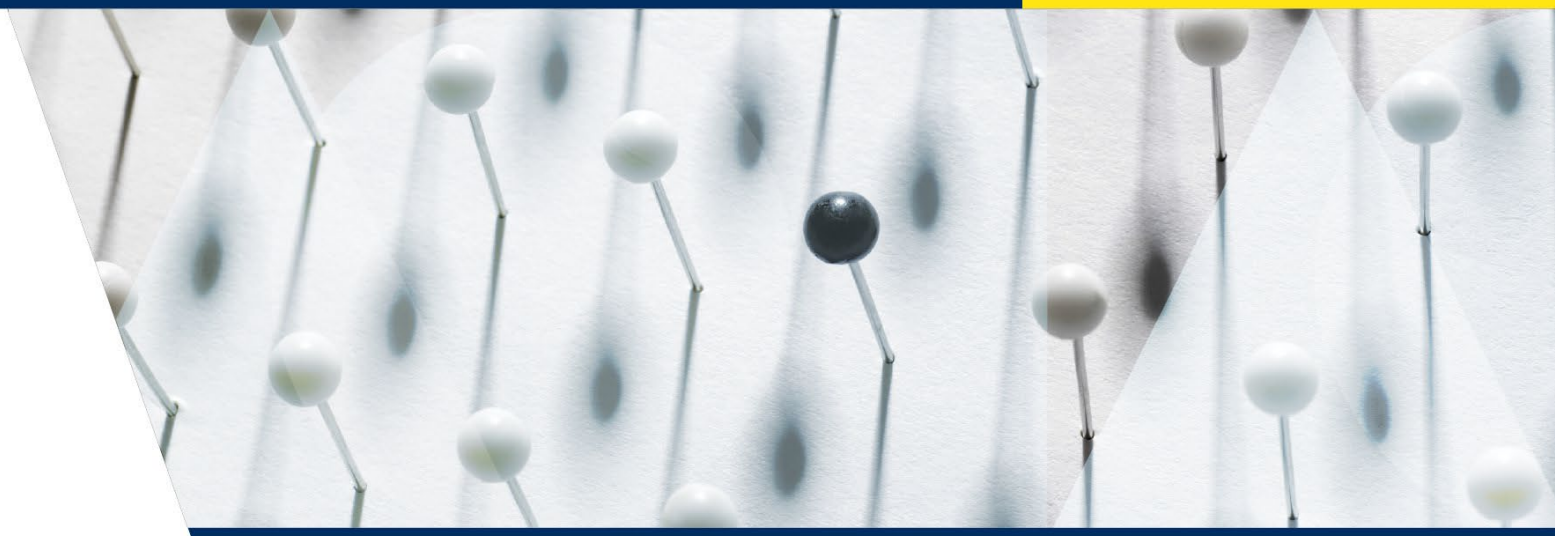
MANUAL



Manual i së drejtës evropiane në fushën e mbrojtjes së të dhënave

botimi 2018

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Dorëshkrimi i këtij Manuali u përfundua në prill të 2018-ës.

Variante të përditësuara do të publikohen në të ardhmen në faqen e internetit të FRA-së: fra.europa.eu, në faqen e internetit të Këshilli të Evropës: coe.int/dataprotection dhe në faqen e internetit të Gjykatës Evropiane të së Drejtave të Njeriut, në rubrikën "Jurisprudenca": ecur.coe.int, dhe në faqen e internetit të Mbikëqyrësit Evropian të Mbrojtjes së të Dhënave: edps.europa.eu.

Fotografitë (kopertina dhe në brendësi): © iStockphoto

Përkthimi në gjuhën shqipe u realizua nga Z. Eldor Budo, Zyra e Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale. FRA nuk mban përgjegjësi për këtë përkthim.

ISBN 978-9928-4481-0-1 (KDIMDP)

Printuar në Tiranë

Printuar në letër të ricikluar pa përmbajtje klori (PCF)

Manual i së drejtës evropiane
në fushën e mbrojtjes
së të dhënave

botimi 2018

Parathënie

Shoqëritë tona po bëhen gjithnjë e më digjitale. Ritmi i zhvillimeve teknologjike dhe i mënyrës së përpunimit të të dhënave personale, na prek të gjithëve çdo ditë dhe në gjithfarë mënyre, për shkak të këtyre ndryshimeve. Kuadri ligjor i Bashkimit Evropian (BE) dhe i Këshillit të Evropës i cili mbikëqyr mbrojtjen e privatësisë dhe të së dhënave personale është rishikuar kohët e fundit.

Evropa është pararoja e mbrojtjes së të dhënave për të gjithë botën. Normat e mbrojtjes së të dhënave të BE-së mbështeten në Konventën 108 të Këshillit të Evropës, instrumentet e BE-së, përfshirë Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave dhe Direktivën e Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale, ashtu si edhe mbi jurisprudencën përkatëse të Gjykatës Evropiane të së Drejtave të Njeriut dhe të Gjykatës së Drejtësisë së Bashkimit Evropian.

Reformat e mbrojtjes së të dhënave që zhvilluan BE-ja dhe Këshilli i Evropës kanë shtrirje të gjerë dhe janë ndonjëherë të ndërlikuara. Ky manual synon të ndërgjegjësojë dhe të shtojë njohuritë mbi rregullat e mbrojtjes së të dhënave, sidomos të juristëve që nuk janë specialistë të fushës, të cilët përballen me çështje të mbrojtjes së të dhënave në punën e tyre.

Manuali është përgatitur nga Agjencia e Bashkimit Evropian për të Drejtat Themelore (FRA), nga Këshilli i Evropës (së bashku me Zyrën e Kancelarit të Gjykatës Evropiane të së Drejtave të Njeriut) dhe nga Mbikëqyrësi Evropian i Mbrojtjes së të Dhënave. Ky manual përditëson botimin e vitit 2014 dhe bën pjesë në një seri manualësh ligjorë, të përgatitur bashkërisht nga FRA-ja dhe nga Këshilli i Evropës.

Ne u shprehim falënderimet tona autoriteteve të mbrojtjes së të dhënave të Belgjikës, Estonisë, Francës, Gjeorgjisë, Hungarisë, Irlandës, Italisë, Monakos, Zvicrës dhe Mbretërisë së Bashkuar për ndihmën e tyre të çmuar në hartimin e variantit paraprak të manualit. Gjithashtu, ne i shprehim mirënjohjen Njësisë së Mbrojtjes së të Dhënave të Komisionit Evropian dhe Njësisë së saj të Qarkullimit dhe Mbrojtjes Ndërkombëtare të të Dhënave. Falënderojmë Gjykatën e Drejtësisë së Bashkimit Evropian për mbështetjen me dokumentacion të dhënë gjatë punimeve përgatitore të këtij manuali.

Christos Giakoumopoulos Drejtor i Përgjithshëm i të Drejtave të Njeriut dhe Sundimit të Ligjit të Këshillit të Evropës	Giovanni Buttarelli Mbikëqyrësi Evropian i Mbrojtjes së të Dhënave	Michael O'Flaherty Drejtori i Agjencisë së Bashkimit Evropian për të Drejtat Themelore

Përmbajtja

PARATHËNIE 3

SHKURTIME DHE AKRONIME 10

SI TA PËRDORIM KËTË MANUAL? ..... **Error! Bookmark not defined.**

1. KONTEKSTI DHE SFONDI I SË DREJTËS EVROPIANE NË FUSHËN E MBROJTJES SË TË DHËNAVE 16

1.1. E drejta për mbrojtje të të dhënave personale 20

Pikat kryesore 20

1.1.1. E drejta për respektim të jetës private dhe e drejta për mbrojtje të të dhënave personale: një përshkrim i shkurtër 20

1.1.2. Kuadri ligjor ndërkombëtar: Kombet e Bashkuara.. **Error! Bookmark not defined.**

1.1.3. Konventa Evropiane e të Drejtave të Njeriut..... **Error! Bookmark not defined.**

1.1.4. Konventa 108 e Këshillit të Evropës

1.1.5. Legjislacioni i mbrojtjes së të dhënave të Bashkimit Evropian

1.2. Kufizime të së drejtës për mbrojtje të të dhënave personale 35

Pikat kryesore

1.2.1. Kriteret për ndërhyrje të justitifkuar sipas KEDNJ-së..... **Error! Bookmark not defined.**

1.2.2. Kushtet për kufizime të ligjshme sipas Kartës së të Drejtave Themelore të BE-së ..... **Error! Bookmark not defined.**

1.3. Ndërveprimi me të drejta dhe interesa të tjera legjitime

Pikat kryesore

1.3.1 Liria e shprehjes

1.3.2 Fshehtësia profesionale

1.3.3 Liria e fesë dhe besimit

1.3.4 Liria e arteve dhe shkencave

1.3.5. Mbrojtja e pronësisë intelektuale

1.3.6. Mbrojtja e të dhënave dhe interesave ekonomikë

2. TERMINOLOGJIA E MBROJTJES SË TË DHËNAVE 69

2.1. Të dhënat personale 72

Pikat kryesore 72

2.1.1. Aspektet kryesore të konceptit të të dhënave personale 73

2.1.2. Kategoritë e veçanta të të dhënave personale 83
2.2. Përpunimi i të dhënave 84
Pikat kryesore
2.2.1 Koncepti i përpunimit të të dhënave
2.2.2 Përpunimi automatik i të dhënave
2.2.3 Përpunimi jo-automatik i të dhënave
2.3. Përdoruesit e të dhënave personale 87
Pikat kryesore 87
2.3.1. Kontrolluesit dhe përpunuesit 87
2.3.2. Marrësit dhe palët e treta 94
2.4. Pëlqimi 95
Pikat kryesore 95
3. PARIMET THEMELORE TË SË DREJTËS EVROPIANE NË FUSHËN E MBROJTJES SË TË DHËNAVE ..... Error! Bookmark not defined.
3.1. Parimet e përpunimit të ligjshëm, të drejtë dhe transparent ..... **Error! Bookmark not defined.**
Pikat kryesore ..... **Error! Bookmark not defined.**
3.1.1. Përpunimi i ligjshëm ..... **Error! Bookmark not defined.**
3.1.2. Përpunimi i drejtë ..... **Error! Bookmark not defined.**
3.1.3. Përpunimi transparent
3.2. Parimi i kufizimit të qëllimit ..... **Error! Bookmark not defined.**
Pikat kryesore ..... **Error! Bookmark not defined.**
3.3. Parimi i minimizimit të të dhënave ..... **Error! Bookmark not defined.**
Pikat kryesore ..... **Error! Bookmark not defined.**
3.4. Parimi i saktësisë së të dhënave ..... **Error! Bookmark not defined.**
Pikat kryesore ..... **Error! Bookmark not defined.**
3.5. Parimi i kufizimit të mbajtjes së të dhënave ..... **Error! Bookmark not defined.**
Pikat kryesore ..... **Error! Bookmark not defined.**
3.6. Parimi i sigurisë së të dhënave
Pikate kryesore
3.7. Parimi i përgjegjshmërisë
Pikat kryesore
4. RREGULLAT E SË DREJTËS EVROPIANE NË FUSHËN E MBROJTJES SË TË DHËNAVE ..... Error! Bookmark not defined.

4.1. Rregullat e përpunimit të ligjshëm 139
Pikat kryesore 139
4.1.1. Bazat ligjore për përpunimin e të dhënave ..... **Error! Bookmark not defined.**
4.1.2. Përpunimi i kategorive të veçanta të të dhënave (të dhënat sensitive) ..... **Error! Bookmark not defined.**
4.2 Rregullat në lidhje me sigurinë e përpunimit ..... **Error! Bookmark not defined.**
Pikat kryesore ..... **Error! Bookmark not defined.**
4.2.1. Elementet e sigurisë së të dhënave ..... **Error! Bookmark not defined.**
4.2.2. Konfidencialiteti ..... **Error! Bookmark not defined.**
4.2.3 Njoftimet për shkeljet ndaj të dhënave personale
4.3. Rregullat në lidhje me përgjegjshmërinë dhe nxitjen e përputhshmërisë ..... **Error! Bookmark not defined.**
Pikat kryesore ..... **Error! Bookmark not defined.**
4.3.1. Nëpunësit e Mbrojtjes së të Dhënave ..... **Error! Bookmark not defined.**
4.3.2. Regjistrimi i aktiviteteve përpunuese ..... **Error! Bookmark not defined.**
4.3.3. Vlerësimet e ndikimit tek mbrojtja e të dhënave dhe konsultimet paraprake
4.3.4. Kodet e sjelljes
4.3.5 Certifikimi
4.4. Mbrojtja e të dhënave që në fazën e konceptimit dhe me parapërzgjedhje..... **Error! Bookmark not defined.**
Pikat kryesore ..... **Error! Bookmark not defined.**
5. MBIKËQYRJA E PAVARUR..... Error! Bookmark not defined.
Pikat kryesore
5.1. Pavarësia ..... **Error! Bookmark not defined.**
5.2. Kompetencat dhe tagrat
5.3. Bashkëpunimi
5.4. Bordi Evropian i Mbrojtjes së të Dhënave
5.5. Mekanizmi i Njëtrajtshmërisë sipas GDPR-së
6. TË DREJTAT E SUBJEKTEVE DHE ZBATIMI I TYRE ..... Error! Bookmark not defined.
6.1. Të drejtat e subjekteve të të dhënave ..... **Error! Bookmark not defined.**
Pikat kryesore ..... **Error! Bookmark not defined.**
6.1.1. E drejta për t'u informuar ..... **Error! Bookmark not defined.**
6.1.2. E drejta për korrigjim

6.1.3. E drejta e fshirjes ("e drejta për t'u harruar")

6.1.4. E drejta e kufizimit të përpunimit

6.1.5. E drejta e transferueshmërisë së të dhënave

6.1.6. E drejta për të kundërshtuar

6.1.7. Vendim-marrja individuale e automatizuar, përfshirë profilizimin

6.2. Mjetet juridike, përgjegjësia, penalitetet dhe kompensimi **Error! Bookmark not defined.**

Pikat kryesore ..... **Error! Bookmark not defined.**

6.2.1. E drejta për të paraqitur ankesë tek autoriteti mbikëqyrës ..... **Error! Bookmark not defined.**

6.2.2. E drejta për një mjet mbrojtës gjyqësor efikas ..... **Error! Bookmark not defined.**

6.2.3. Përgjegjësia dhe e drejta për kompensim

6.2.4. Sanksionet

7. TRANSFERIMET DHE QARKULLIMET NDËRKOMBËTARE TË TË DHËNAVE PERSONALE ..... Error! Bookmark not defined.

7.1. Natyra e transferimeve të të dhënave personale..... **Error! Bookmark not defined.**

Pikat kryesore ..... **Error! Bookmark not defined.**

7.2. Lëvizja/qarkullimi i lirë i të dhënave personale ndërmjet Shteteve Anëtare, ose Palëve Kontraktuese ..... **Error! Bookmark not defined.**

Pikat kryesore

7.3. Transferimet e të dhënave personale drejt vendeve të treta/vendeve që nuk janë palë, ose organizatave ndërkombëtare

Pikat kryesore

7.3.1. Transferimet mbi bazën e një vendimi përshtatshmërie

7.3.2. Transferimet me garanci të mjaftueshme

7.3.3. Përjashtimet në situata të caktuara

7.3.4. Transferimet bazuar në marrëveshje ndërkombëtare

8. MBROJTJA E TË DHËNAVE NË KONTEKSTIN E POLICISË DHE DREJTËSISË PENALE ..... Error! Bookmark not defined.

8.1. E drejta e KiE-së në fushën e mbrojtjes së të dhënave në lidhje me çështje të sigurisë kombëtare, policisë dhe drejtësisë penale ..... **Error! Bookmark not defined.**

Pikat kryesore ..... **Error! Bookmark not defined.**

8.1.1. Rekomandimi për policinë

8.1.2. Konventa e Budapestit mbi Krimin Kibernetik

8.2. E drejta e BE-së në fushën e mbrojtjes së të dhënave në lidhje me policinë dhe drejtësinë penale ..... **Error! Bookmark not defined.**

Pikat kryesore ..... **Error! Bookmark not defined.**

8.2.1. Direktiva e Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale

8.3. Intrumente të tjera ligjore specifike të mbrojtjes së të dhënave për çështje të zbatimit të ligjit ..... **Error! Bookmark not defined.**

8.3.1. Mbrojtja e të dhënave në agjencitë gjyqësore dhe ligjzbatuese të BE-së

8.3.2. Mbrojtja e të dhënave në sistemet e përbashkëta të informacionit në nivel BE-je

9. LLOJE TË VEÇANTA TË DHËNASH DHE RREGULLAT PËRKATËSE TË MBROJTJES SË TË DHËNAVE

9.1. Komunikimet elektronike

Pikat kryesore

9.2. Të dhënat e punësimit

Pikat kryesore

9.3. Të dhënat e shëndetit

Pikat kryesore

9.4. Përpunimi i të dhënave për qëllime kërkimore dhe statistikore

Pikat kryesore

9.5. Të dhënat financiare

Pikat kryesore

10. SFIDAT MODERNE TË MBROJTJES SË TË DHËNAVE PERSONALE

10.1.1. Të dhënat masive, algoritmet dhe inteligjenca artificiale

10.1.2. Ekuilibrimi i përfitimeve dhe risqeve të të dhënave masive

10.1.3. Problematika në lidhje me mbrojtjen e të dhënave

10.2. Web-et 2.0 dhe 3.0: rrjetet sociale dhe Objektet e Lidhura në Internet

10.2.1. Përkufizimi i web-it 2.0 dhe 3.0

10.2.2. Ekuilibrimi i përfitimeve dhe risqeve

10.2.3. Problematika në lidhje me mbrojtjen e të dhënave

LEXIME PLOTËSUESE ..... **Error! Bookmark not defined.**

JURISPRUDENCA..... **Error! Bookmark not defined.**

Jurisprudencë e përzgjedhur e Gjykatës Evropiane të të Drejtave të Njeriut **Error! Bookmark not defined.**

Jurisprudencë e përzgjedhur e Gjykatës së Drejtësisë së Bashkimit Evropian.....**Error! Bookmark not defined.**

Shkurtime dhe akronime

APK Autoritete të përbashkëta kontrolli

BCR Rregullat e Detyrueshme të Korporatave

BE Bashkimi Evropian

CCTV Televizion me qark të mbyllur

C-SIS Sistemi Qendror i Informacionit të Schengen-it

DPA Autoriteti i Mbrojtjes së të Dhënave

DPO Nëpunës i Mbrojtjes së të Dhënave

DUDNJ Deklarata Universale e të Drejtave të Njeriut

EDPB Bordi Evropian i Mbrojtjes së të Dhënave

EDPS Mbikëqyrësi Evropian i të Dhënave Personale

EFSA Autoriteti Evropian i Sigurisë Ushqimore

EFTA Shoqata evropiane e shkëmbimeve të lira

eu-LISA Agjencia e Bashkimit Evropian për Menaxhimin e Sistemeve TI në Shkallë të Gjerë

ENISA Agjencia Evropiane për Sigurinë e Rrjeteve dhe të Informacionit

ENU Njësi Kombëtare Europol-i

EPPO Zyra e Prokurorit Evropian

ESMA Autoriteti Evropian i Tregjeve Financiare

eTEN Rrjetet Trans-evropiane të Telekomunikacioneve

EuroPriSe Certifikimi Evropian i Mbrojtjes së të Dhënave

FRA Agjencia e Bashkimit Evropian për të Drejtat Themelore

FZ Fletore Zyrtare

GDPR Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave

GPS Sistem Global Lokalizimi

GJDBE Gjykata e Drejtësisë së Bashkimit Evropian (përpara dhjetorit 2009, Gjykata e Drejtësisë së Komunitetit Evropian, GJED)

GJEDNJ Gjykata Evropiane e të Drejtave të Njeriut

GKM Grup i Koordinimit të Mbikëqyrjes

HEE Hapësira Ekonomike Evropiane

TIK Teknologji Informacioni dhe Komunikimi

ISP Operator Shërbimi Interneti

Karta Karta e të Drejtave Themelore të Bashkimit Evropian

KiE Këshilli i Evropës

KE Komuniteti Evropian

KEDNJ Konventa Evropiane e të Drejtave të Njeriut

Konventa 108 Konventa për mbrojtjen e personave në lidhje me përpunimin automatik të të dhënave personale (Këshilli i Evropës).

Protokolli i Amendimeve (CETS nr. 223) i Konventës 108 u miratua nga Komiteti i Ministrave të Këshillit të Evropës më 18 maj 2018, në sesionin e 128-të të mbajtur në Elsinore të Danimarkës. Togfjalëshi "Konventa 108 e Modernizuar" i referohet Konventës së ndryshuar me Protokollin CETS nr. 223.

LTKiE Lista e Traktateve të Këshillit të Evropës

MAE Urdhër Arresti Evropian

MMK Menaxhimi i Marrëdhënieve me Klientët

N-SIS Sistem Kombëtar Informacioni të Schengen-it

OECD Organizata për Bashkëpunim dhe Zhvillim Ekonomik

OJQ Organizatë Jo-qeveritare

OKB Organizata e Kombeve të Bashkuara

PNDCP Pakti Ndërkombëtar për të Drejtat Civile dhe Politike

PIN Numër Identifikimi Personal

PNR Regjistri i Emrave të Pasagjerëve

SEPA Zona e Unifikuar e Pagesave në Euro

SID Sistem Informacioni Doganor

SIS Sistem Informacioni i Schengen-it

SWIFT Shoqata Botërore e Telekomunikimit Ndër-bankar

TFBE Traktati i Funksionimit të Bashkimit Evropian

TBE Traktati i Bashkimit Evropian

VIS Sistem Informacioni i Vizave

Si ta përdorim këtë manual?

Ky manual zbërthen në hollësi normat ligjore të mbrojtes së të dhënave, të miratuara nga Bashkimi Evropian (BE) dhe Këshilli i Evropës (KiE). Manuali është konceptuar në mënyrë të tillë, që të ndihmojë juristët që nuk janë specialistë të fushës së mbrojtjes së të dhënave, avokatët, gjyqtarët dhe të tjerë që kryejnë veprimtari në fushën e së drejtës, ashtu si edhe ata të cilët punojnë për organizma të tjerë, sikurse për organizatat jo-qeveritare (OJQ-të), të cilët mund të hasin problematika ligjore që kanë të bëjnë me mbrojtjen e të dhënave.

Manuali shërben si një pikë e parë referimi për të drejtën në fushën e mbrojtjes së të dhënave të BE-së dhe Konventën Evropiane të së Drejtave të Njeriut (KEDNJ), ashtu si edhe për Konventën e KiE-së për Mbrojtjen e Personave nga Përpunimi Automatik i të Dhënave Personale (Konventa 108) dhe instrumentet e tjera ligjore të KiE-së.

Secili kapitull, paraqet fillimisht një tabelë që përmbledh dispozitat ligjore në fuqi, që kanë të bëjnë me temat që trajtohen në secilin kapitull. Tabelat mbulojnë të drejtën e KiE-së dhe të BE-së dhe përfshijnë jurisprudencë të përzgjedhur të Gjykatës Evropiane të të Drejtave të Njeriut (GJEDNJ) dhe Gjykatës së Drejtësisë së Bashkimit Evropian (GJDBE). Më pas paraqiten ligjet përkatëse të dy rendeve të ndryshme evropiane, se si ato zbatohen për temat e caktuara që trajtohen. Kjo i mundëson lexuesve të shohin se ku përputhen dhe ku ndryshojnë këto dy sisteme ligjore, si dhe të gjejnë informacione të rëndësishme që lidhet me situatën e tyre, sidomos nëse ata janë subjekte vetëm të legjislacionit të KiE-së. Në disa kapituj, kur është e nevojshme për të ndihmuar në prezantimin e përmbajtjes, rendi i temave në tabela mund të ndryshojë pak nga ai në vijim brenda kapitullit. Manuali ofron gjithashtu një shikim të shkurtër të përgjithshëm të kuadrit të Kombeve të Bashkuara.

Juristët nga shtetet jo anëtare të BE-së, të cilat janë shtete anëtare të KiE-së dhe aderojnë në GJEDNJ dhe në Konventën 108, mund të konsultojnë informacionin që ka të bëjë me vendet e tyre, duke vizituar drejtpërdrejt seksionet që lidhen me KiE-në. Juristët nga shtetet jo anëtare të BE-së duhet gjithashtu të kenë parasysh se me miratimin e Rregullores së Mbrojtjes së të Dhënave të BE-së, rregullat e mbrojtjes së të dhënave të BE-së zbatohen për organizatat dhe njësitë e tjera të cilat nuk janë të vendosura në BE, nëse përpunojnë të dhëna personale dhe u ofrojnë mallra e shërbime subjekteve të të dhënave në Bashkim, apo nëse monitorojnë sjelljen e këtyre subjekteve të të dhënave.

