërkon atë. Gjithashtu, transferimi duhet të jetë strikt dhe objektiv i nevojshëm për përfundimin ose ekzekutimin e një kontrate ndërmjet kontrolluesit të të dhënave dhe një pale të tretë në interes të subjektit të të dhënave. Transferimi i të dhënave personale nga BE te një shtet i tretë i cili nuk siguron mbrojtje të mjaftueshme të të dhënave, lejohet për një interes jetësor të subjektit të të dhënave. Ky përjashtim zbatohet dukshëm për transferimin lidhur me informacione mjekësore të subjektit të të dhënave në rastin e një urgjence mjekësore, trajtimi mjekësor ose çdo përkujdesje mjekësore e nevojshme që duhet t`i

[467] Po aty. Paragrafi 2.

jepet subjektit. Përjashtimi nuk do të zbatohet për çdo arsye tjetër e cila nuk lidhet drejtpërdrejt me subjektin e të dhënave (p.sh nuk lejohet të zbatohet në interes të kërkimeve mjekësore, statistikave, etj.). Ndërsa për sa i përket transferimit ndërkombëtar të të dhënave që duhet të autorizohen,[468] transferimi ndërkombëtar i të dhënave personale me një shtet që nuk ka nivel të mjaftueshëm të mbrojtjes së të dhënave, në raste të tjera nga ato të parashikuara në nenin 8 të këtij ligji, bëhet me autorizim të komisionerit kur parashtron siguri të mjaftueshme në lidhje me mbrojtjen e privatësisë dhe të të drejtave e lirive themelore të njeriut, si dhe në lidhje me ushtrimin e së drejtës përkatëse.

Gjithashtu, Komisioneri, pasi bën vlerësimin sipas përcaktimeve të pikës 1 të këtij neni dhe të pikës 1 të nenit 8, mund të japë autorizimin për transferimin e të dhënave personale në shtetin marrës, duke përcaktuar kushte dhe detyrime. Komisioneri nxjerr udhëzime për lejimin e disa kategorive të transferimeve ndërkombëtare të të dhënave personale në një shtet që nuk ka nivel të mjaftueshëm të mbrojtjes së të dhënave personale. Në këto raste, kontrolluesi përjashtohet nga kërkesa për autorizim. Kontrolluesi, përpara transferimit të të dhënave, bën kërkesë për autorizim te komisioneri. Në kërkesë, kontrolluesi duhet të garantojë respektimin e interesave për ruajtjen e sekretit të subjektit të të dhënave jashtë Republikës së Shqipërisë.[469] Që kontrolluesit të sigurohen që të dhënat personale që ata dërgojnë në një vend pa nivel të përshtatshëm të mbrojtjes janë të mbrojtura në nivelin që kërkohet, duhet që të përfshijnë masat e nevojshme për mbrojtjen e të dhënave në një kontratë të lidhur me institucionin marrës në vendin e mbërritjes.

4.2.3 Përpunimi i veçantë i të dhënave

Kapitulli i III, përcakton mënyrën e përpunimit të të dhënave për qëllime historike, shkencore dhe statistikore duke siguruar se nuk janë përpunuar për të marrë masa ose vendime për një individ. Transmetimi i të dhënave sensitive për kërkimet shkencore bëhet vetëm kur ekziston një interes i rëndësishëm publik. Të dhënat personale përdoren vetëm nga person të cilët janë të detyruar të ruajnë konfidencialitetin. Ruajtja e konfidencialitetit (fshehtësi, afërsi, familjaritet, besim) si

[468] Neni 9.

[469] Po aty. Paragrafi 1,2,3 dhe 4.

një e drejtë themelore e individit për mbrojtjen e të dhënave të tij, nuk duhet të dalë si një pengesë e dorës së dytë, ndaj të drejtës së lirisë së shprehjes së gazetarit apo çdo subjekti tjetër të parashikuar sipas këtij neni. Është e vërtetë se liria e shprehjes nuk i nënshtrohet censurës paraprake, por kjo censurë nuk ka të bëjë me mospasjen e të drejtës së individit për të mbrojtur të dhënat e tij personale. Duhet pasur parasysh që e drejta e jetës private të përshtatet me rregullat që rregullojnë lirinë e të shprehurit. Ndërsa, në rastet kur përdorimi i të dhënave bëhet në një formë që lejon identifikimin e subjektit të të dhënave, të dhënat duhet të kodohen menjëherë në mënyrë që subjektet të mos jenë më të identifikueshme. Të dhënat personale të koduara përdoren vetëm nga persona të cilët janë të detyruar të ruajnë konfidencialitetin.[470]

Për përpunimin e të dhënave personale dhe lirinë e të shprehurit [471] është Komisioneri që përcakton me udhëzim të veçantë kushtet dhe kriteret kur për qëllime gazetarie, letrare dhe artistike, mund të bëhen përjashtime nga detyrimet që rrjedhin nga nenet 5, 6, 7, 8, 18 dhe 21 të këtij ligji. Përjashtimet sipas këtij neni, mund të lejohen deri në atë masë për aq sa ato pajtojnë të drejtën për mbrojtjen e të dhënave personale me rregullat që administrojnë lirinë e informimit. Kur veprimet e kontrolluesit ose përpunuesit bien në kundërshtim me pikat e mësipërme dhe kodin etik përbëjnë kundërvajtje administrative.

Është pranuar tashmë se të drejtat themelore të individit nuk janë të pakufizuara dhe kufizimi qëndron pikërisht aty ku e drejta e individit ndeshet në radhë të parë me të drejtën konkrete të një individi tjetër apo kur peshorja anon dukshëm nga interesi publik dhe jo nga interesi i ngushtë i individit. Në këtë kuptim, kushdo që përpunon të dhëna personale vetëm për qëllime gazetarie, literature ose artistike, do të ndeshet në radhë të parë me të drejtën e individit, subjekt i këtyre të dhënave personale, për t`i mbrojtur ato.

Gjatë zbatimit të kësaj dispozite duhet të bëhet kujdes që nga Kontrolluesit të balancohen nevojat e tyre për përdorimin e informacionit personal me të drejtën e individit për respektimin e së drejtës së privatësisë së tij. Gjithsesi e drejta e lirisë së shprehjes së gazetarit rregullohet e kufizohet me ligjin për mbrojtjen e të dhënave personale dhe Kodin etik të gazetarit i cili duhet të miratohet pa humbur kohë, që do të

[470] Neni 10.

[471] Neni 11.

përcaktojë standarde në sjelljen e gazetarëve dhe do jetë dhe një mbrojtje për vetë gazetarin.

4.2.4 Të drejtat e subjektit të të dhënave

Kapitulli i IV (Nenet 12-17) përcakton të drejtat e subjekteve dhe krijon mbrojtje për ta. Në mënyrë të veçantë këto të drejta janë e drejta e informimit, aksesit, për të kërkuar bllokimin, korrigjimit ose fshirjes, vendimmarrjes automatike të kundërshtimit, ankimit dhe kompensimit të dëmit. Në lidhje me të drejtën për informim dhe akses, ligji parashikon se kontrolluesi duhet gjatë mbledhjes së të dhënave personale, të informojë në mënyrë të përshtatshme dhe të qartë pa pagesë dhe kundrejt një kërkese me shkrim të subjektit, për disa elementë të caktuar në lidhje me të dhënat personale. Informacioni për të dhënat komunikohet në formën në të cilën ishin në kohën kur është bërë kërkesa.[472] Pastaj kontrolluesi, brenda 30 ditëve nga data e marrjes së kërkesës, informon subjektin e të dhënave ose i shpjegon atij arsyet e mosdhënies së informacionit. Gjithashtu, e drejta për akses, sipas pikës 1 të këtij neni, ushtrohet në përputhje me parimet kushtetuese të lirisë së shprehjes dhe informacionit, lirisë së shtypit dhe sekretit profesional dhe mund të kufizohet nëse cenon interesat e sigurisë kombëtare, politikën e jashtme, interesat ekonomikë dhe financiarë të shtetit, parandalimin dhe ndjekjen e veprave penale. Në rast se aksesi mohohet, duke argumentuar se cenohen interesat e sigurisë kombëtare, politika e jashtme, interesat ekonomikë dhe financiarë të shtetit, parandalimi dhe ndjekja e veprave penale ose liria e shprehjes dhe informimit apo liria e shtypit, subjekti i të dhënave mund t'i kërkojë Komisionerit të kontrollojë përjashtimin në rastin konkret. Komisioneri informon subjektin e të dhënave për masat e marra. Ligji nuk përcakton në mënyrë specifike se si jepet aksesi. Një mënyrë e mundshme është që subjektit të të dhënave t'i jepet një kopje e të dhënave. Një tjetër mënyrë është që subjektit të të dhënave t'i jepet mundësi që t'i shikojë të dhënat etj. Një mënyrë është një letër e thjeshtë ose nëse mënyrat elektronike janë të pranueshme, një e-mail mund të jetë i mjaftueshëm. Sidoqoftë, jo çdo njeri do të jetë i lumtur të shkruajë një letër të tillë dhe mund të jetë e dobishme për Komisionerin të nxjerrë një formë e cila mund të përdoret nëse është e nevojshme. Megjithatë, kjo duhet të bëhet e qartë që përdorimi i formës nuk është i detyrueshëm

[472] Neni 12, paragrafi 1.

dhe ky akses mund të jepet në çdo formë që kërkesa e shkruar bëhet. Një tjetër mënyrë është që subjektit të të dhënave t'i jepet mundësi që t'i shikojë të dhënat etj. Kërkesa e personit ndaj Komisionerit duhet të bëhet në ndonjë nga mënyrat e shkruara. Megjithatë, përsëri, ajo duhet të jetë e dobishme në një formë për përdorim, në qoftë se subjekti i të dhënave dëshiron. Kjo i përket Komisionerit të vendosë nëse ajo do të përdorë një formë të caktuar për të bërë afrimin e mëtejshëm më kontrolluesin e të dhënave dhe një formë të mëtejshme për të raportuar rezultat subjektit të të dhënave. Një e drejtë tjetër e subjektit të të dhënave është dhe e drejta për të kërkuar bllokimin, korrigjimin ose fshirjen e të dhënave personale[473] ku në këtë dispozitë shprehet qartë e drejta e individit për të kërkuar korrigjimin ose fshirjen e të dhënave, kur vihet në dijeni se të dhënat rreth tij nuk janë të rregullta, të vërteta, të paplota ose janë përpunuar dhe mbledhur në kundërshtim me dispozitat e këtij ligji. Kërkesa mund të bëhet me shkrim ose me gojë me anë të një shënimi të kontrolluesit të të dhënave. Këtë kërkesë të individit kontrolluesi duhet ta shqyrtojë dhe nëse sjell bindjen se kërkuesi ka të drejtë, duhet të korrigjojë ose fshijë të dhënat e parregullta.

Ligjvënësi ka vënë dhe një afat prej 30 ditësh nga marrja e kërkesës të subjektit të të dhënave, brenda së cilës Kontrolluesit duhet të njoftojnë për përpunimin e ligjshëm të të dhënave si dhe kryerjen ose moskryerjen e korrigjimit apo të fshirjes. Kjo, për t'i dhënë mundësi subjektit të të dhënave që të realizojë të drejtën e ankimit tek Komisioneri, kur kontrolluesi nuk bën korrigjim ose fshirjen e të dhënave të kërkuara. Në këtë dispozitë është bërë e qartë se edhe në rastin kur kontrolluesi nuk njofton ose refuzon të njoftojë subjektin e të dhënave lidhur me kërkesën, subjekti i të dhënave ka të drejtë të ankohet te Komisioneri. Në këtë rast, Komisioneri ka kompetencë që të ndërmarrë një hetim. Nëse ai konstaton se të dhënat janë të gabuara apo se po përpunohen në mënyrë të paligjshme, mund të urdhërojë kontrolluesin që t'i korrigjojë apo t'i fshijë ato. Mos korrigjimi apo mos fshirja e të dhënave që janë të gabuara apo të përpunuara në mënyrë të gabuar është shkelje administrative.

E drejta për vendimmarrje automatike[474] është një lloj vlerësimi për individët, e kryer krejtësisht pa ndërhyrjen e njeriut. Ajo kryhet kur kompjuterët programohen për të vlerësuar informacionin për individët që kërkojnë një shërbim apo përfitim të veçantë

[473] Neni 13.

[474] Neni 14.

(p.sh. kredi) përkundrejt kritereve të përcaktuara. Vendimi nëse këta individë mund ta përfitojnë shërbimin apo përfitimin varet krejtësisht nga rezultati i gjeneruar nga ky vlerësim automatik. Individët kanë të drejtë që të mos jenë subjekt i vendimeve të tilla nëse vendimet shkaktojnë efekte ligjore mbi ta ose i ndikojnë në mënyrë të drejtpërdrejtë kur vlerësojnë aspekte personale që lidhen me individët, sidomos efikasitetin e tyre në punë, besueshmërinë apo sjelljen. Shumë e rëndësishme është e drejta e subjektit të të dhënave për të kundërshtuar[475] ku subjekti i të dhënave ka të drejtë të ngrejë në çdo kohë kundërshtimin për përpunimin e të dhënave lidhur me të, përveç kur parashikohet ndryshe me ligj. Duke qenë se kjo e drejtë i lejon individët që të (kundërshtojnë) parandalojnë një përpunim që do të ishte i ligjshëm, do të duhet të jetë diçka që mund të shkaktojë dëm të madh ose shqetësim të konsiderueshëm për individin në fjalë ose për një individ tjetër. Ndonjëherë për shembull, bërja e ditur e të dhënave personale të një individi tek bashkëshorti apo partneri mund të shkaktojë probleme të mëdha familjare. Nëse bashkëshorti ka punuar për kontrolluesin që përpunon të dhëna, individi mund t'i kërkojë kontrolluesit që të mos e lejojë partneren t'i shohë të dhënat e tij. Nëse kërkesat justifikohen, kontrolluesit duhet të ndërmarrin veprimet e nevojshme si të informojnë individin nëse është ndërmarrë apo jo një veprim.

Nëse kontrolluesit nuk e përmbushin kërkesën e individit, atëherë ai ka të drejtë që të ankohet te Komisioneri. Komisioneri mund të ndërmarrë një hetim dhe nëse është me vend, mund të urdhërojë kontrolluesit që të përmbushin kërkesat.

Çdo person ka të drejtë të ankohet[476] nëse pretendon se i janë shkelur të drejtat, liritë dhe interesat e ligjshëm për të dhënat personale. Ka të drejtë të ankohet ose të njoftojë komisionerin dhe të kërkojë ndërhyrjen e tij për vënien në vend të së drejtës së shkelur. Pas këtij ankimi, në përputhje me Kodin e Procedurës Civile, subjekti i të dhënave mund të ankohet në gjykatë.

Shkaktimi i dëmit dhe shpërblimi i tij[477] është një kategori juridike që rregullohet nga Kodi Civil. Është kjo arsyeja që organi kompetent për përcaktimin e dëmit dhe detyrimin për shpërblimin e tij, është gjykata dhe jo Komisioneri. Dëmi sipas

[475] Neni 15.

[476] Neni 16.

[477] Neni 17.

Kodit Civil mund të jetë material (shpenzimet e kryera, humbja e pësuar apo fitimi i munguar -neni 640) ose moral, jo pasuror (dëmtim të shëndetit ose cenim në nderin e personalitetin e tij-neni 625).

4.2.5 Detyrimet e kontrolluesit dhe të përpunuesit, njoftimi dhe siguria e të dhënave personale

Kapitulli i V (Nenet 18-20) parashikon detyrimet e kontrolluesit dhe përpunuesit ku specifikohen së pari detyrimet e kontrolluesit si detyrimi për informim, detyrimi për korrigjim ose fshirje e të dhënave personale dhe së dyti detyrimet e përpunuesit. Informacioni duhet të jepet pas grumbullimit, sa më shpejt që të jetë e mundur. Kur të dhënat mblidhen nga individët e interesuar, informacioni mund të jepet në kohën e grumbullimit të të dhënave. Ligji nuk parashikon formën e dhënies së informacionit. Nëse të dhënat merren nga personi me anë të telefonit, informacioni do të jepet gojarisht. Shpesh, është e përshtatshme që kontrolluesi ta hedhë informacionin në një formular të printuar ose në një letër e cila i dërgohet personave të interesuar për një tjetër qëllim. Për institucionet që i grumbullojnë të dhënat personale on-line, informacioni duhet të përfshihet në një deklaratë në faqen e internetit. Në lidhje me detyrimin për korrigjim ose fshirje e të dhënave personale, mund të themi se sipas kësaj çdo kontrollues gjatë procesit të përpunimit të të dhënave personale të subjekteve të të dhënave është i detyruar të kryejë vetë korrigjimin apo fshirjen e të dhënave personale, kur vëren se janë të parregullta, të pavërteta, të paplota ose janë përpunuar në kundërshtim me dispozitat e ligjit "Për mbrojtjen e të dhënave personale". Jo vetëm kaq, por ligjvënësi ka garantuar se edhe kur subjekti i të dhënave vëren se të dhënat e tij po përpunohen në mënyrë të parregullt, janë të pavërteta ose janë përpunuar në kundërshtim me ligjin, ka të drejtë të kërkojë tek kontrolluesi korrigjimin ose fshirjen e të dhënave të parregullta.

Veç kësaj, sipas kësaj dispozite, kur është rasti, kontrolluesi detyrohet të informojë dhe marrësin e të dhënave personale për korrigjimin ose fshirjen e të dhënave personale, të transmetuara para korrigjimit apo fshirjes. Si marrës të të dhënave, në këtë rast mund të jetë përpunuesi që ka lidhur kontratë me kontrolluesin ose çdo kontrollues tjetër që i transmetohen të dhënat konform ligjit. Ndërsa për detyrimet e përpunuesit, dispozitat e ligjit përcaktojnë se Kontrolluesit, për përpunimin e të dhënave

personale, mund të punësojnë përpunues dhe ndërmjet tyre duhet të lidhet një kontratë ku të merret përsipër garantimi për përdorimin e ligjshëm dhe të sigurt të të dhënave. Ligjshmëria dhe siguria për përdorimin e të dhënave personale nga përpunuesi parashikohet në nenet 5-11 dhe 27 të ligjit për mbrojtjen e të dhënave personale. Kapitulli i VI (Nenet 21-26) parashikon përgjegjësinë e kontrolluesit për të njoftuar Komisionerin për përpunimin e të dhënave personale, përmbajtjen e njoftimit, procedurën e shqyrtimit, kontrollin paraprak, fillimin e përpunimit dhe publikimin e përpunimeve.

Për sa i përket njoftimit, mund të themi se nga ky përcaktim, kontrolluesit duhet të njoftojnë Komisionerin vetëm një herë, përveç rasteve kur ka ndonjë ndryshim që do të thotë se njoftimi që është dhënë fillimisht është i gabuar.[478] P.sh. një bankë ka për qëllim që të përpunojë të dhëna personale me qëllim ofrimin e shërbimeve personale bankare. Ajo duhet t'i tregojë këtë Komisionerit. Sapo Komisioneri të jetë njoftuar, banka mund të vijojë me përpunimin e të dhënave personale për atë qëllim që ka nevojë që t'i thotë përsëri Komisionerit. Sidoqoftë, nëse më vonë banka vendos që t'i përpunojë të dhënat personale për një qëllim tjetër, për shembull për dhënien e shërbimit të sigurimit, ajo duhet t'i thotë Komisionerit për qëllimin e ri. Ligji nuk përcakton një formë të caktuar të njoftimit. Këtë mund ta përcaktojë Komisioneri. Kontrolluesit duhet të japin informacion edhe për një përpunim që përjashtohet nga njoftimi duke u përqendruar në emrin e adresën e kërkuesit, qëllimin e përpunimit që ata bëjnë, kategoritë e të dhënave personale që ata përpunojnë dhe kategoritë e personave të cilëve të dhënat u bëhen të ditura. Deklarimi i qëllimit të përpunimit do të konsiderohet nga më të rëndësishmit, pasi qëllimit të përpunimit të të dhënave personale i është kushtuar një vëmendje e veçantë nga ligjvënësi në ligjin numër 9887, datë 10.03.2008 *"Për mbrojtjen e të dhënave personale"*. Sipas këtij ligji, përpunimi i të dhënave personale duhet të jetë një proces i bazuar në ligj dhe i drejtë, duke garantuar mbrojtjen maksimale të subjekteve të këtyre të dhënave. Theksojmë se për të realizuar njoftimin në lidhje me qëllimin subjektet kontrollues duhet të kenë vëmendjen maksimale për të arritur në konkluzionin se përpunimi i të dhënave bëhet për një qëllim

[478] Çabej (Pogaçe), F., Gjoleka, A., Shala, A. (2010). "*Komentar i ligjit për mbrojtjen e të dhënave personale*", Tiranë, fq.47.

apo për disa qëllime, se mund të plotësoni disa kuadrate nëse përpunimi i të dhënave personale realizohet nga ana juaj për shkak të disa qëllimeve.

Sipas Nenit 23, Zyra e Komisionerit, specialistët e Drejtorisë së Regjistrimit, shqyrtojnë të gjitha njoftimet dhe kur njoftimi është i pamjaftueshëm, ai urdhëron kontrolluesin të plotësojë të dhënat duke përcaktuar edhe afatin kohor. Shqyrtuesi i njoftimit verifikon informacionin e deklaruar në kuadrin e përgjithshëm që ai të jetë sa më i plotë, i qartë dhe i kuptueshëm si dhe verifikon ligjshmërinë e përpunimit, kryesisht për sa i përket përpunimit të të dhënave sensitive dhe transferimeve ndërkombëtare, sipas kushteve të përcaktuara në Nenin 24 të Ligjit. Në bazë të nenit 24 "Kontrolli paraprak", autorizimi i Komisionerit kërkohet kur përpunohen të dhëna sensitive dhe kur kontrolluesit kërkojnë të transferojnë të dhënat personale në vende që nuk kanë nivel të mjaftueshëm të mbrojtjes së të dhënave, parashikuar në pikën 1 të nenit 9. *Përpunimin e të dhënave*,[479] si rregull kontrolluesit e nisin sapo njoftimi të jetë bërë dhe nuk kanë detyrimin që të presin përgjigjen e Komisionerit. Por për këtë ka dy përjashtime që kontrolluesit duhet të presin autorizimin e Komisionerit para se të vazhdojnë përpunimin e të dhënave: kur përpunimi i të dhënave sensitive kërkon autorizimin e Komisionerit dhe kur kontrolluesit kërkojnë të transferojnë të dhënat personale në vende të tjera, për rrethana që kërkojnë autorizimin e Komisionerit. Për publikimin e njoftimeve, qëllimi i njoftimit është publikimi i përpunimeve në regjistrin e hapur për publikun që administrohet nga Komisioneri, parashikuar në nenin 26. Nuk publikohen informacionet që kanë të bëjnë me sigurinë e aplikuar nga ana e subjektit kontrollues së deklaron.