Juristët nga Shtetet Anëtare të BE-së duhet t'u referohen të dyja seksioneve, duke qenë se këto shtete u nënshtrohen të dy rendeve juridike. Vlen të theksohet se reformat dhe modernizimi i rregullave të mbrojtjes së të dhënave në Evropë u zhvilluan paralelisht, si për sa i përket kuadrit të Këshillit të Evropës (Konventa 108 e modernizuar, e ndryshuar me Protokollin CETS nr. 223) dhe të BE-së (miratimi i Rregullores së Përgjithshme të Mbrojtjes së të Dhënave dhe Direktivës 2016/680/BE). Autoritetet rregullatore të të dy sistemeve ligjore janë kujdesur së tepërmi që të garantojnë njëtrajtshmëri dhe përputhshmëri midis të dy kuadrove ligjorë. Në këtë mënyrë, reformat kanë harmonizuar më tej të drejtën në fushën e mbrojtjes së të dhënave në KiE dhe në BE. Për lexuesit që kanë nevojë për më tepër informacion në lidhje me një

çështje të caktuar, mund të shkojnë tek seksioni "Lexo më shumë" i manualit, ku mund të gjejnë një listë referencash me materiale më të specializuara. Për informacion në lidhje me dispozitat e Konventës 108 dhe Protokollit shtesë të saj të vitit 2001, lexuesit duhet t'i referohen edicionit të 2014-ës së këtij manuali.

E drejta e KiE-së paraqitet në formën e referencave të shkurtra, që kanë të bëjnë me çështje të Gjykatës Evropiane të së Drejtave të Njeriut (GJEDNJ), të cilat janë përzgjedhur nga një numër i madh gjykimesh e vendimesh ekzistuese të GJEDNJ-së në lidhje me çështje të mbrojtjes së të dhënave.

E drejta e BE-së mbështetet në masa legjislative të miratuara, në dispozitat përkatëse të traktateve dhe të Kartës së të Drejtave Themelore të Bashkimit Evropian, sikurse janë interpretuar në jurisprudencën e GJDBE-së. Gjithashtu, manuali paraqet opinione dhe udhëzues të miratuar nga Grupi i Punës së Nenit 29, organi këshillimor i ngritur nga Direktiva e Mbrojtjes së të Dhënave, për të këshilluar Shtetet Anëtare të BE-së me ekspertizën e tij. Ai do të zëvendësohet nga Bordi Evropian i Mbrojtjes së të Dhënave (EDPB) që nga data 25 maj 2018 e në vijim.

Jurisprudenca e përshkruar, apo cituar në këtë manual, ofron shembuj të nxjerrë nga korpusi i rëndësishëm i jurisprudencës së GJEDNJ-së dhe GJDBE-së. Udhërrëfyesi në fund të këtij manuali, ka për qëllim të ndihmojë lexuesin që të kërkojë jurisprudencën në internet. Jurisprudenca e GJDBE-së e paraqitur lidhet me Direktivën e mëparshme të Mbrojtjes së të Dhënave. Gjithsesi, interpretimet e GJDBE-së mbeten të zbatueshme me të drejtat dhe detyrimet përkuese të përcaktuara nga Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave.

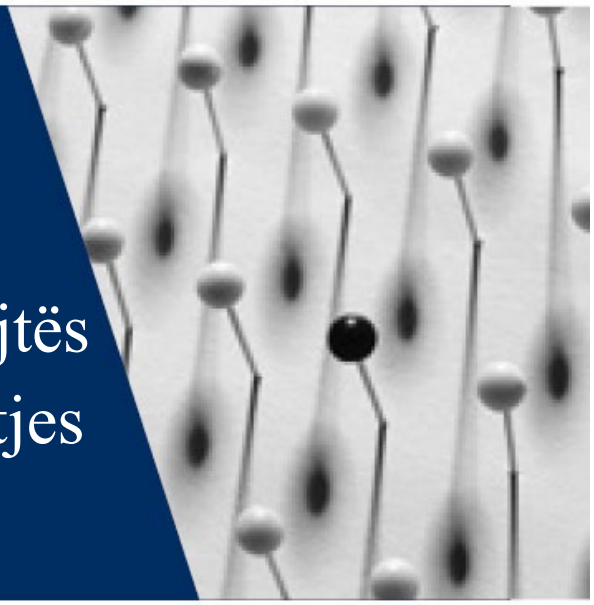
Gjithashtu, janë paraqitur shembuj konkretë dhe skenarë hipotetikë, brenda kutive me sfond blu, të cilat kanë për qëllim të ilustrojnë zbatimin në praktikë të rregullave evropiane në fushën e mbrojtjes së të dhënave, veçanërisht kur nuk ekziston jurisprudencë specifike nga GJEDNJ-ja apo GJDBE-ja. Kutitë e tjera me sfond gri paraqesin shembuj të marrë nga burime të ndryshme nga jurisprudenca e GJEDNJ-së dhe GJDBE-së, sikurse legjislacioni dhe opinionet e miratuara nga Grupi i Punës së Nenit 29.

Manuali nis me një përshkrim të shkurtër të rolit të të dy sistemeve ligjore, sikurse përcaktohet nga e drejta e GJEDNJ-së dhe e BE-së (Kapitulli 1). Kapitujt 2 deri 8 mbulojnë aspektet në vijim:

- Terminologjia e mbrojtjes së të dhënave;
- Parimet kryesore të së drejtës evropiane në fushën e mbrojtjes së të dhënave;
- Rregullat e së drejtës evropiane në fushën e mbrojtjes së të dhënave;
- Mbikëqyrja e pavarur;
- Të drejtat e subjekteve të të dhënave dhe zbatimi i tyre;
- Transferimet dhe qarkullimet ndërkufitare të të dhënave personale;
- Mbrojtja e të dhënave në kontekstin e policisë dhe drejtësisë penale;
- Rregulla të tjera evropiane të mbrojtjes së të dhënave në fusha të caktuara;
- Sfidat moderne për mbrojtjen e të dhënave personale.

1

Konteksti dhe sfondi i së drejtës evropiane në fushën e mbrojtjes së të dhënave



BE	Çështje të trajtuara	KiE
E drejta për mbrojtje të të dhënave		
Traktati i Funksionimit të Bashkimit Evropian, Neni 16 Karta e të Drejtave Themelore të Bashkimit Evropian (Karta), neni 8 (e drejta për mbrojtje të të dhënave personale) Direktiva 95/46/KE për mbrojtjen e personave fizikë nga përpunimi i të dhënave personale dhe mbi lëvizjen e lirë të këtyre të dhënave (Direktiva për Mbrojtjen e të Dhënave), FZ 1995 L281 (në fuqi deri në maj 2018) Vendimi Kuadër i Këshillit 2008/977/JHA mbi mbrojtjen e të dhënave personale të përpunuara në kontekstin e policisë dhe bashkëpunimit gjyqësore për çështje penale FZ 2008 L 350 (në fuqi deri në maj 2018)		KEDNJ, Neni 8 (e drejta për respektim të jetës private the familjare, të banesës dhe të korrespondencës) Konventa e Modernizuar për mbrojtjen e personave nga përpunimi automatik i të dhënave personale (Konventa 108 e Modernizuar)

Rregullore (BE) 2016/679 mbi mbrojtjen e personave fizikë në lidhje me përpunimin e të dhënave personale dhe për lëvizjen e lirë të këtyre të dhënave dhe shfuqizimin e Direktivës 95/46/KE (Rregullore e Përgjithshme e Mbrojtjes së të Dhënave) FZ 2016 L 119 Direktiva (BE) 2016/680 mbi mbrojtjen e personave fizikë në lidhje me përpunimin e të dhënave personale nga autoritetet kompetente për qëllime të parandalimit, hetimit, zbulimit ose ndjekjes së veprave personale ose ekzekutimin e dënimeve penale dhe mbi lëvizjen e lirë të këtyre të dhënave dhe shfuqizimin e Vendimit Kuadër të Këshillit 2008/977/JHA (Mbrojtja e të Dhënave për Autoritetet Policore dhe të Drejtësisë), FZ 2016 L 119 Direktiva 2002/58/EC në lidhje me përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike (Direktiva mbi privatësinë dhe komunikimet elektronike) FZ 2002 L 201 Rregullorja (KE) nr. 45/2011 mbi mbrojtjen e personale në		

lidhje me përpunimin e të dhënave personale nga institucionet dhe organet e Komunitetit dhe mbi lëvizjen e lirë të këtyre të dhënave (Rregullorja e Mbrojtjes së të Dhënave të Institucioneve të BE-së), FZ 2001 L 8		
Kufizimet e së drejtës për mbrojtje të të dhënave personale		
Karta, neni 52, pika 1 Rregullorja e Mbrojtjes së të Dhënave, neni 23 GJDBE, Çështje të bashkuara C-92/09 dhe C-93/09, *Volker und Markus Schecke GbR* dhe *Hartmut Eifert k. Land Hessen* [GC], 2010		KEDNJ, neni 8, pika 2 Konventa 108 e Modernizuar, neni 11 GJEDNJ, *S. and Marper k. Mbretërisë së Bashkuar* [GC], nr. 30562/04 dhe 30566/04, 2008
Ekuilibrimi i të drejtave		
GJDBE, çështje të bashkuara C-92/09 dhe C-93/09, *Volker und Markus Schecke GbR* dhe *Hartmut Eifert k. Land Hessen*, [GC] 2010	**E përgjithshme**	
GJDBE, C-73/07, *Tietosuojavaltuutettu k. Satakunnan Markkinapörssi Oy dhe Satamedia Oy* [GC], 2008 GJDBE, C-131/12, *Google Spain SL, Google Inc. k. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014	**Liria** **e Shprehjes**	GJEDNJ, *Axel Springer AG k. Gjermanisë* [GC], nr. 39954/08, 2012 GJEDNJ, *Mosley k. Mbretërisë së Bashkuar*, nr. 48009, 2011 GJEDNJ, *Bohlen k. Gjermanisë*, nr. 53495/09, 2015

GJDBE, C-28/08 P, *European Commission k. The Bavarian Lager Co. Ltd* [GC], 2010 GJDBE, C-615/13P, *ClientEarth, PAN Europe k. EFSA*, 2015	**Aksesi në dokumente**	GJEDNJ, *Magyar Helsinki Bizottság k. Hungarisë* [GC], nr. 18030/11, 2016
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 90	**Sekreti profesional**	GJEDNJ, *Pruteanu k. Rumanisë*, nr. 30181/05, 2015
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 91	**Liria e fesë ose e besimit**	
	Liria e arteve dhe shkencave	GJEDNJ, *Vereinigung bildender Künstler k. Austrisë*, nr. 68345/01, 2007
GJDBE, C-275/06, *Productores de Música de España (Promusicae) k. Telefónica de España SAU* [GC], 2008	**Mbrojtja e pronës**	
GJDBE, C-131/12, *Google Spain SL, Google Inc. k. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 GJDBE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce k. Salvatore Manni*, 2017	**Të drejtat ekonomike**	

1.1. E drejta për mbrojtje të të dhënave

Pikat kryesore

- Sipas nenit 8 të KEDNJ-së e drejta e një personi për mbrojtje nga përpunimi i të dhënave personale, bën pjesë tek e drejta për respektim të jetës private dhe familjare, të banesës dhe korrespondencës.
- Konventa 108 e KiE-së është akti i parë ligjor detyrues në nivel ndërkombëtar, i cili trajton në mënyrë të posaçme mbrojtjen e të dhënave. Konventa iu nënshtrua një procesi modernizimi, i cili u plotësua me miratimin e Protokollit të ndryshimit të saj CETS nr. 223.
- Në të drejtën e BE-së, mbrojtja e të dhënave njihet si e drejtë themelore e veçantë, e afirmuar në nenin 16 të Traktatit të Funksionimit të BE-së, si dhe në nenin 8 të Kartës së të Drejtave Themelore të BE-së.
- Në të drejtën e BE-së, mbrojtja e të dhënave u rregullua për herë të parë me anë të Direktivës së Mbrojtjes së të Dhënave më 1995.
- Për shkak të zhvillimeve të shpejta teknologjike, BE-ja miratoi legjislacion të ri në vitin 2016, për të përshtatur rregullat e mbrojtjes së të dhënave në epokën digjitale. Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave të BE-së nisi zbatimin në maj 2018, duke shfuqizuar Direktivën e Mbrojtjes së të Dhënave.
- Bashkë me Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave, BE-ja miratoi legjislacion mbi përpunimin e të dhënave personale nga autoritetet shtetërore, për qëllime ligjzbatuese. Direktiva (BE) 2017/680 përcakton rregullat dhe parimet e mbrojtjes së të dhënave që rregullojnë përpunimin e të dhënave personale për qëllime të parandalimit, hetimit, zbulimit dhe ndjekjes së veprave penale, ose ekzekutimit të dënimeve penale.

1.1.1. E drejta për respektim të jetës private dhe e drejta për mbrojtje të të dhënave personale: një hyrje e shkurtër

E drejta për respektim të jetës private dhe e drejta për mbrojtje të të dhënave personale, edhe pse janë të lidhura ngushtë, janë të drejta të ndryshme. E drejta për privatësi, e cila përcaktohet në legjislacionin evropian si e drejta për respektim të jetës private, u shfaq në legjislacionin ndërkombëtar të të drejtave të njeriut, në Deklaratën Universale të të Drejtave të Njeriut (DUDNJ) të miratuar më 1948, si një nga të drejtat themelore të njeriut të mbrojtura. Menjëherë pas miratimit të DUDNJ-së, edhe Evropa e afirmoi këtë të drejtë tek Konventa Evropiane e të Drejtave të Njeriut (KEDNJ), që është një traktat me fuqi ligjore detyruese për Palët e saj Kontraktuese dhe është hartuar në vitin 1950. KEDNJ-ja përcakton se secili ka të drejtën për respektim të jetës private dhe familjare, banesës dhe korrespondencës së tij, apo të saj. Ndërhyrja e autoriteteve publike tek kjo e drejtë është e ndaluar, përveçse kur ndërhyrja është

në përputhje me ligjin, bëhet për interesa të rëndësishme dhe legjitime dhe është e nevojshme në një shoqëri demokratike.

DUDNJ-ja dhe KEDNJ-ja u miratuan shumë kohë përpara zhvillimit të kompjuterëve, internetit dhe shfaqjes së shoqërisë së informacionit. Këto zhvillime kanë sjellë përparësi të mëdha për njerëzit dhe shoqërinë, duke përmirësuar cilësinë e jetës, efikasitetin dhe prodhimin. Njëkohësisht, ato paraqesin rreziqe të reja për të drejtën për respektim të jetës private. Në përgjigje të nevojës për norma specifike që rregullojnë mbledhjen dhe përdorimin e informacioneve personale, u shfaq një koncept i ri privatësie, i njohur në disa juridiksione si "privatësia e informacionit" dhe në disa të tjera si "e drejta për vetë-përcaktim informativ".[1] Ky koncept çoi në zhvillimin e rregullimeve ligjore specifike, të cilat sigurojnë mbrojtje të të dhënave personale.

Mbrojtja e të dhënave në Evropë nisi në vitet 70, me miratimin nga ana e disa shteteve të legjislacionit për kontrollin e përpunimit të informacioneve personale nga autoritetet publike dhe shoqëritë e mëdha tregtare.[2] Në vijim, u miratuan instrumente të mbrojtjes së të dhënave në nivel evropian[3] dhe me kalimin e viteve, mbrojtja e të dhënave u zhvillua si një vlerë e ndryshme, e cila nuk përfshihet tek e drejta për respektim të jetës private. Në rendin juridik të BE-së, mbrojtja e të dhënave njihet si e drejtë themelore, e veçantë nga e drejta themelore për respektim të jetës private. Kjo ndarje ngre pikëpyetje në lidhje me marrëdhënien dhe ndryshimet midis këtyre dy të drejtave.

E drejta për respektim të jetës private dhe e drejta për mbrojtje të të dhënave personale janë të lidhura ngushtë. Të dyja përpiqen të mbrojnë vlera të ngjashme, d.m.th. autonominë dhe dinjitetin e personave, duke u dhënë një sferë personale në të cilën ata mund të zhvillojnë lirisht personalitetet, të mendojnë e formojnë opinionet e tyre. Në këtë mënyrë, ato janë një parakusht thelbësor për ushtrimin e lirive të tjera themelore, sikurse lirinë e shprehjes, lirinë e tubimit dhe bashkimit paqësor dhe lirinë e besimit fetar.

Këto dy të drejta ndryshojnë për sa i përket formulimit dhe fushëveprimit të tyre. E drejta për respektim të jetës private konsiston në një ndalim të përgjithshëm të ndërhyrjes, me përjashtim të disa kritereve të interesit publik të cilat mund të justifikojnë ndërhyrjen në disa raste. Mbrojtja e të dhënave personale shihet si një e drejtë moderne dhe aktive,[4] që vendos një sistem kontrolli dhe ekuilibri për të mbrojtur personat sa herë që të dhënat e tyre personale përpunohen. Përpunimi duhet të pajtohet me komponentët thelbësorë të mbrojtjes së të dhënave

---

[1] Gjykata Kushtetuese Federale Gjermane njohu të drejtën për vetë-përcaktim informativ në çështjen e vitit 1983 *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1ff. Gjykata e konsideroi vetë-përcaktimin informativ si derivat të së drejtës themelore për respektim të personalitetit, të mbrojtur në Kushtetutën Gjermane. GJEDNJ-ja pranoi në një çështje të 2017-ës se neni 8 i KEDNJ-së "parashikon të drejtën për të krijuar vetë-përcaktim informativ". Shih GJEDNj, *Satakunnan Markkinapörssi Oy and Satamedia Oy k. Finland*, nr. 931/13, 27 qershor 2017, paragrafi 137.

[2] Shteti Gjerman Hesse, miratoi ligjin e parë të mbrojtjes së të dhënave në 1970, i cili zbatohej vetëm në atë shtet. Në 1973, Suedia miratoi ligjin e parë kombëtar të mbrojtjes së të dhënave në botë. Nga fundit i viteve 1980, disa shtete evropiane (Franca, Gjermania, Vendet e Ulëta dhe Mbretëria e Bashkuar) miratuan gjithashtu legjislacion për mbrojtjen e të dhënave.

[3] Konventa e Këshillit të Evropës për mbrojtjen e personave nga Përpunimi Automatik i të Dhënave Personale (Konventa 108) u miratua në 1981. BE-ja miratoi instrumentin e saj të parë gjithëpërfshirës të mbrojtjes së të dhënave më 1995: Direktiva 95/46/EC mbi mbrojtjen e personave në lidhje me përpunimin e të dhënave personale dhe mbi lëvizjen e lirë të këtyre të dhënave.

[4] Avokatja e Përgjithshme Sharpston e përshkruan çështjen si të tillë që përfshin dy të drejta të veçanta: e drejta "klasike" për mbrojtje të privatësisë dhe një e drejtë më "moderne", e drejta për mbrojtje të të dhënave. Shih GJDBE, Çështje të bashkuara C-92/09 dhe C-93/02, *Volker und Markus Schecke GbR k. Land Hessen*, *Opinion of Advocate General Sharpston*, 17 qershor 2010, paragrafi 71.

personale, domethënë me mbikëqyrjen e pavarur dhe respektimin e të drejtave të subjektit të të dhënave.[5]

Neni 8 i Kartës së të Drejtave Themelore të BE-së (Karta) nuk përcakton vetëm të drejtën për mbrojtje të të dhënave personale, por parashikon gjithashtu vlerat kryesore që lidhen me këtë të drejtë. Ai përcakton se përpunimi i të dhënave personale duhet të jetë i drejtë, për qëllime specifike dhe i bazuar tek pëlqimi i personit të përfshirë, ose tek një kriter legjitim të përcaktuar me ligj. Personat duhet të kenë të drejtën e aksesit tek të dhënat personale dhe të bëjnë korrigjimin e tyre dhe respektimi i kësaj të drejte duhet t'i nënshtrohet kontrollit të një autoriteti të pavarur.

E drejta për mbrojtje të të dhënave personale aktivizohet sa herë që përpunohen të dhënat personale; për rrjedhojë, ajo është më e gjerë se sa e drejta për respektim të jetës private. Çdo përpunim të dhënash personale është subjekt mbrojtjeje të përshtatshme. Mbrojtja e të dhënave ka të bëjë me të gjitha llojet e të dhënave personale dhe të përpunimeve të të dhënave, pavarësisht marrëdhënies me privatësinë dhe ndikimit tek ajo. Përpunimi i të dhënave personale mund të cenojë gjithashtu të drejtën për jetë private, sikurse tregohet në rastet e mësipërme. Gjithsesi, që të aktivizohen rregullat e mbrojtjes së të dhënave, nuk është e domosdoshme të demonstrohet se është bërë një shkelje e jetës private.

E drejta për privatësi ka të bëjë me situata në të cilat është cenuar një interes privat, ose "jeta private" e një individi. Sikurse demonstrohet përgjatë këtij manuali, "jeta private" është interpretuar gjerësisht në jurisprudencë si koncept që përfshin situata intime, informacion sensitiv, ose konfidencial, informacion i cili mund të ndikojë në perceptimin e publikut ndaj personit dhe madje edhe në jetën profesionale e sjelljen publike të dikujt. Gjithsesi, vlerësimi nëse ka pasur, apo ka një ndërhyrje në "jetën private" varet nga konteksti dhe rrethanat e secilit rast.

Nga ana tjetër, çdo aktivitet që përfshin përpunim të dhënash personale mund të hyjë në fushëveprimin e rregullave të mbrojtjes së të dhënave dhe të aktivizojë të drejtën për mbrojtje të të dhënave personale. Kur për shembull, një punëdhënës regjistron informacione në lidhje me emrat dhe pagat e punonjësve, thjesht regjistrimi i këtij informacioni nuk mund të konsiderohet si ndërhyrje në jetën private. Sidoqoftë, ndërhyrja mund të argumentohet kur për shembull, një punëdhënës ka transferuar informacionet personale të punëmarrësve tek palë të treta. Në çdo rast, punëdhënësit duhet të respektojnë rregullat e mbrojtjes së të dhënave, sepse regjistrimi i informacionit në lidhje me punëmarrësit përbën përpunim të dhënash.

Shembull: tek çështja *Digital Rights Ireland,*[6] iu kërkua GJDBE-së të vendoste në lidhje me vlefshmërinë e Direktivës 2006/24/KE, për sa i takon të drejtave themelore për mbrojtje të të dhënave personale dhe respektim të jetës private, të përcaktuara në Kartën e të Drejtave Themelore të BE-së. Direktiva detyronte operatorët e shërbimeve të komunikimeve elektronike publike, ose rrjeteve publike të komunikimit, që të mbanin të dhënat e telekomunikimeve të qytetarëve deri në dy vite, për të siguruar që të dhënat të ishin të

[5] Hustinx, P., EDPS Speeches & Articles, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, korrik 2013.
[6] GJDBE, Çështje të bashkuara C-293/12 dhe C-594/12, *Digital Rights Ireland k. Minister for Communications, Marine and Natural Resources dhe të Tjerët dhe Kärntner Landesregierung dhe të Tjerët* (GC], 8 prill 2014.

disponueshme për qëllime të parandalimit, hetimit dhe ndjekjes së krimeve të rënda. Masa kishte të bënte vetëm me të dhënat e trafikut, të dhënat e vendndodhjes dhe të dhënat e nevojshme për identifikimin e abonentit, apo përdoruesit dhe nuk gjente zbatim për përmbajtjen e komunikimeve elektronike.
GJDBE-ja vlerësoi se direktiva ndërhynte tek e drejta themelore për mbrojtje të të dhënave personale "sepse ajo parashikon përpunim të dhënash personale".[7] Gjithashtu, Gjykata vlerësoi se direktiva ndërhynte tek e drejta për respektim të jetës private.[8] Të marra në tërësinë e tyre, të dhënat personale të mbajtura në përputhje me direktivën, të cilat mund të aksesohen nga autoritetet kompetente, mundësojnë "nxjerrjen e përfundimeve tepër të sakta rreth jetës private të personave të dhënat e të cilëve janë mbajtur, sikurse zakonet e jetës së përditshme, vendbanimet e përkohshme, apo të përhershme, lëvizjet e përditshme, apo të tjera, aktivitet e zhvilluara, marrëdhëniet shoqërore të këtyre personave dhe mjediset shoqërore të frekuentuara prej tyre".[9] Ndërhyrja tek këto dy të drejta kishte shtrirje të gjerë dhe ishte tepër e rëndë.

GJDBE-ja e shpalli Direktivën 2006/24/KE të pavlefshme, duke dalë në përfundimin se edhe pse ajo synonte përmbushjen e një qëllimi legjitim, ndërhyrja tek të drejtat për mbrojtje të të dhënave personale dhe jetës private ishte e rëndë dhe jo e kufizuar vetëm tek domosdoshmëria.

1.1.2. Kuadri ligjor ndërkombëtar: Kombet e Bashkuara

Kuadri ligjor i Kombeve të Bashkuara nuk e njeh mbrojtjen e të dhënave personale si të drejtë themelore, megjithëse e drejta për privatësi është një e drejtë themelore e përcaktuar prej një kohë të gjatë në rendin ligjor ndërkombëtar. Neni 12 i DUDNJ-së mbi respektimin e jetës private dhe familjare[10] ishte i pari instrument ndërkombëtar që përcaktonte të drejtën e personit për mbrojtje të sferës private ndaj ndërhyrjeve të të tjerëve, sidomos nga ana e shtetit. Edhe pse DUDNJ-ja nuk është një deklaratë detyruese, ajo gëzon status të rëndësishëm, si një instrument themelor i legjislacionit ndërkombëtar të të drejtave të njeriut dhe ka ndikuar në zhvillimin e instrumenteve të tjera të të drejtave të njeriut në Evropë. Pakti Ndërkombëtar për të Drejtat Civile dhe Politike (PNDCP) hyri në fuqi në vitin 1976. Ai shpalli se askush nuk mund t'i nënshtrohet ndërhyrjeve arbitrare, apo të paligjshme tek privatësia, banesa apo letërkëmbimi dhe as duhet t'i shkelet nderi dhe reputacioni i tij në mënyrë të paligjshme. PNDCP-ja është traktat ndërkombëtar që angazhon 169 palët e saj në respektimin dhe garantimin e ushtrimit të të drejtave civile të personave, përfshirë të drejtën për privatësi.

Që nga viti 2013, Kombet e Bashkuara kanë miratuar dy rezoluta mbi çështjet e privatësisë të emërtuara "e drejta për privatësi në epokën digjitale"[11] për t'iu përgjigjur zhvillimit të teknologjive të reja dhe sinjalizimet mbi përgjimet masive të kryer në disa shtete (sinjalizimet e Snowden-it). Këto rezoluta dënojnë ashpër përgjimet masive dhe theksojnë ndikimit që ato kanë tek të drejtat themelore për privatësi dhe lirinë e shprehjes dhe tek funksionimi i një

[7] *Ibid.,* paragrafi 36.
[8] *Ibid.,* paragrafët 32-35.
[9] *Ibid.,* paragrafi 27.
[10] Kombet e Bashkuara (OKB), Deklarata Universale e të Drejtave të Njeriut (DUDNJ), 10 dhjetor 1948.
[11] Shih OKB, Asambleja e Përgjithshme, Resolution on the right to privacy in the digital age, A/RES/68/167, Nju Jork, 18 dhjetor 2013; dhe OKB, Asambleja e Përgjithshme, Revised draft resolution on the right to privacy in the digital age, A/C.3/69/L.26/Rev.1, Nju Jork, 19 nëntor 2014.

shoqërie aktive dhe demokratike. Megjithëse nuk janë ligjërisht detyruese, ato ndezën një debat të rëndësishëm ndërkombëtar të nivelit të lartë, në lidhje me privatësinë, teknologjitë e reja dhe survejimin. Ato çuan edhe në caktimin e një Raportuesi të Posaçëm për të drejtën e privatësisë, i ngarkuar për mbështetjen dhe mbrojtjen e kësaj të drejte. Detyrat konkrete të raportuesit përfshijnë mbledhjen e informacionit mbi praktikat dhe eksperiencat kombëtare në lidhje me privatësinë dhe sfidat që burojnë nga teknologjitë e reja, shkëmbimin dhe mbështetjen e praktikave më të mira dhe identifikimin e pengesave të mundshme.

Ndërsa rezolutat e mëparshme përqendroheshin në pasojat negative të përgjimeve masive dhe përgjegjësinë e shteteve për të kufizuar kompetencat e autoriteteve informative, rezolutat e kohëve të fundit pasqyrojnë një zhvillim të rëndësishëm të diskutimeve mbi privatësinë në Kombet e Bashkuara.[12] Rezolutat e miratuara në 2016-ën dhe 2017-ën ritheksojnë domosdoshmërinë për të kufizuar kompetencat e agjencive informative dhe dënojnë survejimin në masë. Gjithsesi, ato shprehin qartë edhe se "aftësia gjithnjë e në rritje e shoqërive tregtare për të mbledhur, përpunuar dhe përdorur të dhëna personale, mund të përbëjë rrezik për ushtrimin e së drejtës për privatësi në epokën digjitale". Në këtë mënyrë, përveç përgjegjësisë së autoriteteve shtetërore, rezolutat theksojnë përgjegjësinë e sektorit privat për respektimin e të drejtave të njeriut dhe u bëjnë thirrje shoqërive të informojnë përdoruesit në lidhje me mbledhjen, përdorimin, shkëmbimin dhe mbajtjen e të dhënave personale dhe të përcaktojnë politika transparente përpunimi.

1.1.3. Konventa Evropiane e të Drejtave të Njeriut

Këshilli i Evropës u themelua pas Luftës së Dytë Botërore, për të bashkuar shtetet e Evropës për promovimin e shtetit të së drejtës, demokracisë, të drejtave të njeriut dhe zhvillimit shoqëror. Për këtë qëllim, në vitin 1950, ai miratoi KEDNJ-në, e cila hyri në fuqi në vitin 1953.

Palët Kontraktuese kanë detyrimin ndërkombëtar të zbatojnë KEDNJ-në. Të gjitha shtetet anëtare të KiE-së e kanë përfshirë, ose zbatuar tashmë KEDNJ-në në legjislacionin e tyre kombëtar, i cili i detyron ato të veprojnë në përputhje me dispozitat e konventës. Palët Kontraktuese duhet të respektojnë të drejtat e përcaktuara në konventë gjatë ushtrimit të çdo veprimtarie, apo kompetence. Këtu përfshihet veprimtaria që kryejnë për sigurinë kombëtare. Vendime të rëndësishme të Gjykatës Evropiane të së Drejtave të Njeriut (GJEDNJ) kanë përfshirë veprimtaritë shtetërore në fushat sensitive të legjislacionit dhe praktikës së sigurisë kombëtare.[13] Gjykata është shprehur qartë se aktivitetet e survejimit ndërhyjnë tek e drejta për respektim të jetës private.[14]

Për të garantuar që Palët Kontraktuese të zbatojnë detyrimet e tyre sipas KEDNJ-së, u themelua GJEDNJ-ja në vitin 1959 në Strasburg të Francës. GJEDNJ-ja garanton që shtetet të zbatojnë detyrimet e tyre që burojnë nga Konventa, nëpërmjet shqyrtimit të ankesave nga persona, grupe personash, OJQ, apo persona juridikë, të cilët pretendojnë se është kryer një shkelje e

[12] OKB, Asambleja e Përgjithshme, Revised draft resolution on the right to privacy in the digital age, A/C.3/71/L.39/ Rev.1, Nju Jork, 16 nëntor 2016; OKB, Këshilli i të Drejtave të Njeriut, The right to privacy in the digital age, A/HRC/34/L.7/Rev.1, 22 mars 2017.

[13] Shih për shembull: GJEDNJ, *Klass dhe të Tjerët k. Gjermanisë*, nr. 5029/71, 6 shtator 1978; GJEDNJ, *Rotaru k. Rumanisë* [ÇB] , nr. 28341/95, 4 maj 200 dhe GJEDNJ, *Szabó dhe Vissy k. Hungarisë*, nr. 37138/14, 12 janar 2016.

[14] *Ibid.*

konventës. GJEDNJ-ja mund të shqyrtojë gjithashtu çështje ndërshtetërore, të ndërmarra nga një apo më shumë shtete anëtare të KiE-së, kundër një shteti tjetër anëtar.

Deri në vitin 2018, Këshilli i Evropës ka në përbërje 47 Palë Kontraktuese, 28 prej të cilave janë gjithashtu Shtete Anëtare të BE-së. Kërkuesit të cilët i drejtohen GJEDNJ-së nuk duhet të jenë detyrimisht shtetas të Palëve Kontraktuese, megjithëse shkeljet e pretenduara mund të kenë ndodhur në juridiksionin e një Pale Kontraktuese.

E drejta për mbrojtje të të dhënave personale është pjesë përbërëse e të drejtave të mbrojtura nga neni 8 i KEDNJ-së, i cili garanton të drejtën për respektim të jetës private dhe familjare, banesës dhe letërkëmbimit dhe përcakton kushtet sipas së cilave lejohen kufizimet e këtyre të drejtave.[15]

GJEDNJ-ja ka shqyrtuar shumë situata që përfshijnë problematika të mbrojtjes së të dhënave. Në to përfshihen interceptimi i komunikimeve,[16] forma të ndryshme të përgjimit nga sektori privat dhe publik[17] dhe mbrojtja nga mbajtja e të dhënave personale nga autoritetet publike.[18] Respekti për jetën private nuk është e drejtë absolute, meqenëse ushtrimi i së drejtës për privatësi mund të cënojë të drejta të tjera, sikurse lirinë e shprehjes dhe aksesin në informacion dhe anasjelltas. Kështu, Gjykata përpiqet të ekuilibrojë këto të drejta të ndryshme. Ajo ka qartësuar se neni 8 i KEDNJ-së nuk i detyron shtetet vetëm të mos kryejnë veprime të cilat mund të shkelin këtë të drejtë të përcaktuar në konventë, por që në rrethana të caktuara të jenë edhe nën detyrimin pozitiv për të garantuar në mënyrë aktive respektim efikas të jetës private dhe familjare.[19] Në kapitujt përkatës përshkruhen në hollësi shumë nga këto çështje.

1.1.4. Konventa 108 e Këshillit të Evropës

Me shfaqjen e teknologjisë së informacionit në vitet 60', u rrit nevoja për rregulla më të hollësishme për mbrojtjen e personave nëpërmjet mbrojtjes së të dhënave të tyre personale. Në mesin e viteve 70, Komiteti i Ministrave të Këshillit të Evropës miratoi rezoluta të ndryshme mbi mbrojtjen e të dhënave personale, duke iu referuar nenit 8 të KEDNJ-së.[20] Në vitin 1981, u hap për nënshkrim një Konventë për mbrojtjen e personave në lidhje me përpunimin automatik të të dhënave personale (Konventa 108)[21]. Konventa 108 ishte dhe mbetet i vetmi instrument ndërkombëtar me fuqi ligjore detyruese në fushën e mbrojtjen së të dhënave.

Konventa 108 gjen zbatim për të gjitha përpunimet e të dhënave, që kryhen si nga sektori privat, ashtu edhe nga ai publik, përfshirë përpunimin e të dhënave nga ana e autoriteteve gjyqësore dhe ligjzbatuese. Ajo mbron individët nga abuzimet që mund të shoqërojnë përpunimin e të dhënave personale. Për sa i përket përpunimit të të dhënave personale, parimet e përcaktuara

---

[15] Këshilli i Evropës, Konventa Evropiane për të Drejtat e Njeriut, CETS nr. 005, 1950.
[16] Shih, për shembull: GJEDNJ, *Malone k. Mbretërisë së Bashkuar,* nr. 8691/79, 2 gusht 1984; GJEDNJ, *Copland k. Mbretërisë së Bashkuar,* nr. 62617/00, 3 prill 2007, ose GJEDNJ, *Mustafa Sezgin Tannkulu k. Turqisë,* nr. 27473/06, 18 korrik 2017.
[17] Shih, për shembull: GJEDNJ, *Klass dhe të Tjerët k. Gjermanisë,* nr. 5029/71, 6 shtator 1978; GJEDNJ, *Uzun k. Gjermanisë,* nr. 35623/05, 2 shtator 2010.
[18] Shih, për shembull: GJEDNJ, *Roman Zakharov k. Rusisë,* nr. 47143/06, 4 dhjetor 2015; GJEDNJ, *Szabó dhe Vissy k. Hungarisë*, nr. 37138/14, 12 janar 2016.
[19] Shih për shembull: GJEDNJ, *I k. Finlandës,* nr. 20511/03, 17 korrik 2008, *K.U. k. Finlandës,* nr. 2872/02, 2 dhjetor 2008.
[20] Këshilli i Evropës, Komiteti i Ministrave (1973), Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, 26 shtator 1973; Council of Europe, Committee of Ministers (1974), Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, 20 shtator 1974.
[21] Këshilli i Evropës, Konventa për Mbrojtjen e Personave në lidhje me Përpunimin Automatik të të Dhënave Personale, CETS nr. 108, 1981.

në konventë kanë të bëjnë veçanërisht me mbledhjen e drejtë dhe të ligjshme dhe përpunimin automatik të të dhënave, për qëllime legjitime të përcaktuara. Kjo do të thotë se të dhënat nuk duhen përdorur në mënyrë të papajtueshme me këto qëllime dhe nuk duhen mbajtur për një kohë më të gjatë se sa është e nevojshme. Ato kanë të bëjnë gjithashtu me cilësinë e të dhënave, në mënyrë të veçantë që ato duhet të jenë të mjaftueshme, të rëndësishme dhe jo të tepërta (proporcionaliteti), ashtu si edhe të sakta.

Përveç parashikimit të garancive për përpunimin e të dhënave personale dhe detyrimeve në lidhje me sigurinë e të dhënave, në mungesë të masave të përshtatshme ligjore, ajo ndalon përpunimin e të dhënave "sensitive" – të cilat lidhen me racën, mendimet politike, shëndetin, besimin fetar, jetën seksuale apo të dhënat penale të një personi.

Konventa sanksionon gjithashtu të drejtën e individit për t'u vënë në dijeni mbi informacionin që mbahet në lidhje me të dhe nëse është e nevojshme, të kërkojë korrigjimin e tij. Kufizimet e të drejtave të përcaktuara në konventë, janë të mundura vetëm kur prevalojnë interesat të tjera, sikundër siguria shtetërore, apo mbrojtja. Gjithashtu, konventa parashikon qarkullimin e lirë të të dhënave personale ndërmjet Palëve të saj Kontraktuese dhe përcakton disa kufizime për qarkullimet drejt shteteve ku kuadri ligjor nuk ofron mbrojtje të barasvlershme.

Vlen të theksohet se Konventa 108 është detyruese për shtetet të cilat e kanë ratifikuar. Ajo nuk i nënshtrohet mbikëqyrjes gjyqësore të GJEDNJ-së, por është marrë në konsideratë në jurisprudencën e GJEDNJ-së në kontekstin e nenit 8 të KEDNJ-së. Ndër vite, Gjykata ka përcaktuar se mbrojtja e të dhënave personale është pjesë e rëndësishme e së drejtës për respektim të jetës private (neni 8) dhe ka ndjekur parimet e Konventës 108 për të vendosur nëse ka pasur apo jo ndërhyrje tek kjo e drejtë themelore.[22]

Komiteti i Ministrave ka miratuar rekomandime të ndryshme që nuk kanë fuqi ligjore detyruese, me qëllim që të zhvillojë më tej parimet dhe rregullat e përgjithshme të përcaktuara në Konventën 108. Këto rekomandime kanë ndikuar në zhvillimin e së drejtës evropiane në fushën e mbrojtjes së të dhënave. Për shembull, për vite me radhë, i vetmi instrument në Evropë që rregullonte përdorimin e të dhënave personale në sektorin e policisë ishte Rekomandimi për Policinë[23]. Parimet që përfshin ky rekomandim, sikurse mënyrat e mbajtjes së skedarëve të të dhënave dhe domosdoshmërinë për zbatimin e rregullave të qarta, për sa i takon personave që lejohen të kenë akses në këto dosje, u zhvilluan më tej dhe janë reflektuar në legjislacionin pasues të BE-së.[24] Disa rekomandime të kohëve të fundit synojnë t'u përgjigjen sfidave të epokës digjitale – për shembull, në lidhje me përpunimin e të dhënave në kontekstin e punësimit (shih Seksionin 9).

Të gjitha Shtetet Anëtare të BE-së kanë ratifikuar Konventën 108. Më 1999, u propozuan disa ndryshime tek Konventa 108, për t'i mundësuar BE-së të bëhej palë, por nuk hynë kurrë në

[22] Shih, për shembull: GJEDNJ, *Z. K. Finlandës,* nr. 22009/93, 25 shkurt 1997.
[23] Këshilli i Evropës, Komiteti i Ministrave (1987), Rekomandimi Rec(87) 15 për shtetet anëtare që rregullon përdorimin e të dhënave personale në sektorin e policisë, Strasburg, 17 shtator 1987.
[24] Direktiva 95/46/EC e Parlamentit Evropian dhe e Këshillit e 24 tetorit 1995 për mbrojtjen e individëve në lidhje me përpunimin e të dhënave personale si edhe lëvizjen e lirë të këtyre të dhënave, FZ L 281, 23 nëntor 1995.

fuqi.[25] Në vitin 2001, u miratua një Protokoll Shtesë i Konventës 108, i cili parashikonte dispozita në lidhje me qarkullimet ndërkufitare të të dhënave, drejt shteteve të cilat nuk janë palë, të ashtuquajtura shtete të treta dhe detyrimin për ngritjen e autoriteteve kombëtare mbikëqyrëse të mbrojtjes së të dhënave.[26]

Konventa 108 është e hapur për anëtarësim nga ana e Palëve jo Kontraktuese të KiE-së. Potenciali i Konventës si një standard i përbotshëm, së bashku me karakterin e saj të hapur, shërbejnë si bazë për promovimin e mbrojtjes së të dhënave në nivel global. Deri më sot, 51 shtete janë palë të Konventës 108. Në to bëjnë pjesë të gjitha shtetet anëtare të Këshillit të Evropës (47 shtete); Uruguai, i cili ishte i pari shtet jo Evropian i cili u anëtarësua në gusht 2013 dhe Mauriciusi, Senegali dhe Tunizia, të cilët u anëtarësuan në vitet 2016 dhe 2017.

Kohët e fundit konventa i është nënshtruar një procesi modernizimi. Konsultimi publik i zhvilluar në vitin 2011, konfirmoi dy objektivat kryesorë të punës: përforcimin e mbrojtjes së privatësisë në arenën digjitale dhe fuqizimin e mekanizmit të disiplinimit. Procesi i modernizimit u përqendrua mbi këto objektiva dhe u plotësua me miratimin e protokollit të ndryshimit të Konventës 108 (Protokolli CETS nr. 223). Puna u krye paralelisht me reforma të tjera të instrumenteve ndërkombëtare në fushën e mbrojtjes së të dhënave dhe me reformën e rregullave të mbrojtjes së të dhënave të BE-së, e cila nisi në vitin 2012. Autoritetet rregullatore në nivel të Këshillit të Evropës dhe të BE-së janë kujdesur së tepërmi që të garantojnë konsekuencë dhe përputhshmëri midis të dy kuadrove ligjorë. Modernizimi e ruan karakterin e përgjithshëm dhe elastik të konventës dhe e përforcon potencialin e saj, si një instrument universal i së drejtës në fushën e mbrojtjes së të dhënave. Me anë të tij riafirmohen dhe stabilizohen parimet e rëndësishme, si dhe ofrohen të drejta të reja për individët, duke rritur njëkohësisht përgjegjësitë e njësive që përpunojnë të dhëna personale, duke garantuar më shumë përgjegjshmëri. Për shembull, individët të cilëve u përpunohen të dhënat, kanë të drejtën të kërkojnë të vihen në dijeni mbi arsyetimin për kryerjen e përpunimit të të dhënave dhe të drejtën ta kundërshtojnë përpunimin. Ndaj rritjes gjithnjë e më të madhe të profilizimit në botën e internetit, konventa përcakton të drejtën e personit, për të mos iu nënshtruar vendimeve të mbështetura vetëm në përpunim automatik, pa iu marrë parasysh mendimi. Zbatimi efikas i rregullave të mbrojtjes së të dhënave nga autoritetet e pavarura mbikëqyrëse të Palëve Kontraktuese, konsiderohet si thelbësore për zbatimin praktik të konventës. Për këtë qëllim, konventa e modernizuar thekson që është e nevojshme të pajisen autoritetet mbikëqyrëse me kompetenca dhe funksione të efektshme dhe të gëzojnë pavarësi të vërtetë në përmbushjen e misionit të tyre.

1.1.5. Legjislacioni i mbrojtjes së të dhënave të Bashkimit Evropian

Legjislacioni i BE-së përbëhet nga e drejta parësore dhe dytësore e BE-së. Traktatet, domethënë Traktati i Bashkimit Evropian (TBE) dhe Traktati i Funksionimit të Bashkimit Evropian (TFBE), janë miratuar nga të gjitha Shtetet Anëtare të BE-së dhe formojnë "të drejtën parësore

[25] Këshilli i Evropës, Ndryshime të Konventës për mbrojtjen e personave nga përpunimi automatik i të Dhënave Personale (ETS nr. 108) miratuar nga Komiteti i Ministrave, në Strasburg, më 15 qershor 1999.
[26] Këshilli i Evropës, Protokolli Shtesë i Konventës për mbrojtjen e personave nga përpunimi automatik i të dhënave personale, në lidhje me autoritetet mbikëqyrëse dhe qarkullimet ndërkufitare të të dhënave, CETS nr. 181, 2001. Me modernizimin e Konventës 108, ky Protokoll nuk vijon të zbatohet, meqenëse dispozitat e tij janë përditësuar dhe integruar në Konventën e Modernizuar 108.

të BE-së". Rregulloret, direktivat dhe vendimet e BE-së janë miratuar nga institucionet e BE-së, autoritete të cilin ua japin traktatet dhe përbëjnë "të drejtën dytësore të BE-së".

Mbrojtja e të dhënave në të drejtën parësore të BE-së

Traktatet themeluese të Komunitetit Evropian nuk përmbanin asnjë dispozitë në lidhje me drejtat e njeriut apo mbrojtjen e tyre, meqenëse Komuniteti Ekonomik Evropian ishte parashikuar fillimisht si një organizatë rajonale, e përqendruar tek integrimi ekonomik dhe krijimi i një tregu të përbashkët. Një parim themelor mbi të cilin u mbështet dhe u zhvillua Komuniteti Evropian – i cili është njësoj i vlefshëm edhe sot – është parimi i delegimit. Sipas këtij parimi, BE-ja vepron vetëm brenda kufijve të kompetencave që i janë deleguar nga Shtetet Anëtare, sikurse reflektohet në traktatet e BE-së. Ndryshe nga Këshilli i Evropës, traktatet e BE-së nuk përfshijnë një kompetencë të qartë për sa i përket çështjeve të të drejtave themelore.

Meqenëse në GJDBE janë paraqitur çështje në lidhje me shkelje të të drejtave të njeriut, në fushën e zbatimit së të drejtës së BE-së, GJDBE-ja kë bërë interpretim domethënës të traktateve. Për t'u dhënë më tepër mbrojtje individëve, ajo i integroi të drejtat themelore në të ashtuquajturat parime të përgjithshme të së drejtës së BE-së. Sipas GJDBE-së, këto parime të përgjithshme pasqyrojnë thelbin e mbrojtjes së të drejtave të njeriut, që gjendet në kushtetutat kombëtare dhe tek traktatet e të drejtave të njeriut, veçanërisht tek KEDNJ-ja. GJDBE-ja është shprehur se diçka e tillë do të garantonte pajtueshmërinë e së drejtës së BE-së me këto parime.

Duke pranuar se politikat e saj mund të kenë ndikim tek të drejtat e njeriut dhe duke u përpjekur për të afruar qytetarët "më pranë" BE-së, kjo e fundit shpalli në vitin 2000 Kartën e të Drejtave Themelore të Bashkimit Evropian (Karta). Ajo përmbledh të gjithë gamën e të drejtave civile, politike, ekonomike dhe shoqërore të qytetarëve evropianë, duke sintetizuar traditat kushtetuese dhe detyrimet ndërkombëtare që janë të përbashkëta për Shtetet Anëtare. Të drejtat e përshkruara në Kartë ndahen në gjashtë seksione: dinjiteti, liritë, barazia, solidariteti, të drejtat e shtetasve dhe drejtësia.

Fillimisht, thjesht një dokument politik, Karta u bë ligjërisht e detyrueshme[27] si legjislacion parësor i BE-së (shih nenin 6, pika 1 të TBE-së) me hyrjen në fuqi të Traktatit të Lisbonës më 1 dhjetor 2009.[28] Dispozitat e Kartës i drejtohen institucioneve dhe organeve të BE-së, duke i detyruar të respektojnë të drejtat e renditura në të gjatë përmbushjes së detyrave të tyre. Dispozitat e Kartës janë gjithashtu detyruese për Shtetet Anëtare kur zbatojnë legjislacionin e BE-së.

Karta nuk garanton vetëm respektimin e jetës private dhe familjare (neni 7), por përcakton gjithashtu të drejtën për mbrojtje të të dhënave personale (neni 8). Karta e ngre qartësisht këtë mbrojtje në nivelin e një të drejte themelore të legjislacionit të BE-së. Institucionet dhe organet e BE-së duhet të garantojnë e respektojnë këtë të drejtë, ashtu si Shtetet Anëtare kur zbatojnë legjislacionin e Bashkimit (neni 51 i Kartës). Meqenëse u hartua shumë vite pas Direktivës për Mbrojtjen e të Dhënave, neni 8 i Kartës duhet trajtuar si mishërim i së drejtës pararendëse të

[27] BE (2012), Karta e të Drejtave Themelore të Bashkimit Evropian, FZ 2012 C 326.
[28] Shih variantet e konsoliduara të Komunitetit Evropian (2012), Traktati i Bashkimit Evropian, FZ 2012 C 326; dhe Komuniteti Evropian (2012), TFBE, FZ 2012 C 326.

BE-së në fushën e mbrojtjes së të dhënave. Rrjedhimisht, Karta jo vetëm që përmend qartësisht të drejtën për mbrojtje të të dhënave në nenin 8, pika 1, por edhe i referohet parimeve kryesore të mbrojtjes së të dhënave në nenin 8, pika 2. Po ashtu, neni 8, pika 3 e Kartës kërkon që një autoritet i pavarur të kontrollojë zbatimin e këtyre parimeve.