Kapitulli i VII (Nenet 27-28) parashikon sigurinë e të dhënave personale ku përcakton masat për sigurinë e të dhënave personale dhe konfidencialitetin e të dhënave personale.

Është e rëndësishme që të dhënat personale të mbahen të sigurta dhe që të mos keqpërdoren apo korruptohen në ndonjë mënyrë. Siguria nuk ka të bëjë vetëm me marrjen e masave fizike, megjithëse këto janë shumë të rëndësishme. Siguria gjithashtu ka të bëjë me organizimin e punës në një mënyrë të tillë që risku të minimizohet, për shembull duke siguruar që personeli të mund t'i shohë të dhënat vetëm kur kjo është e nevojshme që ata të kryejnë punën e tyre në mënyrën e duhur dhe duke e trajnuar

[479] Neni 25.

personelin në lidhje me çfarë duhet dhe nuk duhet të bëjë. Duhet të sigurohet që pajisjet për përpunimin e të dhënave, përdoren vetëm ashtu siç janë autorizuar dhe që gjithë këto pajisje të kenë aparate që parandalojnë përdorimin e paautorizuar. Në përmirësimin e sigurisë ka shumë pajisje teknike që ndihmojnë në përmirësimin e saj. Gjithnjë e më shumë, pajisjet e reja kompjuterike kanë të inkorporuar pajisje sigurie, prandaj përparësi në blerjen e këtyre pajisjeve duhet t'i jepen atyre që ofrojnë elemente të përshtatshëm sigurie.

Të sigurohet që modifikimi, korrigjimi, fshirja dhe transferimi i të dhënave personale dhe veprime të tjera në lidhje me të dhënat personale të regjistrohen dhe të dokumentohen. Konfidencialiteti i të dhënave personale, do të thotë që Kontrolluesit dhe përpunuesit nuk duhet 'ti bëjnë me dije ndonjë personi të paautorizuar të dhëna personale të cilat ata i shohin apo që i mësojnë gjatë punës. Detyrimi për ruajtjen e konfidencialitetit zgjat pambarimisht. Detyrimi nuk mbaron kur personat nuk ushtrojnë më funksionet e tyre. Thyerja e detyrimit të konfidencialitetit përbën vepër penale të parashikuar nga Kodi penal.

4.2.6 Komisioneri për të drejtën e informimit dhe mbrojtjen e të dhënave personale

Një kapitull shumë i rëndësishëm i këtij ligji është kapitulli i VIII i cili parashikon funksionimin e institucionit të "Komisionerit" i cili është shumë i rëndësishëm në mbrojtjen e të drejtës së informimit dhe mbrojtjen e të dhënave personale.[480] Ligji për herë të parë ka krijuar një autoritet mbikëqyrës të pavarur, puna e të cilit është që të sigurojë që nga të gjithë institucionet publike dhe private, përpunimi i të dhënave personale po bëhet sipas disa rregullave të përcaktuara në ligj. [481] Komisioneri për të drejtën e informimit dhe mbrojtjen e të dhënave personale është autoritet mbikëqyrës i pavarur dhe kjo përmendet qartë në nenet 29-38 të ligjit për mbrojtjen e të dhënave personale. Në këto nene dhe në tërësinë e ligjit për mbrojtjen e të dhënave personale përcaktohet se vlerat dhe parimet mbi të cilat vepron ky institucion, janë pavarësia, paanshmëria, profesionalizmi dhe konfidencialiteti. Komisioneri për të drejtën e informimit dhe mbrojtjen e të dhënave personale, duke u vënë në lëvizje me

[480] Neni 29.

[481] Po aty. Paragrafi 1.

ankimin e subjektit të të dhënave si dhe me iniciativën e tij, kur e sheh me vend sipas nenit 30 të ligjit numër 9887, datë 10.3.2008 "Për Mbrojtjen e të Dhënave Personale" kryen hetim administrativ dhe ka të drejtën e aksesit në përpunimet e të dhënave personale si dhe ka të drejtë të mbledhë të gjithë informacionin e nevojshëm për përmbushjen e detyrave të mbikëqyrjes. Këtë hetim Komisioneri e kryen në zbatim të procedurave të parashikuara në Kodin e Procedurave Administrative.

Ndër funksionet e Komisionerit për të Drejtën e Informimit Mbrojtjen e të Dhënave Personale është promovimi i praktikës së mirë në mbrojtjen e të dhënave personale për institucionet private dhe publike.

Të marrë vendime për ankesat dhe duke nxjerrë akte normative lidhur me mbrojtjen e të dhënave personale. Komisioneri caktohet nga Kuvendi dhe ka status të pavarur duke raportuar drejtpërsëdrejti në Parlament sipas përgjegjësive të përcaktuara në ligj. Detyra primare e Komisionerit është mbikëqyrja e mbrojtjes së të dhënave personale, të cilën e realizon në sajë të hetimit të plotë administrativ duke kërkuar/kontrolluar ndër të tjera:

- zbatimin e rregullave të përpunimit të të dhënave personale;
- mbrojtjen e të dhënave gjatë përpunimit;
- plotësimin e kritereve ligjore të përpunimit;
- respektimin e të drejtave të subjekteve të të dhënave dhe rivendosjen e të drejtave të shkelura;
- zbatimin e të gjitha detyrimeve që ngarkon ligji "Për mbrojtjen e të dhënave personale" për informimin, fshirjen, sigurinë e të dhënave personale, dhe ruajtjen e konfidencialitetit të tyre;
- përcaktimin e përgjegjësisë dhe kur ekzistojnë rrethanat e parashikuara në ligj vendos sanksione administrative.[482]

Për realizimin e kompetencave, zyra e Komisionerit vihet në lëvizje me këto mënyra ligjore: (1) Nëpërmjet ankimit drejtuar Komisionerit nga ana e individëve ose kontrolluesve të të dhënave ; (2) Me nismën e vetë zyrës së Komisionerit, nëpërmjet: a) shqyrtimit të njoftimeve që janë të detyruar të dërgojnë kontrolluesit, për të dhënat personale që ata përpunojnë, dhe b) nëpërmjet kontrolleve të programuara nga zyra e

[482] Çabej (Pogaçe), F., Gjoleka, A., Shala, A. (2010). "*Komentar i ligjit për mbrojtjen e të dhënave personale*", Tiranë, fq.64.

Komisionerit, hetimit administrativ dhe inspektimit.[483] Komisioneri gëzon gjithashtu statusin e një organi këshillues në lidhje me aktet e Kuvendit apo institucioneve të tjera shtetërore si dhe me sipërmarrjet e subjekteve kontrolluese të të dhënave që prekin të dhënat personale. Në ligj thuhet se Komisioneri është përgjegjës për dhënien e mendimeve për projekt- aktet ligjore dhe nënligjore që kanë të bëjnë me të dhënat personale si dhe projektet që kërkohen të zbatohen nga kontrolluesit vetëm apo në bashkëpunim me të tjerë.[484] Veprimtaria e Komisionerit karakterizohet nga vendosja e rregullave të hollësishme për sigurimin e të dhënave personale. Gjatë veprimtarisë së tij, praktika administrative e Komisionerit, konsiston në nxjerrjen:

- e rekomandimeve të veçanta për inspektimet që i bëhen kontrolluesve të të dhënave personale dhe zyra e Komisionerit ka nxjerrë disa rekomandime në lidhje me to. Një nga rekomandimet që i bëhet gjyqësorit në zbatim të ligjit në ngarkim të kontrolluesit "Ministria e Drejtësisë", "Për ligjshmërinë e përpunimit të të dhënave Personale në publikimin e vendimeve gjyqësore në portalin e Gjykatave", konsiston që të merren masa që publikimi i vendimeve gjyqësore në portalet e gjykatave të bëhet duke bërë anonime të dhënat personale të subjekteve që marrin pjesë në procese gjyqësore, vendimet gjyqësore që do të hidhen në portalet e gjykatave, pas këtij rekomandimi të jenë pa të dhëna personale të cilat identifikojnë personat pjesëmarrës në proceset gjyqësore, të ndërtohet një strategji lidhur me anonimizimin e të dhënave personale për vendimet e vjetra të cilat aktualisht ndodhen të publikuara ne portale.[485]
- e udhëzime për inspektimet që i bëhen kontrolluesve të të dhënave personale. Zyra e Komisionerit ka nxjerrë urdhër në zbatim të ligjit në ngarkim të kontrolluesit "Gjykata e Rrethit Gjyqësor" Tiranë, pas verifikimit të ankesës të një shtetase drejtuar Komisionerit, e cila lidhet me publikimin e vendimit gjyqësor ne faqen zyrtare të Gjykatës, vendim i cili mbart të dhëna personale të saj. Komisioneri në zbatim të nenit 2 të ligjit nr. 9887 datë 10.03.2008, "Për Mbrojtjen e të Dhënave Personale", dhe Kreut IV të Udhëzimit nr.15 datë 23.12.2011 të Komisionerit për Mbrojtjen e të Dhënave Personale, "Për Përpunimin dhe Publikimin e të Dhënave Personale në

[483] Po aty.

[484] Neni 29 i ligjit nr. 9887.

[485] Rekomandim nr. 8 i Komisionerit për të Drejtën e Informimit Mbrojtjen e të Dhënave Personale, dt.05.06.2013.

Sistemin Gjyqësor", urdhëroi të realizohet në mënyrë të menjëhershme, anonimizimi apo inicializimi i të dhënave personale që i përkasin subjektit ankues, të përfshirë në Vendimin e publikuar në faqen zyrtare të Gjykatës në internet. Të merren masat e duhura teknike dhe organizative për zbatimin e Udhëzimit të mësipërm, për të realizuar anonimizimin apo inicializimin i të dhënave personale që i përkasin subjekteve të përfshira në vendimet gjyqësore që publikohen në faqen zyrtare në internet.[486]

- e vendimeve me qëllim sqarimin e mëtejshëm të dispozitave të ligjit 'Për mbrojtjen e të dhënave personale' dhe evidentimin e saktë të rrethanave në të cilat do të gjejnë zbatim detyrimet e vendosura nga ky ligj ndaj subjekteve kontrolluese të të dhënave personale. Në ligj thuhet se 'procedurat e administrimit të regjistrimit të të dhënave, të hedhjes së të dhënave, të përpunimit dhe nxjerrjes së tyre përcaktohen me vendim të komisionerit.' Për këtë qëllim, zyra e Komisionerit ka nxjerrë vendimin "Për përcaktimin e rregullave të hollësishme për sigurimin e të dhënave personale".[487] Në vendim theksohet domosdoshmëria e ruajtjes së sigurisë të të dhënave mbrojtjes së tyre nga çdo keqpërdorim apo praktikë korruptimi.

Koncepti i sigurisë, vlerësohet jo vetëm në lidhje me marrjen e masave fizike por gjithashtu dhe në organizimin e punës në mënyrë të tillë që rreziku të minimizohet. Ndërmarrja e hapave të nevojshëm me qëllim ndërgjegjësimin dhe trajnimin e stafit për sa i takon nevojës së sigurisë në përpunimin e të dhënave dhe përforcimit të saj, shikohet si një aspekt kyç në rritjen e efektivitetit të mbrojtjes. Një kërkesë tjetër lidhet me marrjen e masave për funksionimin e sistemeve në mënyrë të tillë, që ato të garantojnë shërbimin në mënyrë të vazhdueshme. Këto masa marrin një rëndësi të veçantë në rastet e përpunimit të të dhënave në sektorin e komunikimeve elektronike me qëllim sigurimin e shërbimeve përkatëse të komunikimit, për garantimin ndër të tjera të vazhdimësisë në përdorimin e shërbimit. Për sa i takon marrjes së masave me natyrë teknike, rregullat kryesore lidhen me: instalimin dhe përditësimin e programeve antivirus (barrierave mbrojtëse) në të gjithë pajisjet kompjuterike, përdorimin e fjalëkalimeve në aksesin e të dhënave dhe ndryshimin e tyre periodik,

[486] Urdhër nr.11 i Komisionerit për të Drejtën e Informimit Mbrojtjen e të Dhënave Personale, dt.21.03.2013.

[487] Vendim nr. 1, datë 4.03.2010 i Komisionerit për të Drejtën e Informimit Mbrojtjen e të Dhënave Personale.

kërkesën për t'iu dhënë përparësi në blerje pajisjeve teknike që ofrojnë elemente të përshtatshme sigurie, marrjen e masave për të garantuar që komunikimi të jetë i sigurt dhe të shifrohet, aty ku është i nevojshëm, gjatë transmetimit të të dhënave personale dhe përpunimit e tyre në rrjet. Komisioneri, në rast shkeljesh serioze, të përsëritura ose të qëllimshme të ligjit nga një kontrollues ose përpunues, veçanërisht në rastet e përsëritura të moszbatimit të rekomandimeve të tij, vepron sipas nenit 39 të këtij ligji dhe e denoncon publikisht ose e raporton çështjen në Kuvend dhe në Këshillin e Ministrave. Për rastet që shkelja përbën vepër penale, bën kallëzimin përkatës. Komisioneri krijon një regjistër për dokumentimin e të gjitha njoftimeve dhe autorizimeve që ai kryen në ushtrim të kompetencave të tij, në fushën e mbrojtjes së të dhënave personale si dhe paraqet raport vjetor përpara Kuvendit dhe raporton përpara tij sa herë i kërkohet. Gjithashtu, ai mund t'i kërkojë Kuvendit të dëgjohet për çështje që i çmon të rëndësishme. Institucionet publike dhe private detyrohen nëpërmjet ligjit të bashkëpunojnë me Komisionerin[488] duke i siguruar të gjithë informacionin që ai kërkon për përmbushjen e detyrave si dhe e njoftojnë atë për zbatimin e rekomandimeve të dhëna menjëherë pas mbarimit të afatit të caktuar për kryerjen e tyre. Komisioneri ka akses në sistemin e kompjuterëve, në sistemet e arkivimit, që kryejnë përpunimin e të dhënave personale dhe në të gjithë dokumentacionin, që lidhet me përpunimin dhe transferimin e tyre, për ushtrimin e të drejtave dhe të detyrave që i janë ngarkuar me ligj. Zgjedhja dhe qëndrimi në detyrë i Komisionerit[489] bëhet nga Kuvendi, nëpërmjet një procesi që fillon së pari me propozimin e kandidaturës nga Këshilli i Ministrave për një mandat 5- vjeçar, me të drejtë rizgjedhjeje. Funksioni i punës së Komisionerit është i papajtueshëm me çdo funksion[490] tjetër shtetëror, nuk duhet të jetë i anëtarësuar në asnjë parti politike dhe të mos marrë pjesë në asnjë veprimtari të tyre si dhe me çdo veprimtari tjetër fitimprurëse, me përjashtim të mësimdhënies. Komisioneri për Mbrojtjen e të Dhënave Personale, në respektim të kompetencave të përcaktuara nga

[488] Neni 32 i ligjit nr. 9887, datë 10.03.2008, ndryshuar me ligjin Nr. 48/2012, ndryshuar me ligjin nr.120/2014.

[489] Neni 33.

[490] Neni 34.

ligji, ka miratuar një sërë udhëzimesh[491] të cilat orientojnë në mënyrë të detajuar ruajtjen e të dhënave personale nga subjektet, si më poshtë:

- *Udhëzim Nr. 1 për "Lejimin e disa Kategorive të Transferimeve Ndërkombëtare të të Dhënave Personale në një Shtet që nuk ka Nivel të Mjaftueshëm të Mbrojtjes së të Dhënave Personale".*
- *Udhëzim Nr. 2 për "Detyrimet e Kontrolluesve dhe Përpunuesve Përpara se të Përpunojnë të Dhënat Personale".*
- *Udhëzim Nr. 3 për "Sistemin e Video Survejimit në Ndërtesa, Lokale e Ambiente të Ndryshme".*
- *Udhëzim Nr. 4 për "Marrjen e Masave të Sigurisë së të Dhënave Personale në Veprimtarinë e Fushës së Arsimit".*
- *Udhëzim Nr. 5 për "Rregullat Themelore në lidhje me Mbrojtjen e të Dhënave Personale në Sistemin e Kujdesit Shëndetësor".*
- *Udhëzim Nr. 6 për "Përdorimin korrekt të SMS-ve për qëllime promocionale, reklama, informacione, shitjeve direkt nëpërmjet telefonisë celulare".*
- *Udhëzim Nr. 7 për "Përpunimin e të Dhënave Personale në Sektorin e Arsimit".*
- *Udhëzim Nr. 8 për "Birësimin".*
- *Udhëzim Nr. 9 për "Median e Shkruar dhe Audiovizive".*
- *Udhëzim Nr. 10 për "Përpunimin e të dhënave personale në kuadër të shërbimeve hoteliere".*
- *Udhëzim Nr. 11 për "Përpunimin e të dhënave të punonjësve në sektorin privat".*
- *Udhëzim Nr. 12 për "Për kontrollin e identitetit në hyrje të ndërtesave".*
- *Udhëzim Nr. 13 për disa shtesa dhe ndryshime në udhëzimin nr. 3, datë 05/03/2010 "Mbi sistemin e video survejimit në ndërtesa, lokale e ambiente të ndryshme".*
- *Udhëzim Nr. 14 për "Përpunimin, mbrojtjen dhe sigurinë e të dhënave personale në sektorin e komunikimit elektronik të publikut".*
- *Udhëzim Nr. 15 për "Përpunimin dhe publikimin e të dhënave personale në sistemin gjyqësor".*

[491] http://www.kmdp.al/index.php/sq/legjislacioni/akte-komisionerit/udhezime

- *Udhëzim Nr. 16 për "Mbrojtjen e të dhënave personale në tregtimin e drejtpërdrejtë dhe masat e sigurisë" etj..*

Duke njohur natyrën tepër delikate të çështjeve që lidhen me përpunimin e të dhënave personale nga ana e medias për qëllime të kërkimit dhe përhapjes së informacionit, zyra e Komisionerit ka nxjerrë një udhëzim në të cilin parashtrohen rregullat themelore që duhet të respektohen për mbrojtjen e të dhënave personale nga media gjatë ushtrimit të aktivitetit të saj.[492] Në udhëzimin e Komisionerit jepen orientime të qarta në lidhje me kërkesat që duhet të respektohen nga media kur informacioni i përhapur përcjell fakte në interes publik: 'edhe në prezencën e një fakti në interes publik, publikimi i të dhënave të përpunuara nga përgjimet telefonike duhet të respektojë parametrat e thelbit të informacionit. Nuk duhet të publikohen pjesë nga aspekte ngushtësisht personale ose që kanë lidhje me sferën seksuale.' Dinjiteti njerëzor shihet si një vlerë e lidhur ngushtë me vetë respektin dhe vetëvlerësimin që çdo qenie njerëzore ushqen ndaj vetes dhe si i tillë, shoqërohet domosdoshmërisht nga nevoja për garantimin e një sfere private për zhvillimin e lirë nga çdo ndërhyrje e jashtme të raporteve me botën e jashtme. Në kuptim të këtij udhëzimi, do të konsiderohen se përbëjnë fakte në interes publik, të dhënat që lidhen me interesa të sigurisë kombëtare; integritetin territorial ose sigurinë publike; parandalimin e trazirave apo krimit; mbrojtjen e shëndetit ose moralit; mbrojtjen e reputacionit ose të drejtave të të tjerëve; parandalimin e zbulimit të informacioneve konfidenciale ose për të garantuar paanshmërinë e pushtetit gjyqësor, etj. Për garantimin e privatësisë së komunikimeve kërkohet gjithashtu që gazetarët 'të mos publikojnë tekstet e mesazheve, diskutimet telefonike që kanë të bëjnë me jetën private të të interesuarve, raportet e tyre personale ose interesit profesional'.

4.2.7 Sanksionet administrative dhe dispozitat e fundit

[492] Udhëzim nr. 9, dt. 15.09.2010 "*Për rregullat themelore në lidhje me mbrojtjen e të dhënave personale në median e shkruar, vizive dhe audiovizive*".

Kapitulli IX parashikon sanksionet administrative[493] për shkelje të rregullave të përpunimit të të dhënave me kusht që dënimet duhet të jenë në përpjesëtim me peshën e veprës ngarkuar[494] si dhe ankimin dhe ekzekutimin e gjobave. Komisioneri, me anë të specialistëve, verifikon shkakun e vënies në lëvizje dhe kur e sheh me vend mund të ndërmarrë një hetim duke respektuar procedurën ligjore të parashikuar në nenet 46-104 të K.Pr.Administrative. Në përfundim të gjykimit, kur vërtetohet faji si dhe kushtet e parashikuara në nenin 30/2 të ligjit "Për mbrojtjen e të dhënave personale" (Në rast shkeljesh, të përsëritura ose të qëllimshme të ligjit nga një kontrollues ose përpunues, veçanërisht në rastet e përsëritura të moszbatimit të rekomandimeve të tij), konsideron shkeljen kundërvajtje administrative dhe sipas shkallës së fajit dhe të rrethanave që kanë sjellë shkeljen vendoset dënimi i diferencuar i kundërvajtësit me gjobë, sipas përcaktimeve të sakta në pikat 1,2,3,4 të nenit 39 të këtij ligji.