Miratimi i Traktatit të Lisbonës është një pikë referimi për zhvillimin e legjislacionit të mbrojtjes së të dhënave, jo vetëm sepse i dha Kartës statusin e një dokumenti ligjor detyrues në nivelin e legjislacionit parësor, por edhe sepse përcaktoi të drejtën për mbrojtje të të dhënave personale. Kjo e drejtë parashikohet konkretisht në nenin 16 të TFBE-së, tek ajo pjesë e traktatit e cila i kushtohet parimeve të përgjithshme të BE-së. Neni 16 krijon gjithashtu një bazë të re ligjore, duke i dhënë BE-së kompetencën për të miratuar legjislacion për çështje të mbrojtjes së të dhënave. Ky është një zhvillim i rëndësishëm, për shkak se rregullat e mbrojtjes së të dhënave të BE-së, sidomos Direktiva e Mbrojtjes së të Dhënave, mbështeteshin fillimisht mbi bazën ligjore të tregut të brendshëm dhe mbi nevojën për të përafruar legjislacionet kombëtare, në mënyrë që të mos pengohej lëvizja e lirë e të dhënave brenda BE-së. Neni 16 i TFBE-së ofron tashmë një bazë ligjore të pavarur për një qasje moderne, gjithëpërfshirëse ndaj mbrojtjes së të dhënave, e cila mbulon të gjitha çështjet që janë kompetencë e BE-së, përfshirë këtu edhe bashkëpunimin policor dhe gjyqësor për çështjet penale. Neni 16 i TFBE-së pohon gjithashtu se respektimi i rregullave të mbrojtjes së të dhënave, të miratuara në zbatim të saj, duhet t'i nënshtrohet kontrollit të autoriteteve mbikëqyrëse të pavarura. Neni 16 shërbeu si bazë ligjore për miratimin e një reforme tërësore të rregullave të mbrojtjes së të dhënave në 2016-ën, konkretisht Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave dhe Direktiva e Mbrojtjes së të Dhënave për Autoritetet e Policisë dhe Drejtësisë Penale (shih më poshtë).

Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave

Nga viti 1995 deri në maj 2018, instrumenti kryesor ligjor i BE-së për mbrojtjen e të dhënave ishte Direktiva 95/46/KE e Parlamentit Evropian dhe e Këshillit, e 24 tetorit 1995 mbi mbrojtjen e personave në lidhje me përpunimin e të dhënave personale dhe mbi lëvizjen e lirë të këtyre të dhënave (Direktiva e Mbrojtjes së të Dhënave).[29] Ajo u miratua në 1995-n, në një kohë kur disa Shtete Anëtare kishin miratuar më herët ligje kombëtare të mbrojtjes së të dhënave[30] dhe buroi nga nevoja për të harmonizuar këto ligje, për të garantuar nivel të lartë mbrojtjeje dhe qarkullim të lirë të të dhënave personale ndërmjet Shteteve Anëtare të ndryshme. Lëvizja e lirë e mallrave, kapitaleve, shërbimeve dhe njerëzve në tregun e brendshëm nevojiste qarkullim të lirë të të dhënave, i cili nuk mund të realizohej përveçëse nëse Shtetet Anëtare mbështeteshin në një nivel të njëtrajtshëm të mbrojtjes së të dhënave.

Direktiva e Mbrojtjes së të Dhënave reflektonte parimet e mbrojtjes së të dhënave që përmbanin tashmë ligjet kombëtare dhe Konventa 108, shpesh duke i zgjeruar ato. Ajo mbështetej në mundësinë që jepte neni 11 i Konventës 108 për të shtuar instrumente mbrojtjeje. Në mënyrë

[29] Direktiva 95/46/EC e Parlamentit Evropian dhe e Këshillit e 24 tetorit 1995 për mbrojtjen e individëve në lidhje me përpunimin e të dhënave personale si edhe lëvizjen e lirë të këtyre të dhënave, FZ 1995 L 281.

[30] Shteti gjerman Hesse miratoi ligjin e parë në botë të mbrojtjes së të dhënave më 1970, i cili zbatohej vetëm në atë shtet. Suedia miratoi *Datalagen-in* më 1973; Gjermania miratoi *Bundesdatenschutzgestez*-in më 1976; dhe Franca miratoi *Loi relatif à l'informatique, aux fichiers et aux libertés* më 1977. Në Mbretërinë e Bashkuar, *Data Protection Act-i* u miratua më 1984. Në fund, Vendet e Ulëta miratuan *Wet Persoonregistraties-in* më 1989.

të veçantë, parashikimi në direktivë i mbikëqyrjes së pavarur si instrument për përmirësimin e zbatimit të rregullave të mbrojtjes së të dhënave, rezultoi një kontribut i rëndësishëm për funksionimin efikas të së drejtës evropiane në fushën e mbrojtjes së të dhënave. Për rrjedhojë, ky komponent u integrua në të drejtën e KiE-së në vitin 2001, me anë të Protokollit Shtesë të Konventës 108, çka vërteton bashkëveprimin e ngushtë dhe ndikimin pozitiv të këtyre instrumenteve tek njëri-tjetri përgjatë viteve.

Direktiva e Mbrojtjes së të Dhënave themeloi në BE një sistem mbrojtjeje të të dhënave të hollësishëm dhe gjithëpërfshirës. Sidoqoftë, duke iu referuar sistemit ligjor të BE-së, direktivat nuk janë drejtpërdrejtë të zbatueshme dhe duhen transpozuar në legjislacionet kombëtare të Shteteve Anëtare. Pashmangshmërisht, në transpozimin e dispozitave të direktivës, Shteteve Anëtare u lihet një fushë e caktuar veprimi. Megjithëse synimi ishte që direktiva të siguronte harmonizim të plotë[31] (dhe nivel të plotë mbrojtjeje), në praktikë ajo u transpozua në mënyra në të ndryshme në Shtetet Anëtare. Si rezultat, nëpër BE u miratuan rregulla të ndryshme për mbrojtjen e të dhënave, me përkufizime dhe rregulla të interpretuara në mënyra të ndryshme në legjislacionet kombëtare. Niveli i zbatimit të ligjit dhe masat e sanksioneve ishin gjithashtu të ndryshme ndërmjet Shteteve Anëtare. Së fundi, kishin ndodhur ndryshime të mëdha në teknologjinë e informacionit, krahasuar me periudhën e hartimit të direktivës, në vitet 1990. Të gjitha këto arsye së bashku nxitën reformën e legjislacionit të mbrojtjes së të dhënave të BE-së.

Si rezultat i reformës, në prill 2016, pas diskutimesh intensive, u miratua Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave. Debati mbi domosdoshmërinë e modernizimit të rregullave të mbrojtjes së të dhënave të BE-së nisi në vitin 2009, kur Komisioni ndërmori një konsultim publik, mbi kuadrin e ardhshëm ligjor të së drejtës themelore për mbrojtje të të dhënave personale. Komisioni publikoi propozimin për rregulloren në janar 2012, duke nisur kështu një proces të gjatë legjislativ negociatash midis Parlamentit Evropian dhe Këshillit të BE-së. Pas miratimit, Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave parashikonte një periudhë dy-vjeçare tranzicioni. Ajo u bë plotësisht e zbatueshme më 25 maj 2018, kur u shfuqizua Direktiva e Mbrojtjes së të Dhënave.

Miratimi i Rregullores së Përgjithshme të Mbrojtjes së të Dhënave në 2016-ën modernizoi legjislacionin e mbrojtjes së të dhënave, duke e përshtatur mbrojtjen e të drejtave themelore në kontekstin e sfidave ekonomike e shoqërore të epokës digjitale. GDPR-ja ruan dhe zhvillon parimet bazë dhe të drejtat e subjektit të të dhënave të përcaktuara në Direktivën e Mbrojtjes së të Dhënave. Gjithashtu, ajo parashikon detyrime të reja për organizatat, të cilat duhet të zbatojnë privatësinë që në fazën e konceptimit dhe privatësinë me parapërzgjedhje, të caktojnë Nëpunës të Mbrojtjes së të Dhënave në rrethana të caktuara, të zbatojnë të drejtën e re të transferueshmërisë së të dhënave dhe të respektojnë parimin e përgjegjshmërisë. Sipas së drejtës së BE-së, rregulloret janë drejtpërdrejt të zbatueshme; nuk ka nevojë të nxirret akt zbatimi. Në këtë mënyrë, Rregullorja e Mbrojtjes së të Dhënave ofron një strukturë të vetme rregullash të mbrojtjes së të dhënave për të gjithë BE-në, duke krijuar rregulla konsekuente të

[31] GJDBE, Çështje të bashkuara C-468/10 dhe C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) dhe Federación de Comercio Electrónico y Marketing Directo (FECEMD)k. Administración del Estado*, 24 nëntor 2011, paragrafi 29.

mbrojtjes së të dhënave anembanë BE-së dhe mjedis sigurie juridike, nga i cili mund të përfitojnë operatorët ekonomike dhe individët në cilësinë e "subjekteve të të dhënave".

Gjithsesi, edhe pse Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave është drejtpërdrejt e zbatueshme, Shtetet Anëtare duhet të përditësojnë ligjet e tyre ekzistuese të mbrojtjes së të dhënave, për t'u përafruar plotësisht me rregulloren, duke reflektuar gjithashtu fushëveprimin që u është lënë për dispozitat specifike të pikës 10 të preambulës. Rregullat dhe parimet kryesore të përcaktuara në rregullore dhe të drejtat e përforcuara që ajo u njeh personave, përbëjnë një pjesë të madhe të këtij manuali dhe paraqiten në kapitujt në vijim. Rregullorja përcakton rregulla gjithëpërfshirëse për sa i takon fushës së zbatimit territorial. Ajo zbatohet si për shoqëritë tregtare të vendosura në BE, ashtu edhe për kontrolluesit dhe përpunuesit që janë të vendosur jashtë BE-së, të cilët u ofrojnë mallra, ose shërbime subjekteve të të dhënave në BE, apo monitorojnë sjelljen e tyre. Meqenëse shumë shoqëri tregtare të huaja që operojnë në fushën e teknologjisë, zotërojnë një pjesë të madhe të tregut evropian dhe miliona klientë nga BE-ja, është e rëndësishme që këto organizata t'u nënshtrohen rregullave të mbrojtjes së të dhënave të BE-së, për të garantuar mbrojtjen e individëve dhe konkurrencë të ndershme.

Mbrojtja e të dhënave nga autoritetet e zbatimit të ligjit – Direktiva 2016/680

Direktiva e shfuqizuar e Mbrojtjes së të Dhënave ofronte një regjim gjithëpërfshirës të mbrojtjes së të dhënave. Ky regjim tashmë është përforcuar me miratimin e Rregullores së Përgjithshme të Mbrojtjes së të Dhënave. Megjithëse ishte gjithëpërfshirëse, fusha e zbatimit të Direktivës së Mbrojtjes së të Dhënave të shfuqizuar kufizohej vetëm në aktivitetet në kuadër të tregut të brendshëm dhe në veprimtarinë e autoriteteve publike, përveç autoriteteve ligjzbatuese. Në këtë mënyrë, nevojitej miratimi i instrumenteve të veçanta për të arritur qartësinë dhe ekuilibrin e duhur midis mbrojtjes së të dhënave dhe interesave të tjera legjitime dhe për të zgjidhur sfidat që janë veçanërisht të rëndësishme në sektorë të caktuar, sikurse është rasti i normave që rregullojnë përpunimin e të dhënave personale nga autoritetet ligjzbatuese.

Instrumenti i parë ligjor i BE-së për rregullimin e kësaj çështjeje ishte Vendimi Kuadër i Këshillit 2008/977/JHA për mbrojtjen e të dhënave personale të përpunuara në kuadër të bashkëpunimit policor dhe gjyqësor për çështje penale. Rregullat e tij zbatoheshin vetëm për të dhënat e policisë dhe ato gjyqësore, kur shkëmbehen midis Shteteve Anëtare. Përpunimi i të dhënave personale nga autoritetet e ligjzbatuese në nivel kombëtar përjashtohej nga fusha e zbatimit të tij.

Direktiva 2016/680 për mbrojtjen e personave fizikë në lidhje me përpunimin e të dhënave personale nga autoritetet kompetente për qëllime të parandalimit, hetimit, zbulimit, apo ndjekjes së veprave penale, ose ekzekutimit të dënimeve penale dhe lëvizjen e lirë të këtyre të dhënave[32] e cila njihet si Direktiva e Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale e zgjidhi këtë situatë. Direktiva u miratua paralelisht me Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave, shfuqizoi Vendimin Kuadër 2008/977/JHA dhe krijoi një sistem gjithëpërfshirës të mbrojtjes së të dhënave personale për autoritetet e zbatimit të

[32] Direktiva (BE) 2016/680 e Parlamentit Evropian dhe e Këshillit e 27 prillit 2016 për mbrojtjen e personave fizikë në lidhje me përpunimin e të dhënave personale nga autoritetet kompetente për qëllime të parandalimit, hetimit, zbulimit ose ndjekjes së veprave penale ose ekzekutimit të dënimeve penale dhe lëvizjen e lirë të këtyre të dhënave, FZ 119, 4 maj 2016.

ligjit, duke njohur njëkohësisht veçoritë e përpunimit të të dhënave në lidhje me sigurinë publike. Ndërsa Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave përcakton rregullat e përgjithshme për mbrojtjen e individëve, për sa i takon përpunimit të të dhënave të tyre personale dhe garanton lëvizjen e lirë të këtyre të dhënave brenda BE-së, direktiva përcakton rregullat specifike për mbrojtjen e të dhënave në fushat e bashkëpunimit gjyqësor dhe bashkëpunimit policor për çështjet penale. Direktiva 2016/680 gjen zbatim kur një autoritet kompetent përpunon të dhëna personale për qëllime të parandalimit, hetimit, zbulimit ose ndjekjes së veprave penale. Kur autoritetet kompetente përpunojnë të dhëna personale për qëllime të ndryshme nga të sipërpërmendurat, gjen zbatim regjimi i përgjithshëm i Rregullores së Përgjithshme të Mbrojtjes së të Dhënave. Ndryshe nga paraardhësi i saj (Vendimi Kuadër i Këshillit 2008/977/JHA), fusha e zbatimit të Direktivës 2016/680 shtrihet edhe tek përpunimi që autoritetet ligjzbatuese kryejnë në nivel kombëtar dhe nuk kufizohet tek shkëmbimet e këtyre të dhënave midis Shteteve Anëtare. Gjithashtu, direktiva synon të vendosë ekuilibër midis të drejtave të personave dhe objektivave legjitime të përpunimit për qëllime sigurie.

Për të arritur këtë, direktiva garanton të drejtën për mbrojtje të të dhënave personale dhe parimet thelbësore që duhet të rregullojnë përpunimin e të dhënave, duke ndjekur ngushtësisht rregullat dhe parimet e përcaktuara në Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave. Të drejtat e individëve dhe detyrimet që u janë ngarkuar kontrolluesve, për shembull në lidhje me sigurinë e të dhënave, mbrojtjen e të dhënave që në fazën e konceptimit dhe me parapërzgjedhje dhe njoftimet për shkeljet ndaj të dhënave, u përngjajnë të drejtave dhe detyrimeve në Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave. Direktiva merr gjithashtu parasysh dhe mundohet të zgjidhë sfidat e reja teknologjike, të cilat mund të cënojnë rëndë individët, sikurse përdorimi i teknikave të profilizimit nga autoritetet ligjzbatuese. Si parim, vendimet e mbështetura vetëm në përpunimin automatik, përfshirë profilizimin, duhet të jenë të ndaluara.[33] Gjithashtu, ato nuk duhet të mbështeten në të dhëna sensitive. Këto parime u nënshtrohen disa përjashtimeve të parashikuara në direktivë. Po ashtu, përpunimi nuk duhet të shkaktojë diskriminim të askujt.[34]

Direktiva përmban gjithashtu rregulla për të garantuar përgjegjshmërinë e kontrolluesve. Këta të fundit duhet të caktojnë një nëpunës për mbrojtjen e të dhënave, i cili duhet të monitorojë zbatimin e rregullave të mbrojtjes së të dhënave, të informojë dhe këshillojë njësinë dhe nëpunësit që kryejnë përpunimin mbi detyrimet e tyre dhe të bashkëpunojë me autoritetin mbikëqyrës.

Përpunimi i të dhënave personale në sektorin e policisë dhe të drejtësisë penale i nënshtrohet tashmë mbikëqyrjes nga ana e autoriteteve të pavarura mbikëqyrëse. Si regjimi ligjor i përgjithshëm i mbrojtjes së të dhënave, ashtu edhe regjimi specifik i mbrojtjes së të dhënave për çështje të zbatimit të ligjit dhe çështje penale duhet të respektojnë kriteret e Kartës së të Drejtave Themelore të BE-së.

[33] Direktiva e Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale, neni 11, pika 1.
[34] *Ibid.,* neni 11, pika 2 dhe 3.

Regjimi specifik për përpunimin e të dhënave në kontekstin e bashkëpunimit policor dhe gjyqësor i përcaktuar nga Direktiva e Mbrojtjes së të Dhënave për Autoritetet e Policisë dhe të Drejtësinë Penale përshkruhet në hollësi në Seksionin 8.

Direktiva e privatësisë dhe komunikimeve elektronike

Edhe në sektorin e komunikimeve elektronike u vlerësua e nevojshme të hartohen rregulla speciale për mbrojtjen e të dhënave. Me zhvillimin e internetit, telefonisë fikse e asaj të lëvizshme, ishte e rëndësishme të garantohej respektimi i të drejtave të përdoruesve për privatësi dhe konfidencialitet. Direktiva 2002/58/EC[35] në lidhje me përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në komunikimet elektronike (Direktiva e privatësisë dhe komunikimeve elektronike ose Direktiva e-Privatësi) përcakton rregullat për sigurinë e të dhënave personale në këto rrjete, njoftimin për shkeljet ndaj të dhënave personale dhe konfidencialitetin e komunikimeve.

Për sa i përket sigurisë, operatorët e shërbimeve të komunikimeve elektronike, midis të tjerash, duhet të garantojnë që aksesi tek të dhënat personale të kufizohet vetëm tek personat e autorizuar dhe të parandalojnë shkatërrimin, humbjen apo dëmtimin aksidental të të dhënave personale.[36] Kur ekziston rrezik për shkelje të sigurisë së rrjetit publik të komunikimeve, operatorët duhet të njoftojnë abonentët në lidhje me këtë rrezik.[37] Nëse pavarësisht masave të sigurisë të marra, ndodh një shkelje e sigurisë, operatorët duhet të njoftojnë autoritetin kombëtar kompetent, i cili është i ngarkuar me zbatimin e direktivës, në lidhje me shkeljen ndaj të dhënave personale. Në disa raste, operatorët janë të detyruar të njoftojnë edhe individët për shkeljet ndaj të dhënave personale, konkretisht kur shkelja ka të ngjarë të cenojë të dhënat personale, apo privatësinë e tyre.[38] Konfidencialiteti i komunikimeve përcakton që dëgjimi, përgjimi, regjistrimi, ose çdo lloj tjetër survejimi, apo interceptimi i komunikimeve dhe të dhënave të trafikut, është në parim i ndaluar. Direktiva ndalon gjithashtu komunikimet e pa kërkuara (shpesh të quajtura "spam"), përveçse kur përdoruesit kanë dhënë pëlqimin e tyre dhe nëse zbatojnë rregulla për vendosjen e "*cookies*-ve" në kompjuterë dhe pajisje të tjera. Këto detyrime thelbësore negative tregojnë qartësisht se konfidencialiteti i komunikimeve është i lidhur ngushtësisht me mbrojtjen e të drejtës për respektim të jetës private, të sanksionuar në nenin 7 të Kartës dhe me të drejtën për mbrojtje të të dhënave personale, të sanksionuar në nenin 8 të Kartës.

Në janar 2017, Komisioni publikoi një propozim për një rregullore në lidhje me respektimin e jetës private dhe mbrojtjen e të dhënave personale në komunikimet elektronike, e cila synon të zëvendësojë Direktivën e e-Privatësisë. Reforma ka për qëllim të përafrojë rregullat e komunikimeve elektronike, me regjimin e ri të mbrojtjes së të dhënave të vendosur nga Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave. Rregullorja re do të jetë drejtpërdrejtë e zbatueshme në mbarë BE-në; çdo individ do të gëzojë të njëjtin nivel mbrojtje të komunikimeve elektronike, ndërsa operatorët e shërbimeve të telekomunikimit dhe shoqëritë

[35] Direktiva 2002/58/EC e Parlamentit Evropian dhe e Këshillit e 12 korrikut 2002 në lidhje me përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në komunikimet elektronike, FZ L 201 (Direktiva e privatësisë dhe komunikimeve elektronike ose Direktiva e-Privatësi).
[36] Direktiva e privatësisë dhe komunikimeve elektronike, neni 4, pika 1.
[37] *Ibid*., neni 4, pika 2.
[38] *Ibid*., neni 4, pika 3.

tregtare të përfitojnë nga qartësia e dispozitave, nga siguria juridike dhe nga ekzistenca e një pakete të vetme rregullash në të gjithë BE-në. Rregullat e propozuara mbi konfidencialitetin e komunikimeve elektronike do të zbatohen gjithashtu edhe për aktorët e rinj që ofrojnë shërbime komunikimi elektronik, të cilët nuk mbulohen nga Direktiva e e-Privatësisë. Kjo e fundit mbulonte vetëm operatorët tradicionalë të shërbimeve të telekomunikimit. Për shkak të rritjes masive të përdorimit të shërbimeve të tilla si Skype, WhatsApp, Facebook Messenger dhe Viber për dërgimin e mesazheve, apo thirrjeve, këto shërbime *over-the-top* (OTT) do të përfshihen tashmë në fushën e zbatimit të rregullores dhe do të duhet të zbatojnë kriteret e saj për mbrojtjen e të dhënave, privatësinë dhe sigurinë. Gjatë periudhës së hartimit të këtij manuali, është duke u zhvilluar një proces legjislativ në lidhje me rregullat e e-Privatësisë.

Rregullorja nr. 45/2001

Meqenëse Direktiva e Mbrojtjes së të Dhënave gjente zbatim vetëm për Shtetet Anëtare të BE-së, nevojitej një instrument tjetër ligjor për të rregulluar mbrojtjen e të dhënave në përpunimin e të dhënave personale, nga ana e institucioneve dhe organeve të BE-së. Rregullorja (KE) nr. 45/2001 për mbrojtjen e personave në lidhje me përpunimin e të dhënave personale nga institucionet dhe organet e Komunitetit dhe lëvizjen e lirë të këtyre të dhënave (Rregullorja për Mbrojtjen e të Dhënave e Institucioneve të BE-së) e përmbush këtë objektiv.[39]

Rregullorja nr. 45/2001 ndjek me besnikëri parimet e regjimit të përgjithshëm të mbrojtjes së të dhënave të BE-së dhe i zbaton këto parime për përpunimin e të dhënave që zhvillohet nga institucionet dhe organet e BE-së gjatë ushtrimit të funksioneve të tyre. Gjithashtu, ajo cakton një autoritet mbikëqyrës të pavarur për të monitoruar zbatimin e dispozitave të saj, Mbikëqyrësin Evropian të Mbrojtjes së të Dhënave (EDPS). EDPS-ja ka kompetenca mbikëqyrjeje dhe ka për detyrë të monitorojë përpunimin e të dhënave personale në institucionet dhe organet e BE-së dhe të shqyrtojë e hetojë ankesa për shkelje të pretenduara të rregullave të mbrojtjes së të dhënave. Gjithashtu ai këshillon institucionet dhe organet e BE-së për të gjitha çështjet që kanë të bëjnë me mbrojtjen e të dhënave personale, duke nisur nga iniciativat ligjore, tek hartimi i rregulloreve të brendshme të përpunimit të të dhënave.

Në janar 2017, Komisioni Evropian paraqiti një propozim për një rregullore të re për përpunimin e të dhënave nga ana e institucioneve të BE-së, e cila do të shfuqizojë rregulloren e tanishme. Ashtu si edhe me reformimin e Direktivës së e-Privatësisë, reformimi i Rregullores nr. 45/2001 do të modernizojë dhe përafrojë rregullat e saj, me regjimin e ri të mbrojtjes së të dhënave të vendosur nga Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave.

Roli i GJDBE-së

GJDBE-ja ka kompetencën për të përcaktuar nëse një Shtet Anëtar i ka plotësuar detyrimet sipas së drejtës së BE-së në fushën e mbrojtjes së të dhënave dhe për të interpretuar legjislacionin e BE-së, me qëllim që të garantojë zbatimin efikas dhe të njëtrajtshëm të tij në të gjithat Shtetet Anëtare. Që prej miratimit të Direktivës së Mbrojtjes së të Dhënave më 1995, është krijuar një korpus i konsiderueshëm jurisprudence, i cila qartëson fushën e zbatimit dhe

[39] Rregullorja (EC) nr. 45/2001 e Parlamentit Evropian dhe e Këshillit e 18 dhjetorit 2000 për mbrojtjen e personave në lidhje me përpunimin e të dhënave personale nga institucionet dhe organet e Komunitetit dhe lëvizjen e lirë të këtyre të dhënave, FZ 2001 L 8.

kuptimin e parimeve të mbrojtjes së të dhënave dhe të drejtës themelore për mbrojtje të të dhënave, të sanksionuar në nenin 8 të Kartës. Megjithëse direktiva është shfuqizuar dhe instrumenti i ri ligjor, Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave ka hyrë tashmë në fuqi, jurisprudenca ekzistuese mbetet e rëndësishme dhe e vlefshme për interpretimin dhe zbatimin e parimeve të mbrojtjes së të dhënave të BE-së, në masën që parimet dhe konceptet thelbësore të Direktivës së Mbrojtjes së të Dhënave të jenë ruajtur në GDPR.

1.2. Kufizimet e së drejtës për mbrojtje të të dhënave personale

Pika kryesore

- E drejta për mbrojtje të të dhënave nuk është një e drejtë absolute; ajo mund të kufizohet nëse është e nevojshme për përmbushjen e një objektivi të interesit të përgjithshëm, ose për të mbrojtur të drejtat dhe liritë e të tjerëve.
- Kushtet për kufizimin e së drejtave për respektim të jetës private dhe për mbrojtje të të dhënave personale renditen në nenit 8 të KEDNJ-së dhe nenin 52, pika 1 të Kartës. Ato janë zhvilluar dhe interpretuar nëpërmjet jurisprudencës së GJEDNJ-së dhe GJDBE-së.
- Referuar së drejtës së KiE-së në fushën e mbrojtjes së të dhënave, përpunimi i të dhënave personale përbën ndërhyrje të ligjshme tek e drejta për respektim të jetës private dhe mund të kryhet vetëm nëse:
  - Është në përputhje me ligjin;
  - Synon përmbushjen e një qëllimi legjitim;
  - Respekton thelbin e të drejtave dhe lirive themelore;
  - Është i nevojshëm dhe proporcional në një shoqëri demokratike, për përmbushjen e një qëllimi legjitim.
- Rendi juridik i BE-së vendos kushte të ngjashme për kufizimet në ushtrimin e të drejtave themelore që mbrohen nga Karta. Çdo kufizim i çdo të drejte themelore, përfshirë atë për mbrojtje të të dhënave, mund të jetë i ligjshëm vetëm nëse:
  - Është në përputhje me ligjin;
  - Respekton thelbin e së drejtës;
  - Është i nevojshëm, me kusht që t'i nënshtrohet parimit të proporcionalitetit; dhe
  - Ndjek një objektiv të interesit të përgjithshëm të njohur nga BE-ja, ose nevojën për të mbrojtur të drejtat e të tjerëve.

E drejta themelore për mbrojtje të të dhënave personale sipas nenit 8 të Kartës nuk është e drejtë absolute, "por duhet vlerësuar në raport me funksionin e saj në shoqëri".[40] Në këtë mënyrë, neni 52, pika 1 e Kartës pohon se mund të vendosen kufizime për ushtrimin e të drejtave të garantuar nga nenet 7 dhe 8 të Kartës, për sa kohë që ato kufizime janë të parashikuara në ligj, respektojnë thelbin e atyre të drejtave e lirive dhe i nënshtrohen parimit të proporcionalitetit, janë të nevojshme dhe përmbushin objektivat e interesit të përgjithshëm të njohura nga BE-ja, ose nevojën për mbrojtur të drejtat dhe liritë e të tjerëve.[41]Po në këtë mënyrë, në sistemin e KEDNJ-së, mbrojtja e të dhënave garantohet nga nenit 8 dhe ushtrimi i asaj të drejte mund të kufizohet, kur është e nevojshme për të ndjekur një qëllim legjitim. Ky seksion trajton kushtet për ndërhyrje sipas KEDNJ-së, sikurse është interpretuar në jurisprudencën e GJEDNJ-së, si dhe kushtet për kufizime të ligjshme sipas nenit 52 të Kartës.

1.2.1 Kriteret për ndërhyrje të justifikuar sipas KEDNJ-së

Përpunimi i të dhënave personale mund të përbëjë ndërhyrje tek e drejta e subjektit të të dhënave për respektim të jetës private, të mbrojtur nga neni 8 i KEDNJ-së.[42] Siç shpjegohet më lart (shih seksionin 1.1.1 dhe seksionin 1.1.4.), ndryshe nga rendi juridik i BE-së, KEDNJ-ja nuk e dallon mbrojtjen e të dhënave personale si të drejtë themelore të veçantë, por si pjesë e të drejtave të mbrojtura nën të drejtën për respektim të jetës private. Kështu, jo çdo aktivitet që përfshin përpunim të dhënash personale mund të hyjë në fushën e zbatimit të nenit 8 të KEDNJ-së. Që të aktivizohet neni 8 duhet së pari të përcaktohet nëse është cenuar një interes privat, apo jeta private e një personi. GJEDNJ-ja e ka trajtuar nocionin e "jetës private" në jurisprudencën e saj si një koncept të gjerë, i cili mbulon edhe aspekte të jetës profesionale, apo sjellje publike. Ajo ka përcaktuar gjithashtu se mbrojtja e të dhënave personale është pjesë e rëndësishme e së drejtës për respektim të jetës private. Gjithsesi, pavarësisht interpretimit të zgjeruar të jetës private, jo të gjitha llojet e përpunimeve do të cenonin *per se* të drejtat e mbrojtura nga neni 8.

Kur GJEDNJ-ja vlerëson se aktivitete përpunimi të caktuara prekin të drejtën e individëve për respektim të jetës private, ajo verifikon nëse ndërhyrja është e justifikuar. E drejta për respektim të jetës private nuk është e drejtë absolute, por duhet ekuilibruar dhe bashkërenduar me interesa dhe të drejta të tjera legjitime, qofshin ato të personave të tjerë (interesa private), apo të shoqërisë në tërësi (interesa publike).

Kushtet sipas së cilave mund të justifikohet ndërhyrja janë:

Në përputhje me ligjin

Referuar jurisprudencës së GJEDNJ-së, ndërhyrja është në përputhje me ligjin nëse mbështetet në një dispozitë të legjislacionit të brendshëm, që paraqet disa cilësi të caktuara. Ligji duhet të jetë "i aksesueshëm nga personat e interesuar dhe efektet e tij të jenë të parashikueshme".[43]

---

[40] Shih, për shembull, GJDBE, Çështje të bashkuara C-92/09 dhe C-93/09, *Volker und Markus Schecke GbR dhe Hartmut Eifert k. Land Hessen* [ÇB] , 9 nëntor 2010, paragrafi 48.

[41] *Ibid*., paragrafi 50.

[42] GJEDNJ, *S. dhe Marper k. Mbretërisë së Bashkuar* [ÇB] , nr. 30562/04 dhe 30566/04, 8 dhjetor 2008, paragrafi 67.

[43] GJEDNJ, *Amann k. Zvicrës* [ÇB] , nr. 27798/95, 16 shkurt 2000, paragrafi 50; shih gjithashtu GJEDNJ, *Kopp k. Zvicrës*, nr. 23224/94, 25 mars 1998, paragrafi 55 dhe GJEDNJ, *Iordachi dhe të Tjerët k. Moldavisë*, nr. 25198/02, 10 shkurt 2009, paragrafi 50.

Rregulli është i parashikueshëm "nëse është formuluar me aq saktësi sa t'i mundësojë çdo individi – nëse është e nevojshme edhe duke e këshilluar – të rregullojë sjelljen e tij".[44] Gjithashtu, "shkalla e saktësisë që kërkohet për "ligjin" në lidhje me këtë, varet nga objekti".[45]

Shembuj: tek *Rotaru k. Rumanisë,*[46] kërkuesi pretendoi shkelje të së drejtës së tij për respektim të jetës private për shkak të mbajtjes dhe përdorimit të dosjes me informacionet e tij personale nga ana e Shërbimit Informativ Rumun. GJEDNJ-ja vërejti se legjislacioni i brendshëm lejonte mbledhjen, regjistrimin dhe arkivimin e informacionit në lidhje me sigurinë kombëtare në dosje sekrete, por nuk përcaktonte asnjë kufizim të ushtrimit të këtyre kompetencave, duke e lënë në vlerësimin e autoriteteve. Për shembull, legjislacioni i brendshëm nuk përcaktonte llojin e informacionit që mund të përpunohej, kategoritë e njerëzve ndaj të cilëve mund të merren masa survejimi, rrethanat në të cilat mund të merren këto masa, apo procedurat që duhen ndjekur. Për rrjedhojë, Gjykata doli në përfundimin se legjislacioni i brendshëm nuk pajtohej me kriterin e parashikueshmërisë së nenit 8 të KEDNJ-së dhe se ky nen ishte shkelur.

Tek *Taylor-Sabori k. Mbretërisë së Bashkuar,*[47] kërkuesi ishte vendosur nën përgjim nga ana e policisë. Duke përdorur një "pager" të klonuar, policia kishte mundur të interceptonte mesazhet që i dërgoheshin atij. Kërkuesi ishte arrestuar me akuzën e trafikimit të lëndëve narkotike në bashkëpunim. Një pjesë e aktakuzës përbëhej nga kopje të teksteve të mesazheve të marra njëkohësisht në *pager*-in e tij, të cilat policia i kishte transkriptuar. Sidoqoftë, gjatë kohës që zhvillohej gjyqi ndaj kërkuesit, nuk ekzistonte asnjë dispozitë në legjislacionin britanik që rregullonte interceptimin e komunikimeve të transmetuara nëpërmjet një sistemi privat të telekomunikimeve. Për pasojë, ndërhyrja tek këto të drejta nuk kishte qenë "në përputhje me ligjin". GJEDNJ-ja doli në përfundimin se ishte shkelur neni 8 i KEDNJ-së.

Vukota-Bojić k. Zvicrës[48] kishte të bënte me përgjimin e kërkueses, një agjente sigurimesh, nga hetues privatë, të angazhuar nga shoqëria e sigurimeve ku ajo punonte. GJEDNJ-ja u shpreh se megjithëse masa e përgjimit që kundërshtohej në kërkesë, ishte porositur nga një shoqëri private sigurimesh, ishte shteti ai që i kishte dhënë kësaj të fundit të drejtën për të paguar shpenzime në kuadër të sigurimit të detyrueshëm shëndetësor dhe për të vjelë kontributet. Shteti nuk mund të përjashtojë veten nga përgjegjësitë që rrjedhin nga Konventa duke deleguar detyrimet e tij tek organizmat private, apo individët. Legjislacioni i brendshëm duhet të parashikonte garancitë e duhura të mbrojtjes nga abuzimi, në mënyrë që ndërhyrja tek të drejtat e përcaktuara në nenin 8 të KEDNJ-së të ishte "në përputhje me ligjin". Për çështjen në fjalë, GJEDNJ-ja doli në përfundimin se kishte pasur shkelje të nenit 8 të KEDNJ-së, për shkak se legjislacioni i brendshëm nuk kishte përcaktuar qartë shtrirjen dhe mënyrën e ushtrimit të kompetencës që u ishte dhënë shoqërive të sigurimit, për të vepruar si autoritete publike në raste mosmarrëveshjesh në lidhje me sigurimet, për të përgjuar një person të siguruar. Në mënyrë të veçantë, legjislacioni nuk kishte parashikuar garancitë e duhura për mbrojtjen nga abuzimi.

[44] GJEDNJ, *Amann k. Zvicrës* [ÇB], nr. 27798/95, 16 shkurt 2000, paragrafi 56; shih gjithashtu GJEDNJ, *Malone k. Mbretërisë së Bashkuar*, nr. 8691/79, 2 gusht 1984, paragrafi 66; GJEDNJ, *Silver dhe të Tjerët k. Mbretërisë së Bashkuar*, nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 mars 1983, paragrafi 88.

[45] GJEDNJ, *The Sunday Times k. Mbretërisë së Bashkuar*, nr. 6538/74, 26 prill 1979, paragrafi 49; shih gjithashtu GJEDNJ, *Silver dhe të Tjerët k. Mbretërisë së Bashkuar*, nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 mars 1983, paragrafi 88.

[46] GJEDNJ, *Rotaru k. Rumanisë* [ÇB], nr. 28341/95, 4 maj 2000, paragrafi 57; shih gjithashtu GJEDNJ, *Association for European Integration and Human Rights dhe Ekimdzhiev k. Bullgarisë*, nr. 62540/00, 28 qershor 2007; GJEDNJ, *Shimovolos k. Rusisë*, nr. 30194/09, 21 qershor 2011; dhe GJEDNJ, *Vetter k. Francës*, nr. 59842/00, 31 maj 2005.

[47] GJEDNJ, *Taylor-Sabori k. Mbretërisë së Bashkuar*, nr. 47114/99, 22 tetor 2002.

[48] GJEDNJ, *Vukota-Bojić k. Zvicrës*, nr. 61838/10, 18 tetor 2016, paragrafi 77.

Qëllimi legjitim

Qëllimi legjitim mund të jetë qoftë një nga interesat publike të përmendura, ashtu edhe mbrojtja e të drejtave dhe lirive të të tjerëve. Sipas nenit 8, pika 2 të KEDNJ-së, qëllimet legjitime, të cilat mund të justifikojnë një ndërhyrje, janë interesat e sigurisë kombëtare, sigurisë publike, ose mirëqenies ekonomike të një vendi, parandalimit të trazirave ose krimit, mbrojtjes së shëndetit, ose moralit dhe mbrojtjes së të drejtave dhe lirive të personave të tjerë.

Shembull: tek çështja *Peck k. Mbretërisë së Bashkuar*,[49] kërkuesi tentoi të vetëvritej në rrugë, duke prerë damarët, pa e ditur se një kamera vëzhgimi ishte duke e filmuar. Pasi policia, e cila ishte duke vëzhguar kamerat, e shpëtoi, ia kaloi filmimet mediave, të cilat i publikuan pa e fshehur fytyrën e kërkuesit. GJEDNJ-ja u shpreh se nuk kishte pasur arsye të rëndësishme, apo të mjaftueshme që të justifikonin përhapjen e drejtpërdrejtë të filmimeve tek publiku nga ana e autoriteteve, pa marrë pëlqimin e kërkuesit, apo pa fshehur identitetin e tij. Gjykata vendosi se ishte shkelur neni 8 i KEDNJ-së.

E domosdoshme në një shoqëri demokratike

GJEDNJ-ja ka theksuar se "nocioni i domosdoshmërisë nënkupton që ndërhyrja duhet të përputhet me një nevojë të ngutshme shoqërore dhe sidomos të jetë proporcionale me qëllimin legjitim të ndjekur".[50] Kur merr në shqyrtim nëse një masë është e domosdoshme për të adresuar një nevojë të ngutshme shoqërore, GJEDNJ-ja analizon rëndësinë dhe përshtatshmërinë e saj në raport me qëllimin e ndjekur. Për këtë qëllim, ajo mund të marrë parasysh nëse ndërhyrja përpiqet të zgjidhë një problem, i cili nëse nuk zgjidhet mund të shkaktojë pasoja negative për shoqërinë, nëse ka prova se ndërhyrja mund të zbusë këto pasoja negative dhe cili është këndvështrimi i përgjithshëm i shoqërisë mbi problemin në fjalë.[51] Për shembull, mbledhja dhe mbajtja e të dhënave personale nga shërbimet e sigurisë, në lidhje me persona të caktuar, të cilët kanë lidhje me lëvizje terroriste, do të përbënte ndërhyrje tek e drejta e individit për respektim të jetës private, paçka se i shërben një nevoje të madhe dhe të ngutshme shoqërore: sigurisë kombëtare dhe luftës kundër terrorizmit. Për të përmbushur kriterin e domosdoshmërisë, ndërhyrja duhet të jetë edhe proporcionale. Tek jurisprudenca e GJEDNJ-së, proporcionaliteti trajtohet në suazën e konceptit të domosdoshmërisë. Proporcionaliteti kërkon që ndërhyrja tek të drejtat e mbrojtura nga KEDNJ-ja, të mos shkojë përtej asaj çka është e nevojshme për përmbushjen e qëllimit legjitim të ndjekur. Faktorë të rëndësishëm që duhen marrë parasysh kur vlerësohet proporcionaliteti janë qëllimi i ndërhyrjes, veçanërisht numri i personave të prekur dhe garancitë, apo udhëzimet që janë dhënë për kufizimin e shtrirjes së saj, apo të pasojave negative tek të drejtat e individëve.[52]

[49] GJEDNJ, *Peck k. Mbretërisë së Bashkuar,* nr. 44647/98, 28 janar 2003, paragrafi 85.
[50] GJEDNJ, *Leander k. Suedisë*, nr. 9248/81, 26 mars 1987, paragrafi 58.
[51] Grupi i Punës i Nenit 29 për Mbrojtjen e të Dhënave (Article 29 Working Party) (2014), *Opinion on the application of the necessity and proportionality concepts and data protection within the law enforcement sector*, WP 211, Bruksel, 27 shkurt 2014, fq. 7–8.
[52] *Ibid.,* fq. 9-11.

Shembull: tek çështja *Khelili kundër Zvicrës,*[53] gjatë një kontrolli, policia i gjeti kërkueses disa kartëvizita në të cilat shkruhej: "Grua e këndshme, e bukur, mbi të tridhjetat, në kërkim të një burri për të dalë për një pije së bashku, ose për të dalë së bashku herë pas here. Tel. nr. [...]". Kërkuesja pretendonte se pas kontrollit, policia regjistroi emrin e saj në dosje si prostitutë, zanat të cilin ajo e mohonte vazhdimisht. Kërkuesja kërkonte që fjala "prostitutë" të fshihej nga dosjet kompjuterike të policisë. GJEDNJ-ja pranoi në parim se në disa rrethana, ruajtja e të dhënave personale të një individi, bazuar në dyshimin se ai person mund të kryejë një vepër tjetër penale, është proporcionale. Gjithsesi, në rastin e kërkueses, dyshimet për ushtrim prostitucioni dukeshin tepër të zbehta dhe të përgjithshme, nuk mbështeteshin në fakte konkrete, duke qenë se ajo nuk ishte dënuar kurrë për ushtrim të paligjshëm prostitucioni dhe rrjedhimisht nuk mund të konsiderohej se përputhej me një "nevojë të ngutshme shoqërore", sipas kuptimit të nenit 8 të KEDNJ-së. Duke theksuar se u takonte autoriteteve të provonin saktësinë e të dhënave të ruajtura në lidhje me kërkuesen dhe rëndësinë e ndërhyrjes tek të drejtat e saj, Gjykata vendosi se mbajtja e fjalës "prostitutë" në dosjet policore për vite me radhë, nuk kishte qenë e nevojshme në një shoqëri demokratike. Gjykata doli me përfundimin se ishte shkelur neni 8 i KEDNJ-së.

Shembull: tek *S. dhe Marper k. Mbretërisë së Bashkuar,*[54] të dy kërkuesit ishin arrestuar dhe akuzuar për vepra penale. Policia u mori gjurmët e gishtave dhe kampionët e ADN-së, në përputhje me Ligjin për Policinë dhe Provat Penale. Kërkuesit nuk ishin dënuar kurrë për veprat penale: njëri ishte liruar nga gjykata, ndërsa procedimi penal për kërkuesin e dytë ishte pushuar. Megjithatë, gjurmët e tyre të gishtave, profilet e ADN-së dhe kampionet qelizore ishin mbajtur dhe magazinuar nga policia në një bazë të dhënash dhe legjislacioni kombëtar lejonte mbajtjen e tyre pa asnjë afat kohor. Ndërsa Mbretëria e Bashkuar argumentonte se mbajtja e tyre ndihmonte në identifikimin e personave që kryejnë vepra penale në të ardhmen, ndaj dhe synonte përmbushjen e qëllimit legjitim të parandalimit dhe zbulimit të krimit, GJEDNJ-ja e vlerësoi ndikimin tek e drejta e kërkuesit për respektim të jetës private si të pajustifikuar. Ajo ritheksoi se parimet thelbësore të mbrojtjes së të dhënave përcaktojnë që mbajtja e të dhënave duhet të jetë proporcionale në raport me qëllimin e mbledhjes dhe se afatet e mbajtjes së tyre duhet të jenë të kufizuara. Gjykata pranoi se zgjerimi i bazës së të dhënave, duke përfshirë edhe profilet e ADN-së jo vetëm të personave të dënuar, por edhe të të gjithë individëve të cilët kishin qenë të dyshuar, por jo të dënuar, mund të ndihmonte për zbulimin dhe parandalimin e krimit në Mbretërinë e Bashkuar, megjithatë ajo kishte mbetur "e habitur nga natyra e përgjithshme dhe që s'bënte dallim, e kompetencës për të mbajtur të dhënat".[55]

Për shkak të sasisë së pasur të informacionit gjenetik dhe shëndetësor që përmbajnë kampionet qelizore, ndërhyrja tek e drejta për jetë private të kërkuesit ishte tepër e rëndë. Gjurmët e gishtave dhe kampionet mund të merren nga personat e arrestuar dhe të mbahen për një kohë të pacaktuar në bazën e të dhënave të policisë, pavarësisht karakterit dhe seriozitetit të veprës penale dhe madje edhe për vepra penale që nuk dënohen me heqje lirie. Për më tepër, mundësia që kishin individët e shpallur të pafajshëm, që të dhënat e tyre të hiqeshin nga baza e të dhënave, ishte e kufizuar. Së fundi, GJEDNJ-ja i kushtoi rëndësi të veçantë faktit se njëri kërkues ishte njëmbëdhjetë vjeç në kohën e arrestimit. Mbajtja e të dhënave personale të një të mituri i cili nuk është dënuar, mund të jetë tepër e dëmshme për shkak të vulnerabilitetit dhe rëndësisë së zhvillimit dhe integrimit të tyre në shoqëri.[56]

[53] GJEDNJ, *Khelili k. Zvicrës,* nr. 16188/07, 18 tetor 2011.
[54] GJEDNJ, *S. dhe Marper k. Mbretërisë së Bashkuar* [ÇB] , nr. 30562/04 dhe 30566/04, 4 dhjetor 2008.
[55] *Ibid.,* paragrafi 119.
[56] *Ibid.,* paragrafi 124.

Gjykata vendosi unanimisht se mbajtja e të dhënave përbënte cenim jo proporcional të së drejtës për jetë private dhe nuk mund të konsiderohej si e domosdoshme në një shoqëri demokratike.

Shembull: tek çështja *Leander kundër Suedisë,*[57] GJEDNJ-ja vendosi se survejimi i fshehtë i personave që aplikojnë për punësim në poste me rëndësi për sigurinë kombëtare, në vetvete, nuk binte ndesh me normat e domosdoshmërisë në një shoqëri demokratike. Garancitë specifike të parashikuara nga legjislacioni kombëtar për mbrojtjen e interesave të subjektit të të dhënave, për shembull, kontrolle nga parlamenti dhe nga Ministri i Drejtësisë, e detyruan GJEDNJ-në të dilte në përfundimin se sistemi suedez i kontrollit të personelit respektonte kërkesat e nenit 8, pika 2 të KEDNJ-së. Duke pasur parasysh fushën e gjerë të vlerësimit që kishte në dispozicion, shteti i paditur kishte të drejtë të çmonte se në rastin e kërkuesit, interesat e sigurisë kombëtare prevalonin mbi ato individuale. Gjykata doli në përfundimin se nuk kishte pasur shkelje të nenit 8 të KEDNJ-së.

1.2.2. Kushtet për kufizime të ligjshme sipas Kartës së të Drejtave Themelore të BE-së

Struktura dhe formulimi i Kartës ndryshon nga ai i KEDNJ-së. Karta nuk përdor nocionin e ndërhyrjes tek të drejtat e garantuara, por përmban një dispozitë për kufizimin, apo kufizimet e ushtrimit të së drejtave dhe lirive të njohura nga Karta.

Sipas nenit 52, pika 1, kufizimet e ushtrimit të së drejtave dhe lirive të njohura nga Karta dhe rrjedhimisht të ushtrimit të së drejtës për mbrojtje të të dhënave personale, janë të pranueshme vetëm nëse:

- Janë të përcaktuara me ligj; dhe
- Respektojnë thelbin e së drejtës për mbrojtje të të dhënave; dhe
- U nënshtrohen parimit të proporcionalitetit, janë të domosdoshme;[58] dhe
- Përmbushin objektivat e interesit të përgjithshëm të njohura nga Bashkimi, ose nevojën për të mbrojtur të drejtat dhe liritë e të tjerëve.

Meqenëse mbrojtja e të dhënave personale është një e drejtë themelore e veçantë dhe e dallueshme në rendin juridik të BE-së, e mbrojtur nga neni 8 i Kartës, çdo përpunim i të dhënave personale përbën në vetvete ndërhyrje tek kjo e drejtë. Nuk ka rëndësi nëse të dhënat personale lidhen me jetën private të një individi, janë sensitive, apo nëse subjektet e të dhënave janë cënuar në ndonjë mënyrë. Që të jetë e ligjshme, ndërhyrja duhet të respektojë të gjitha kushtet e renditura në nenin 52, pika 1 të Kartës.

Të parashikuara me ligj

Kufizimet e së drejtës për mbrojtje të të dhënave personale duhet të jenë të parashikuara me ligj. Ky kriter nënkupton që kufizimet duhet të mbështeten në një bazë ligjore, e cila të jetë e qartë dhe e parashikueshme sa duhet, si dhe e formuluar me saktësi të mjaftueshme për t'i mundësuar individëve që të kuptojnë detyrimet dhe të rregullojnë sjelljet e tyre. Gjithashtu,

[57] GJEDNJ, *Leander k. Suedisë*, nr. 9248/81, 26 mars 1987, paragrafët 59 dhe 67.
[58] Mbi vlerësimin e domosdoshmërisë së masave që kufizojnë të drejtën themelore për mbrojtje të të dhënave personale, shih EDPS (2017), *Necessity Toolkit*, Bruksel, 11 prill 2017.

baza ligjore duhet të përcaktojë qartësisht fushën e saj të veprimit dhe mënyrën e ushtrimit të kompetencave nga ana e autoriteteve kompetente, për të mbrojtur individët nga ndërhyrja arbitrare. Ky interpretim i përngjet kriterit për "ndërhyrje të ligjshme" të jurisprudencës së GJEDNJ-së[59] dhe është theksuar që kuptimi i shprehjes "të parashikuara me ligj" të përdorur në Kartë të jetë i njëjtë me atë të përshkruar në KEDNJ.[60] Jurisprudenca e GJEDNJ-së dhe sidomos koncepti i "cilësisë së ligjit" që ajo ka zhvilluar përgjatë viteve, është një element i rëndësishëm që duhet marrë parasysh nga GJDBE-ja gjatë interpretimit të fushës së veprimit të nenit 52, pika 1 të Kartës.[61]

Respektimi i thelbit të së drejtës

Në rendin juridik të BE-së, çdo kufizim i të drejtave themelore të mbrojtura nga Karta, duhet të respektojë thelbin e atyre të drejtave. Kjo do të thotë se kufizimet të cilat janë të tepruara dhe cenuese aq sa të privojnë një të drejtë themelore nga përmbajtja bazë e saj, janë të pajustifikueshme. Nëse thelbi i së drejtës është kompromentuar, kufizimi duhet të konsiderohet i paligjshëm, pa analizuar më tej nëse i shërben një objektivi të interesit të përgjithshëm, apo nëse plotëson kriterin e domosdoshmërisë dhe proporcionalitetit.