Veç kësaj në dispozitën e sipërme është përcaktuar dhe e drejta e Komisionerit që për të njëjtat arsye "në rast shkeljesh serioze, të përsëritura ose të qëllimshme të ligjit nga një kontrollues ose përpunues, veçanërisht në rastet e përsëritura të moszbatimit të rekomandimeve të tij" sipas shkallës së shkeljes që ta denoncojë publikisht ose ta raportojë çështjen në Kuvend dhe në Këshillin e Ministrave. Kjo është një tjetër garanci për zbatimin e kërkesave të ligjit "Për mbrojtjen e të dhënave personale" nga të gjithë kontrolluesit publikë dhe privatë. Po kështu, kur gjatë hetimit administrativ ose në përfundim të tij konstatohet se veprimet e kontrolluesit dhe përpunuesit apo punonjësve të tij përbëjnë vepër penale, atëherë Komisioneri e denoncon çështjen në organe kompetente sipas kërkesave të nenit 281 të Kodit të Procedurës Penale. Në ligj është përcaktuar saktë dhe procedura e ankimit, afati i paraqitjes, dispozitat ligjore referuese dhe organi kujt duhet t'i drejtohet. Sipas ligjit për kundërvajtjet, gjykata pas shqyrtimit të çështjes, ka të drejtë të vendosë lënien në fuqi të vendimit të Komisionerit për gjobën, të pushojë çështjen kur nuk vërtetohet ose të zbusë masën e dënimit ose të ndryshojë llojin e masës. Procedura e ekzekutimit të vendimit të Komisionerit për gjobën e vendosur është faza e fundit e tepër e rëndësishme. Në këtë nen janë përcaktuar

[493] Neni 39 i ligjit nr. 9887, datë 10.03.2008, ndryshuar me ligjin Nr. 48/2012, ndryshuar me ligjin nr.120/2014.

[494] "*E drejta administrative - Parimet administratës publike*", fq. 8 në faqen e internetit www.data.planetar.edu.al

qartë procedura për ekzekutimin e vendimit të Komisionerit për gjobën, afati, shndërrimi i vendimit në titull ekzekutiv dhe ekzekutimi i tij nga përmbaruesi gjyqësor mbi kërkesën e Komisionerit. Duhet pasur parasysh se dënimi i sipërm nuk mund të ekzekutohet me kalimin e një viti nga data e marrjes së vendimit . Kapitulli i X është i fundit në ligj me nenet 42-44 dhe parashikon aktet nënligjore, shfuqizimet e bëra në ligj dhe hyrjen në fuqi të tij.

Në Shqipëri, në vitin 1999 për herë të parë është miratuar ligji nr.8517, datë 22.07.1999 "Për mbrojtjen e të dhënave personale", i cili parashikonte disa rregulla të përpunimit të të dhënave personale, por linte në dëshirën e organeve publike e private zbatimin e tyre. Shtetasit kishin të drejtën e ankimit ndaj organeve mbajtëse e përpunuese të të dhënave personale te Avokati i Popullit i cili kishte vetëm kompetenca rekomanduese për organet që nuk respektonin rregullat e mbajtjes dhe përpunimit të të dhënave personale dhe orientonte ankuesin për të drejtën e ankimimit.

4.3 Mbrojtja në Ligjin Penal

Kodi Penal (KP) përmban dispozitat përkatëse penale për shkeljen e privatësisë. Në mënyrë të veçantë, neni 121 i Kodit Penal për ndërhyrjet e padrejta në jetën private në mbrojte të konfidencialitetit të komunikimeve, neni 122 në mos përhapjen e sekreteve private dhe neni 123 i Kodit Penal për pengimin ose shkeljen e fshehtësisë së korrespondencës për të garantuar sigurinë e komunikimit.

4.3.1 Neni 121 i Kodit Penal

Ndërhyrja e padrejtë në jetën private të individit[495] është përcaktuar si një akt i padrejtë duke mos marrë pëlqimin e personit në vendosjen e aparaturave që shërbejnë për dëgjim apo regjistrim të fjalëve ose të figurave, dëgjimin, regjistrimin ose transmetimin i fjalëve, fiksimin, regjistrimin ose transmetimin e figurave, si dhe ruajtjen për publikim apo publikimi i këtyre të dhënave që ekspozojnë një aspekt të jetës private të personit, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim gjer në dy vjet.

[495] Neni 121 i Kodit Penal të Republikës së Shqipërisë.

4.3.2 Neni 122 i Kodit Penal

Kodi i Penal, për të parandaluar përhapjen e një sekreti[496] që i përket jetës private të një personi nga ai që e siguron atë për shkak të detyrës ose të profesionit, kur detyrohet të mos e përhapë pa qenë i autorizuar, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim gjer në një vit. Po kjo vepër, e kryer me qëllim fitimi ose për të dëmtuar një person tjetër, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim gjer në dy vjet.

4.3.3 Neni 123 i Kodit Penal

Nevoja për të mbrojtur fshehtësinë e komunikimit nuk kufizohet vetëm me fshehtësinë e teksteve të shkruara por dhe me fshehtësinë e telekomunikacionit të cilat janë shprehje e të drejtës më të veçantë të personalitetit dhe të drejtës së individit. Kodi Penal, parashikon nëpërmjet nenit 123 se “pengimi ose shkelja e fshehtësisë së korrespondencës nga shtetasit e thjeshtë”, konsiderohet vepër penale. Konkretisht, në këtë dispozitë thuhet se: “Kryerja me dashje e veprimeve të tilla si asgjësimi, mosdorëzimi, hapja dhe leximi i letrave apo çdo korrespondencë tjetër si dhe ndërprerja ose vënia nën kontroll, dëgjimi i bisedave telefonike, telegrafike ose çdo mjeti tjetër telekomunikimi, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim gjer në dy vjet”. Nga ky formulim, vërejmë se format e shkeljes së fshehtësisë së korrespondencës/komunikimit të parashikuara në këtë dispozitë kanë karakter ilustrues dhe jo shterues. Shprehemi kështu duke u mbështetur edhe në emërtimin e dispozitës. Në emërtim përfshihet shprehja pengimi ose shkelja e fshehtësisë së korrespondencës. Kjo do të thotë që në hapësirën e zbatimit të nenit 123 do të bien të gjitha ato veprime që pengojnë ose cenojnë fshehtësinë e komunikimit dhe që janë të një rëndësie të tillë për t’u ndëshkuar penalisht. Mënyra e formulimit të dispozitës shpreh vizionin largpamës të legjislatorit. Në kushtet e zhvillimeve të vrullshme teknologjike – informatike, ligjvënësi duket të ketë vlerësuar se kjo mënyrë formulimi e dispozitës krijon mundësinë e zbatimit të saj edhe për forma dhe mënyra të tjera të shkeljes së fshehtësisë së komunikimit që nuk janë përmendur shprehimisht në dispozitë dhe që nuk mund të parashikoheshin prej ligjvënësit në kohën e formulimit të saj. Ashtu si çdo

[496] Po aty.

figurë vepre penale, edhe vepra e pengimit ose shkeljes së fshehtësisë së komunikimit përbëhet nga katër elementë: objekti, ana objektive, subjekti dhe ana subjektive.

a. Objekt juridik i kësaj vepre penale janë marrëdhëniet juridike të vendosura nga shteti për të ruajtur fshehtësinë e korrespondencës/ komunikimit, si një ndër të drejtat kushtetuese të personit, të mbrojtura posaçërisht me legjislacionin penal nga veprimet ose mosveprimet kriminale.

b. Objekt material është korrespondenca/komunikimi postar, telegrafik, telefonik ose çdo mjet tjetër të komunikimi.

Ana objektive. Nga ana objektive vepra kryhet me veprime ose mosveprime të kundërligjshme, me forma dhe mënyra të ndryshme, si me asgjësim, mosdorëzim të letrave,[497] hapjen dhe leximin e tyre apo çdo komunikimi tjetër si dhe me ndërprerjen[498] ose vënien nën kontroll të aparateve telefonike, dëgjimin e bisedave telefonike ose çdo mjeti tjetër telekomunikimi. Për të pasur këtë figurë vepre penale, mjafton konsumimi i një prej formave apo mënyrave të treguara më lart, pa qenë nevoja për ardhjen e ndonjë pasoje tjetër. Kjo do të thotë që figura e veprës penale e parashikuar nga neni 123 konsiderohet e kryer nëse vërtetohet një nga rrethanat e përmendura në dispozitë, pavarësisht ardhjes ose jo të ndonjë pasoje. Gjithashtu duhet theksuar se për të përcaktuar nëse është shkelur ose jo fshehtësia e korrespondencës/komunikimit, nuk ka rëndësi fakti nëse përmbajtja e saj është apo jo e fshehtë, pasi korrespondenca komunikimi në vetvete konsiderohet nga ligji si e fshehtë.

Mjafton fakti që një person, me dashje, ka hapur dhe ka lexuar një letër që nuk i drejtohet atij apo ka dëgjuar një bisedë telefonike të zhvilluar midis personave të tjerë, për të qenë përpara konsumimit të veprës penale të parashikuar nga neni 123.

Këtu duhet të kemi parasysh, që mund të ketë raste kur shkelësi nuk e ka hapur letrën por megjithatë ka arritur të njihet me përmbajtjen e saj në një mënyrë tjetër si p.sh. duke e vëzhguar letrën përkundrejt dritës. Në praktikën gjyqësore të huaj vepra është konsideruar e kryer edhe në rastin kur nuk është lexuar përmbajtja e letrës së shkruar, por subjekti thjesht ka marrë dijeni mbi natyrën e objektit që ndodhet në një zarf të mbyllur. Për sa i përket konsumimit të kësaj vepre penale në formën e përgjimit

[497] Në rastin e postës elektronike me mosdorëzim do të kuptojmë privimin në mënyrë të përkohshme ose përfundimtare të marrësit prej e-mail-it të tij.

[498] Me ndërprerje do të kuptojmë ndalimin e një bisede ose komunikimi që ka nisur ndërkohë.

të komunikimeve personale, në praktikën gjyqësore të huaj është vënë në dukje se veprimi në fjalë duhet të plotësojë këto kushte:

1. subjektet e përgjuara duhet të komunikojnë ndërmjet tyre me synimin e qartë për të përjashtuar persona të huaj nga konteksti i komunikimit dhe sipas mënyrave, të tilla që ruajnë fshehtësinë e komunikimit.
2. është i nevojshëm përdorimi i instrumenteve teknike të kapjes së sinjaleve (elektromekanike ose elektronike) veçanërisht pushtues dhe të fshehtë, që janë të aftë të shmangin masat mbrojtëse elementare.
3. duhet të vërtetohet plotësisht cilësia e të qenit i huaj (i jashtëm) në komunikim e subjektit, i cili në mënyrë të fshehtë, shkel fshehtësinë e bisedës.

Për sa i takon elementit subjektiv që shoqëron kryerjen e veprimeve që shkelin fshehtësinë ose paprekshmërinë e korrespondencës, kërkohet që veprimet të jenë kryer me dashje të drejtpërdrejtë ose të tërthortë.[499]

Konsumimi i anës objektive të veprës në lidhje me postën elektronike. Për shkak të natyrës së veçantë që kanë mesazhet e transmetuara nëpërmjet postës elektronike është e rëndësishme që të trajtojmë shkurtimisht se në çfarë mënyre mund të shkelet fshehtësia dhe paprekshmëria e këstij komunikimi dhe që sjell në mënyrë direkte pasoja të rënda në sferën e të dhënave personale dhe privatësisë. Gjatë transmetimit të tyre, mesazhet e-mail, udhëtojnë nëpër një rrjet të caktuar të komunikimeve elektronike publike. Konkretisht mesazhi fillimisht merret nga ofruesi i shërbimit të rrjetit të komunikimit publik të dërguesit dhe më pas i ritransmetohet ofruesit të shërbimit të marrësit i cili e ruan atë në një kuti postare të posaçme derisa marrësi të mos e ketë shkarkuar mesazhin në pajisjen e tij. Rruga që përshkon mesazhi nga dërguesi tek marrësi jo gjithmonë është e drejtpërdrejtë, por mund të jetë tepër e ndërlikuar. Paketat prej bite-sh në të cilat vendoset mesazhi, përshkojnë rrjetin duke u adresuar drejt portave të ndryshme që i zhvendosin drejt destinacioneve të ndryshme përfundimtare.[500] Gjatë kalimit në një prej portave të përdorura për transmetim, mesazhi mund të lexohet ose për më tepër të modifikohet përveçse kur është i koduar. Nga ana tjetër, kemi parasysh që nuk ekziston një mjet mbajtës në trajtë letre i mesazhit i cili mund të hiqet,

[499] Elezi, I. (2007). "*E Drejta Penale (Pjesa e Posaçme)*", Tiranë, fq.171.

[500] Mund të ndodhë psh. që një mesazh i dërguar me anë të postës elektronike nga Tirana në Madrid të kalojë nëpër shumë porta, madje edhe në SH.B.A përpara se të mbërrijë në destinacion.

shkatërrohet ose asgjësohet. Për këtë arsye, në lidhje me mesazhet e- mail, vepra penale e pengimit ose shkeljes së fshehtësisë së korrespondencës nuk mund të konsumohet nëpërmjet shkatërrimit ose asgjësimit të tyre. Megjithatë, kjo vepër penale mund të kryhet nëpërmjet fshirjes së mesazhit nga memoria e kompjuterit të server-it, dërguesit ose marrësit. Për mesazhet e-mail të koduara, vepra penale e shkeljes së fshehtësisë së korrespondencës nuk mund të kryhet nëpërmjet hapjes dhe leximit të tyre, për arsye se vetë natyra e këtyre mesazheve përjashton kryerjen e të tilla veprimeve nga persona të cilët nuk kanë çelësin përkatës të dekriptimit.[501] Megjithatë, kodimi siguron fshehtësinë e mesazhit por jo paprekshmërinë e tij. Si rrjedhim edhe këto mesazhe mund të jenë objekt i fshirjes nga ana e subjektit kriminal. Në sajë të zhvillimeve më të fundit shkencore, mesazheve e-mail mund t'iu sigurohet shkalla më e lartë e sigurisë nëpërmjet zbatimit të teknikave të Steganografisë.[502] Duke qenë se nëpërmjet zbatimit të këtyre teknikave, ekzistenca e mesazhit mbetet e fshehtë për persona të ndryshëm nga dërguesi apo marrësi i tij. Përjashtohet jo vetëm mundësia që mesazhi të hapet dhe të lexohet, por gjithashtu edhe mundësia e fshirjes së tij. *Subjekti aktiv dhe pasiv.* Subjekt aktiv i veprës është çdo person që ka mbushur moshën për përgjegjësi penale dhe është i përgjegjshëm.

Përderisa kemi të bëjmë me kundra vajtje penale, subjekt aktiv mund të jetë çdo person që ka mbushur moshën 16 vjeç dhe që është i përgjegjshëm, shtetas shqiptar ose shtetas i huaj. Subjekt pasiv mund të jetë çdo person fizik. Personat juridikë nuk mund të jenë subjekte pasive të kësaj vepre penale.

Vepra penale e "pengimit ose shkeljes së fshehtësisë së korrespondencës" është vendosur në kreun II të kodit penal "Vepra penale kundër personit", dhe konkretisht në seksionin VIII të këtij kreu, të emërtuar 'Vepra penale kundër moralit dhe dinjitetit'.

Sikurse shihet nga vendi që zë kjo vepër në strukturën e kodit penal, objekti juridik që merret në mbrojtje në rastet e shkeljes së fshehtësisë së korrespondencës lidhet me mbrojtjen e një të drejte themelore që i përket personit. Objekti grupor i

[501] Dekriptimi është procesi i kundërt i kodimit. Nëpërmjet dekriptimit deshifrohet mesazhi i koduar, duke u përftuar përmbajtja origjinale e mesazhit.

[502] Me "steganografi" kuptojmë shkrimin e fshehtë ku nëpërmjet zbatimit të teknikave steganografike fshehjet ekzistenca e mesazhit. Vetëm personi që dërgon e-mail dhe marrësi i tij janë në dijeni të ekzistencës së tij.

veprave penale që përfshihen në seksionin VIII të kodit ka të bëjë me mbrojtjen e marrëdhënieve juridike penale të vendosura për të siguruar moralin dhe dinjitetin të cilat janë dy cilësi që lidhen domosdoshmërisht me qeniet njerëzore. Për më tepër, sikurse është trajtuar hollësisht edhe në kapitullin e parë të punimit, e drejta për respektimin e fshehtësisë së korrespondencës vlerësohet si një nga drejtimet në të cilat ushtrohet efektivisht e drejta e individit për jetë private. Edhe kjo e drejtë, për nga vetë natyra e saj lidhet me mbrojtjen e interesave të çdo personi për të zhvilluar lirisht dhe pa ndërhyrje marrëdhëniet me njerëz të tjerë. Në rastin kur kemi ndërhyrje të padrejta në korrespondencën zyrtare që mbajnë institucione të ndryshme të administratës publike apo në korrespondencën e mbajtur nga persona juridikë privatë gjatë ushtrimit të aktiviteteve me natyrë profesionale ose tregtare, nuk mund të zbatohet përgjegjësi penale sipas nenit 123.

E drejta për respektimin e fshehtësisë së korrespondencës sikurse ka gjetur sanksionim në kushtetutë dhe në instrumentet ndërkombëtare për mbrojtjen e të drejtave dhe lirive themelore, shtrin mbrojtjen e saj vetëm ndaj korrespondencës të shkëmbyer prej personave fizikë. Edhe në doktrinën tonë penale pranohet se 'fshehtësia e korrespondencës shkelet me anë të veprimeve të ndryshme që shprehen në hapjen e letrave personale e zyrtare, por që i përkasin një personi të caktuar, si shtetas dhe jo si person zyrtar, me hapjen e telegrameve, dëgjimit të bisedave telefonike dhe mjeteve te tjera të komunikimit'.[503]

Korrespondenca zyrtare që mbajnë institucione të ndryshme të administratës publike apo korrespondenca e mbajtur nga persona juridikë privatë gjatë ushtrimit të aktiviteteve me natyrë profesionale ose tregtare, nuk mund të gëzojë mbrojtje të veçantë në bazë të kësaj të drejte. Në rastin kur korrespondenca dërgohet ose merret nga një person juridik nuk kemi implikim të çështjeve që lidhen me të drejtën e personit juridik për privatësi, pasi kjo e drejtë është e lidhur ngushtësisht me pasjen e cilësive humane nga ana e titullarit të saj. Në rast se një person juridik publik ose privat do të ishte subjekt pasiv i ndërhyrjeve të padrejta në korrespondencë, atëherë do të ishim përpara cenimit të interesave të ndryshme legjitime të këtyre subjekteve.

[503] Elezi, I. (1983). "*E Drejta Penale e Republikës Popullore Socialiste të Shqipërisë (pjesa e posaçme)*". Tiranë: Shtypshkronja 'Mihal Duri', fq. 461.

Në një situatë të tillë, mbrojtja juridike e komunikimeve të institucioneve të administratës publike apo subjekteve tregtare nuk do të bazohej në pretendimin për garantimin e privatësisë së kësaj korrespondence më shumë se sa në mbrojtjen e interesave të ligjshme që mund të cenohen nga çdo ndërhyrje e paautorizuar e subjekteve të treta në këto komunikime. Interesat që merren në mbrojtje në rastin e ndëshkimit të ndërhyrjeve në komunikimet e mbajtura nga administrata publike kanë të bëjnë, sipas rastit, me mbrojtjen e informacioneve të klasifikuara sekret shtetëror, mbrojtjen e të dhënave personale që mbahen dhe përpunohen në sistemet kompjuterike të institucioneve përkatëse, garantimin e integritetit të sistemeve kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo të çdo sistemi tjetër kompjuterik, me rëndësi publike, funksionimi i të cilave mund të rrezikohet apo cenohet seriozisht nga sulmet e ndërmarra. Ndërsa, interesat që mbrohen në sajë të garantimit të fshehtësisë së komunikimeve profesionale apo tregtare kanë të bëjnë me mbrojtjen e sekretit tregtar, të dhënave bankare dhe financiare, përmbushjen e detyrimit të sipërmarrësve të rrjeteve të komunikimeve elektronike publike për të garantuar sigurinë dhe cilësinë e shërbimit të ofruar, mbrojtjen nga ndërhyrjet abuzive në të dhënat personale të klientëve të tyre, kur këto të dhëna përpunohen automatikisht etj. Nëse komunikimet zyrtare ose ato me natyrë tregtare mbahen në formë elektronike duke përdorur metodat e ndryshme të komunikimit që ofrojnë shërbimet e shoqërisë së informacionit, atëherë veprimet e paligjshme për përgjimin e tyre mund të dënohen në bazë të nenit të 293/a të kodit penal ‘përgjimi i paligjshëm i të dhënave kompjuterike’, ku thuhet se ‘përgjimi i paligjshëm me mjete teknike i transmetimeve jopublike, i të dhënave kompjuterike nga/ose brenda një sistemi kompjuterik, përfshirë emetimet elektromagnetike nga një sistem kompjuterik, që mbart të dhëna të tilla kompjuterike, dënohet me burgim nga tre deri në shtatë vjet.’ Kjo dispozitë e shtrin mbrojtjen e saj ndaj çdo transmetimi me natyrë jopublike që zhvillohet nëpërmjet një sistemi kompjuterik. Ligjvënësi këtu ka qenë i kujdesshëm dhe jo pa qëllim nuk ka përdorur termin transmetime private. Nëse mbrojtja e ofruar nga dispozita do të shtrihej vetëm ndaj transmetimeve private të të dhënave kompjuterike, do të mbeteshin pa ndëshkuar të gjitha ato veprime të ndërmarra për përgjimin e transmetimeve të tjera kompjuterike që jo domosdoshmërisht kanë natyrë private apo konfidenciale. Kështu p.sh. përgjimi komunikimeve elektronike midis organeve të ndryshme të administratës publike apo

midis tyre dhe strukturave në varësi, apo komunikimeve të subjekteve tregtare private ndërmjet tyre ose me klientët e tyre, që nuk kanë natyrë private nuk do të gjenin mbrojtje të veçantë nëse zbatimi i dispozitës do të lidhej vetëm me transmetimet private të të dhënave kompjuterike.

Shprehja 'transmetime jopublike' ka të bëjë me mënyrën e transmetimit të komunikimeve dhe jo me natyrën e tyre private apo zyrtare. Kjo do të thotë që subjektet komunikuese duhet të kenë zgjedhur një mënyrë komunikimi të përshtatshme për të ndaluar aksesin e paautorizuar të personave të tretë. Kështu p.sh. do të konsiderohet një transmetim me natyrë jopublike, çdo komunikim midis një shoqërie tregtare dhe klientëve të saj që bazohet në përdorimin e fjalëkalimeve për të hyrë në kanalin përkatës të komunikimit apo në kodimin (enkriptimin) e mesazheve të shkëmbyera midis këtyre subjekteve.