Shembull: çështja *Schrems*[62] kishte të bënte me mbrojtjen e personave në lidhje me transferimin e të dhënave personale të tyre tek shtete të treta, në rastin konkret, në Shtetet e Bashkuara. Schrems-i, një qytetar austriak, përdorues i Facebook-ut prej disa vitesh, depozitoi një ankesë pranë autoritetit mbikëqyrës të mbrojtjes së të dhënave të Irlandës, për të denoncuar transferimin e të dhënave të tij personale nga dega irlandeze e Facebook-ut tek Facebook Inc.-u dhe serverat e vendosur në SHBA, ku ato përpunoheshin. Ai argumentonte se bazuar në zbulimet e sinjalizuesit amerikan Edward Snowden, mbi aktivitetet e survejimit që zhvillonin shërbimet informative amerikane, legjislacioni dhe praktika e SHBA-ve nuk ofronte mbrojtje të mjaftueshme të të dhënave personale të transferuara në territorin e tyre. Snowden-i kishte sinjalizuar se Agjencia Kombëtare e Sigurisë përgjonte drejtpërdrejt serverët e firmave, sikurse të Facebook-ut dhe mund të lexonte përmbajtjen e bisedave dhe mesazheve private.

Transferimet e të dhënave drejt SHBA-ve mbështeteshin mbi bazën e një vendimi të Komisionit për nivel të mjaftueshëm të mbrojtjes, të miratuar në vitin 2000, i cili lejonte transferimet drejt shoqërive tregtare të SHBA-ve, të cilat vetë-angazhoheshin për mbrojtjen e të dhënave personale të transferuara nga BE-ja dhe për respektimin e të ashtuquajturave "parime të Portit të Sigurt" (*Safe Harbour principles*). Kur çështja iu paraqit GJDBE-së, kjo e fundit shqyrtoi vlefshmërinë e vendimit të Komisionit bazuar tek Karta. Ajo ritheksoi se mbrojtja e të drejtave themelore në BE kërkon që përjashtimet dhe kufizimet e këtyre të drejtave të zbatohen vetëm kur është e domosdoshme. GJDBE-ja vlerësoi se legjislacioni që autorizonte aksesin e autoriteteve publike në mënyrë të përgjithshme tek përmbajtja e komunikimeve elektronike, "cënonte thelbin e së drejtës themelore për respektim të jetës private, të garantuar nga neni 7 i Kartës". E drejta do të bëhej e pakuptimtë nëse autoritetet

[59] EDPS (2017), *NecessityToolkit,* Bruksel, 11 prill 2017, fq. 4; shih po ashtu GJDBE, *Opinion 1/15 of the Court (Grand Chamber),* 26 korrik 2017.
[60] GJDBE, Çështje të bashkuara C-203/15 dhe C-698/15, *Tele2 Sverige AB k. Post- och telestyrelsen* and *Secretary of State for the Home Department k. Tom Watson, Peter Brice, Geoffrey Lewis, Opinion i Avokatit të Përgjithshëm Saugmandsgaard Øe*, publikuar më 19 korrik 2016, paragrafi 140.
[61] GJDBE, C-70/10, *Scarlet Extended SA k. Société belge des auteurs compositeurs et éditeurs (SABAM), Opinion i Avokatit të Përgjithshëm Cruz Villalón*, publikuar më 14 prill 2011, paragrafi 100.
[62] GJDBE, C-362/14, *Maximilian Schrems k. Data Protection Commissioner* [ÇB] , 6 tetor 2015.

publike të SHBA-ve do të autorizoheshin të hynin në mënyrë të parregullt, pa asnjë justifikim objektiv të bazuar mbi vlerësime konkrete të sigurisë kombëtare ose të parandalimit të krimit, të cilat të jenë specifike për individin e përfshirë dhe pa i shoqëruar ato praktika survejimi me masa të përshtatshme sigurie ndaj abuzimit me pushtetin.

Gjithashtu GJDBE-ja vërejti se "legjislacioni i cili nuk parashikon asnjë mundësi për individin që të ndjekë rrugën gjyqësore, me qëllim që t'i jepet akses tek të dhënat personale në lidhje me të, ose të korrigjojë apo të fshijë ato të dhëna", shkel të drejtën themelore për mbrojtje gjyqësore të efektshme (neni 47 i Kartës). Kështu, Vendimi "Porti i Sigurt" nuk siguronte nivel të barasvlershëm të mbrojtjes së të drejtave themelore nga ana e SHBA-ve me atë të BE-së sipas direktivës të interpretuar mbështetur tek Karta. Për pasojë, GJDBE-ja e shfuqizoi vendimin.[63]

Shembull: tek çështja *Digital Rights Ireland,*[64] GJDBE-ja shqyrtoi përputhshmërinë e Direktivës 2006/24/EC (Direktiva e Mbajtjes së të Dhënave) me nenet 7 dhe 8 të Kartës. Direktiva detyronte operatorët e shërbimeve të komunikimeve elektronike të mbanin të dhënat e trafikut dhe të vendndodhjes për një periudhë prej të paktën gjashtë muajsh deri në 24 muaj dhe t'u jepnin akses autoriteteve kombëtare kompetente tek ato të dhëna për qëllime të parandalimit, hetimit, zbulimit dhe ndjekjes së krimeve të rënda. Direktiva nuk lejonte mbajtjen e përmbajtjes së komunikimeve elektronike. GJDBE-ja vërejti se të dhënat që operatorët duhet të mbanin në zbatim të direktivës përfshinin të dhëna të nevojshme për gjurmimin dhe identifikimin e burimit dhe destinacionit të komunikimit, datën, orën dhe kohëzgjatjen e komunikimit, numrin thirrës, numrat e thirrur dhe adresat e IP-ve. Ato të dhëna, "në tërësinë e tyre, mund të lejojnë të nxirren përfundime tepër të sakta në lidhje me jetët private të personave, të dhënat e të cilëve mbahen, sikurse zakonet e jetës së përditshme, vendbanimet e përkohshme ose të përhershme, lëvizjet e përditshme ose të tjera, aktivitetet e zhvilluara, marrëdhëniet shoqërore të atyre personale dhe ambientet shoqërore të frekuentuara prej tyre".

Në këtë mënyrë, mbajtja e të dhënave personale sipas direktivës përbënte ndërhyrje tepër serioze tek të drejtat për mbrojtje të privatësisë dhe të të dhënave personale. Gjithsesi, GJDBE-ja u shpreh se ndërhyrja nuk prekte negativisht thelbin e këtyre të drejtave. Për sa i përket së drejtës për privatësi, thelbi i saj nuk cënohej, pasi direktiva nuk lejonte aksesin tek përmbajtja e komunikimeve elektronike. Në mënyrë të ngjashme, thelbi i së drejtës për mbrojtje të të dhënave personale nuk cenohej, meqenëse direktiva detyronte operatorët e shërbimeve të komunikimeve elektronike të respektonin disa parime të mbrojtjes së të dhënave dhe të sigurisë së të dhënave dhe të zbatonin masat e duhura teknike dhe organizative për këtë qëllim.

Domosdoshmëria dhe proporcionaliteti

[63] Vendimi i GJDBE-së për të shfuqizuar Vendimin e Komisionit 520/2000/KE bazohej gjithashtu edhe në kritere të tjera, të cilat do të shqyrtohen në seksione të tjera të këtij manuali. Në mënyrë të veçantë, GJDBE-ja vlerësoi se vendimi kufizonte në mënyrë të paligjshme kompetencat e autoriteteve kombëtare mbikëqyrëse të mbrojtjes së të dhënave. Gjithashtu, në regjimin e "Portit të Sigurt" nuk ekzistonin mjete juridike për individët në rast se ata dëshironin të kishin akses tek të dhënat personale në lidhje me ta dhe/ose të kryenin korrigjimin ose fshirjen e tyre. Kështu, thelbi i së drejtës themelore për mbrojtje të efektshme gjyqësore të mishëruar në nenin 47 të Kartës ishte kompromentuar gjithashtu.

[64] GJDBE, Çështje të bashkuara C-293/12 dhe C-594/12, *Digital Rights Ireland k. Minister for Communications, Marine and Natural Resources dhe të Tjerët dhe Kärntner Landesregierung dhe të Tjerët* [ÇB] , 8 prill 2014.

Neni 52, pika 1 përcakton se në përputhje me parimin e propocionalitetit, mund të bëhen kufizime në ushtrimin e të drejtave dhe lirive themelore të njohura nga Karta, vetëm nëse ato janë të domosdoshme.

Kufizimi mund të jetë i **domosdoshëm** nëse është e nevojshme të miratohen masa për objektivin e interesit publik të ndjekur, por domosdoshmëria, sikurse është interpretuar nga GJDBE-ja, nënkupton gjithashtu që masat e miratuara të jenë më pak ndërhyrëse krahasuar me opsionet e tjera për arritjen e të njëjtit qëllimi. Për kufizimet e së drejtave për respektim të jetës private dhe mbrojtje të të dhënave personale, GJDBE-ja analizon rigorozisht domosdoshmërinë, duke theksuar se "përjashtimet dhe kufizimet duhet të zbatohen vetëm në masën që është absolutisht e nevojshme". Nëse një kufizim vlerësohet si i domosdoshëm, është gjithashtu e nevojshme të vlerësohet nëse ai është proporcional.

Proporcionalitet do të thotë që përfitimet që burojnë nga kufizimi të jenë më të mëdha sesa dëmet që ky i fundit shkakton tek ushtrimi i të drejtës themelore përkatëse.[65] Për të zvogëluar dëmet dhe risqet e ushtrimit të së drejtave për privatësi dhe mbrojtje të të dhënave, është e rëndësishme që kufizimet të përmbajnë masat e duhura të mbrojtjes.

Shembull: tek çështja *Volker und Markus Schecke,*[66] GJDBE-ja doli në përfundimin se vendosja e një detyrimi për publikimin e të dhënave personale të secilit personi fizik që ishte subjekt përfitues ndihme nga fonde të caktuara bujqësore, pa bërë asnjë dallim bazuar në kriteret përkatëse, sikurse periudha në të cilën këta persona e kanë përfituar këtë lloj ndihme, intervalet e dhënies së ndihmës, apo lloji dhe sasia e saj, Këshilli dhe Komisioni kishin tejkaluar kufijtë e parimit të proporcionalitetit.

Rrjedhimisht, GJDBE-ja vendosi se ishte e nevojshme të shpallte të pavlefshme disa dispozita të Rregullores së Këshillit (EC) nr. 1290/2005 dhe të deklaronte të pavlefshme Rregulloren nr. 259/2008 në tërësinë e saj.[67]

Shembull: tek *Digital Rights Ireland,*[68] GJDBE-ja u shpreh se ndërhyrja tek e drejta për privatësi shkaktuar nga Direktiva e Mbajtjes së të Dhënave, nuk cënonte thelbin e asaj të drejte, meqenëse ajo e ndalonte mbajtjen e përmbajtjes së komunikimeve elektronike. Megjithatë, ajo doli në përfundimin se direktiva shkonte ndesh me nenet 7 dhe 8 të Kartës dhe e shpalli të pavlefshme. Për shkak se të dhënat e trafikut dhe të vendndodhjes, duke i kombinuar dhe të marra në tërësinë e tyre, mund të analizoheshin dhe mundësonin skicimin e një tabloje të hollësishme të jetëve private të individëve, kjo përbënte cënim të rëndë të këtyre të drejtave. GJDBE-ja mori parasysh se direktiva kërkonte mbajtjen e të gjitha të dhënave të trafikut në lidhje me telefoninë fikse, telefoninë e lëvizshme, aksesin në internet, postën elektronike dhe telefoninë në internet, duke gjetur zbatim tek të gjitha pajisjet e komunikimit elektronik – përdorimi i të cilave është i përhapur gjerësisht në jetën e përditshme të njerëzve. Praktikisht, ajo përbënte interferencë që prekte krejt popullsinë e Evropës. Sipas GJDBE-së, duke pasur parasysh shtrirjen dhe seriozitetin e ndërhyrjes,

[65] EDPS (2017), *Necessity Toolkit*, fq. 5.
[66] GJDBE, Çështje të bashkuara C-92/09 dhe C-93/09, *Volker und Markus Schecke GbR dhe Hartmut Eifert k. Land Hessen* [ÇB] , 9 nëntor 2010, paragrafët 89 dhe 86.
[67] Rregullore e Këshillit (EC) nr. 1290/2005 e 21 qershorit 2005 mbi financimin e politikës së përbashkët bujqësore, FZ 2005 L 209; Rregullore e Komisionit (EC) nr. 259/2008 e 18 marsit 2008 që përcakton rregullat e hollësishme për zbatimin e Rregullores së Këshillit (EC) nr. 1290/2005 për sa i përket publikimit të informacionit mbi subjektet përfituese të fondeve që burojnë nga Fondi Evropian i Garancisë Bujqësore (EAGF) dhe Fondi Bujqësor Evropian për Zhvillim Rural (EAFRD), FZ 2008 L 76.

[68] GJDBE, Çështje të bashkuara C-293/12 dhe C-594/12, *Digital Rights Ireland Ltd k. Minister for Communications, Marine and Natural Resources dhe të Tjerët dhe Kärntner Landesregierung dhe të Tjerët* [ÇB] , 8 prill 2014, parag. 39.

mbajtja e të dhënave të trafikut dhe të vendndodhjes mund të justifikohej vetëm për qëllime të luftës kundër krimeve të rënda. Gjithashtu, direktiva nuk përcaktonte asnjë kriter objektiv i cili të mund të garantonte që aksesi nga ana e autoriteteve kompetente kombëtare **tek të dhënat e mbajtura**, të kufizohej vetëm **tek të dhënat e domosdoshme**. Për më tepër, ajo nuk përmbante kushte materiale dhe procedurale që të rregullonin aksesin dhe përdorimin e të dhënave të mbajtura nga ana e autoriteteve kombëtare, të cilat nuk i nënshtroheshin kontrollit paraprak nga një gjykatë, apo organ tjetër i pavarur.

GJDBE-ja arriti në një përfundim të ngjashëm tek çështjet e bashkuara *Tele2 Sverige AB k. Post- och telestryrelsen* dhe *Secretary of State for the Home Department k. Tom Watson dhe të Tjerëve*.[69] Këto çështje kishin të bënin me mbajtjen e të dhënave të trafikut dhe të vendndodhjes të "të gjithë abonentëve dhe përdoruesve të regjistruar dhe të të gjitha pajisjeve të komunikimit elektronik ashtu si edhe të të dhënave të trafikut" pa "dallim, kufizim, apo përjashtim sipas qëllimit të ndjekur".[70] Në çështjen në fjalë, mbajtja e të dhënave nuk kushtëzohej nga fakti nëse personi kishte lidhje ose jo, drejtpërdrejt apo tërthorazi, me vepra penale të rënda. Për shkak se mungonte lidhja midis të dhënave të mbajtura dhe një kërcënimi ndaj sigurisë publike, apo kufizimeve kohore ose gjeografike, GJDBE-ja doli në përfundimin se legjislacioni kombëtar tejkalonte kufijtë e domosdoshmërisë për qëllime të luftës kundër krimeve të rënda.[71]

Një qasje të ngjashme në lidhje me domosdoshmërinë ka edhe Mbikëqyrësi Evropian i Mbrojtjes së të Dhënave tek *Necessity Toolkit,*[72] i cili ka për qëllim të ndihmojë në vlerësimin e përputhshmërisë së masave të propozuara me ligjin e BE-së për mbrojtjen e të dhënave. Ai është përgatitur për të udhëzuar politikanët dhe ligjvënësit e BE-së, të cilët janë të ngarkuar me përgatitjen ose analizimin e masave që përfshijnë përpunimin e të dhënave personale dhe me kufizimin e së drejtës për mbrojtje të të dhënave personale dhe të drejtave e lirive të tjera të përcaktuara në Kartë.

Objektivat e interesit të përgjithshëm

Çdo kufizim në ushtrimin e të drejtave të njohura nga Karta, që të jetë i justifikuar, duhet të jetë në përputhje me objektivat e interesit të përgjithshëm të njohura nga Bashkimi, ose me nevojën për të mbrojtur të drejtat dhe liritë e personave të tjerë. Për sa i përket së drejtës për të mbrojtur të drejtat dhe liritë e të tjerëve, e drejta për mbrojtje të të dhënave personale shpesh ndërvepron me të drejta të tjera themelore. Seksioni 1.3 ofron një analizë të hollësishme të këtyre ndërveprimeve. Ndërsa për sa i takon objektivave të interesit të përgjithshëm, në to përfshihen objektivat e përgjithshëm të BE-së të përcaktuara në nenin 3 të Traktatit mbi Bashkimin Evropian (TBE), sikurse nxitjen e paqes dhe të mirëqenies së popujve të tij, drejtësisë shoqërore dhe mbrojtjes dhe krijimit të një hapësire të lirisë, sigurisë dhe drejtësisë, në të cilit lëvizja e lirë e personave është e garantuar, së bashku me masat e duhura për parandalimin dhe luftën kundër krimit, ashtu si edhe me objektivat dhe interesat e tjera të përgjithshme të mbrojtura nga dispozitat specifike të traktateve.[73] Në këtë drejtim, Rregullorja

[69] GJDBE, Çështje të bashkuara C-203/15 dhe C-698/15, *Tele2 Sverige AB k. Post- och telestryrelsen dhe Secretary of State for the Home Department k. Tom Watson dhe të Tjerët* [ÇB] , 21 dhjetor 2016, parag. 105–106.
[70] *Ibid*., parag. 105.
[71] *Ibid*., parag. 107.
[72] EDPS (2017), *Necessity Toolkit*, Bruksel, 11 prill 2017.
[73] Shpjegime në lidhje me Kartën e të Drejtave Themelore (2007/C 303/02), FZ 2007 nr. C 303, fq. 17-35.

e Përgjithshme e Mbrojtjes së të Dhënave e specifikon më tej pikën 1 të nenit 52 të Kartës: neni 23, pika 1 e Rregullores rendit një sërë objektivash të interesit të përgjithshëm, të cilat konsiderohen legjitime për kufizimin e të drejtave të individëve, me kusht që kufizimi të respektojë thelbin e së drejtës për mbrojtje të të dhënave personale dhe të jetë i domosdoshëm dhe proporcional. Siguria dhe mbrojtja kombëtare, parandalimi i krimit, mbrojtja e interesave të rëndësishme ekonomike dhe financiare të BE-së ose Shteteve Anëtare, shëndeti publik dhe siguria sociale, janë disa nga synimet e interesit publik të përmendura në të.

Është e rëndësishme të përkufizohet dhe shpjegohet në hollësi të mjaftueshme objektivi i interesit të përgjithshëm që synon kufizimi, për shkak se domosdoshmëria e kufizimit do të analizohet referuar atij sfondi. Përshkrimi i qartë dhe i hollësishëm i objektivit të kufizimit dhe masave të propozuara është thelbësor për të bërë të mundur që të vlerësohet nëse është i domosdoshëm.[74] Objektivi i synuar dhe domosdoshmëria e proporcionalitetit i kufizimit janë të lidhura ngushtë.

Shembull: *Schwarz k. Stadt Bochum*[75] kishte të bënte me kufizimet e së drejtës për respektim të jetës private dhe së drejtës për mbrojtje të të dhënave personale, që rrjedhin nga marrja dhe depozitimi i gjurmëve të gishtave kur autoritetet e Shteteve Anëtare lëshojnë pasaporta.[76] Kërkuesi aplikoi në Stadt Bochum për pasaportë, por refuzoi t'i merreshin gjurmët e tij të gishtave, për pasojë Stadt Bochum-i refuzoi të pranonte aplikimin e tij për pasaportë. Më pas, ai iu drejtuar një gjykate gjermane, duke kërkuar që t'i lëshohej pasaporta pa iu marrë gjurmët e gishtave. Gjykata gjermane ia referoi çështjen GJDBE-së, ku kërkonte të dinte nëse neni 1, pika 2 e Rregullores 2252/2004 mbi standardet për karakteristikat e sigurisë dhe ato biometrike në pasaporta dhe dokumente udhëtimit të lëshuara nga Shtetet Anëtare duhet të konsiderohej i vlefshëm.
GJDBE-ja theksoi se gjurmët e gishtave **përbëjnë të dhëna personale**, meqenëse ato përmbajnë objektivisht informacion unik në lidhje me individët, i cili mundëson identifikimin e tyre me saktësi, ndërsa marrja dhe depozitimi i gjurmëve të gishtave përbën përpunim. Ky përpunim, i cili rregullohet nga neni 1, pika 2 e Rregullores nr. 2252/2004, përbën kërcënim për të drejtat për respektim të jetës private dhe mbrojtje të të dhënave personale.[77] Gjithsesi, neni 52, pika 1 e Kartës lejon kufizime në ushtrimin e këtyre të drejtave, për aq kohë sa këto kufizime janë të parashikuara me ligj, respektojnë thelbin e atyre të drejtave dhe janë në përputhje me parimin e proporcionalitetit, janë të domosdoshme dhe përmbushin vërtet objektivat e interesit të përgjithshëm të njohura nga Bashkimit, ose nevojën për të mbrojtur të drejtat dhe liritë themelore të të tjerëve.

Tek kjo çështje, GJDBE-ja vërejti fillimisht se kufizimi që rridhte nga marrja dhe depozitimi i gjurmëve të gishtave kur lëshohen pasaporta, duhet konsideruar si i **parashikuar me ligj**, meqenëse ato veprime janë të përcaktuara në nenin 1, pika 2 të Rregullores nr. 2252/2004. Së dyti, kjo rregullore ishte hartuar për të parandaluar falsifikimin e pasaportave dhe përdorimin e tyre të paligjshëm. Në këtë mënyrë, neni 1, pika 2 synon ndër të tjera të parandalojë hyrjen e paligjshme në BE dhe për këtë shkak ndjek një objektiv të interesit të përgjithshëm të njohur nga Bashkimi. Së treti, nga provat që kishte në dispozicion GJDBE-ja nuk dukej e as ishte pretenduar që kufizimet e bëra ndaj ushtrimit të këtyre të drejtave në këtë çështje, nuk kishin respektuar thelbin e këtyre të drejtave. Së katërti, depozitimi i

[74] EDPS (2017), *Necessity Toolkit*, Bruksel, 11 prill 2017, fq. 4.
[75] GJDBE, C-291/12, *Michael Schwarz k. Stadt Bochum,* 17 tetor 2013.
[76] *Ibid.,* pagrafët 33-36.
[77] *Ibid.,* paragrafët 27-30.

gjurmëve të gishtave në një pajisje regjistrimi me siguri të lartë, sikurse parashikohet nga ajo dispozitë, kërkon teknologji të sofistikuar. Ky depozitim mund të reduktojë rrezikun e falsifikimit të pasaportave dhe të lehtësojë punën e autoriteteve përgjegjëse për kontrollin e autenticitetit të pasaportave në kufijtë e BE-së. Fakti se kjo metodë nuk është plotësisht e sigurt, nuk është vendimtar. Megjithëse kjo metodë nuk përjashton të gjithë personat e paautorizuar që të pranohen, mjafton që ajo redukton ndjeshëm mundësinë e këtij pranimi. Bazuar në sa më sipër, GJDBE-ja doli në përfundimin se marrja dhe depozitimi i gjurmëve të gishtave të përcaktuar në nenin 1, pika 2 të Rregullores nr. 2252/2004 ishin të përshtatshme për arritjen e qëllimeve të ndjekura nga ajo rregullore dhe më tej për objektivin e parandalimit të hyrjes së paligjshme në BE.[78]

BJDBE-vlerësoi me pas nëse ky përpunim ishte i domosdoshëm, duke vërejtur se veprimi në fjalë kishte të bënte thjesht me marrjen e gjurmëve të dy gishtave, të cilat, për më tepër, përgjithësisht mund të shihen nga të tjerët, kështu që ky nuk është një veprim me karakter intim. Gjithashtu, ai nuk shkakton ndonjë shqetësim të veçantë fizik, apo mendor për personin e prekur, më tepër sesa kur atij personi i merret imazhi i fytyrës. Duhet theksuar gjithashtu se e vetmja alternativë reale përkundër marrjes së gjurmëve të gishtave që i ishte paraqitur GJDBE-së gjatë procedimit, ishte skanimi i irisit. Në dosjen gjyqësore që ishte depozituar pranë GJDBE-së nuk gjendej asnjë element i cili të provonte që kjo procedurë e fundit, do të ndërhynte më pak tek të drejtat e njohura nga nenet 7 dhe 8 të Kartës, sesa marrja e gjurmëve të gishtave. Gjithashtu, për sa i përket efektshmërisë së atyre dy metodave, është e ditur se teknologjia e njohjes së irisit nuk është ende aq e zhvilluar sa teknologjia e njohjes së gjurmëve të gishtave, aktualisht është shumë më e kushtueshme se procedura për krahasimin e gjurmëve të gishtave dhe për këtë arsye është më pak e përshtatshme për përdorim të përgjithshëm. Për rrjedhojë, GJDBE-ja nuk ishte në dijeni të ndonjë mase e cila të ishte e efektshme sa duhet, për arritjen e qëllimit të mbrojtjes nga përdorimi i paligjshëm i pasaportave dhe më pak cenuese për të drejtat e njohura nga nenet 7 dhe 8 të Kartës, se sa masat që rrjedhin nga metoda e bazuar tek përdorimi i gjurmëve të gishtave.[79]

GJDBE-ja vërejti se neni 4, pika 3 e Rregullores nr. 2252/2004 përcakton qartë se gjurmët e gishtave mund të përdoren vetëm për verifikimin e autenticitetit të pasaportës dhe identitetit të poseduesit të saj, ndërsa neni 1, pika 2 e rregullores nuk parashikonte depozitim tjetër të gjurmëve të gishtave përveçse tek vetë pasaporta, e cila i përket vetëm poseduesit të saj. Në këtë mënyrë, rregullorja nuk parashikonte bazë ligjore për arkivim të centralizuar të të dhënave të mbledhura sipas atij qëllimi, apo për përdorimin e këtyre të dhënave për qëllime të tjera veç parandalimit të hyrjes së paligjshme në BE.[80] Mbështetur në vlerësimet e mësipërme, GJDBE vendosi se nga shqyrtimi i çështjes së referuar, nuk u gjet asgjë që mund të cënonte vlefshmërinë e nenit 1, pika 2 të Rregullores nr. 2252/2004.