Megjithatë, është e rëndësishme të përmendim faktin se rastin kur korrespondenca zyrtare ose tregtare mbahet në trajtë të shkruar, fizike, nuk ka ende një dispozitë të veçantë që do të mbulonte format e ndërhyrjeve të paligjshme në të.

KAPITULLI V: RREGULLIMI I VEÇANTË LIGJOR NË SHQIPËRI PËR MBROJTJEN E TË DHËNAVE PERSONALE NË FUSHËN E KOMUNIKIMEVE ELEKTRONIKE

Kuadri ekzistues legjislativ shqiptar për mbrojtjen e privatësisë në komunikimet elektronike, konsiston me miratimin e ligjit nr. 9918, datë 19.05.2008 për

"Komunikimet elektronike në Republikën e Shqipërisë",[504] në të cilin u inkorporua Direktiva 2002/58/KE e Parlamentit Evropian dhe e Këshillit që vlen "Për përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike", si dhe Direktiva 97/66/KE e Parlamentit Evropian dhe e Këshillit "Për përpunimin e të dhënave personale dhe privatësisë në sektorin e telekomunikacioneve". Ligji u ndryshua me ligjin nr. 102/2012 "Për disa ndryshime dhe shtesa në ligjin nr. 9918", datë 19.5.2008 për "Komunikimet elektronike në Republikën e Shqipërisë"[505] dhe për të forcuar kuadrin institucional në mbrojte të të dhënave personale të komunikimeve elektronike u miratua dhe udhëzimi nr. 14, datë 22.12.2011 për "Përpunimin, mbrojtjen dhe sigurinë e të dhënave personale në sektorin e komunikimit elektronik të publikut" i Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale".[506]

5.1 Ligji nr. 9918, datë 19.05.2008 për "Komunikimet elektronike në Republikën e Shqipërisë", i ndryshuar, qëllimi i rregullimit ligjor dhe fusha e zbatimit të tij

Në nenin 1 të ligjit 9918, datë 19.05.2008 theksohet se qëllimi i ligjit është që nëpërmjet parimit të asnjanësisë teknologjike të promovohet konkurrenca dhe infrastruktura efiçente në komunikimet elektronike dhe të garantohet shërbimi i duhur dhe i përshtatshëm në territorin e Republikës së Shqipërisë.[507] Në përcaktimin e fushës së zbatimit, ligjvënësi nuk ka marrë përsipër të përshkruajë ato forma të komunikimeve elektronike që do të bien në hapësirën rregulluese të ligjit. Në vend të kësaj, janë përcaktuar në mënyrë të qartë ato forma komunikimesh të cilat nuk i nënshtrohen rregullimit të ligjit. Përqasja e ndjekur bazohet në një qëllim praktik për t'i dhënë një shtrirje sa më të gjerë zbatimit të ligjit. Çdo përpjekje për të bërë një përcaktim shterues të sferës së komunikimeve elektronike, që do të gjenin rregullim në bazë të ligjit, mbart rrezikun e mbulimit jo të plotë të formave të shumëllojshme nëpërmjet të cilave mund të

[504] Ligji nr. 9918, datë 19.05.2008 "*Për Komunikimet Elektronike në Republikën e Shqipërisë*".

[505] Ligjin nr. 102/2012 "*Për disa ndryshime dhe shtesa në ligjin nr. 9918*", datë 19.5.2008 "*Për Komunikimet Elektronike në Republikën e Shqipërisë*" i ndryshuar.

[506] Udhëzimi" nr. 14, datë 22.12.2011 "*Për përpunimin, mbrojtjen dhe sigurinë e të dhënave personale në sektorin e komunikimit elektronik të publikut" i Komisionerit Për të Drejtën e Informimit dhe Mbrojtjes së të Dhënave Personale*".

[507] Neni 1 i Ligjit nr. 9918, i ndryshuar.

marrin jetë komunikimet elektronike, duke pasur parasysh në mënyrë të veçantë dinamikën e zhvillimit të teknologjisë së informacionit. Në nenin 2 të ligjit thuhet se 'ky ligj nuk zbatohet për përmbajtjen e shërbimeve të ofruara nëpërmjet rrjeteve të komunikimeve elektronike; për pajisjet e komunikimeve të ndërtuara dhe të përdorura ekskluzivisht për qëllime të mbrojtjes dhe sigurisë kombëtare[508] si dhe për transmetimet radiotelevizive, për sa kohë nuk është përcaktuar ndryshe në legjislacionin në fuqi. Në lidhje me përjashtimin e parë, mund të themi se ligji nuk gjen zbatim mbi përmbajtjen e shërbimeve të ofruara nëpërmjet rrjeteve të komunikimeve elektronike, pasi ky aspekt i komunikimit ka të bëjë me aktivitetin e ushtruar nga pajtimtarët ose përdoruesit e shërbimeve të cilët në varësi të interesave që ndjekin, i japin shërbimit një përmbajtje të caktuar. Ndërkohë, ligji merr përsipër që të rregullojë aktivitetin e operatorëve të rrjeteve dhe ofruesve të shërbimeve elektronike, në mënyrë të tillë, që gjatë ushtrimit të veprimtarisë së tyre, të respektojnë të drejtat dhe interesat e ligjshëm të përdoruesve të shërbimeve, të respektojnë parimet e konkurrencës së ndershme, të garantojnë një infrastrukturë efiçente në komunikimet elektronike si dhe të garantojnë shërbimet e duhura dhe të përshtatshme në lidhje me këto komunikime. Në këtë mënyrë, veprimtaria e ushtruar nga ofruesit e shërbimeve të komunikimeve elektronike, lidhet ngushtësisht me përpunim të dhënash të jashtme të komunikimit, të ndryshme nga përmbajtja e tij të cilat janë të nevojshme për të ofruar shërbimet në fjalë dhe për të garantuar realizimin me efiçencë të tyre. Përjashtimi i pajisjeve të komunikimeve të ndërtuara dhe të përdorura ekskluzivisht për qëllime të mbrojtjes dhe sigurisë kombëtare nga fusha e rregullimit të ligjit, lidhet drejtpërsëdrejti me natyrën e veçantë të komunikimeve që realizohen me anë të tyre. Si rrjedhim, përdorimi i këtyre pajisjeve do të bëhet në përputhje me rregullat përkatëse të brendshme dhe ligjet e posaçme që disiplinojnë veprimtarinë e punës së subjekteve të ngarkuara me detyra të caktuara në fushën e mbrojtjes dhe sigurisë kombëtare. Arsyeja e përjashtimit të transmetimeve radiotelevizive nga fusha e rregullimit të ligjit lidhet me faktin se këto lloj transmetimesh janë të drejtuara ndaj një numri të pakufizuar personash. Në këto rrethana, ato nuk përmbajnë një nga karakteristikat kryesore që shoqëron procesin e komunikimit, atë të kufizimit të numrit të përdoruesve dhe mundësisë së përcaktimit të

[508] Në veçanti pajisje të tilla, si sistemet radio dhe pajisjet fundore të telekomunikacioneve të përdorura prej këtyre shërbimeve.

tyre. Ky interpretim mbështetet plotësisht në shpjegimin e dhënë në ligj mbi konceptin e komunikimit. Sipas ligjit, "komunikim" është shkëmbimi ose transmetimi i informacionit ndërmjet një numri të kufizuar përdoruesish, por që nuk përfshin transmetimin e informacionit që është pjesë e transmetimeve radio-televizive nëpërmjet rrjeteve të komunikimeve elektronike, përveç rasteve kur informacioni mund të ketë të bëjë me një pajtimtar ose përdorues të mirënjohur të cilët marrin këtë informacion.[509]

Nga ky përcaktim, shikojmë se për më tepër, në situata të caktuara të cilat duhen vlerësuar si përjashtim nga rregullimi i përgjithshëm, transmetimet radio-televizive mund të konsiderohen si komunikime në kuptim të ligjit. Këtu bëhet fjalë për rastin kur është e mundur që të identifikohet pajtimtari apo përdoruesi, në drejtim të të cilit transmetohet informacioni siç mund të jetë p.sh. informacioni i transmetuar në kuadër të shërbimit të ofrimit të transmetimeve video sipas kërkesës (video-on-demand service).[510]

5.2 Mbrojtja e të Dhënave dhe e Privatësisë

5.2.1 Ruajtja e fshehtësisë së komunikimeve

Parimi i fshehtësisë së komunikimeve që është një nga hallkat kryesore për mbrojtjen e të dhënave personale dhe privatësisë, parashtron ndaj sipërmarrësve të shërbimeve të komunikimeve publike kërkesën për ruajtjen e fshehtësisë së përmbajtjes së komunikimit prej të gjithë personave të ndryshëm nga bashkë komunikuesit. Detyrimi për ruajtjen e fshehtësisë së komunikimeve zbatohet gjithashtu edhe për të dhënat e trafikut si dhe të dhënat për përpjekjet e pasuksesshme për vendosjen e lidhjes.[511] Për këtë qëllim, ligji ka vendosur mbi sipërmarrësit e shërbimeve detyrimin për të marrë masa ndaj sistemeve të komunikimeve elektronike dhe të përpunimit të të dhënave, për të mbrojtur sekretin e komunikimeve elektronike dhe të të dhënave vetjake

[509] Neni 3, pika 13.

[510] Koment nr. 16 i Direktivës 2002/58/KE.

[511] Gjithashtu, ky parashikim i ligjit është në koherencë të plotë me jurisprudencën e Gjykatës Evropiane të të Drejtave të Njeriut, ku në mënyrë konstante dhe të vazhdueshme është pranuar fakti se fshehtësia e korrespondencës shtrihet edhe në të dhënat e jashtme të komunikimit sikurse janë të dhënat në lidhje me datën, orën kohëzgjatjen e bisedës dhe numrin e thirrur. Shiko: *P.G. dhe J.H. kundër Mbretërisë së Bashkuar, vendim nr. 44787/98, dt. 25.12.2001*.

si dhe për të ndaluar aksesin e paautorizuar në sistemet e komunikimeve elektronike dhe të përpunimit të të dhënave.[512]

Masat që kërkohen të merren, mund të lidhen me aspekte teknike të ndërtimit dhe funksionimit të sistemeve ose me aspekte të organizimit të personelit të përfshirë në administrimin tyre. Nga njëra anë, këto masa mund të bazohen në ndërtimin apo adaptimin e kapaciteteve teknike të nevojshme për të shmangur hyrjet e paautorizuara në sistemet përkatëse të transmetimit apo përpunimit të të dhënave si dhe hyrje të tjera abuzive, që mund të kryhen në tejkalim të autorizimit prej personave që kanë akses në shfrytëzimin e sistemeve. Nga ana tjetër, me rëndësi të veçantë paraqitet edhe hartimi dhe vendosja e kodeve të brendshme të etikës të cilat të përcaktojnë qartë të drejtat dhe detyrat e personelit që kujdeset për mbarëvajtjen e realizimit të shërbimit të komunikimit elektronik publik.

Respektimi i detyrimit, nënkupton ndërtimin nga ana e këtyre subjekteve në fjalë, të mekanizmave të përshtatshëm që garantojnë ruajtjen e natyrës së fshehtë të komunikimit gjatë fazave të ndryshme të transmetimit të tij, nga njëri prej bashkë komunikuesve, tek tjetri. Kuptohet se secili sipërmarrës do të jetë përgjegjës për marrjen e masave mbrojtëse për atë pjesë të procesit të transmetimit të komunikimit që kontrollohet efektivisht prej tij. Gjithashtu duhet të parashikohen në mënyrë të qartë edhe masa të tjera ligjore që vendosin detyrimin për ruajtjen e sekretit profesional mbi punonjësit e sipërmarrësve të shërbimeve.[513] Në nenin 121 pika 4 të ligjit thuhet se "ndalohet marrja, regjistrimi, publikimi dhe përdorimi i të dhënave dhe i mesazheve të transmetuara nga rrjeti i komunikimeve elektronike dhe që nuk janë për publikun si dhe dhënia e tyre personave të paautorizuar, për sa kohë që nuk përcaktohet ndryshe në legjislacionin në fuqi". Një parashikim i tillë, nënkupton qartë se përcaktimet ligjore që ndëshkojnë format klasike të përgjimit të bisedave telefonike duhet të shtrijnë veprimin e tyre edhe ndaj mjeteve të tjera të komunikimit. Në koherencë me këto kërkesa, në ligjin tonë penal janë përfshirë një sërë dispozitash të reja që inkriminojnë forma të ndryshme të ndërhyrjeve abuzive apo përgjimit të të dhënave të transmetuara nëpërmjet

[512] Neni 121/1 i Ligjit nr. 9918, datë 19.05.2008 "*Për Komunikimet elektronike në Republikën e Shqipërisë*" i ndryshuar.

[513] Po aty. Neni 121/2.

rrjeteve të komunikimeve elektronike publike.[514] Këto dispozita marrin në konsideratë më së miri kontekstin e veçantë në të cilin kryhen veprimet e paligjshme dhe garantojnë nivelin e duhur të mbrojtjes në përputhje me veçoritë e veprave në fjalë. Vëmendje e veçantë i është kushtuar ruajtjes së konfidencialitetit të komunikimeve në rastet kur aksesi apo regjistrimi i të dhënave që lidhen me to, është i nevojshëm për të mundësuar ofrimin e shërbimit specifik të komunikimeve publike apo për vërtetimin e faktit që një komunikim i caktuar ka ndodhur realisht.[515] Në këto rrethana, është e mundur që të sigurohet një nivel i caktuar ndërhyrjeje në komunikime, por vetëm në masën që kjo është e nevojshme për realizimin e qëllimit të synuar. Kushti thelbësor që duhet të respektohet është proporcionaliteti midis qëllimit që kërkohet të arrihet dhe mënyrave të ndërhyrjes. Së pari, regjistrimi, ruajtja, transferimi i komunikimeve lejohet kur kjo është e nevojshme për përcjelljen e mesazheve të faksit, të postës elektronike, të sekretarisë telefonike, mesazheve zanore, mesazheve të shkurtra apo për rastet e parashikuara me ligj. Në vijim, kur informacioni apo përmbajtja e komunikimit nuk është më e nevojshme për ofrimin e shërbimit specifik të komunikimeve publike, sipërmarrësit duhet ta fshijnë atë sa më shpejt që të jetë e mundur teknikisht. Së dyti, regjistrimi i komunikimeve dhe i të dhënave shoqëruese të trafikut lejohet me qëllim sigurimin e evidencës së transaksioneve në treg ose të ndonjë komunikimi tjetër biznesi.[516] Në këtë kuptim, regjistrimi mund të kryhet p.sh. në rastin e blerjeve nëpërmjet telefonit apo ndaj telefonatave të kryera nga punonjësit e një shoqërie që ushtron veprimtari të marketingut nëpërmjet komunikimeve telefonike. Regjistrimi i komunikimit në këto raste është plotësisht i justifikuar nga nevoja për vërtetimin e faktit që transaksioni tregtar ka ndodhur dhe sqarimin e rrethanave në të cilat ai ka ndodhur, në mënyrë që të shmangen keqinterpretimet e mëvonshme, me dashje ose jo, mbi këto fakte nga secila prej palëve të përfshira në transaksion. Nga ana tjetër, regjistrimi i komunikimeve të tjera me natyrë biznesi mund të justifikohet me nevojën për matjen e performancës së realizimit të shërbimit. Së treti, lejohet regjistrimi i komunikimeve dhe i të dhënave shoqëruese të

[514] Përveç këtyre dispozitave janë përcaktuar dhe: neni 192/b "*Hyrja e paautorizuar kompjuterike*", neni 293/a "*Përgjimi i paligjshëm i të dhënave kompjuterike*", neni 293/b "*Ndërhyrja në të dhënat kompjuterike*" etj.

[515] Neni 123.

[516] Po aty. Neni 123/5.

trafikut brenda strukturave të ngarkuara me ligj për marrjen e thirrjeve të emergjencës, me qëllim regjistrimin, identifikimin dhe zgjidhjen e tyre. Arsyeja e regjistrimit të komunikimeve nga këto struktura justifikohet nga interesi i tyre primar për të fiksuar të dhëna të caktuara që lidhen me një situatë emergjente (siç mund të jetë p.sh. njoftimi për kryerjen e një vepre penale, për nevojën urgjente për ndihmë mjekësore etj.). Të dhënat e mbledhura nga regjistrimi, ndihmojnë strukturat përkatëse në identifikimin e ngjarjeve të njoftuara dhe në kuptimin sa më të qartë të rrethanave që lidhen me to.[517]

Së fundmi, vlen të theksohet se ndalimi i marrjes, regjistrimit, përdorimit të të dhënave dhe i mesazheve të transmetuara nga rrjeti i komunikimeve elektronike dhe që nuk janë për publikun, nuk zbatohet në rastet kur këto veprime janë të nevojshme për kryerjen e detyrave të tyre, nga ana e agjencive ligj zbatuese.

Në këto rrethana, realizimi i një interesi publik të lidhur me ushtrimin e detyrave nga ana institucioneve shtetërore, prevalon mbi interesin privat të respektimit të fshehtësisë së komunikimeve.[518] Megjithatë, duhet që krahas ekzistencës së rrethanave që parashtrojnë nevojën e ndërhyrjes, veprimet e autoritetit përkatës të jenë të autorizuara nga ligji. Parashikimi me ligj i rasteve se kur një subjekt i tretë, i jashtëm në një komunikim, mund të ketë akses në të dhëna që lidhen me të, shërben si një garanci për shmangien e ndërhyrjeve arbitrare në këtë drejtim duke mos i lënë të tilla çështje në vlerësimin e praktikës administrative e cila shpesh mund të karakterizohet nga fleksibiliteti dhe subjektivizmi.

5.3 Konfigurimet e Fundit Ligjore në Fushën e Sigurisë të Komunikimeve Elektronike

5.3.1 Udhëzimi nr. 14, datë 22.12.2011 "Për përpunimin, mbrojtjen dhe sigurinë e të dhënave personale në sektorin e komunikimit elektronik të publikut"

Udhëzimi nr.14 i datës 22.12.2011 "Për përpunimin, mbrojtjen dhe sigurinë e të dhënave personale në sektorin e komunikimit elektronik të publikut" është miratuar në zbatim të nenit 30 dhe shkronjës *f*, pika 1 e nenit 31 të ligjit nr. 9887, datë 10.03.2008 "Për Mbrojtjen e të Dhënave Personale", nga Komisioneri për të Drejtën e Informimit

[517] Po aty.

[518] Neni 121/4.

dhe Mbrojtjen e të Dhënave Personale. Ky udhëzim zbatohet për qarkullimin dhe vendndodhjen e të dhënave në këto dy subjekte: personat juridik dhe personat fizik si dhe me të dhënat e nevojshme lidhur me identifikimin e abonentit apo përdoruesit të regjistruar. Ky udhëzim nuk zbatohet për përmbajtjen e komunikimeve elektronike.[519] Udhëzimi ka si qëllim sigurimin e një niveli të barasvlershëm për mbrojtjen e të drejtave dhe lirive themelore dhe në veçanti të drejtën për privatësi, duke marrë parasysh përpunimin e të dhënave personale në sektorin e komunikimit elektronik dhe për të garantuar lëvizjen e lirë të të dhënave dhe të pajisjeve të shërbimeve të komunikimit elektronik në vend.[520]

Kontrolluesit që marrin të dhëna personale nga një subjekt i të dhënave deklarojnë qartë që kanë për të përmbushur një ose më shumë qëllime specifike të ligjshme. Mbledhja e të dhënave në mënyrë rutinë dhe pa dallim është e kundërligjshme.[521] Parimet e mbrojtjes së të dhënave përcaktojnë se ofruesit e shërbimeve sigurojnë që në dispozicion të komunikimit elektronik publik, zbatohen parimet e sigurisë për sa i përket të dhënave që duhen ruajtur si më poshtë: a) të dhënat e mbajtura të jenë të cilësisë së njëjtë me ato të të dhënave në rrjet dhe subjektet gëzojnë të njëjtën siguri dhe mbrojtje të të dhënave të tyre; b) të dhënat të jenë subjekt i masave të duhura teknike dhe organizative për mbrojtjen e tyre kundër shkatërrimit aksidental ose të paligjshëm, humbjes aksidentale, të magazinimit të paautorizuar apo përpunimit, përdorimit dhe zbulimit të paligjshëm; c) të dhënat të jenë subjekt i masave të duhura teknike dhe organizative për të siguruar që ato të mund të aksesohen vetëm nga personeli i autorizuar; dhe d) të dhënat, përveç atyre që janë në disponim dhe ruhen, të shkatërrohen në fund të periudhës së ruajtjes.[522] Për sa i përket konfidencialitetit të komunikimeve, Kontrolluesit garantojnë konfidencialitetin e komunikimeve dhe të dhënave qarkulluese që kanë të bëjnë me të, sipas qëllimit të një rrjeti të komunikimit publik dhe shërbimit të komunikimit elektronik publikisht të disponueshëm, sipas legjislacionit kombëtar. Kontrolluesit ndalojnë dëgjimin, shtypjen, magazinimin ose lloje të tjera përgjimi ose mbikëqyrje të komunikimeve dhe të dhënat qarkulluese në

[519] Neni 1 i Udhëzimit nr.14 të datës 22.12.2011.

[520] Neni 2 i Udhëzimit nr.14.

[521] Neni 3 i Udhëzimit nr.14.

[522] Neni 6 i Udhëzimit nr.14.

fjalë nga persona të ndryshëm nga përdoruesit, pa dhënien e pëlqimit të përdoruesve të interesuar, përveç kur janë ligjërisht të autorizuar për të vepruar kështu.[523] Ofruesit e shërbimeve për sigurinë dhe informimin për sigurinë marrin masat e duhura për të mbrojtur sigurinë e shërbimeve të tyre, nëse është e nevojshme në bashkëpunim me ofruesin e rrjetit dhe informojnë abonentët për ndonjë rrezik të veçantë të thyerjes së sigurisë së rrjetit. Ata që ofrojnë në dispozicion të publikut shërbimet e komunikimit elektronik në Internet, informojnë përdoruesit dhe abonentët për masat që duhet të marrin për të mbrojtur sigurinë e tyre të komunikimit për shembull duke përdorur lloje të veçanta të programeve, antiviruseve apo ndonjë mjet tjetër mbrojtës. Kërkesa për të informuar abonentët për rreziqet e sigurisë së veçantë nuk e shkarkon një ofrues të shërbimit nga detyrimi për të marrë me shpenzimet e veta, masat e nevojshme dhe të menjëhershme për të përmirësuar çdo rrezik të ri e të paparashikuar të sigurisë dhe të rivendosin nivelin normal të sigurisë së shërbimit.[524]

Për ruajtjen e të dhënave,[525] Kontrolluesit duhet të jenë të qartë në lidhje me periudhën e kohës për të cilat të dhënat personale mbahen dhe arsyet përse informacioni është duke u mbajtur. Nëse qëllimi për të cilin merren të dhënat ka pushuar dhe informacioni personal nuk është më i nevojshëm, të dhënat fshihen ose tjetërsohen në një mënyrë të sigurt. Të dhënat anonimizohen për të hequr çdo të dhënë personale. Në mënyrë që të përputhet me këtë kërkesë ligjore, kontrolluesit e të dhënave caktojnë përgjegjësi specifike dhe vendosin procedurat për të siguruar që dosjet të zbrazen rregullisht dhe se të dhënat personale nuk janë mbajtur më gjatë se sa ka qenë e nevojshme.

Orientimet në lidhje me shërbimin e Komunikimit Elektronik të Publikut kanë të bëjnë vetëm për të dhënat e krijuara ose të përpunuara si pasojë e një komunikimi ose një shërbimi komunikimi dhe nuk kanë të bëjnë me të dhënat që ka përmbajtja e informacionit të komunikuar. Së fundmi, për numëratorin e abonentëve,[526] kontrolluesi duhet të sigurojnë që abonentët të jenë të informuar, pa pagesë dhe para se ata të jenë përfshirë në numëratorë, në lidhje me qëllimin e një numëratori të shtypur apo

[523] Neni 8 i Udhëzimit nr.14.

[524] Neni 9 i Udhëzimit nr.14.

[525] Neni 10 i Udhëzimit nr.14.

[526] Neni 11 i Udhëzimit nr.14.

elektronik të abonentëve, në dispozicion të publikut në të cilin përfshihen të dhënat e tyre personale dhe në çdo mundësi të mëtejshme të shfrytëzimit bazuar në funksionet e kërkimit të përfshira në versionet elektronike të numëratorit. Kontrolluesit, sigurojnë që abonentëve i është dhënë mundësia për të përcaktuar nëse të dhënat e tyre personale janë të përfshira në një numërator publik dhe nëse po, masën për të cilat të dhëna të tilla janë relevante për qëllimin e numëratorit të përcaktuar nga dhënësi i numëratorit dhe për të verifikuar, korrigjuar ose për të tërhequr të dhëna të tilla. Me anë të këtij udhëzimi, Komisioneri përcakton përgjegjësit në zbatim të udhëzimit që janë të gjithë kontrolluesit publikë e privatë në territorin e Republikës së Shqipërisë. Moszbatimi i kërkesave të këtij udhëzimi, përbën shkelje të ligjit për mbrojtjen e të dhënave personale dhe dënohet sipas nenit 39 të tij.[527]

5.3.2 Udhëzimi nr. 40, datë 13.06.2014 "Për përdorimin e shërbimit të internetit dhe postës elektronike zyrtare në institucionet publike në kuadër të mbrojtjes së të dhënave personale"

Udhëzimi nr. 40 i datës 13.06.2014 "Për përdorimin e shërbimit të internetit dhe postës elektronike zyrtare në institucionet publike në kuadër të mbrojtjes së të dhënave personale" është mbështetur në shkronjën "c" të pikës 1 të nenit 30 të ligjit nr. 9887, datë 10.03.2008 "Për mbrojtjen e të dhënave personale", i ndryshuar e miratuar nga Komisioneri për të Drejtë e Informimit dhe Mbrojtjen e të Dhënave Personale. Ky është një nga konfigurimet e fundit ligjore, për sa i përket mbrojtjes së të dhënave personale në komunikimet elektronike. Qëllimi i këtij Udhëzimi është përcaktimi i rregullave të detyrueshme për zbatim nga institucionet publike dhe strukturat përkatëse të cilat administrojnë sistemet e informacionit gjatë përdorimit të internetit dhe postës elektronike në vendin e punës nga ana e punonjësve.[528] Ky Udhëzim i Komisionerit në përputhje me ligjin për mbrojtjen e të dhënave personale dhe qëllimin e këtij udhëzimi, përpiqet që të shpjegojë disa terma të specifikuar teknik, duke i dhënë kuptimin e duhur.[529] Në këtë Udhëzim përcaktohet se punonjësit duhet të përdorin postën elektronike dhe shërbimin e internetit të institucionit vetëm me qëllim të

[527] Neni 12 i Udhëzimit nr.14.

[528] Pika 1 e Udhëzimit nr. 40, dt. 13.06.2014.

[529] Pika 2 e Udhëzimit nr. 40.

përmbushjes së detyrave të ngarkuara nga punëdhënësit dhe se punonjësit duhet të informohen qartë nga institucioni publik, nëpërmjet politikës së privatësisë mbi aksesin e lejuar në internet. Politika e privatësisë përditësohet në përputhje me opinionet e publikuara nga Komisioneri.[530]

Gjithashtu punonjësit informohen qartë nga institucioni publik në të cilin ata ushtrojnë marrëdhënien e tyre të punës, nëpërmjet politikës së privatësisë mbi aksesin e lejuar në internet. Politika e privatësisë përditësohet në përputhje me opinionet e publikuara nga Komisioneri. Strukturat përkatëse, në përputhje me legjislacionin për mbrojtjen e të dhënave personale, nuk monitorojnë të dhënat personale të punonjësve gjatë përdorimit të internetit në vendin e punës me përjashtim të rasteve të urdhëruara me shkrim nga titullari i institucionit. Urdhri për të kryer monitorimin, i cili u bëhet i ditur punonjësve paraprakisht, duhet të përcaktojë qartë qëllimin specifik për kryerjen e këtij veprimi.[531]

Aksesi në e-mail-et e brendshme të punonjësve, të cilët nuk janë të pranishëm përkohësisht në vendin e punës, duhet të bëhet vetëm në rast të një domosdoshmërie absolute dhe pasi të jetë informuar punonjësi në fjalë. Në çdo rast, aksesi autorizohet nga eprori i drejtpërdrejtë dhe kjo procedurë duhet të dokumentohet.

Pas largimit të punëmarrësit nga puna, punëdhënësi duhet të lajmërojë punëmarrësin përpara se t'i çaktivizohet adresa elektronike, në mënyrë që ai të fshijë të dhënat personale të tij, që mund të ketë mbajtur në këtë adresë, të cilat nuk cenojnë marrëdhënien me punëdhënësin apo t'i marrë ato me mjetet e duhura në prezencë të strukturës përkatëse.[532] Udhëzimi i mësipërm është i detyrueshëm për zbatim nga çdo institucion publik dhe strukturë përkatëse pranë tij, të cilët administrojnë serverat dhe kanë akses në sistemet e informacionit[533] dhe moszbatimi i detyrimeve të këtij udhëzimi nga institucioni publik, përbën shkelje të ligjit "Për mbrojtjen e të dhënave personale" dhe dënohet sipas nenit 39 të tij.

[530] Pika 4 e Udhëzimit nr. 40.

[531] Pika 6 e Udhëzimit nr. 40.

[532] Pika 9 e Udhëzimit nr. 40.

[533] Pika 12 e Udhëzimit nr. 40.

Në Shqipëri, kuadri rregullator i çështjeve që lidhen me përdorimin e shërbimit të internetit dhe postës elektronike mbetet jo i plotë, pasi problemi ende nuk ka gjetur rregullim në sektorin privat të punësimit.

5.4 Autoritetet Rregullative

Në ligjin nr. 9918, datë 19.05.2008 "Për komunikimet elektronike në Republikën e Shqipërisë" përcaktohen përgjegjësitë e tre Autoriteteve të përfshirë në mbrojtjen e të dhënave personale në sektorin e komunikimeve elektronike. Këto autoritete janë: Ministri, Autoriteti i Komunikimeve Elektronike dhe Postare (AKEP) dhe Autoriteti i Mediave Audiovizive (AMA).[534] Nëpërmjet ligjit. nr. 9918/2008 kërkohet që të kryet një detyrë e vështirë për të qartësuar dhe të koordinuar kompetencat e autoriteteve të Pavarura Administrative për mbrojtjen më të mirë të të drejtave të abonentëve/shfrytëzuesve të shërbimeve të komunikimeve elektronike.

5.4.1 Ministri

Ministri përgjegjës si një autoritet i administrativ i pavarur, në zbatim të ligjit nr. 9918/2008, ka këto kompetenca të përcaktuara ku harton dhe paraqet në Këshillin e Ministrave propozimet për politikën e sektorit të komunikimeve elektronike. Ndjek zbatimin e politikës së Qeverisë të Republikës së Shqipërisë në sektorin e komunikimeve elektronike. Harton projekt aktet ligjore e nënligjore për zhvillimin e sektorit të komunikimeve elektronike. Ai mund të nxjerrë urdhra dhe udhëzime për të plotësuar kuadrin rregullator, të përcaktuar nga ky ligj dhe politikat e Qeverisë për sektorin e komunikimeve elektronike.

Përfaqëson Republikën e Shqipërisë në organizmat ndërkombëtarë në fushën e komunikimeve elektronike. Harton dhe nënshkruan në emër të Republikës së Shqipërisë, marrëveshje ndërkombëtare, dypalëshe dhe shumëpalëshe, në fushën e komunikimeve elektronike. Ai ndjek zbatimin e detyrimeve për fushën e komunikimeve elektronike që rrjedhin nga traktatet ndërkombëtare, ku aderon Republika e Shqipërisë. Kërkon dhe përpunon të dhënat statistikore nga sipërmarrësit që kryejnë veprimtari në fushën e komunikimeve elektronike. Bashkëpunon me Ministrinë e Mbrojtjes, Ministrinë e Brendshme dhe Shërbimin Informativ të Shtetit për çështje të fushës së

[534] Neni 4 i Ligjit nr. 9918/2008 "*Për komunikimet elektronike në Republikën e Shqipërisë*".

komunikimeve elektronike që kanë të bëjnë me mbrojtjen dhe sigurinë kombëtare. Harton Planin Kombëtar të Frekuencave dhe punon për harmonizimin e këtij plani me politikat ndërkombëtare të zhvillimit të spektrit të frekuencave. Miraton kufizimet e mundshme për dhënien e frekuencave dhe procedurat përkatëse të tenderimit për dhënien e tyre, bazuar në propozimet e AKEP-it. Miraton ofruesin e shërbimit universal dhe procedurat përkatëse për zgjedhjen e ofruesit/ofruesve të shërbimit universal, bazuar në propozimet e AKEP-it. Bashkërendon shërbimet kombëtare të radiondërlidhjes bregdetare si dhe mbështet veprimtarinë e radioamatorizmit në Republikën e Shqipërisë.[535]

5.4.2 Autoriteti i komunikimeve elektronike dhe postare (AKEP)

Një ndër autoritetet e pavarur më të rëndësishëm të ligjit nr. 9918, datë 19.05.2008 është Autoriteti i Komunikimeve Elektronike dhe Postare, i cili është organi rregullator në fushën e komunikimeve elektronike dhe të shërbimit postar i cili mbikëqyr kuadrin rregullator të përcaktuar nga ky ligj, nga ligji për shërbimin postar dhe nga politikat e zhvillimit të përcaktuara nga Këshilli i Ministrave si dhe është garant i mbrojtjes së të dhënave personale dhe privatësisë.[536] AKEP-i ushtron funksionet në përputhje me këtë ligj dhe me aktet e tjera ligjore si dhe në përputhje me politikat sektoriale kombëtare të zhvillimit të komunikimeve elektronike dhe me marrëveshjet ndërkombëtare në fushën e komunikimeve elektronike ku Republika e Shqipërisë është palë. Rregullimi në fushën e komunikimeve elektronike duhet të respektojë parimin e paanshmërisë teknologjike. Teknologjitë dhe shërbimet e reja si edhe tregjet e sapokrijuara do të jenë subjekt i rregullimit, sipas këtij ligji, deri në masën e nevojshme për të parandaluar deformimet e konkurrencës dhe për të arritur objektivat e këtij ligji. AKEP-i nxit konkurrencën efiçente për sigurimin e rrjeteve dhe të shërbimeve të komunikimeve elektronike, facilitetet shoqëruese dhe shërbimet e tjera. Një ndër objektivat rregullatorë të AKEP është mbrojtja e interesave të përdoruesve të shërbimeve të komunikimeve elektronike, për të mbrojtur të dhënat personale dhe privatësinë e përdoruesve.[537]

[535] Neni 5 i Ligjit nr. 9918.

[536] Neni 6/1 i Ligjit nr. 9918.

[537] Neni 7, shkronja “b” e Ligjit nr. 9918.

Pra, në raste të evidentimit të shkeljeve të të dhënave personale, ushtrohet kontrollit nga Autoriteti i Komunikimeve Elektronike dhe Postare (AKEP) si organizmi kryesor monitorues në fushën e komunikimeve elektronike.

Kompetencat e AKEP janë të shumta në fushën e komunikimeve elektronike dhe më të rëndësishmet janë:

- Ai mbikëqyr, kontrollon dhe monitoron veprimtaritë e sipërmarrësve të rrjeteve të komunikimeve elektronike dhe të shërbimeve të komunikimeve elektronike, në përputhje me këtë ligj dhe aktet e tjera në zbatim të këtij ligji;
- rregullon aksesin dhe interkoneksionin midis rrjeteve të komunikimeve elektronike, në përputhje me përcaktimet e këtij ligji, akteve nënligjore në zbatim të tij, si dhe siguron që sipërmarrësit të mos diskriminohen dhe të kenë mundësi të barabarta, kushte transparente, objektive dhe të ndershme;
- kryen regjistrimin e sipërmarrësve të rrjeteve të komunikimeve elektronike dhe ofruesve të shërbimeve të komunikimeve elektronike në përfundim të procesit të njoftimit;
- cakton numrat dhe seritë numerike të sipërmarrësve të rrjeteve të komunikimeve elektronike publike dhe të shërbimeve të komunikimeve elektronike;
- zgjidh mosmarrëveshjet ndërmjet sipërmarrësve të rrjeteve të komunikimeve elektronike dhe shërbimeve të komunikimeve elektronike, sipas parashikimeve të këtij ligji;
- krijon, mirëmban dhe përditëson bazën e të dhënave elektronike për sektorin e komunikimeve elektronike dhe siguron që këto të dhëna, në formë informacioni, t'i bëhen të vlefshme publikut, në përputhje me rregullat për informimin publik dhe të ruajtjes së konfidencialitetit;
- mbledh të dhëna dhe informacion nga sipërmarrësit e rrjeteve dhe shërbimeve të komunikimeve elektronike;
- merr masat, që sipërmarrësit e rrjeteve të komunikimeve elektronike dhe të shërbimeve të komunikimeve elektronike të zbatojnë detyrimet, që kanë të bëjnë me mbrojtjen e interesave të vendit, të sigurisë publike edhe në rast lufte apo gjendje të jashtëzakonshme etj..[538]

[538] Neni 8 i Ligjit nr. 9918.

5.4.3 Autoriteti i Mediave Audiovizive (AMA)

Autoriteti i Mediave Audiovizive rregullon median elektronike në Republikën e Shqipërisë. AMA nisi të funksionojë si autoritet pas miratimit të vendimit nr.545, datë 11.08.2011, të Këshillit të Ministrave, ku ndryshoi dhe zëvendësoi, "Këshillin Kombëtar të Radios dhe Televizionit" (KKRT) me "Autoritetin i Mediave Audiovizive" (AMA).[539]

Ligji nr. 97/2013 "Për Mediat Audiovizive në Republikën e Shqipërisë", parashikon mënyrën e organizimit dhe funksionimit të AMA-s. AMA është person juiridik publik, i pavarur me autoritet rregullator në fushën e shërbimeve të transmetimeve audio dhe audiovizive dhe shërbimeve të tjera mbështetëse në territorin e Republikës së Shqipërisë.[540] Pavarësia në ushtrimin e funksioneve të saj është një parim i rëndësishëm që sigurohet nëpërmjet disa dispozitave të këtij ligji. Nga ana tjetër, ligji parashikon në mënyrë të shprehur papajtueshmëritë e anëtarëve të AMA-s të cilat tentojnë të garantojnë pavarësinë e tyre nga politika dhe bota e biznesit.[541] AMA përbëhet nga Kryetari, Zëvendëskryetari dhe 5 anëtarë.[542]

Funksionet kryesore të AMA-s janë:[543] shqyrtimi i propozimeve dhe aplikimeve për ushtrimin e shërbimeve të transmetimit, përfshirë aplikimet për transmetime

---

[539] Pika "a" e VKM nr.545, dt.11.08.2011 të ndryshuar.

[540] Neni 6, pika1 dhe 2 e ligjit nr. 97/2013 "Për Mediat Audiovizive në Republikën e Shqipërisë".

[541] Anëtarë të AMA-s nuk mund të jenë individët që:

a) janë anëtarë të partive dhe shoqatave politike, kandidojnë për deputet apo janë zgjedhur të tillë gjatë 2 legjislaturave të fundit, kanë konkurruar për kryetar të njësive vendore në zgjedhjet e fundit të organizuara për to apo kanë ushtruar detyrën e kryetarit të bashkisë, anëtarit të Këshillit të Ministrave apo të prefektit gjatë 3 vjetëve të fundit, si dhe ata që janë anëtarë të Këshillit të Ankesave, AKEP-it apo punonjës të këtij të fundit;

b) janë persona të lidhur, sipas përcaktimeve të ligjit nr. 9367, datë 7.4.2005 "*Për parandalimin e konfliktit të interesave në ushtrimin e funksioneve publike*" ose që kanë në pronësi pjesë kapitali apo aksione të shoqërive tregtare, si dhe të drejta të tjera në fushën e transmetimeve audiovizive, reklamës, prodhimeve të përmbajtjes së transmetimeve audiovizive, rrjeteve të komunikimit elektronik apo persona të punësuar gjatë vitit të fundit, anëtarë të organeve drejtuese apo këshilluese të këtyre subjekteve apo të lidhur me ndonjë licencë me këto subjekte.

[542] Neni 8, pika 1 e ligjit nr. 97/2013 "*Për Mediat Audiovizive në Republikën e Shqipërisë*".

[543] Neni 19, pika 1 e ligjit nr. 97/2013.

numerike dhe dhënia e autorizimeve ose licencave përkatëse, në përputhje me këtë ligj, përfshirë shërbimet e ofruara nga RTSH-ja;[544] lëshon dhe heq licencat dhe/ose autorizimet me shumicë të cilësuar dhe garantimi i konkurrencës së ndershme, duke siguruar njëkohësisht zhvillimin e mëtejshëm të RTSH-së;[545] AMA kërkon nga administrata shtetërore, gjykatat, bankat dhe organizma të tjerë përkatës, si dhe nga titullarët e subjekteve të licencuar informacione, që i gjykon të nevojshme për të kontrolluar vërtetësinë e të dhënave të paraqitura nga aplikuesit. Këto të dhëna përdoren vetëm për zbatimin e detyrave të ngarkuara nga ky ligj. Përhapja dhe botimi i tyre nuk lejohet në mbrojtje të kuadrit të të dhënave personale dhe privatësisë[546] etj..

Për sa i përket mbrojtjes së të dhënave personale dhe mbrojtjes së privatësisë AMA si autoritet nuk ka asnjë kompetencë të përcaktuar ligjore në lidhje me kontrollin e subjekteve ligjore të licensuara prej saj, në mbrojtje të kuadrit ligjor të të dhënave personale dhe privatësisë.

Organi i cili është ngarkuar nga ligji për shqyrtimin e ankesave është Këshilli i Ankesave, i cili caktohet nga AMA me shumicë të cilësuar dhe përbëhet nga kryetari dhe 2 anëtarë, specialistë të fushës së medias, të cilët emërohen për një periudhë 3-vjeçare, me të drejtë riemërimi jo më shumë se një herë.[547] Objekti i punës së Këshillit të Ankesave është mbikëqyrja e zbatimit të kodit dhe rregulloreve të miratuara nga AMA, që kanë të bëjnë sidomos me respektimin e dinjitetit e të drejtave të tjera themelore të njeriut, në mënyrë të veçantë mbrojtjen e të miturve, të drejtës për informacion dhe sensibilizimit të opinionit publik, lidhur me respektimin e normave morale dhe etike në programet e ofruesve të shërbimeve audiovizive.[548]

Për realizimin në mënyrë të plotë të funksioneve të saj, AMA ka këto kompetenca:[549]

a) lëshon licenca dhe/ose autorizime;
b) u kërkon mbajtësve të licencave dhe/ose autorizimeve realizimin e detyrimeve financiare ndaj AMA-s;
c) siguron zbatimin e kushteve të licencave dhe/ose autorizimeve të lëshuara prej

[544] Po aty. Shkronja “a”.

[545] Po aty. Shkronja “b” dhe “c”.

[546] Po aty. Pika 7.

[547] Neni 20, pika 1 e ligjit nr. 97/2013.

[548] Po aty. Pika 2.

[549] Neni 23 ligjit nr. 97/2013.

saj;

ç) ndërmerr, mbështet apo autorizon studime.

AMA, për realizimin e funksionimit të saj, administron fondet e veta sipas legjislacionit në fuqi. Gjithashtu në ligj është parashikuar dhe raportimi i AMA në Kuvend, i cili bëhet, jo më vonë se data 31 mars i çdo viti, për mënyrën e përmbushjes së funksioneve dhe veprimtarive të veta për vitin paraardhës, përfshirë raportimin për realizimin e planit financiar.[550] Raporti vjetor duhet të përfshijë informacion mbi zhvillimin e transmetimeve në drejtim të personave me nevoja të veçanta shqisore dhe veçanërisht zhvillimin e arritur për qëllimet e përcaktuara në rregulloren e transmetimit.[551]

[550] Neni 28, pika 1 e ligjit nr. 97/2013.