Marrëdhënia e Kartës me KEDNJ-në

Pavarësisht formulimeve të ndryshme, kushtet për kufizime të ligjshme të këtyre të drejtave në nenin 52, pika 1 të Kartës të kujtojnë nenin 8, pika 2 të KEDNJ-së në lidhje me të drejtën për respektim të jetës private. Në jurisprudencën përkatëse, GJDBE-ja dhe GJEDNJ-ja shpesh u referohen gjykimeve të njëra-tjetrës, si pjesë e një dialogu konstant midis dy gjykatave, për të interpretuar në mënyrë harmonike rregullat e mbrojtjes së të dhënave. Neni 52, pika 3 e Kartës

[78] *Ibid.*,paragrafët 35-45.
[79] GJDBE, C-291/12, *Michael Schwarz k. Stadt Bochum,* 17 tetor 2013, paragrafët 46-53.
[80] *Ibid.,* paragrafët 56-61.

përcakton se, "për aq sa kjo Kartë përmban të drejta të cilat përkojnë me të drejtat e garantuara nga Konventa për Mbrojtjen e të Drejtave dhe Lirive Themelore të Njeriut, kuptimi dhe fushëveprimi i atyre të drejtave duhet të jetë i njëjtë me ato të përcaktuara nga Konventa në fjalë". Sidoqoftë, neni 8 i Kartës nuk përkon drejtpërdrejt me një nen të KEDNJ-së.[81] Neni 52, pika 3 e Kartës ka të bëjë me përmbajtjen dhe fushëveprimin e të drejtave të mbrojtura nga secili rend juridik dhe jo me kushtet për kufizimin e tyre. Megjithatë, referuar kontekstit më të gjerë të dialogut dhe bashkëpunimit midis dy gjykatave, GJDBE-ja mund të marrë në konsideratë në analizën e saj kriterin për kufizim të ligjshëm sipas nenit 8 të KEDNJ-së, sikurse është interpretuar nga GJEDNJ-ja. Edhe skenari i kundërt, ku GJEDNJ-ja mund t'i referohet kushteve për kufizim të ligjshëm të përcaktuara në Kartë, është gjithashtu i mundshëm. Në çdo rast, duhet pasur parasysh gjithashtu që në KEDNJ nuk ka një ekuivalent të përsosur të nenit 8 të Kartës, i cili t'i referohet mbrojtjes së të dhënave personale dhe veçanërisht të drejtave të subjektit të të dhënave, kritereve ligjore për përpunimin dhe mbikëqyrjes nga një autoritet i pavarur. Disa elementë të nenit 8 të Kartës mund të gjenden në jurisprudencën e GJEDNJ-së të zhvilluar në bazë të nenit 8 të KEDNJ-së dhe në lidhje me Konventën 108.[82] Kjo lidhje garanton ekzistencën e frymëzimit reciprok midis GJDBE-së dhe GJEDNJ në çështjet e fushës së mbrojtjes të dhënave.

[81] EDPS (2017), *Necessity Toolkit*, Bruksel, 11 prill 2017, fq. 6.
[82] Shpjegime në lidhje me Kartën Evropiane të të Drejtave Themelore (2007/C 303/02), neni 8.

1.3. Ndërveprimi me të drejta dhe interesa të tjera legjitime

Pikat kryesore

- E drejta për mbrojtje të të dhënave shpesh ndër vepron me të drejta të tjera, sikurse me lirinë e shprehjes dhe me të drejtën për të marrë e dhënë informacion.
- Ky ndërveprim është shpesh ambivalent: ndërsa ka situata në të cilat e drejta për mbrojtje të të dhënave personale është në tension me një të drejtë të caktuar, ka situata të tjera ku e drejta për mbrojtje të të dhënave personale garanton në mënyrë të efektshme respektimin e së njëjtës të drejte. Është për shembull rasti i lirisë së shprehjes, duke qenë se sekreti profesional është përbërës i së drejtës për respektim të jetës private.
- Nevoja për të mbrojtur të drejtat dhe liritë e të tjerëve është një nga kriteret e përdorura për të vlerësuar kufizimin e ligjshëm të së drejtës për mbrojtje të të dhënave.
- Kur në lojë janë të drejta të ndryshme, gjykatat duhet t'i ekuilibrojnë në mënyrë që ato të drejta të pajtohen mes tyre.
- Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave detyron Shtetet Anëtare të harmonizojnë të drejtën për mbrojtje të të dhënave personale me lirinë e shprehjes dhe të informimit.
- Shtetet Anëtare mund të miratojnë gjithashtu rregulla specifike në legjislacionin kombëtar, me qëllim që të harmonizojnë të drejtën për mbrojtje të të dhënave personale me aksesin publik në dokumentet zyrtare dhe detyrimet e sekretit profesional.

E drejta për mbrojtje të të dhënave personale nuk është e drejtë absolute; kushtet për kufizim të ligjshëm të kësaj të drejte janë dhënë në hollësi më lart. Një nga kriteret për kufizime të ligjshme të të drejtave, e njohur si nga e drejta e KiE-së dhe nga ajo e BR-së, është që ndërhyrja tek mbrojtja e të dhënave të jetë e domosdoshme për mbrojtjen e të drejtave dhe lirive të të tjerëve. Kur mbrojtja e të dhënave ndër vepron me të drejta të tjera, si GJEDNJ-ja ashtu edhe GJDBE-ja janë shprehur në mënyrë të përsëritur se kur zbatohet dhe interpretohet neni 8 i KEDNJ-së dhe neni 8 i Kartës, nevojitet të bëhet ekuilibrimi me të drejtat e tjera.[83] Se si arrihet ky ekuilibër, do të ilustrohet me disa shembuj të rëndësishëm.

Përveç ekuilibrit që duhet të gjejnë këto gjykata, nëse është e nevojshme, shtetet mund të miratojnë legjislacion për të harmonizuar të drejtën për mbrojtje të të dhënave personale me të drejta të tjera. Për këtë arsye, Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave parashikon një sërë fushash ku mund të bëhen shmangie në nivel kombëtar.

[83] GJEDNJ, *Von Hannover k. Gjermanisë (No. 2)* [ÇB], nr. 40660/08 dhe 60641/08, 7 shkurt 2012; GJDBE, Çështje të bashkuara C-468/10 dhe C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) dhe Federación de Comercio Electrónico y Marketing Directo (FECEMD) k. Administración del Estado*, 24 nëntor 2011, parag. 48; GJDBE, C-275/06, *Productores de Música de España (Promusicae) k. Telefónica de España SAU* [ÇB], 29 janar 2008, parag. 68.

Për sa i përket lirisë së shprehjes, GDPR-ja detyron Shtetet Anëtare të harmonizojnë me ligj "të drejtën për mbrojtje të të dhënave personale sipas kësaj Rregulloreje me të drejtën për lirinë e shprehjes dhe të informimit, përfshirë përpunimin për qëllime gazetarie dhe për qëllime të shprehjes akademike, artistike apo letrare".[84] Shtetet Anëtare mund të miratojnë gjithashtu ligje për të harmonizuar mbrojtjen e të dhënave me aksesin publik në dokumentet zyrtare dhe detyrimet e sekretit profesional, të mbrojtura si një formë e së drejtës për respektim të jetës private.[85]

1.3.1 Liria e shprehjes

Një nga të drejtat që ndër vepron më së shumti me të drejtën për mbrojtje të të dhënave është e drejta për lirinë e shprehjes.

Liria e shprehjes mbrohet nga neni 11 i Kartës ("Liria e shprehjes dhe informimit"). Kjo e drejtë përfshin "lirinë për të pasur opinione dhe për të marrë e dhënë informacion dhe ide pa ndërhyrje nga autoriteti publik dhe pavarësisht kufijve". Liria e informimit, sipas nenit 11 të Kartës dhe nenit 10 të KEDNJ-së, mbron të drejtën jo vetëm për dhënë, por edhe për të *marrë* informacion.

Kufizimet e lirisë së shprehjes duhet të bëhen në përputhje me kriteret e parashikuara në nenin 52, pika 1 të Kartës, të përshkruara më lart. Gjithashtu, neni 11 i korrespondon nenit 10 të KEDNJ-së. Sipas nenit 52, pika 3 të Kartës, kur ajo përmban të drejta të cilat korrespondojnë me të drejtat e garantuara nga KEDNJ-ja, "kuptimi dhe fushëveprimi i atyre të drejtave duhet të jetë i njëjtë me ato të përcaktuara nga Konventa në fjalë". Për rrjedhojë, kufizimet që mund të bëhen ligjërisht tek e drejta e garantuar nga neni 11 i Kartës, nuk mund të tejkalojnë ato të përcaktuara në nenin 10, pika 2 të KEDNJ-së – domethënë ato duhet të jenë të përcaktuara me ligj dhe të domosdoshme në një shoqëri demokratike "për mbrojtjen [...] e reputacionit ose të të drejtave të të tjerëve". Këto të drejta përfshijnë në mënyrë të veçantë të drejtën për respektim të jetës private dhe të drejtën për mbrojtje të të dhënave personale.

Marrëdhënia midis mbrojtjes së të dhënave personale dhe lirisë së shprehjes rregullohet me nenin 85 të Rregullores së Përgjithshme të Mbrojtjes së të Dhënave, i titulluar "Përpunimi dhe liria e shprehjes dhe e informimit". Sipas këtij neni, Shtetet Anëtare duhet të harmonizojnë të drejtën për mbrojtje të të dhënave personale me të drejtën për lirinë e shprehjes dhe të informimit. Në mënyrë të veçantë, përjashtimet dhe shmangiet nga kapitujt specifikë të Rregullores së Përgjithshme të Mbrojtjes së të Dhënave duhet të bëhen për qëllim gazetarie, ose për qëllime të shprehjes akademike, artistike ose letrare, kur ato janë të nevojshme për të harmonizuar të drejtën për mbrojtje të të dhënave personale me lirinë e shprehjes dhe të informimit.

Shembull: tek çështja *Tietosuojavaltuutettu k. Satakunnan Markkinapörssi Oy dhe Satamedia Oy*,[86] GJDBE-së iu kërkua të përkufizonte marrëdhënien midis mbrojtjes së të

[84] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 85.
[85] *Ibid.,* nenet 86 dhe 90.

[86] GJDBE, C-73/07, *Tietosuojavaltuutettu k. Satakunnan Markkinapörssi Oy dhe Satamedia Oy* [ÇB], 16 dhjetor 2008, parag. 56, 61 dhe 62.

dhënave dhe lirisë së shtypit.[87] Gjykatës iu desh të shqyrtonte përhapjen nëpërmjet një shërbimi SMS nga ana e shoqërisë, të të dhënave tatimore të rreth 1.2 milion personave fizikë, të marra në mënyrë të ligjshme nga autoritetet tatimore finlandeze. Autoriteti mbikëqyrës i mbrojtjes së të dhënave të Finlandës kishte miratuar një vendim, i cili detyronte shoqërinë të ndalonte përhapjen e këtyre të dhënave. Shoqëria u ankua në gjykatën kombëtare kundër vendimit, e cila nga ana e saj kërkoi qartësimin nga GJDBE-ja mbi interpretimin e Direktivës së Mbrojtjes së të Dhënave. GJDBE-a duhet të verifikonte në mënyrë të veçantë nëse përpunimi i të dhënave personale, të cilat u vunë në dispozicion nga autoritetet tatimore, me qëllim që t'u mundësonin abonentëve të telefonave celularë që të merrnin të dhënat tatimore të personave të tjerë fizikë, duhej të konsiderohej si aktivitet i kryer vetëm për qëllime gazetarie. Pasi doli në përfundimin se aktivitetet e shoqërisë përbënin "përpunim të të dhënave personale", sipas kuptimit të nenit 3, pika1 të Direktivës së Mbrojtjes së të Dhënave, GHDBE-a analizoi nenin 9 të direktivës (mbi përpunimin e të dhënave personale dhe lirinë e shprehjes). Gjykata fillimisht theksoi rëndësinë e së drejtës së lirisë së shprehjes në çdo shoqëri demokratike dhe u shpreh se nocionet që lidhen me atë të drejtë, sikurse nocioni i gazetarisë, duhet të interpretohen në mënyrë të zgjeruar. Më tej, ajo vuri në dukje se për t'i ekuilibruar këto dy të drejta themelore, përjashtimet dhe kufizimet e së drejtës për mbrojtje të të dhënave, duhet të zbatohen vetëm për aq sa është e domosdoshme. Në ato kushte, GJDBE-ja vlerësoi se kryerja e këtyre aktiviteteve, sikurse ato të kryera nga shoqëritë në fjalë, që kanë të bëjnë me të dhënat që merren nga dokumente, të cilat konsiderohen si dokumente publike sipas legjislacionit kombëtar, mund të cilësohen "aktivitete gazetarie", nëse objektivi i tyre është përhapja e informacionit, mendimeve apo ideve tek publiku, pavarësisht mjetit të përdorur për transmetimin e tyre. Ajo vendosi po ashtu se këto aktivitete nuk janë ekskluzivitet i operatorëve të sektorit të medias, por mund të ndërmerren edhe për qëllime fitimprurëse. Gjithsesi, në lidhje me rastin konkret, GJDBE-ja ia la gjykatës kombëtare të përcaktonte nëse ishte ky rasti, referuar fakteve të çështjes.

E njëjta çështje u shqyrtua edhe nga GJEDNJ-ja, pasi gjykata kombëtare vendosi, bazuar në udhëzimet e GJDBE-së, se urdhri i autoritetit mbikëqyrës për të ndaluar publikimin e të gjitha informacioneve tatimore ishte ndërhyrje e justifikuar tek liria e shprehjes së shoqërisë. GJEDNJ-ja e mbështeti këtë këndvështrim.[88] Ajo përcaktoi se edhe pse kishte një ndërhyrje tek e drejta e shoqërisë për të dhënë informacion, kjo ndërhyrje ishte në përputhje me ligjin, kishte qëllim legjitim dhe ishte e nevojshme në një shoqëri demokratike.

Gjykata rikujtoi kriteret e jurisprudencës të cilat duhet të udhëzojnë autoritetet kombëtare dhe vetë GJEDNJ-në kur ekuilibrojnë lirinë e shprehjes me të drejtën për respektim të jetës private. Kur bëhet fjalë për diskursin politik apo për një debat mbi një çështje me interes publik, fushëveprimi për kufizim të së drejtës për të marrë e dhënë informacion është i pakët, për shkak se publiku ka të drejtë të informohet, "dhe kjo është një e drejtë thelbësore në një shoqëri demokratike". [89] Megjithatë, artikujt e shtypit që synojnë vetëm të kënaqin kuriozitetin e lexuesve të caktuar në lidhje me hollësitë e jetës private të personave, nuk mund të konsiderohen si të tilla që kontribuojnë në debatin me interes publik. Shmangia nga normat e mbrojtjes së të dhënave për qëllime gazetarie ka si qëllim t'u mundësojë gazetarëve të kenë akses, të mbledhin dhe të përpunojnë të dhëna, në mënyrë që të mund të kryejnë

[87] Çështja lidhej me interpretimin e nenit 9 të Direktivës së Mbrojtjes së të Dhënave – tashmë i zëvendësuar nga neni 85 i Rregullores së Përgjithshme të Mbrojtjes së të Dhënave – i cili përcakton: "Shtetet Anëtare parashikojnë përjashtime, ose shmangie nga dispozitat e këtij Kapitulli, Kapitullit IV dhe Kapitullit VI, për përpunimin e të dhënave personale të kryer vetëm për qëllime gazetarie, ose për qëllime të shprehjes artistike apo letrare, nëse ato janë të nevojshme për të harmonizuar të drejtën për privatësi me rregullat e lirisë së shprehjes".

[88] GJEDNJ, *Satakunnan Markkinapörssi Oy dhe Satamedia Oy k. Finlandës*, nr. 931/13, 27 qershor 2017.

[89] *Ibid.,* parag. 169.

aktivitetet e tyre gazetareske. Kështu, vërtet që kishte interes publik në dhënien e aksesit dhe lejimin e shoqërisë kërkuese që të mblidhte e përpunonte sasitë e mëdha të të dhënave tatimore në fjalë. Përkundër kësaj, Gjykata vlerësoi se nuk kishte interes publik në përhapjen masive të këtyre të dhënave të papërpunuara nga ana e gazetave, në formë të pandryshuar dhe pa asnjë input analitik. Informacioni tatimor mund t'i ketë shërbyer një pjese kureshtare të publikut për të kategorizuar individët sipas statusit ekonomik të tyre dhe shuar etjen e publikut për informacion në lidhje me jetët private të të tjerëve. Diçka e tillë nuk mund të konsiderohet si kontribut për një debat me interes publik.

Shembull: tek çështja *Google Spain,*[90] GJDBE-ja vlerësoi nëse Google-i ishte i detyruar të fshinte informacione të vjetra në lidhje me vështirësitë financiare të kërkuesit nga rezultatet e listës së saj të kërkimit. Kur në motorin e kërkimit të Google-it bëhej një kërkim duke përdorur emrin e kërkuesit, rezultatet e kërkimit ofronin lidhje interneti me artikuj të vjetër gazetash, që përmendin lidhjen e tj me procedurat e falimentit. Kërkuesi e konsideroi këtë shkelje të së drejtës së tij për respektim të jetës private dhe për mbrojtje të të dhënave personale, duke qenë se procedura ishte përmbyllur prej vitesh, çka i bënte këto referenca të panevojshme.

GJDBE-ja qartësoi fillimisht se motorët e kërkimit të internetit dhe rezultatet e kërkimit që pasqyrojnë të dhëna personale, mund të ofrojnë një profil të detajuar për një individ. Për shkak të digjitalizimit në rritje të shoqërisë, kërkesa për saktësi të të dhënave dhe që publikimi i tyre të mos shkojë përtej domosdoshmërisë, d.m.th. dhënia e informacionit për publikun, është thelbësore për të garantuar nivel të lartë të mbrojtjes së të dhënave për individët. "Kontrolluesi për sa i përket atij përpunimi, duhet të garantojë në kuadër të përgjegjësive, kompetencave dhe aftësive të tij, që përpunimi plotëson kriteret" e së drejtës së BE-së, me qëllim që garancitë ligjore të përcaktuara të jenë plotësisht të efektshme. Kjo do të thotë se e drejta që të dhënat personale të fshihen kur përpunimi nuk është më i nevojshëm apo i papërdorshëm, mbulon gjithashtu motorët e kërkimit, të cilët kanë rezultuar të jenë kontrollues e jo thjesht përpunues (shih Seksionin 2.3.1).

Ndërsa shqyrtonte nëse Google-i duhet të hiqte lidhjet e internetit që kishin të bënin me kërkuesin, GJDBE-ja u shpreh se individët kanë të drejtën që të dhënat e tyre personave të fshihen nga rezultatet e kërkimit të një motori kërkimi në internet, me disa kushte. Kjo e drejtë mund të aktivizohet kur informacioni në lidhje me një person është i pasaktë, i papërshtatshëm, i pavlerë ose i tepërt në raport me qëllimet e përpunimit të të dhënave. GJDBE-ja pranoi se kjo e drejtë nuk është absolute; ajo duhet ekuilibruar me të drejta të tjera, në mënyrë të veçantë me interesin dhe të drejtën e publikut të gjerë për të pasur akses në informacion. Çdo kërkesë për fshirje duhet të vlerësohet rast pas rasti, për të gjetur ekuilibrin midis së drejtës themelore të subjektit të të dhënave për mbrojtje të të dhënave personale dhe jetës private nga njëra anë dhe interesave legjitimë të të gjithë përdoruesve të internetit nga ana tjetër. GJDBE-ja dha udhëzime në lidhje me faktorët që duhen marrë në konsideratë kur bëhet ekuilibrimi. Një faktor veçanërisht i rëndësishëm është natyra e informacionit. Nëse informacioni është sensitiv për jetën private të një personi dhe kur nuk ekziston interes publik që informacioni të jetë i disponueshëm, mbrojtja e të dhënave dhe privatësisë prevalon të drejtën e publikut të gjerë për të pasur akses në informacion. Përkundrazi, kur me sa duket subjekti i të dhënave është figurë publike, ose kur informacioni

[90] GJDBE, C-131/12,*Google Spain SL, Google Inc. k. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [ÇB] , 13 maj 2014, parag. 81–83.

ka natyrë të tillë që e justifikon dhënien e aksesit në informacion për publikun e gjerë, atëherë ndërhyrja tek të drejtat themelore për mbrojtje të të dhënave privatësi është e justifikuar.

Në vijim të gjykimit, Grupi i Punës së Nenit 29 miratoi një udhëzues mbi zbatimin e vendimit të GJDBE-së. Udhëzuesi përfshin një listë të kritereve të përgjithshme që duhen ndjekur nga autoritetet mbikëqyrëse kur trajtojnë ankesa në lidhje me kërkesat e personave për fshirje dhe për t'i orientuar në ekuilibrimin e të drejtave.[91]

Për sa i përket harmonizimit të së drejtës për mbrojtje të të dhënave me të drejtën për lirinë e shprehjes, GJEDNJ-ja ka marrë disa vendime të rëndësishme.

Shembull: tek çështja *Axel Springer AG k. Gjermanisë,*[92] GJEDNJ-ja u shpreh se urdhri për të kufizuar shoqërinë kërkuese të publikonte një artikull në lidhje me arrestimin dhe dënimin e një aktori të mirënjohur, shkelte nenin 10 të KEDNJ-së. GJEDNJ-ja ritheksoi kriteret që duhen marrë në konsideratë kur ekuilibrohet e drejta për lirinë e shprehjes me të drejtën për respektim të jetës private, sikurse përcaktohet në jurisprudencën e saj:

- Nëse ngjarja që trajtonte artikulli i publikuar ishte me interes të përgjithshëm;
- Nëse personi ishte figurë publike; dhe
- Si ishte siguruar informacioni dhe nëse ishte i besueshëm.

GJEDNJ-ja konstatoi se arrestimi dhe dënimi i aktorit ishte fakt gjyqësor publik dhe pwr pasojë ishte me interes publik; se aktori ishte i aq i njohur sa të cilësohej figurë publike; dhe se informacioni ishte siguruar nga prokuroria dhe saktësia e tij nuk vihej në diskutim nga palët. Rrjedhimisht, kufizimi i publikimit të vendosur ndaj shoqërisë nuk kishte qenë proporcional me qëllimin legjitim të mbrojtjes së jetës private të kërkuesit. Gjykata doli në përfundimin se kishte pasur shkelje të nenit 10 të KEDNJ-së.

Shembull: çështja *Coudec dhe Hachette Filipacchi Associés k. Francës*[93] kishte të bënte me publikimin nga ana e një reviste të përjavshme franceze të një interviste me znj. Coste, e cila pretendonte se Princi Albert i Monakos ishte babai i djalit të saj. Intervista përshkruante gjithashtu marrëdhënien e znj. Coste me princin dhe mënyrën se si ai kishte reaguar ndaj lindjes së fëmijës, shoqëruar me fotografi të princit me fëmijën. Princi Albert u ankua ndaj shoqërisë publikuese për shkelje të së drejtës së tij për mbrojtje të jetës private. Gjykatat franceze vendosën se publikimi i artikullit kishte shkaktuar dëmtime të pariparueshme ndaj Princit Albert dhe kishin urdhëruar botuesin të paguante dëmet dhe të publikonte çështjen gjyqësore në kopertinën e revistës. Botuesit e revistës e dërguan çështjen në GJEDNJ, me pretendimin se vendimet e gjykatave franceze kishin ndërhyrë në mënyrë të pajustifikueshme tek e drejta e tyre për lirinë e shprehjes. GJEDNJ-ja duhej të ekuilibronte të drejtën e Princit Albert për respektim të jetës private, me të drejtën e shprehjes së botuesit dhe të drejtën e publikut të gjerë për t'u informuar. E drejta e znj. Coste për të ndarë historinë e saj me

[91] Grupi i Punës së Nenit 29 (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, WP 225, Bruksel, 26 nëntor 2014.
[92] GJEDNJ, *Axel Springer k. Gjermanisë* [ÇB], nr. 39954/08, 7 shkurt 2012, parag. 90 dhe 91.
[93] GJEDNJ,*Coudec dhe Hachette Filipacchi Associés k. Francës* [ÇB], nr. 40454/07, 10 nëntor 2015.

publikun dhe interesi i fëmijës që marrëdhënia e tij atë-fëmijë të vërtetohej zyrtarisht, ishin gjithashtu të rëndësishme për t'u marrë në konsideratë.