[551] Po aty.Pika 2.

KAPITULLI VI: KONKLUZIONET DHE REKOMANDIMET

6.1 Kufijtë e rinj të privatësisë

Përpjekjet në nivel global për mbrojtjen e të dhënave personale dhe privatësisë nga rritja e rrezikut të zhvillimit të shpejtë të teknologjive të informacionit është e pamohueshme. Instrumentet legjislative në nivel ndërkombëtar dhe kombëtar dëshmojnë përpjekjen që kushtëzon mbrojtjen e të dhënave personale dhe privatësisë si të drejta të njeriut dhe reduktimin e tyre, në të mira të mbrojtura me kushtetutë. A janë vendosur përfundimisht kufijtë e mbrojtjes të privatësisë? Teoria e Brandeis dhe Warren për të drejtën që dikush të jetojë i vetmuar (to be let alone),[552] e kuptueshme për kushtet e shekullit të 19-të, duket se nuk ka asnjë vend sot. Ne jetojmë në epokën e aksesit ku qasja në shërbime e rrjete dhe pjesëmarrja në një seri aktivitetesh transferohet në hapësira kibernetike dhe rrjete kompjuterike.[553]

Koncepti i jetës private ka ndryshuar përgjithmonë. Shoqëria u bë globalizuar dhe komplekse. Është e pamundur pjesëmarrja jonë në këtë detyrë të lirë, në një numër organesh me shumë të dhëna personale dhe respektivisht pa qasjen tonë në informacionet e të tjerëve.[554] Shpërndarja e informacionit në të gjitha fushat ku personi përfshihet edhe nëse janë agjenci qeveritare ose rrethe miqësore dhe fisnore, ka marrë përmasa të tilla ku tani është e qartë se njerëzit e duan dhe dhënia e pëlqimit për të ndarë informacionin rreth tyre është shumë më e lehtë sesa në të kaluarën.[555] Pra, kush është i shqetësuar për mbrojtjen e të dhënave personale dhe privatësisë? Përfundimisht, më të shumtit nga ne, pranojnë kufizimin e të drejtave tona që të mos qëndrojmë jashtë zakoneve që tashmë janë aktivitete të zakonshme sociale. Pranojmë kufizimet e të drejtës tonë për mbrojtjen e jetës private në një mjedis frike, të përgjithësuar nga ndërkombëtarizimi i terrorizmit dhe format e tjera të krimit. Ekziston privatësia në njërën anë dhe siguria, pjesëmarrja në shoqërinë e informacionit nga ana tjetër. Balanca

[552] Warren, S. D. Brandeis, L. D. (1890). "*The Right to privacy*", Harvard Law Review.

[553] Rifkin, J. (2001). "*The Age of Access: How the Shift from Ownership to Access is Transforming Modern Life*", fq. 221.

[554] Mendel, T., Puddephatt, A., Wagner, B. (2012). "*Global Survey on Internet Privacy and Freedom of Expression*", fq.102.

[555] Lessig, L. (2013). "*Remix: Making Art and Commerce Thrive in the Hybrid Economy*", fq.181.

do të vijë vetëm përmes një kuadri institucional të sofistikuar që mund të përshtatet me zhvillimet teknologjike dhe zakonet shoqërore si dhe zhvillimet e tjera të mëtejshme. Në vitin 2000, Scott McNeally, zyrtar administrativ në kompaninë Sun Microsystems, në një deklaratë për mbrojtjen e të dhënave personale në mjedisin e korporatave, shkaktoi reagime të shumta. Ai tha se: "Tashmë ju nuk keni privatësi – Kapërcejeni atë!" (You already have zero Privacy - Get over it!).[556] Këtë pikëpamje pesimiste duket se e refuzon Peter Hustinx, ish Mbikëqyrësi Evropian për Mbrojtjen e të Dhënave Personale. Në një takim të veçantë me specialistë të fushës, të organizuar më 10 Tetor 2007 nga kompania Google për privatësinë në internet, ai tha se nuk është dakord me këtë pikëpamje pesimiste dhe se legjislacioni në kombinim me teknologjinë dhe edukimin e përdoruesve të internetit do të na lejojë që të përballemi në mënyrë adekuate me rreziqet që lidhen me përdorimin e tij.[557]

6.2 Kuadri rregullator ndërkombëtar, evropian dhe kombëtar

Edhe pse ka dallime në perceptimin për sa i përket koncepteve dhe fushës së mbrojtjes të privatësisë dhe të dhënave personale në nivel ndërkombëtar, evidentohen përpjekje serioze për mbrojtjen e të dhënave personale dhe privatësisë në nivel ndërkombëtar dhe komunitar. Në nenin 12 të Deklaratës Universale të të Drejtave të Njeriut të OKB-së dhe në nenin 17 të Paktit për të Drejtat Civile dhe Politike si dhe Rekomandimin e Organizatës për Bashkëpunim dhe Zhvillim Ekonomik, të vitit 1980 për "Parimet e mbrojtjes së privatësisë së individit dhe flukset ndërkufitare të të dhënave personale", mbrojtja e privatësisë ishte si një kusht për gëzimin e të drejtave themelore të njeriut. Në Evropë, u hartua dhe u nënshkrua nga shtetet evropiane "Konventa Evropiane për të Drejtat e Njeriut" (KEDNJ) e cila është një tekst parimesh që përbën bazën për zhvillimin e të drejtës të mbrojtjes së të dhënave personale. Ndoqën më pas, së pari, të ashtuquajturit Legjislacioni evropian i "gjeneratës së parë" si ai gjerman "Ligji i Hesse" dhe ai francez "Ligji 78-17", në vazhdim legjislacioni evropian i "gjeneratës së dytë" me krijimin e "Marrëveshjes Shengen" dhe legjislacioni evropian i

[556] Dowding, M. (2011). "*Privacy: Defending an Illusion*", fq.23.

[557] Hustinx, P. (2007). "*Online Privacy: Reconsidering Policy Options for the Digital Age*" , takim i organizuar me speialistë të fushës nga Kompania Google.

“gjeneratës së tretë”, të tilla si Karta e të Drejtave Themelore të Njeriut të Bashkimit Evropian, Direktiva 95/46/KE e “Rekomandimi Nr R (99), Direktiva 97/66/KE dhe Direktiva 2002/58/KE e cila u amendua nga Direktiva 2009/136/KE dhe Direktiva 2006/24/KE.

Në Shqipëri, korniza legjislative që parapriu detyrimin për të transpozuar Direktivën 2002/58/KE e amenduar me Direktivën 2006/24/KE të Parlamentit Europian dhe të Këshillit, datë 15 mars 2006, “Për ruajtjen e të dhënave të krijuara ose të përpunuara lidhur me ofrimin e shërbimeve të komunikimeve elektronike të disponueshme për publikun ose të rrjeteve të komunikimit publik” me ligjin nr.102/2012 “Për disa ndryshime dhe shtesa” në ligjin nr. 9918, datë 19.5.2008 “Për komunikimet elektronike në Republikën e Shqipërisë” ishte tashmë një kornizë që rregullonte kryesisht çështjet e mbrojtjes së konfidencialitetit të komunikimeve elektronike. Më pas, rregullimet vijuan me Udhëzimin e Komisionerit nr. 14, datë 22.12.2011 “Për përpunimin, mbrojtjen dhe sigurinë e të dhënave personale në sektorin e komunikimit elektronik të publikut” dhe me Udhëzimin e Komisionerit nr. 40, datë 13.06.2014 “Për përdorimin e shërbimit të internetit dhe postës elektronike zyrtare në institucionet publike në kuadër të mbrojtjes së të dhënave personale”. Shteti shqiptar, duke transferuar Direktivën Evropiane 2002/58/KE në ligjin kombëtar ka arritur të krijojë një kornizë institucionale për të siguruar në mënyrë adekuate të drejtat e qytetarëve për jetën private dhe të dhënat personale me gjithë problematikat e hasura, por ka ende për t’u bërë në këtë aspket.

6.2.1 Konstatime dhe Rekomandime në lidhje me ligjin nr. 9887, datë 10.03.2008 “Për mbrojtjen e të dhënave personale” i ndryshuar.

1. Përcaktimi i proçedurave dhe kushteve që duhet të plotësohen për të pasur një akses të ligjshëm tek të dhënat personale

-Është shumë e rëndësishme që gjatë trajtimit të të dhënave të trafikut të komunikimeve dhe të vendndodhjes nga ana e organeve kompetente, të jenë të përcaktuara qartë në ligj, proçedurat që duhet të ndiqen dhe kushtet që duhet të plotësohen në mënyrë që aksesi në të dhënat e ruajtura të jetë në përputhje me kërkesat e domosdoshmërisë së

ndërhyrjes në të dhënat personale dhe proporcionalitetit të interesit të përgjithshëm që synohet të arrihet me mjetin e përdorur.

2. Rishikimi i ligjit për të arritur një mbrojtje më të mirë të të dhënave personale në përputhje me standartet ndërkombëtare

-Është e nevojshme të shikohet mundësia e një rishikimi të ligjit në mënyrë që të arrihet një përqasje e cila garanton më së miri të drejtën e individit për jetë private dhe për mbrojtjen e të dhënave personale në përputhje me standardet e vendosura në instrumentat ndërkombëtare dhe ligjet e brendshme që mbrojnë posaçërisht këto të drejta.

-Ajo që duhet thënë është se në amendamentet e mëtejshme të këtij ligji do të ishte e domosdoshme zgjerimi i përkufizimit të shumë termave të fushës së mbrojtjes së të dhënave personale, pasi është fushë e re e pa lëvruar asnjëherë më parë.

3. Të drejtat e subjektit të të dhënave

-E drejta për akses, ushtrohet në përputhje me parimet kushtetuese të lirisë së shprehjes dhe informacionit, lirisë së shtypit dhe sekretit profesional dhe mund të kufizohet nëse cenon interesat e sigurisë kombëtare, politikën e jashtme, interesat ekonomikë dhe financiarë të shtetit, parandalimin dhe ndjekjen e veprave penale. Në rast se aksesi mohohet, duke argumentuar se cenohen interesat e sigurisë kombëtare, politika e jashtme, interesat ekonomikë dhe financiarë të shtetit, parandalimi dhe ndjekja e veprave penale ose liria e shprehjes dhe informimit apo liria e shtypit, subjekti i të dhënave mund t'i kërkojë komisionerit të kontrollojë përjashtimin në rastin konkret. Komisioneri informon subjektin e të dhënave për masat e marra. Ligji nuk përcakton në mënyrë specifike se si jepet aksesi, dhe në këtë rast ka nevojë për ndryshime legjislative në këtë aspekt në mënyrë që format e dhënies së aksesit të jenë sa më të qarta në mënyrë që të evitohen abuzimet.

4. Detyrimet e kontrolluesit dhe të përpunuesit, njoftimi dhe siguria e të dhënave personale

-Informacioni duhet të jepet pas grumbullimit, sa më shpejt që të jetë e mundur. Kur të dhënat mblidhen nga individët e interesuar, informacioni mund të jepet në kohën e grumbullimit të të dhënave. Ligji nuk parashikon formën e dhënies së informacionit dhe

në këtë kontekst duhen bër ndryshime duke parashikuar dhe parashtruar në mënyrë specifike modalitetet grumbullimit të të dhënave dhe detyrimet e kontrolluesit dhe të përpunuesit së të dhënave.

-Për sa i përket njoftimit, mund të themi se nga ky përcaktim, kontrolluesit duhet të njoftojnë Komisionerin vetëm një herë, përveç rasteve kur ka ndonjë ndryshim që do të thotë se njoftimi që është dhënë fillimisht është i gabuar. Ligji nuk përcakton një formë të caktuar të njoftimit. Këtë mund ta përcaktojë Komisioneri.

5. Rregullimi i ndërhyrjes se autoriteteve shtetërore në të dhënat personale

- Ne ligjin për mbrojtjen e të dhënave personale mungojnë parashikime të veçanta ne lidhje me rregullimin e ndërhyrjes se autoriteteve shtetërore në të dhënat personale të qytetareve, kur të dhënat përdoren për të garantuar sigurinë kombëtare, sigurinë publike, parandalimin dhe hetimin e kryerjes së një vepre penale, apo ndjekjen e autorëve të saj.

Një problem që vihet re në lidhje me këto raste, është mungesa e përcaktimit të kushteve specifike në të cilat autoritetet ligj zbatuese do të marrin dijeni mbi të dhënat personale, si dhe e kategorive të subjekteve që autorizohen të kenë akses në këto të dhëna.

Mungojnë parashikime të veçanta në lidhje me: a) seriozitetin e veprave penale për parandalimin ose ndjekjen e të cilave, shtrohet nevoja e aksesit në të dhënat personale apo e rrezikshmërisë së aktiviteteve kundër rendit dhe sigurisë publike, që do të justifikonin ndërhyrjen në këto të dhëna; b) subjektet të cilët janë të autorizuar për të marrë akses në të dhënat në rast se vërtetohen rrethanat e kërkuara; c) mënyrën se si do të ruhen apo përpunohen në vijim këto të dhëna pas momentit që ato vihen në dispozicion të autoriteteve shtetërore.

6.2.2 Konstatime dhe Rekomandime në lidhje me ligjin nr. 9918, datë 19.05.2008 për "Komunikimet elektronike në Republikën e Shqipërisë", i ndryshuar.

2. Mbrojtja e të Dhënave dhe e Privatësisë në lidhje me përpunimin e të dhënave në shërbimet e komunikimeve elektronike te realizuara në një rrjet privat

-Mos përfshirja e komunikimeve elektronike me natyrë jopublike në kuadrin rregullues aktual të ligjit është pasojë e ndikimit të drejtpërdrejtë prej Direktivës 2002/58 /KE 'Për

përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike'.

-Në tekstin e Direktivës thuhet se ajo do të gjejë zbatim vetëm në lidhje me përpunimin e të dhënave në shërbimet e komunikimeve elektronike publike të kryera nëpërmjet rrjeteve të komunikimeve publike. Ky fakt nuk është pozitiv sepse rrjetet private po marrin një rëndësi gjithnjë e më të madhe në jetën e përditshme, e bashkëshoqëruar kjo me risqe gjithnjë e në rritje ndaj tyre, dhe në mënyrë të veçantë sepse këto rrjete janë duke u bërë akoma më specifike.

-Nga sa më sipër është e nevojshme të shikohet mundësia e një rishikimi të ligjit në mënyrë që të arrihet një përqasje e cila garanton më së miri të drejtën e individit për jetë private dhe për mbrojtjen e të dhënave personale në përputhje me standardet e vendosura në instrumentat ndërkombëtare dhe ligjet e brendshme që mbrojnë posaçërisht këto të drejta.

6.2.3 Kuadri rregullator i çështjeve që lidhen me përdorimin e shërbimit të internetit dhe postës elektronike zyrtare të punëmarrësve në kuadër të mbrojtjes së të dhënave personale

- Aktualisht, ekziston Udhëzimi nr. 40, datë 13.06.2014 i "Komisionerit për të drejtën e informimit dhe mbrojtjen e të dhënave personale", "Për përdorimin e shërbimit të internetit dhe postës elektronike zyrtare në institucionet publike në kuadër të mbrojtjes së të dhënave personale", por nuk kemi një rregullim të përcaktuar ligjor për sektorin privat të punësimit. Në këtë kontekst është e nevojshme që të miratohet një udhëzim i ri nga ana e "Komisionerit për të drejtën e informimit dhe mbrojtjen e të dhënave personale" që të parashikojë dhe të përcaktojë të gjitha modalitetet me qëllim rregullimin e përdorimin e shërbimit të internetit dhe postës elektronike zyrtare të punëmarrësve në sektorin privat duke garantuar kështu mbrojtjen e të dhënave personale në këtë sektor në mënyrë të ngjashme me rregullimin që i bëhet kësaj problematike në sektorin publik sipas udhëzimit nr.40.

BIBLIOGRAFIA

A. Literatura

- Akrivopoulou, Ch. dhe Psygkas, A., (2010). "*Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*".

- Akrivopoulou, Ch. M. (2012). "*Human Rights and Risks in the Digital Era: Globalization and the Effects of Information Technologies*".

- Alston, Ph. dhe De Schutter, O. (2005). "*Monitoring Fundamental Rights in the EU: The Contribution of the Fundamental Agency*".

- Anne, C. dhe Meuwese M. (2008). "*Impact Assessment in European Union Lawmaking*".

- Artikulli i New York Times "*Strong privacy laws may explain data security in Europe*", 4 fq.

- Axford, B. (2013). "*Theories of Globalization*".

- Berger, A. (1968). "*Encyclopedic Dictionary of Roman Law"* - Volume 43, 807 fq.

- Bergkamp, L. (2002). "*EU data protection policy, the privacy fallacy: adverse effects of europe's data protection policy in an information–driven economy*", Computer Law &Security Report, fq. 31-47.

- Bergkamp, L. dhe Dent, J. (2002). "*Data Protection in Europe and the Internet: An Analysis of the European Community's Privacy Legislation in the Context of the World Wide Web*", 14 fq.

- Berglund, S. (2009). "*Putting Politics into Perspective: A Study of the Implementation of the EU Utilities Directives*".

- Berkers, F., Goossenaerts, J. dhe Hammer, D. dhe Wortmann, H. (2001). "*Human Models and Data in the Ubiquitous Information Infrastructure*", London-UK.

- Berners - Lee, T. (1989). "*Weaving the Web*".

- Bezzi, M., Duquenoy, P. dhe Fischer-Hübner, S. (2010). "*Privacy and Identity Management for Life*", 5th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/Prime Life International, Summer School, Nice, France, September 9-12, 2009, Revised Selected Paper, 35 fq.

- Bignami, F. (2007). "*Privacy and Law Enforcement in the European Union:The Data Retention Directive*", Chi. J. Int.l Law, 23 fq.
- Bignami, F. (2008). "*The Case for Tolerant Constitutional Patriotism: The right to Privacy Before the European Courts*", Cornell International Law Journal. 40 fq.
- Boehm, F. (2012). "*Information Sharing and Data Protection in the Area of Freedom, Security and Justice-Towards Harmonized Data Protection Principles for Information Exchange at EU-level*".
- Bordo, M. D., Taylor, A. M. dhe Williamson, J. G. (2007). "*Globalization in Historical Perspective*".
- Brouwer, E. R. (2008). "*Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*".
- Buchmann, J. (2014). "*Internet Privacy: Options for adequate realization*".
- Buckland, J. A. (1992). "*Combating computer crime: prevention, detection, investigation*".
- Büllesbach, A. (2010). "*Concise European IT Law"*, Kluwer Law International.
- Butler, M. (2003). "*Spam - the meat of the problem*", në Computer Law & Security Report, fq, 388-391.
- Bygrave, L. (1998). "*Data Protection Pursuant to the Right of Privacy in Human Rights Treaties*", International Journal Of Law and Information Technology, fq 247-284.
- Çabej (Pogaçe), F., Gjoleka, A. dhe Shala, A. (2010). "*Komentar i ligjit për mbrojtjen e të dhënave personale*", Tiranë.
- Cartelli, A., Palma M. (2009). "*Encyclopedia of Information Communication Technology*".
- Castells, M. (2000). "*The Internet Galaxy, - Reflections on the Internet, Business and Society*", Oxford University Press 1, fq. 73-87.
- Catannaci, J. dhe Misfud-Bonnici, J. (2005). "*Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty*", Information & Communications Technology Law, fq. 5-15.

- Cate, F. (1998). "*Privacy and Telecommunications*", Wake Forest Law Review, 50 fq.
- Chalmers, D., Davies, G. dhe Monti, G. (2010). "*European Union Law: Cases and Materials*".
- Choo, A. L. T. (2008). "*Abuse of Process and Judicial Stays of Criminal Proceedings*".
- Clarke, R. A.dhe Knake, K. (2012). "*Cyber War: The Next Threat to National Security and What to Do About It*".
- Colvin, M. (2000). "*The Schengen Information System: A Human Rights Audit: a Justice Report*".
- Conn, K. (2002). "T*he Internet and the Law: What Educators Need to Know?*".
- Cooke, Ph., De Laurentis, C. dhe MacNeill, S. (2010). "*Platforms of Innovation: Dynamics of New Industrial Knowledge Flows*".
- Craig, P. P. dhe Burke, G. (2011). "*The Evolution of EU Law*".
- Cremer, H.J. (2010). "*Human Rights and the Protection of Privacy in Tort Law: A Comparison between English and German Law*".
- Carozza, P. G. dhe Carozza-Wright P. (2013). "*Regional Protection of Human Rights*", Volume 1.
- Di Federico, G. (2011). "*The EU Charter of Fundamental Rights: From Declaration to Binding Instrument*".
- Dowding, M. (2011). "*Privacy: Defending an Illusion*".
- Ehlers D. (2007). *"European Fundamental Rights and Freedoms"*.
- Elezi, I. (1983). "*E Drejta Penale e Republikës Popullore Socialiste të Shqipërisë (pjesa e posaçme)*". Tiranë: Shtypshkronja 'Mihal Duri'.
- Elezi, I. (2007). "*E Drejta Penale (Pjesa e Posaçme)*", Tiranë.
- Fischetti, M. (2008). "*Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*".
- Flichy, P. (1995). "*The history of modern communications - in the public sphere and private life*".

- Frackman, A., Martin, R. C. dhe Ray, C. (2002). "*Internet and Online Privacy: A Legal and Business Guide*".
- Froomkin, M. (2000). "*The Death of Privacy*", Stanford Law Review.
- Frowein – Peukert - EMRK Komentar, Engel Verlag (1996).
- Fuchs, Ch., Boersma, K. dhe Albrechtslund, A. (2012). "*Internet and Surveillance: The Challenges of Web 2.0 and Social Media*".
- Futja e teknologjive të reja që lidhen me përdorimin e telefonave celularë në Revistën WIRED "Inside the GPS revolution", 12 shkurt 2009.
- Geronta, A. (2002). "*Protecting citizens from electronic processing of personal data*".
- Gibson, W. (1984). "*Neuromancer*" .
- Gibson, W. (2004). "*Neuromancer - Ace Hardcove*r".
- Gillies, L. (2013). "*Electronic Commerce and International Private Law: A Study of Electronic Consumer Contracts*".
- Gomien, D. (2005). "*Short Guide to the European Convention on Human Rights*".
- González Fuster G. (2014). "*The Emergence of Personal Data Protection as a Fundamental Right of the EU*".
- Gormley, K. (1992). "*One Hundred Years of Privacy*".
- Grant, R. A. dhe Bennett C. J. (1999). "*Visions of Privacy: Policy Choices for the Digital Age*".
- Gritzalis, S. (2004). "*Enhancing Web privacy and anonymity in the digital era", Information Management & Computer Security*".
- Guagnin, D., Hempel, L. dhe Oxygen, C. (2012). "*Managing Privacy through Accountability*".
- Gutwirth, S., Leenes, R. dhe De Hert, P. (2012). "*European Data Protection: In Good Health?*"
- Gutwirth, S., Leenes, R. dhe de Hert, P. (2013). "*Reloading Data Protection: Multidisciplinary Insights and Contemporary*".

- Gutwirth, S., Leenes, R. dhe de Hert, P. (2014). "*Reforming European Data Protection Law*".
- Gutwirth, S., Poullet, Y. dhe de Hert P. (2010). "*Data Protection in a Profiled World*".
- Gutwirth, S., Poullet, Y., De Hert, P. dhe Leenes, R. (2011). "*Computers, Privacy and Data Protection: An Element of Choice*".
- Haftor, D. (2010). "*Information and Communication Technologies, Society and Human Beings: Theory and Framework"*.
- Hall, K. (2000). "*Conscience, Expression, and Privacy*".
- Hervey, T. K. dhe McHale, J. V. (2004). "*Health Law and the European Union*".
- Hope, R. A., Savulescu, J. dhe Hendrick, J. (2008). "*Medical Ethics and Law: The Core Curriculum*".
- Hubner, S. (2001). "*Privacy in the Global Information Society*", IT – Security and Privacy, LNCS Springer-Verlag, Berlin – Heidelberg.
- Hustinx, P. (2007). "*Online Privacy: Reconsidering Policy Options for the Digital Age*".
- Hyatt, M. (2001). "*Invasion of privacy: how to protect yourself in the digital age*".
- Kabera Karanja, S. (2008). "*Transparency and Proportionality in the Schengen Information System and Border Control Cooperation*".
- Kaczorowska, A. (2013). "*European Union Law*".
- Khosrowpour, M. (2001). "*Managing Information Technology in a Global Economy*".
- Kiessling, T. dhe Blondeel, Y. (1996). "*The EU Regulatory Framework in Telecommunications-A Critical Analysis, Telecommunications Policy in the EU*".
- Kindt, E. J. (2013). "*Privacy and Data Protection Issues of Biometric Applications: A Comparative legal Analysis*", Law, Governance and Technology Series 12.

- King, I. (2003). "*On – line Privacy in Europe-new regulation for cookies*", Information & Communication Technology Law, fq. 225-236.
- Kirby, M. (1979). "*O.E.C.D. Guidelines on Privacy", Law Reform Commission*.
- Kirby, M. (2011). "*The history, achievement and future of the 1980 OECD guidelines on privacy*".
- Kirkman, G. dhe Cornelius, P. K. (2002) "*The Global Information Technology Report 2001-2002: Readiness for the Networked World*", Oxford University Press, USA, fq. 93-99.
- Kleve, P. dhe Mulder, R. (2008). "*Privacy protection and the right to information, In search of a new balance*".
- Koenig, Ch. dhe Bartosch A. (2009). "*EC Competition and Telecommunications Law*", 2nd Edition.
- Kosta. E (2013). "*Consent in European Data Protection Law*".
- Krogstie, J. (2012). "*Model-Based Development and Evolution of Information Systems: A Quality Approach*".
- Lawson, E. H. dhe Bertucci, M. L. (1996). "*Encyclopedia of Human Rights*".
- Lechner, J. F. (2009). "*Globalization: The Making of World Society*".
- Leith, P. (2006). "*The Socio-legal context of Privacy*", International Journal of Law in Context, fq. 105-136.
- Lessig, L. (2013). "*Remix: Making Art and Commerce Thrive in the Hybrid Economy"*.
- Lindsay, D. (2005). "*An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law*" 29 Melbourne University Law Review, 48 fq.
- Longman dictionary of Contemporary English, Third Ed. (1995).
- Loukeri, G. (1997). "*Harmonization of law on the protection of individuals against the processing of personal data in the European Union*".
- Manuel, C. (2001). "*The Internet Galaxy, Reflections on the Internet, Business and Society*", Oxford.

- Maras. M.H. (2012). "*Counterterrorism*".
- Marcella, A. J. dhe Stucki, C. (2003). "*Privacy Handbook: Guidelines, Exposures, Policy Implementation and International Issues*".
- Marchionini, G. (1997). "*Information Seeking in Electronic Environments*".
- Markesinis, B. S. dhe Unberath H. (2002). "*The German Law of Torts: A Comparative Treatise*".
- Matthews, J. (2005). "*Computer Networking: Internet Protocols (IP) in Action*".
- Mayer-Schönberger V.(1997).*"Generational Development of Data Protection in Europe*" in Philip Agre dhe Marc Rotenberg (eds), "*Technology and Privacy: The New Landscape*", MIT Press, Cambridge, 8 fq.
- Mazower, M. (2009). "*Dark Continent: Europe's Twentieth Century*".
- McGeorge Law Review (2007). - Volume 38, Issues 1-2.
- Mendel, T., Puddephatt, A. dhe Wagner, B. (2012). "*Global Survey on Internet Privacy and Freedom of Expres*sion".
- Mendel, T, Puddephatt, A. dhe Wagner, B. (2012). "*Global Survey on Internet Privacy and Freedom of Expression*".
- Mendel, T., Puddephatt, A. dhe Wagner, B. (2012). "*Global Survey on Internet Privacy and Freedom of Expression*".
- Moore, A. D. (2011). "*Privacy Rights: Moral and Legal Foundations*".
- Mordini, E. dhe De Hert P. (2010). "*Ageing and Invisibility*".
- Morgan, R. dhe Boardman, R. (2012). "*Data Protection Strategy: Implementing Data Protection Compliance*".
- Morley, D. (2008). "*Understanding Computers: Today & Tomorrow, Comprehensive*".
- Morsink, J. (2011) "*The Universal Declaration of Human Rights: Origins, Drafting, and Intent*".
- Nenova, M. B. (2007). "*European Community Electronic Communications and Competition Law*".

- Neuwahl, N. A. dhe Rosas, A. (1995). "*The European Union and Human Rights*".
- Noorda, C., Noorda, C. W. dhe Hanloser, S. (2011). "E-*discovery and Data Privacy: A Practical Guide*"
- Orwell, G. (2003). "*Nineteen Eighty-Four*", Penguin Books", London.
- Parker, D. (1968). "*Rules of Ethics in Information Processing*" Communications of the ACM.
- Peers, S. dhe Ward, A. (2004). "*The European Union Charter of Fundamental Rights*".
- Peng, K. (2014). "*Anonymous Communication Networks: Protecting Privacy on the Web*".
- Pohlman, H. L. (1993). "*Political Thought and the American Judiciary*".
- Portela, I. M. (2010). "*Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues*".
- Poullet, Y. (2009). "*Data protection legislation*: *What is at stake for our society and democracy*?"
- Regan, P. M. (1995). "*Legislating Privacy: Technology, Social Values, and Public Policy*".
- Renucci, J.F. (2005). "*Introduction to the European Convention on Human Rights: The Rights Guaranteed and the Protection Mechanism*", Volume 88.
- Rifkin, J. (2001). "*The Age of Access: How the Shift from Ownership to Access is Transforming Modern Life*".
- Roca, J. G. dhe Santolaya, P. (2012). "*Europe of Rights: A Compendium on the European Convention of Human Rights*".
- Rosenberg, R. (1992). "*The Social Impact of Computers*", Academic Press, New York, NY.
- Rössler, B. (200). "*Privacies: Philosophical Evaluations*".
- Rule, J. B. dhe Greenleaf, G. W. (2010). "*Global Privacy Protection: The First Generation*".

- Sarat, A. (2014). "*A World without Privacy*".
- Schneider, G., Evans, J., dhe Pinard, K. (2009). "*The Internet: Illustrated Series*", Boston: Course Technology Cengage Learning.
- Schrijver, S. Schraeyen, J. (2005). "*Spyware: Innocent espionage in cyberspace?*" Communications Law.
- Shafer, G. (1999). "*The Power of EU Collective Action: The Impact of EU Data Privacy Regulation on US Business Practice*", European Law Journal, fq. 419-437.
- Smith, G. J. H. (2007). "*Internet Law and Regulation*".
- Solove, D. (1983). "*Understanding Privacy*", Harvard University Press, Harvard, 24 fq.
- Solove, D. (2004). "*The Digital Person-Technology and Privacy in the Information Age"*, New York University Press, 32 fq.
- Spindler, G. dhe Börner F. (2005). "*E-Commerce Law in Europe and the USA*".
- Spiro, O. (2013). "*E Drejta e Internetit*".
- Standage, T. (2005). "*The Future of Technology*".
- Stolleis M. (2001). "*Public Law in Germany"*, 1800-1914".
- Stratford, J. (1998). "*Data Protection and Privacy in the United States and Europe*" IASSIST Quarterly.
- Strawbridge, M. (2006). "*Netiquette: Internet Etiquette in the Age of the Blog*".
- Stuckey, K. D. (1996). "*Internet and Online Law*", Law Journal Press.
- Tambini, D., Leonardi, D. dhe Marsden, Ch. T. (2008). "*Codifying Cyberspace: Communications Self-regulation in the Age of Internet Convergence*".
- Tene, O. (2011)."*Privacy, The New generations, International Data Privacy Law*".
- Thompson, N. (2000). "*Instilling Ethics*".
- Torres Pérez, A. (2009). "*Conflicts of Rights in the European Union: A Theory of Supranational Adjudication*".

- Varney, E. (2013). "*Disability and Information Technology: A Comparative Study in Media Regulation*".
- Warren, S. D. dhe Brandeis, L. D. (1890). "*The Right to privacy*", Harvard Law Review.
- Warren, A. dhe Dearnley, J. (2005). "*Data protection legislation in the United Kingdom: from development to statute 1969-84*".
- Weber, R. H. dhe Heinrich, U. I. (2012). "*Anonymization*".
- Webster, F. dhe Blom, R. (2004). "*The Information Society Reader*".
- Weinstein, S. (2003). "*The New European Commission Regulatory Framework for Electronic Communications*", Hertfordshire Law Journal, 15 fq.
- Westby, JR. (2004). "*International Guide to Privacy*".
- Westin, A. (1967). "*Privacy and Freedom*".
- Westin, A. (1972). "*Databanks in a Free Society*".
- Westin, A. (2003). "*Contemporary perspectives on privacy: social and political dimensions of privacy*", Journal of Social Issues.
- Working Paper 37 "*Protection of privacy on the Internet. - An integrated approach of EU data protection online*".
- Wright, D. dhe de Hert, P. (2011). "*Privacy Impact Assessment*".
- Youst-Koh "*Management and discovery of Electronically Stored Information, Computer Law Review and Technology Journal*" – Summer 1997.
- Zaganjori, Xh., Anastasi, A. dhe Çani, E. "*Shteti i së Drejtës në Kushtetutën e Republikës së Shqipërisë*".
- Elgesem, D. (1999). "*The structure of rights in Directive 95/46EC on the protection of individuals with regard to the processing of personal data and the free movement of such data*", Ethics and Information Technology.

B. BURIMET PARËSORE

- LEGJISLACIONI KOMBËTAR

° Kushtetuta e Republikës së Shqipërisë e vitit 1998.

° Kushtetuta e Republikës Popullore Socialiste të Shqipërisë e vitit 1976.

° Kodit Penal i Republikës së Shqipërisë.

° Ligji nr. 8517, datë 22.07.1999 "*Për mbrojtjen e të dhënave personale*"

° Ligji nr. 9887, datë 10.03.2008, ndryshuar me ligjin Nr. 48/2012, ndryshuar me ligjin nr.120/2014 "*Për Mbrojtjen e të Dhënave Personale*".

° Ligji nr. 9918, datë 19.05.2008 "*Për Komunikimet Elektronike në Republikën e Shqipërisë*".

° Ligji nr. 102/2012 për disa ndryshime dhe shtesa në ligjin nr. 9918, datë 19.5.2008 "*Për Komunikimet Elektronike në Republikën e Shqipërisë*" i ndryshuar.

° Ligji nr. 97/2013 "*Për Mediat Audiovizive në Republikën e Shqipërisë*".

° Udhëzimi" nr. 14, datë 22.12.2011 "*Për përpunimin, mbrojtjen dhe sigurinë e të dhënave personale në sektorin e komunikimit elektronik të publikut*" i Komisionerit Për të Drejtën e Informimit dhe Mbrojtjes së të Dhënave Personale.

° Konventa e Strasburgut e firmosur nga Shqipëria në datë 01.28.1981, në 9/6/2004, e ratifikuar në 14/2/2005 dhe hyri në fuqi në 01/06/2005.

° Udhëzim nr. 9, dt. 15.09.2010 "*Për rregullat themelore në lidhje me mbrojtjen e të dhënave personale në median e shkruar, vizive dhe audiovizive*".

° Udhëzimi nr.14 i datës 22.12.2011 "*Për përpunimin, mbrojtjen dhe sigurinë e të dhënave personale në sektorin e komunikimit elektronik të publikut*".

° Udhëzimi nr.40 i Komisionerit, datë 13.06.2014 "Mbi përdorimin e shërbimit të internetit dhe postës elektronike zyrtare në institucionet publike në kuadër të mbrojtjes së të dhënave personale".

° Rekomandim nr. 8 i Komisionerit për të Drejtën e Informimit Mbrojtjen e të Dhënave Personale, datë 05.06.2013.

° Urdhër nr.11 i Komisionerit për të Drejtën e Informimit Mbrojtjen e të Dhënave Personale, datë 21.03.2013.

- Vendim nr. 1, i Komisionerit për të Drejtën e Informimit Mbrojtjen e të Dhënave Personale, datë 4.03.2010.

- Vendimi nr.545, datë 11.08.2011, i Këshillit të Ministrave, ku ndryshoi dhe zëvendësoi, "*Këshillin Kombëtar të Radios dhe Televizionit*" (KKRT) me "*Autoritetin i Mediave Audiovizive*" (AMA).

- **AKTE NDËRKOMBËTARE DHE KOMUNITARE**

- "Deklarata Universale për të Drejtat e Njeriut" e Asamblesë së Përgjithshme të Kombeve të Bashkuara, datë 10 .12. 1948.
- "Paktit Ndërkombëtar mbi të Drejtat Civile dhe Politike", datë 23.03. 1976.
- "Karta e të Drejtave Themelore të Bashkimit Evropian", datë 07.12.2000 dhe hyri në fuqi më 01.12.2009.
- "Konventa Evropiane për të Drejtat e Njeriut", datë 04.11.1950 dhe hyri në fuqi më 03.09.1953.
- "Marrëveshja Shengen", datë 14.06.1985.
- "Traktati i Komunitetit Evropian", datë 25.03.1957.
- 2004/496/EC: Council Decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection Official Journal L 183, 20/05/2004.
- 2004/535/EC: Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection (notified under document number C(2004) 1914) Official Journal L 235, 06/07/2004 P. 0011 – 0022.
- Direktiva 2002/19/KE e Parlamentit Evropian dhe e Këshillit të datës 7 Mars 2002 "*Për aksesin ndaj rrjeteve të komunikimeve elektronike, faciliteteve shoqëruese, si dhe interkoneksionin e tyre*" (Access Directive) EE L 108 e datës 24.04.2002.

- Direktiva 2002/20/KE e Parlamentit Evropian dhe e Këshillit të datës 7 mars 2002 "*Për autorizimin e rrjeteve dhe shërbimeve të komunikimeve elektronike*" (Direktiva e Autorizimit). EE L 108 e datës 24.04. 2002.
- Direktiva 2002/21/KE e Parlamentit Evropian dhe e Këshillit të datës 7 mars 2002 "*Për një kuadër të përbashkët rregullator për rrjetet e komunikimit elektronik dhe shërbimeve*" (Kuadër Direktiva). EE L 108 e datës 24.4.2002.
- Direktiva 2002/22/KE e Parlamentit Evropian dhe e Këshillit të datës 7 mars 2002 "*Për shërbimin universal dhe të drejtat e përdoruesve në lidhje me rrjetet dhe shërbimet e komunikimeve elektronike*" (Direktiva e Shërbimit Universal). EE L 108 e datës 24.4.2002.
- Direktiva 2002/58/KE e Parlamentit Evropian dhe e Këshillit Evropian të datës 12 korrik 2002 "*Për përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike*".
- Direktiva 2006/24/KE e Parlamentit Evropian dhe të Këshillit Evropian të datës 03.2006 "*Për ruajtjen e të dhënave të krijuara ose të përpunuara në lidhje me vënien në dispozicion të publikut të shërbimeve të komunikimeve elektronike ose të rrjeteve të komunikimeve publike*".
- Direktiva 2009/136/KE e Parlamentit Evropian dhe e Këshillit e datës 25 nëntor 2009 amendon Direktivën 2002/22/KE, "*Për shërbimin universal dhe të drejtat e përdoruesve në lidhje me rrjetet e komunikimeve elektronike dhe shërbimeve*".
- Direktiva 95/46/KE e Parlamentit Evropian dhe e Këshillit Evropian të datës 24.10. 1995 "*Për mbrojtjen e individëve në lidhje me përpunimin e të dhënave personale dhe mbi lëvizjen e lirë të këtyre të dhënave*".
- Direktiva 97/66/KE e Parlamentit Evropian dhe e Këshillit të datës 15 dhjetor 1997 "*Për përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e telekomunikacionit*".
- Direktiva 2000/31/KE e Parlamentit Evropian dhe e Këshillit e datës 8 qershor 2000 "*Për aspekte të caktuara ligjore të shërbimeve të shoqërisë së informacionit, në veçanti të tregtisë elektronike, në Tregun e Brendshëm*" ("*Direktiva për tregtinë elektronike").*
- Koment nr. 16 i Direktivës 2002/58/KE.
- Koment nr. 26 i Direktivës 2002/58 KE.

- Koment nr. 34 i Direktivës 2002/58 KE.
- Konventa e Strasburgut "*Për mbrojtjen e individëve në lidhje me Përpunimin Automatik të të Dhënave Personale*" e datës 28.01.1981.
- Memorandum i Komisionit Evropian nr.14/269, *'Frequently Asked Questions: The Data RetentionDirective'*. Bruksel, 08 prill 2014.
- Opinion 4/2007 "*Për Kuptiminn e të Dhënave Personale"*.
- Opinion 4/2007 i Grupit të Punës për mbrojtjen e të dhënave personale '*Mbi konceptin e të dhënave personale*'.
- Opinion shpjegues 20 i Direktivës 2002/58/KE.
- Opinion shpjegues 59 i Direktivës 2009/136 /KE.
- Opinion shpjegues 6 i Direktivës 2006/24/KE.
- Opinion shpjegues 65 i Direktivës 95/46/KE.
- Opinion shpjegues 68 i Direktivës 2009/136/KE.
- Opinioni 2005 mbi propozimin e Direktivës të Parlamentit Evropian dhe Këshillit për ruajtjen e të dhënave të përpunuara në funksion për të siguruar shërbimet publike të komunikimeve elektronike dhe amendimin e Direktivës 2002/58/KE [COM (2005),datë 21.09 .2005, dalë më 21 tetor, 2005].
- Opinioni 3/2006 mbi Direktivën 2006/24/KE, i Parlamentit Evropian dhe Këshillit për ruajtjen e të dhënave të krijuara ose të përpunuara në lidhje me ofrimin e shërbimeve të komunikimeve elektronike të disponueshme për publikun ose të rrjeteve të komunikimeve publike dhe për ndryshimin e Direktivës 2002/58/KE.
- Rekomandimi Nr. R (99) 5 të Komitetit të Ministrave të Shteteve Anëtare "*Për mbrojtjen e privatësisë në internet*".
- Rregulloren (EC) Nr. 2006/2004, "*Për bashkëpunimin ndërmjet autoriteteve kombëtare përgjegjëse për zbatimin e mbrojtjes së konsumatorit*".
- Rregullorja (KE) Nr. 45/2001 e Parlamentit Evropian dhe e Këshillit e datës 18 Dhjetor 2000 mbi mbrojtjen e individëve në lidhje me përpunimin e të dhënave personale nga institucionet dhe organet e Komunitetit dhe mbi lëvizjen e lirë të këtyre të dhënave, Gazeta Zyrtare L 008, 2001/12/01 fq 0001-0022.

C. BURIMET DYTËSORE

- PRAKTIKË GJYQËSORE

Gjykata Evropiane e të Drejtave të Njeriut

° *Niemietz v. Germany,* Application no. 13710/88, dt. 16.12.1992.

° *Amann v. Switzerland,* Application no. 27798/95, dt. 16.02.200.

° *K.U v. Finland,* Application no. 2872/02. 02.12.2008.

° *Klass and Others v. Germany,* Application no. 5029/71, dt. 06.09.1978.

° *Niemitz v.Germany,* Application no. 13710/88, dt.16.12.1992.

° *Copland v.United Kingdom,* Aplication no.62617/00, dt 03.04.2007.

° *Halford v. United Kingdom Government,* Aplication no.20605/92,dt. 25.06.1997.

° *Malone v. the United Kingdom,* Aplication no. 8691/79, dt. 02.08.1984.

° *Amann v. Switzerland,* Aplication no. 27798/95, 65-67, ECHR 2000.

° *Frezzos & Roire v. France,* Aplication no. 29183/1995, ECHR 1995.

° *Narinen v. Finland* , Application no. 45027/98, dt.01.06.2004.

° *P.G. dhe J.H. kundër Mbretërisë së Bashkuar,* Aplication no. 44787/98, dt. 25.12.2001.

° *Caroline of Hanover (Monaco) v. Germany,* Application no. 59320/00, dt. 24.6.2004.

Gjykata Evropiane e Drejtësisë

° *Osterreichischer Rundfunk (ORF) v. Austria,*Vendimi i datës 20.5.2004, C-465/00,C-138/01, Përmbledh. 2003.I-4989.

° *Bodil Linqvist v. Sweden,* Vendimi i datës 6.11.2003, C-101/01, Përmbledh. 2003.I-12971.

- *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others.C-93/12 Digital Rights Ireland,* Vendimi i datës 08.04.2014.

- *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* Vendimi i datës 13.05.2014.

Gjykata Kushtetuese e Republikës së Shqipërisë

- Vendim i Gjykatës Kushtetuese të Republikës së Shqipërisë nr.16 datë 11.11.2004.
- Vendim i Gjykatës Kushtetuese të Republikës së Shqipërisë nr.52 datë 01.12.2011.
- Vendim i Gjykatës Kushtetuese të Republikës së Shqipërisë nr.57 datë 01.12.2014.

- **BURIME NGA WEBSITE ZYRTARE:**

- http://www.wired.com/politics/law/news/1999/01/17538
  FAQE INTERNETI QË PËRMBAN ARGËTIM, KOMUNIKIM, SHKENCË, POLITIKË DHE KULTURË

- http://www.techterms.com/definition/cyberspace
  FJALOR I TERMAVE TË KËRKUESHME KOMPJUTERIKE ME PËRKUFIZIMET E SHPJEGUARA NË GJUHË TË THJESHTË

- http//Cyber.law.harvard.edu/privacy/PrivacyCirca2002.htm
  DOMAIN NË KRYQËZIMIN E TEKNOLOGJISË, RREZIKUT DHE TË LIGJIT

- http://www.capurro.de/infoconcept.html
  FAQE INTERNETI ME OPINIONE SHKENCORE

- http://mondediplo.com/2000/01/14queau
  NJË DOKUMENT I MADH NDËRKOMBËTAR QË ËSHTË ME TË VËRTETË I PAVARUR, QË E SHEH BOTËN NË MËNYRA REALE QË FOKUSOHET NË VENDE QË KA BOTIME

- http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papersand-common-positions-adopted-by-the-working-group

KOMISIONERI PËR MBROJTJEN E TË DHËNAVE DHE LIRINË E INFORMACIONIT NË GJERMANI

- http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-andrecommendations-for-online-social-networks
  AGJENCIA E BASHKIMIT EVROPIAN PËR RRJETIN DHE SIGURINË E INFORMACIONIT

- http://trapster.com/
  NAVIGATOR SOCIAL ME APLIKIME NË CELULARË DHE FAQE INTERNETI, ME KUSHT FALAS

- http://moop.me/inap.php
  APLIKACION INTELIGJENT I RRJETIT ME PROTOKOLL

- http://www.joyity.com/
  MULTIPLAYER MASIV TRANS-REAL

- http://www.folk.uio.no/LEE/publications/%%20inPrivacy20context.pdf20globa
  % UNIVERSITETI I OSLOS

- http://www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html
  UNIVERSITETI KOMBËTAR I AUSTRALISË

- http://www.gavison.com/a2658-privacy-and-the-limits-of-law
  FAQE ZYRTARE E PROFESORIT TË TË DREJTAVE TË NJERIUT NË UNIVERSITETIN E HEBRENJVE

- http://www.nytimes.com/2010/02/28/weekinreview/28liptak.html?_r=1
  GAZETË AMERIKANE E PËRDITSHME

- http://ec.europa.eu/justice_ home /fs j/ privacy/docs/wpdocs/2007/wp136_el.pdf
  FAQE ZYRTARE E KOMISIONIT EVROPIAN

- http://www.edps.Europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/
  Publications/ Papers/Back groundP/05-07_ BP_ accesst odocum ents_EN.pdf
  FAQE ZYRTARE E MBROJTES EVROPIANE SË TË DHËNAVE

- http://sas-space.sas.ac.uk/5452/1/1855-2575-1-SM.pdf
  BIBLOTEKË ONLINE PËR STUDENTËT DHE HULUMTUESIT

- http://ssrn.com/abstract=894079
  BIBLOTEKË ONLINE SHUMË-DISIPLINORE E HULMTIMEVE SHKENCORE

- http: //www. justice.gov/opcl/privstat.htm
  DEPARTAMENTI I DREJTËSISË SË SHBA

- http://www.fourthamendmentsummaries.com/
  FAQE ZYRTARE E GJYKATËS SUPREME TË SHBA

- http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm
  UNIVERSITETI I MASSACHUSETTS LOWELL

- http://cyber.law.harvard.edu/privacy/Gormley100%20Years%20of%20Privacy.hth
  FAQE ZYRTARE E UNIVERSITETIT TË HARWARDIT

- http://www.historyofprivacy.net/
  FAQE INTERNETI INFORMUESE PËR MBROJTJEN E PRIVATËSISË NË SHBA

- http://caselaw.lp.findlaw.com/scripts/cases/clcc.html?court=us&vol=277&invol=438
  OPINIONE TË GJYKATËS SUPREME TË SHBA

- http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=389&invol=347

- http://ssrn.com/abstract=914271
  BIBLOTEKË ONLINE SHUMË-DISIPLINORE E HULMTIMEVE SHKENCORE

- http://www.acm.org
  SHOQATA E MAKINERIVE KOMPJUTERIKE SHBA

- http://plato.stanford.edu/entries/ethics-computer/
  FAQE ZYRTARE E UNIVERSITETIT TË STANFORDIT

- http://elj.warwick.ac.uk/jilt/02-3/cahir.html>
  UNIVERSITETI WARWICK MBRETËRIA E BASHKUAR

- http://www.assemblee-nationale .fr /histoire /dudh/1789.asp
  FAQE ZYRTARE E PARLAMENTIT FRANCEZ

- http://www.conseil-constitutionnel.fr/decision//2009/decisions-par-date/2009/2009-580-dc/de cision-n-2009-580-dc-du-10-juin-2009.42666.html
  FAQE ZYRTARE E KËSHILLIT KUSHTETUES TË REPUBLIKËS FRANCEZE

- http://www.wdi.umich.edu/files/Publications/WorkingPapers/wp418.pdf
  FAQE ZYRTARE E INSTITUTIT WILLIAM DAVIDSON

- http://www.echr.coe.int/NR/rdonlyres/E4317264DB2742F873E1ECCACABB045/0/English .pdf
  FAQE ZYRTARE E GJYKATËS EVROPIANE TË TË DREJAVE TË NJERIUT

- http://www.europarl.europa.eu/charter/pdf/text_el.pdf
  FAQE ZYRTARE E PARLAMENTIT EVROPIAN

- http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
  FAQE ZYRTARE E KËSHILLIT TË EVROPËS

- http://www.datenschutz.rlp.de/downloads/bverfge_65_1_-_volkszaehlung.pdf
  KOMISIONERI SHTETËROR PËR MBROJTJEN E TË DHËNAVE DHE INFORMACIONIT NË GJERMANI

- http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf
  FAQE ZYRTARE E KOMISIONIT EVROPIAN

- http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62001J0101:EL:HTML
  FLETORE ZYRTARE E BASHKIMIT EVROPIAN

- http://law.fordham.edu/publications/articles/200flspub6132. pdf
  UNIVERSITETIT I FORDHAM, FAKULTETI I DREJTËSISË, NEW YORK

- http ://www.europarl.eu.int/committees/en/default.htm
  FAQE ZYRTARE E PARLAMENTIT EVROPIAN

- http://www.austlii.edu.au/au/journals/PLPR/2002/26.html
  BURIM I LIRË AKSESI PËR INFORMACION LIGJOR NË AUSTRALI

- http://www.hicss.hawaii.edu/HICSS_35/HICSSpapers/PDFdocuments/INISC02.pdf
  KONFERENCA NDËRKOMBËTARE HAWAII PËR SHKENCAT E SISTEMIT

- http://www.europarl.europa.eu/pv2/pv2?PRG=DOCPV&APP=PV2&SDOCTA=21&TXTLST=1&TPV=DEF&POS=1&Type_Doc=RESOL&date=50901&DATE F=010905 & TYPEF = A5 & PrgPr ev = TYPEF A5PRG @ @ @ QUERYAPP PV2FILE BIBLIO01NUMERO @ @ 264YEAR @ 01PLAGE@ 1 & Langue = ENG
  FAQE ZYRTARE E PARLAMENTI EVROPIAN

- http://epic.org/epic/about.html
  QENDRA E PRIVATËSISË SË INFORMACIONIT ELEKTRONIK

- http ://www .law.indiana.edu/fclj /pubs/v54/no3/Dunham.pdf
  FAQE ZYRTARE E UNIVERSITETIT TË INDIANA, FAKULTETI I DREJTËSISË MAURER

- http ://www.scholarship .law.duke.Edu/cgi/viewcontent.cgi?article=1027...dltr
  FAQE ZYRTARE E UNIVERSITETIT DUKE, FAKULTETI I DREJTËSISË

- http://epic.org/privacy/carnivore/ 8_02_release.html

QENDRA E PRIVATËSISË SË INFORMACIONIT ELEKTRONIK

- http://www.internetsociety.org/sites/default/file/Digital%20Footprints%20- % 20 an %20 Internet %20 Society%20Reference%20Framework.pdf
  FAQE ZYRTARE E SHOQËRISË SË INTERNETIT

- http://www.wired.com/gadgetlab/2011/04/apple-iphone-tracking/
  FAQE INTERNETI QË PËRMBAN ARGËTIM, KOMUNIKIM, SHKENCË, POLITIKË DHE KULTURË

- http://www.surveillance-and-society.org
  ÇËSHTJET E MBIKQYRJES & SHOQËRIA

- http://cs.ucla.edu/~lk/LK/Bib/PS/paper204.pdf
  UNIVERSITETI I KALIFORNISË, LOS ANGELES, DEPARTAMENTI I SHKENCAVE KOMPJUTERIKE

- http ://www .isoc.org/internet/history /brief.shtml#Introduction
  FAQE ZYRTARE E SHOQËRISË SË INTERNETIT

- http://news.in.egr/science-technology/article/?aid=681425
  REVISTË INFORMUESE

- http://www.webopedia.com/TERM/D/DNS.html (20-12-2008)
  FAQE INTERNETI PËR TERMAT E TEKNOLOGJISË SË INTERNETIT DHE KOMPJUTERAVE

- www.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37el.pdf
  FAQE ZYRTARE E BASHKIMIT EVROPIAN

- http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf
  KORPORATA ISHTE NJË PRODHUES DIXHITAL ELEKTRONIK, I NJOHUR PËR PRODHIMET E SAJ TË INFRASTRUKTURËS TË RRJETIT KOMPJUTERIK

- http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_eng.pdf
  FAQE ZYRTARE E KOMISIONIT EVROPIAN

- http://209.85.139.110/blog_resources/Google_response_Working_Party_06_200 7.pdf FAQE INTERNETI ME OPINIONE TË NDRYSHME SHKENCORE

- http://ec europa.eu/justice _ home fsj/privacy/docs/studies/online-serv.pdf
  FAQE ZYRTARE E KOMISIONIT EVROPIAN

- http://en.wikipedia.org/wiki/Lou_Montulli
  ENCIKLOPEDIA ONLINE NË INTERNET

- http ://w w w .europarl.eu.int/committees/en/default.htm
- http://www.ecomputerlaw.com/articles/show_article.php?article=2002_web_bugs
  LIGJE PËR TEKNOLIGJINE KOMPJUTERIKE, BLOG, ARTIKUJ SHKENCORË
- http://w2.eff.org/Privacy/Marketing/web_bug.html
  FAQE ZYRTARE E FONDACIONIT TË KUFIJVE ELEKTRONIK
- http://www.cdt.org/privacy/031100 spyware.pdf
  QENDRA PËR DEMOKRACI DHE TEKNOLOGJI
- http:/www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37eng.pf
- http://www.vanemery.com/Protocols/SMTP/smtp.html
  FAQE INTERNETI PËR TË DHËNAT E LIDHJEVE DHE INFOVE TË RRJETEVE DHE LIDHJEVE DHE INFOVE TË SISTEMEVE
- http://en.wikipedia.org/wiki/Mailing_list
  ENCIKLOPEDIA ONLINE NË INTERNET
- http://www.newsgroups.com/
  FAQE INTERNETI PËR GRUPET E DISKUTIMIT ONLINE
- http://www.akshi.gov.al/Rregullore/rregullore_per_faqet_zyrtare_te_internetit_te_administrates_publike.pdf
  AGJENCIA KOMBËTARE E SHOQËRISË SE INFORMACIONIT NË SHQIPËRI
- http :// www .icsi.berkeley.edu /gfx/nav/logo.gif
  INSTITUTI NDËRKOMBËTAR I SHKENCAVE KOMPJUTERIKE NË UNIVERSITETIN BERKELEY-KALIFORNI
- http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/3746023.stm (21-11-05)
  FAQE ZYRTARE E KORPORATËS TRANSMETUESE TË LAJMEVE BRITANIKE
- http://europa.eu.int/eurlex/lex/lexuriserv/site/el/com/2004/com2004_0028el01.dc
- http://www.oecd.org
  FAQE ZYRTARE E ORGANIZATËS PËR BASHKËPUNIM EKONOMIK DHE ZHVILLIM
- http://europa.eu.int/rapid/pressReleasesAction.do?Reference=SPEECH/04/55&ormat=HTML &aged= 0&language = EN & g uiLanguage=en 23-9-2005
- http://www.unhchr.ch/udhr/lang/eng.htm

ZYRA E KOMISIONERIT TË LARTË PËR TË DREJTAT E NJERIUT NË OKB

- http://www.unhchr.ch/html/menu3/b/a_ccpr.htm
- http://www.ohchr.org/english/law/ccpr.htm
  ZYRA E KOMISIONERIT TË LARTË PËR TË DREJTAT E NJERIUT NË OKB
- http://www.ohchr.org/english/bodies/hrc/index.htm
- http://www .anu.edu.au/people/Roger.Clarke/DV/PP21C.html
  FAQE ZYRTARE E UNIVERSITETIT TË AUSTRALISË
- http://www.oecd.org/document/18/02340es_2649_34255_1815186_1_1_1_1,00.html
- http://www.unhchr.ch/html/menu3/b/a_ccpr.htm
- http://www.cidh.org/Basicos/English/Basic3.American%20Convention.html
  FAQE ZYRTARE E KOMISIONIT INTER-AMERIKAN MBI TË DREJTAT E NJERIUT
- http://www.achpr.org/english/_info/charter_en.html
  FAQE ZYRTARE E KOMISIONIT AFRIKAN PËR TË DREJTAT E NJERIUT DHE POPUJVE
- http://www1.umn.edu/humanrts/instree/loas2005.html?msource=UNWDEC19001&tr=y&auid =3337655
  FAQE ZYRTARE E UNIVERSITETIT TË MINNESOTA
- http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=00157887#{%22itemid%22:[%22001-57887%22]}
  ÇËSHJE GJYQËSORE TË GJEND
- http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{%22dmdocnumber%22:[%22843777%22],%22itemid%22:[%22001-89964%22]}
- http://hudoc.ech.coe.int/sites/eng/pages/search.aspx#{%22dmdocnumber%22:[%22696374%22],%22itemid%22:[% 22001-58497%22]}
- http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{%22dmdocnumber%22:[%22695387%22],%22itemid%22:[%22001-57510%22]}
- http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{%22dmdocnumber%22:[%22793888%22],%22itemid%22:[%2200173049%22]}
- http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-

58039#{%22itemid%22: [% 2 2 0 01-58039%22]}

- http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{%22dmdocnumber%22:[%22696374%22],%22itemid%22:[%2200158497%22]}

- http://www.garanteprivacy.it/garante/document
  FAQE INTERNETI PËR LIGJISLACIONIN ITALIAN NË MBROJTJEN E TË DHËNAVE PERSONALE

- http://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/KU%20v%20Finland%20en%20presse.pdf
  FAQE ZYRTARE E KËSHILLIT TË EVROPËS

- http://www.mpp-rdg.mpg.de/pdf_dat/burkert.pdf
  ARTIKULL SHKENCOR ONLINE

- http://www.itkommissionen.se/dynamaster/file_archive/030121/991899fe86e3aecaa92d4e5730148f50/5.1%20%20Security%20and%20Vulnerability%20-%20S%F6ren%20% D6man.pdf
  FAQE ZYRTARE E KOMISIONIT TË IT NË SUEDI

- http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm
  FAQE ZYRTARE E KËSHILLIT TË EVROPËS ME TRAKTATET PËRKATËS

- http://www.kmdp.al/web/KMDP_151_1.php
  FAQE ZYRTARE E KOMISIONERIT PËR TË DREJTËN E INFORMIMIT DHE MBROJTJEN E TË DHËNAVE PERSONALE NË SHQIPËRI

- http://europa.eu.int/comm/justice_home/unit/charte/index_en.html

- http://weis2006.econinfosec.org/docs/34.pdf
  WORKSHOP I PESTË MBI EKONOMINË E SIGURISË SË INFORMACIONIT (WEIS 2006). KOLEGJI ROBINSON, UNIVERSITETI I KEMBRIXHIT, ANGLI.

- http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003R2201:IT:HTML
  GAZETA ZYRTARE E BASHKIMIT EVROPIAN

- http://www.export.gov/safeharbor/SH_Overview.asp
  FAQE INTERNETI QË NDIHMON BIZNESIN AMERIKAN TË MARRI PJESË NË TREGUN GLOBAL ME INFORMACION MBI NGJARJET TREGTARE, TARIFAT DHE ASISTENCËN E KËSHILLIMIT TË EKSPORTIT

- http://law.vanderbilt.edu/journals/journal/35-02/Salbu10.pdf
  FAQE ZYRTARE E SHKOLLËS SË TË DREJTËS VANDERBILT-SHBA

- http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:C2006/17O
- http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0492
- http://europeonthestrand.ideasoneurope.eu/2010/07/07/eu-usagreementonswift-bank-data-transfer/
  "IDEA PËR EVROPËN" ËSHTË NJË BLOG HOSTING I CILI OFRON NJË FORUM TË PAVARUR PËR ANALIZA, INFORMACIONE, KOMENTE DHE DEBATE
- http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:195:000: EN:PDF
- http://www.edri.org/files/SWIFT-FAQ-2010-02-09.pdf
  FAQE ZYRTARE E NJË SHOQATË NDËRKOMBËTARE JOFITIM-PRURËSE PËR MBROJTJEN E LIRISË DIGITALE
- http://eurobserver.com/22/32010
  EUROBSERV'ER ËSHTË BAROMETRI PËR PROGRESIN E BËRË NË ÇDO SEKTOR DHE NË ÇDO SHTET ANËTAR TË BASHKIMIT EVROPIAN
- http://www.edri.org/edrigram/number9.5/swift-agreementdatprotection-safeguards
- http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000X1218(01):ENG:HTML
- http://europa.eu/legislation_summaries/glossary/index_e_en.htm
- http://europa.eu/scadplus/glossary/charter_fundamental_rights_el.htm
- www.fd.uc.pt/igc/pdf/papers/john_morjin.pdf
  FAQE ZYRTARE E QENDRËS SË TË DREJTAVE TË NJERIUT PORTUGALI
- http//www.dps.eu.int /legislation/05-09-16_ Montreux _declaration_EN.pdf
  FAQE ZYRTARE E E SAMITIT TË BOTIMEVE TË DITËS DIXHITALE EVROPË
- https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobCmdB&InstranetImage=276580&SecMode=1&DocId=396826&Usage=2
  KOMITETI I MINISTRAVE - KONVENTA E KËSHILLIT TË EVROPËS PËR PARANDALIMIN DHE LUFTËN KUNDËR DHUNËS NDAJ GRAVE DHE DHUNËS NË FAMILJE

- http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp44en.pdf
- http://eurlex. Europa.eu/el/treaties/dat/12002E/htm/C_ 200 23 25 EN . 0 0 3 3 01.html/
- http://www.edps.europa.eu
  FAQE ZYRTARE E SUPERVIZORIT EVROPIAN TË MBROJTJES SË TË DHËNAVE PERSONALE
- http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML
- http://aei.pitt.edu/ 983/01/telecom _convergence_gp _follow_COM _99_ 108.pdf
  ARSHIVA ELEKTRONIKE E INTEGRIMIT EVROPIAN, UNIVERSITETI I PITTSBURGH
- http://europa.eu/ scadplus /leg/el/lvb/l24216.htm
- http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:321E:0001:0331:EN:PDF
- http://www.vorratsdatenspeicherung.de/content/view/16/39/lang,en/
  FAQE INTERNETI PËR SIGURINË E BURIMEVE TË HAPURA NE WEB
- http://www.warwick.ac.uk/fac/soc/law2/elj/jilt/2004_3/rowland/
- http://www.spiegel.de/international/germany/0,1518,681251,00.html (02.03.2010)
  GAZETË E PËRDITSHME GJERMANE
- http://www.datatilsynet.no/upload/Dokumenter/dommer/pressrelease_dataretentida_bundesverf assungsgericht.pdf
  FAQE ZYRTARE E AUTORITETIT NORVEGJEZ PËR MBROJTJEN E TË DHËNAVE PERSONALE
- http://ec.europa.eu/commission_20102014/malmstrom/archive/20110418_data_retention_evaluati on_en.pdf
- http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/484format=HTML&aged=0&lang uage =EL&g ui Langu age=fr
- http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/280&formt=HTML&aged=0&language=EN&guiLanguage=en

- http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0229: ENG:NOT
- http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_eng.pdf
- http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp159_eng.pdf
- http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_el.pdf(14.01.2010)
- http://www.washingtonpost.com/wp-srv/politics/special/watergate/#chapters(20-5-2009)
  GAZETË E PËRDITSHME AMERIKANE
- http://www.kmdp.al/index.php/sq/legjislacioni/akte-komisionerit/udhezime
- http://www.data.planetar.edu.al
  FAQE ZYRTARE E UNIVERSITETIT PLNETAR TIRANË
- http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/ wp168_en.pdf
- http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/441
- http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_el.pdf
- http://www.consilium.Europa.eu/uedocs/cmsdata/docs/pressdata/en/jha/119461.pdf
- https://www.privacyinternational.org/