GJEDNJ-ja u shpreh se publikimi i intervistës përbënte ndërhyrje në jetën private të princit dhe shqyrtoi në vijim nëse ndërhyrja ishte e nevojshme. Ajo vlerësoi se intervista kishte të bënte me një figurë publike dhe me një çështje me interes publik, meqenëse qytetarët e Monakos kishin interes të informoheshin mbi ekzistencën e një fëmije të princit, për shkak se e ardhmja e një monarkie të trashëgueshme "lidhet qenësisht me ekzistencën e pasardhësve", ndaj dhe ishte çështje shqetësuese për publikun.[94] Gjykata theksoi gjithashtu se artikulli i kishte mundësuar znj. Coste dhe fëmijës së saj të ushtronin të drejtën e tyre për lirinë e shprehjes. Gjykatat kombëtare nuk kishin marrë në konsideratë parimet dhe kriteret e përcaktuara nga jurisprudenca e GJENJ-së për ekuilibrimin e së drejtës për respektim të jetës private me të drejtën për lirinë e shprehjes. Ajo doli në përfundimin se Franca kishte shkelur nenin 10 të KEDNj-së mbi lirinë e shprehjes.

Në jurisprudencën e GJEDNJ-së, një nga kriteret më të rëndësishme për sa i takon ekuilibrimit të këtyre të drejtave, është nëse të shprehurit kontribuon në debatin me interes të përgjithshëm publik.

Shembull: tek çështja *Mosley k. Mbretërisë së Bashkuar,*[95] një gazetë e përjavshme kombëtare publikoi fotografi intime të kërkuesit, i cili ishte një figurë e njohur që kishte fituar më pas një padi civile kundër botuesit dhe kishte përfituar kompensim dëmi. Pavarësisht se kishte përfituar kompensim monetar, ai u ankua se kishte mbetur viktimë e shkeljes së të drejtës së tij për privatësi, për shkak se i ishte mohuar mundësia të kërkonte më parë ndalimin e publikimit të fotove në fjalë, pasi nuk ekzistonte një detyrim ligjor që gazeta të njoftonte përpara se të bënte publikimin.
GJEDNJ-ja vërejti se megjithëse përhapja e këtij lloj materiali bëhej përgjithësisht për qëllime argëtimi e jo edukimi, ai pa dyshim kishte përfituar nga mbrojtja e nenit 10 të KEDNJ-së, mbi të cilin mund të prevalojnë dispozitat e nenit 8 të KEDNJ-së, në rastin kur informacioni ishte i natyrës private e intime dhe përhapja e tij nuk përbënte interes publik. Gjithsesi, duhej treguar kujdes i veçantë gjatë shqyrtimit të kufizimeve, të cilat mund të veprojnë si një formë censure përpara publikimit. Duke pasur parasysh efektin shqetësues që mund të shkaktojë ekzistenca e detyrimit për njoftim paraprak, dyshimeve në lidhje me efektshmërinë e tij dhe lirisë së madhe të veprimit në atë fushë, GJEDNJ-ja doli në përfundimin se ekzistenca e një norme ligjore detyruese për njoftim paraprak, nuk parashikohej nga neni 8. Për rrjedhojë, Gjykata vendosi se nuk kishte pasur asnjë shkelje të nenit 8.

Shembull: tek çështja *Bohlen k. Gjermanisë*,[96] kërkuesi, një këngëtar dhe producent i njohur, kishte publikuar një libër autobiografik dhe më pas ishte detyruar me vendim gjyqësor të hiqte disa pasazhe prej tij. Historia ishte trajtuar gjerësisht në median kombëtare dhe një shoqëri produktesh duhani ndërmori një fushatë humoristike publicitare bazuar tek ngjarja, duke përdorur emrin e kërkuesit pa pëlqimin e tij. Kërkuesi nuk arriti të përfitonte kompensim dëmi nga shoqëria reklamuese, për pretendimin se i ishin shkelur të drejtat sipas nenit 8 të KEDNJ-së. GJEDNJ-ja ritheksoi kriterin që orienton ekuilibrin midis së drejtës për respektim të jetës private, me të drejtën për lirinë e shprehjes dhe theksoi se nuk kishte

[94] *Ibid*., parag. 104-116.
[95] GJEDNJ, *Mosley k. Mbretërisë së Bashkuar,* nr. 48009/08, 10 maj 2011, parag. 129 dhe 130.
[96] GJEDNJ, *Bohlen k. Gjermanisë*, nr. 53495/09, 19 shkurt 215, parag. 45-60.

pasur shkelje të nenit 8. Kërkuesi ishte figurë publike dhe reklama nuk i referohej hollësive të jetës së tij private, por një ngjarjeje publike, e cila ishte trajtuar nga media dhe e cila ishte pjesë e një debati publik. Gjithashtu, reklama ishte me karakter humoristik dhe nuk përmbante asgjë denigruese, ose negative, për sa i përket kërkuesit.

Shembull: tek çështja *Biriuk k. Lituanisë*,[97] kërkuesja iu drejtua GJEDNJ-së me pretendimin se Lituania nuk kishte zbatuar detyrimin e saj për të garantuar respektim të së drejtës së saj për privatësi, për shkak se edhe pse një gazetë e rëndësishme kishte shkelur rëndë privatësisë së saj, kërkueses i ishte akorduar një shumë qesharake kompensimi financiar dëmi nga ana e gjykatave kombëtare të cilat kishin shqyrtuar çështjen. Për të akorduar kompensim jo pasuror dëmi, gjykatat kombëtare kishin zbatuar dispozitat e legjislacionit kombëtar mbi informimin e publikut, i cili përcaktonte një tavan të ulët për kompensimin e dëmeve jo pasurore, të shkaktuara nga përhapja e paligjshme e informacionit në lidhje me jetën private të personit nga ana e medias. Çështja buronte nga publikimi i një artikulli që kishte bërë gazeta më e madhe e përditshme e Lituanisë në faqen kryesore, në të cilin raportohej se kërkuesja ishte HIV pozitiv. Artikulli kritikonte gjithashtu sjelljen e kërkueses dhe vinte në pikëpyetje normat e saj morale.

GJEDNJ-ja ritheksoi se mbrojtja e të dhënave personale, aq më tepër e të dhënave mjekësore, kishte rëndësi thelbësore për të drejtën e respektimit të jetës private sipas KEDNJ-së. Konfidencialiteti i të dhënave në lidhje me shëndetin ka rëndësi të veçantë, për shkak se përhapja e të dhënave mjekësore (statusi HIV i kërkueses në këtë rast), mund të cënojë në mënyrë dramatike jetën private dhe familjare të personit, punësimin e tij, apo të saj dhe përfshirjen në shoqëri. Gjykata i dha rëndësi të veçantë faktit që sipas raportimit në gazetë, stafi mjekësor i spitalit kishte dhënë informacion mbi statusin HIV të kërkueses, në shkelje të pastër të detyrimit të tij për ruajtjen e sekretit profesional. Rrjedhimisht, nuk kishte pasur ndërhyrje legjitime tek e drejta e kërkueses për privatësi.

Artikulli ishte publikuar nga shtypi dhe liria e shprehjes është gjithashtu e drejtë themelore sipas KEDNJ-së. Gjithsesi, kur Gjykata vlerësoi nëse ekzistenca e interesit publik justifikonte publikimin e atij lloj informacioni në lidhje me kërkuesen, ajo doli në përfundimin se qëllimi kryesor për publikimin e tij ishte rritja e shitjeve të gazetës, duke shuar kuriozitetin e lexuesve. Ky lloj qëllimi nuk mund të konsiderohet se kontribuon në ndonjë debat me interes të përgjithshëm për shoqërinë. Duke qenë se kjo ishte një çështje "abuzimi të rëndë me lirinë e shtypit", kufizimet e ashpra të zhdëmtimit dhe shuma e ulët e dëmeve jo pasurore të përcaktuara në legjislacionin kombëtar nënkuptonin se Lituania nuk kishte përmbushur detyrimin pozitiv për të mbrojtur jetën private të kërkueses. GJEDNJ-ja vendosi se kishte pasur shkelje të nenit 8 të KEDNJ-së.

E drejta për lirinë e shprehjes dhe e drejta për mbrojtje të të dhënave personale nuk janë gjithnjë në konflikt. Ka raste kur mbrojtja e efektshme e të dhënave personale garanton lirinë e shprehjes.

Shembull: tek çështja *Tele2 Sverige* GJDBE-ja u shpreh se ndërhyrja e shkaktuar nga Direktiva 2006/24 (Direktiva e Mbajtjes së të Dhënave) tek të drejtat themelore të përcaktuara në nenet 7 dhe 8 të Kartës ishte "e zgjeruar dhe mund të konsiderohet si tepër e rëndë. Gjithashtu...fakti se të dhënat mbahen dhe pastaj përdoren pa informuar abonentin

[97] GJEDNJ, *Biriuk k. Lituanisë*, nr. 23373/03, 25 nëntor 2008.

apo përdoruesin e regjistruar, ka mundësi të gjenerojë në mendjen e këtyre të fundit ndjenjën se jetët e tyre private janë subjekt mbikëqyrjeje të vazhdueshme". GJDBE-ja konstatoi se mbajtja e përgjithësuar e të dhënave të trafikut dhe të vendndodhjes mund të ketë ndikim në përdorimin e komunikimeve elektronike dhe "rrjedhimisht në ushtrimin nga ana e përdoruesve të tyre të lirisë së shprehjes, e cila garantohet në nenin 11 të Kartës".[98] Në këtë kuptim, duke kërkuar masa rigoroze sigurie që mbajtja e të dhënave të mos bëhet në mënyrë të përgjithësuar, rregullat e mbrojtjes së të dhënave ndihmojnë në ushtrimin e lirisë së shprehjes.

Për sa i përket të drejtës për t'u informuar, e cila bën gjithashtu pjesë tek liria e shprehjes, ka një ndërgjegjësim gjithnjë e në rritje për sa i takon rëndësisë që ka transparenca e qeverisjes për funksionimin e një shoqërie demokratike. Transparenca është objektiv me interes të përgjithshëm dhe në këtë mënyrë mund të justifikojë ndërhyrjen tek e drejta për mbrojtje të të dhënave, nëse është e nevojshme dhe proporcionale, sikurse shpjegohet në Seksionin 1.2. Për pasojë, në dy dekadat e fundit, e drejta për akses në dokumentet që disponojnë autoritetet publike, është pranuar si një e drejtë e rëndësishme e çdo qytetari të BE-së dhe të çdo personi fizik apo juridik që banon, ose ka selinë në një Shtet Anëtar.

Tek e drejta e KiE-së, mund t'u referohemi parimeve të përcaktuara në Rekomandimin mbi aksesin në dokumentet zyrtare, tek i cili u mbështet hartimi i Konventës mbi Aksesin në Dokumentet Zyrtare (Konventa 205).[99]

Tek e drejta e BE-së, e drejta për akses në dokumente garantohet nga Rregullorja 1049/2001 në lidhje me aksesin publik në dokumentet e Parlamentit, Këshillit dhe Komisionit Evropian (Rregullorja e Aksesit në Dokumente).[100] Neni 42 i Kartës dhe neni 15, pika 3 e TFBE-së e kanë zgjeruar më tej të drejtën për akses në "dokumentet e institucioneve, organeve, zyrave dhe agjencive të Bashkimit, pavarësisht formës së tyre".

Kjo e drejtë mund të hyjë në konflikt me të drejtën për mbrojtje të të dhënave, nëse aksesi në një dokument mund të zbulojë të dhënat personale të të tjerëve. Neni 86 i Rregullores së Përgjithshme të Mbrojtjes së të Dhënave përcakton qartë se të dhënat personale në dokumentet zyrtare që disponojnë autoritetet dhe organet publike, mund të përhapen nga ana e autoritetit ose organit në përputhje me të drejtën e Bashkimit[101] ose Shtetit Anëtar, për të harmonizuar aksesin publik tek dokumentet zyrtare, me të drejtën për mbrojtje të të dhënave, në përputhje me rregulloren.

[98] GJDBE, Çështje të bashkuara C-203/15 dhe C-698/15, *Tele2 Sverige AB k. Post- och telestyrelsen* dhe *Secretary of State for the Home Department k. Tom Watson dhe të Tjerët* [ÇB], 21 dhjetor 2016, paragrafët 37 dhe 101; GJDBE, Çështje të bashkuara C-293/12 dhe C-594/12, *Digital Rights Ireland Ltd k. Minister for Communications, Marine and Natural Resources dhe të Tjerët* dhe *Kärntner Landesregierung dhe të Tjerët* [ÇB] , 8 prill 2014, parag. 28.

[99] Këshilli i Evropës, Komiteti i Ministrave (2002), Rekomandimi Rec (81) 19 dhe Rekomandimi Rec (2002) 2 për shtetet anëtare mbi aksesin në dokumentet zyrtare, 21 shkurt 2002; Këshilli i Evropës, Konventa mbi Aksesin në Dokumentet Zyrtare, CETS nr. 205, 18 qershor 2009. Konventa nuk ka hyrë ende në fuqi.

[100] Rregullorja (KE) nr. 1049/2001 e Parlamentit Evropian dhe e Këshillit e 20 majit 2001 në lidhje me aksesin publik në dokumentet e Parlamentit, Këshillit dhe Komisionit Evropian, FZ 2001 L 145.

[101] Neni 42 i Kartës, neni 15, pika 3 e TFBE-së dhe Rregullorja 1049/2009.

Për rrjedhojë, kërkesat për akses në dokumente, ose informacion që disponohet nga autoritetet publike, mund të duhet të ekuilibrohen me të drejtën për mbrojtje të të dhënave të personave, të dhënat e të cilëve përfshihen në dokumentet e kërkuara.

Shembull: tek *Volker und Markus Schecke dhe Hartmut Eifert k. Land Hessen*,[102] GJDBE-ja duhet të gjykonte në lidhje me proporcionalitetin e publikimit, parashikuar nga legjislacioni i BE-së, të emrave të përfituesve të subvencioneve bujqësore të BE-së dhe të shumave të përfituara. Publikimi synonte të rriste transparencën dhe të kontribuonte në kontrollin e publikut mbi përdorimin e duhur të fondeve publike nga administrata. Disa nga përfituesit e kundërshtuan proporcionalitetin e këtij publikimi.

GJDBE-ja duke vënë në dukje se e drejta për mbrojtje të të dhënave nuk është absolute, mbështeti faktin se publikimi në një faqe interneti i të dhënave të identitetit të përfituesve të dy fondeve bujqësore të BE-së dhe shumës së saktë të përfituar, përbënte ndërhyrje në jetën e tyre private në përgjithësi dhe tek mbrojtja e të dhënave të tyre personale në veçanti.

GJDBE-ja konstatoi se ky cenim i neneve 7 dhe 8 të Kartës, ishte i parashikuar në ligj dhe përmbushte një objektiv të interesit të përgjithshëm, të njohur nga BE-ja dhe konkretisht rritjen e transparencës mbi përdorimin e fondeve të komunitetit. Gjithsesi, GJDBE-ja vlerësoi se publikimi i emrave të personave fizikë, të cilët ishin përfituesit e ndihmës bujqësore të BE-së nëpërmjet këtyre dy fondeve dhe i shumave të sakta të përfituara, përbënte një masë jo proporcionale dhe nuk justifikohej bazuar në nenin 52, pika 1 të Kartës. Ajo pranoi rëndësinë që ka në një shoqëri demokratike informimi i taksapaguesve mbi përdorimin e fondeve publike. Sidoqoftë, meqenëse "nuk mund t'i jepet prioritet automatik objektivit të transparencës, ndaj së drejtës për mbrojtje të të dhënave personale",[103] institucionet e BE-së ishin të detyruara të ekuilibronin interesin e Bashkimit për transparencë, me kufizimin e ushtrimit të së drejtës për privatësi dhe mbrojtje të të dhënave, e cila iu cenua subjekteve përfituese si rezultat i publikimit.

GJDBE-ja vlerësoi se institucionet e BE-së nuk e kishin bërë ekuilibrimin siç duhet, meqenëse ishte e mundur të merreshin masa të cilat do të ndikonin më pak negativisht tek të drejtat themelore të individëve, ndërkohë që do të kontribuohej në mënyrë të efektshme në arritjen e objektivit të transparencës që synonte publikimi. Për shembull, në vend të një publikimi të përgjithshëm që i prekte të gjithë subjektet përfituese, duke dhënë emrat dhe shumat e sakta të përftuara nga secili, mund të ishte bërë një dallim bazuar në kritere të caktuara, si për shembull periudhat në të cilat ata persona kishin përftuar ndihmën, shpeshtësia e dhënies së ndihmës, apo sasia dhe karakteri i saj.[104] Kështu, GJDBE-ja e shpalli pjesërisht të pavlefshëm legjislacionin e BE-së mbi publikimin e informacionit në lidhje me përfituesit e fondeve bujqësore evropiane.

Shembull: tek çështja *Rechnungshof k. Österreichischer Rundfunk dhe të Tjerëve*.[105] GJDBE-ja shqyrtoi pajtueshmërinë e një pjese të legjislacionit të Austrisë me të drejtën e BE-së në fushën e mbrojtjes së të dhënave. Legjislacioni detyronte një organ shtetëror të mblidhte dhe transmetonte të dhëna mbi të ardhurat, për qëllime të publikimit të identitetit dhe të ardhurave të nëpunësve të njësive të ndryshme publike në një raport vjetor të

[102] GJDBE, Çështje të bashkuara C-92/09 dhe C-93/09, *Volker und Markus Schecke GbR dhe Hartmut Eifert k. Land Hessen* [ÇB], 9 nëntor 2010, parag. 47–52, 58, 66–67, 75, 86 dhe 92.
[103] *Ibid.,* parag. 85.
[104] *Ibid.,* parag. 89.
[105] GJDBE,C-465/00, C-138/01 and C-139/09, *Rechnungshof k. Österreichischer Rundfunk dhe të Tjerët dhe Christa Neukomm dhe Jospeh Lauermann k. Österreichischer Rundfunk*, 20 maj 2003.

disponueshëm për publikun e gjerë. Disa persona refuzuan të komunikonin të dhënat e tyre për arsye të mbrojtjes së të dhënave.

Në opinionin e saj, GJDBE-ja u mbështet tek mbrojtja e të drejtave themelore si parim i përgjithshëm i legjislacionit të BE-së dhe tek neni 8 i KEDNJ-së, duke kujtuar faktin se Karta nuk ishte detyruese në atë kohë. Ajo theksoi se mbledhja e të dhënave në lidhje me të ardhurat nga profesioni të një personi dhe në veçanti komunikimi i tyre tek palë të treta, ishin objekt i së drejtës për respektim të jetës private dhe përbënte shkelje të kësaj të drejte. Ndërhyrja mund të justifikohej nëse do të kishte qenë në përputhje me ligjin, për një qëllim legjitim dhe e nevojshme për arritjen e atij qëllimi në një shoqëri demokratike. GJDBE-ja vërejti se legjislacioni austriak synonte një qëllim legjitim, meqenëse objektivi i tij ishte mbajtja e pagave të nëpunësve publikë brenda afateve të arsyeshme – element i cili lidhet gjithashtu edhe me mirëqenien ekonomike të vendit. Gjithsesi, interesi i Austrisë për të garantuar përdorim sa më të mirë të fondeve publike, duhej ekuilibruar me shkallën e ndërhyrjes tek e drejta e personave për respektim të jetës së tyre private.

Megjithëse GJDBE-ja ua linte gjykatave kombëtare të përcaktonin nëse publikimi i të dhënave mbi të ardhurat e individëve ishte i nevojshëm dhe proporcional me qëllimin që synonte legjislacioni, ajo u kërkonte gjykatave kombëtare të vlerësonin nëse ky qëllim mund të arrihej po aq efektivisht me mënyra të tjera më pak ndërhyrëse. Një mënyrë mund të ishte transmetimi i të dhënave personale vetëm tek organet publike mbikëqyrëse dhe jo tek publiku i gjerë.

Në çështje të mëvonshme u pa qartë se ekuilibrimi i mbrojtjes së të dhënave me aksesin në dokumente kërkon një analizë të hollësishme rast pas rasti. Asnjëra nga të drejtat nuk mund të prevalojë tjetrën automatikisht. GJDBE-ja pati rastin të interpretonte të drejtën për akses në dokumente që përmbajnë të dhëna personale në dy çështje.

Shembull: tek *Komisioni Evropian k. Bavarian Lager,* [106] GJDBE-ja përcaktoi fushëveprimin e mbrojtjes së të dhënave personale në kontekstin e aksesit në dokumentet e institucioneve të BE-së dhe marrëdhënien midis Rregullores nr. 1049/2001 (Rregullores së Aksesit në Dokumente) me Rregulloren nr. 45/2001 (Rregulloren e Mbrojtjes së të Dhënave të Institucioneve të BE-së). Shoqëria Bavarian Lager, e themeluar në vitin 1992, importon birrë me shishe në Mbretërinë e Bashkuar, kryesisht për lokale dhe bare. Ajo kishte hasur vështirësi, gjithsesi, për shkak se legjislacioni britanik, *de facto*, favorizonte prodhuesit vendas. Në përgjigje ndaj ankesës së Bavarian Lager-it, Komisioni Evropian vendosi të niste një procedim kundër Mbretërisë së Bashkuar për mospërmbushje të detyrimeve të saj, e cila e detyroi këtë të fundit të amendonte dispozitat e kontestuara dhe t'i harmonizonte ato me legjislacionin e BE-së. Bavarian Lager-i i kërkoi më pas Komisionit Evropian, ndërmjet dokumenteve të tjera, edhe një kopje të proces-verbalit të një takimi, në të cilin kishin marrë pjesë përfaqësuesit e Komisionit, autoriteteve britanike dhe të *Confédération des Brasseurs du Marché Commun* (CBMC). Komisioni pranoi të vinte në dispozicion disa dokumente që kishin të bënin me takimin, por fshiu pesë emra që ishin përmendur në proces-verbal, dy prej të cilëve kishin kundërshtuar shprehimisht bërjen të ditur të identitetit të tyre, ndërsa tre të tjerët Komisioni nuk kishte mundur t'i kontaktonte. Nëpërmjet vendimit të datës 18 mars 2004, Komisioni refuzoi një kërkesë tjetër të Bavarian Lager-it për të marrë proces-verbalin e plotë të takimit, duke cituar në mënyrë të veçantë mbrojtjen e jetës private të atyre

[106] GJDBE, C-28/08, *Komisioni Evropian k. Bavarian Lager Co. Ltd.* [ÇB], 29 qershor 2010.

personave, sikundër garantohet nga Rregullorja e Mbrojtjes së të Dhënave të Institucioneve të BE-së.

Meqenëse Bavarian Lager-i ishte i pakënaqur me këtë vendim, ai iu drejtua Gjykatës së Shkallës së Parë, e cila anuloi vendimin e Komisionit me vendimin e datës 8 nëntor 2007 (çështja T-194/04, *The Bavarian Lager Co. Ltd k. Komisionit të Komunitetit Evropian*), duke theksuar ndër të tjera se thjesht shfaqja e emrave të personave në fjalë në listën e personave që marrin pjesë në një mbledhje, për llogari të organizmit që përfaqësojnë, nuk përbënte cenim të jetës private dhe nuk i rrezikonte aspak jetët private të tyre.

Pas apelimit nga ana e Komisionit, GjDBE-ja anuloi vendimin e Gjykatës së Shkallës së Parë. GJDBE-ja u shpreh se Rregullorja e Aksesit në Dokumente parashikon "një sistem specifik dhe të përforcuar të mbrojtjes së personave, të dhënat personale të të cilëve mund t'i komunikohen publikut në raste të caktuara". Sipas GjDBE-së, kur një kërkesë mbështetur tek Rregullorja e Aksesit në Dokumente ka si qëllim të përfitojë akses në dokumente në të cilat përfshihen të dhëna personale, dispozitat e Rregullores së Mbrojtjes së të Dhënave të Institucioneve të BE-së bëhen te zbatueshme në tërësinë e tyre. GjDBE-ja vendosi më pas se Komisioni kishte të drejtë në refuzimin e kërkesës për akses në proces-verbalin e plotë të mbledhjes së tetorit 1996. Në mungesë të pëlqimit të të pesë pjesëmarrësve në atë mbledhje, Komisioni kishte zbatuar mjaftueshëm detyrimin për transparencë, duke vënë në dispozicion një variant të dokumentit në fjalë me emrat e tyre të fshirë prej tij.

Gjithashtu, sipas GjDBE-së, "duke qenë se Bavarian Lager-i nuk kishte parashtruar asnjë justifikim të shprehur dhe legjitim apo argument bindës, me qëllim që të demonstronte domosdoshmërinë e transferimit të atyre të dhënave personale, Komisioni nuk kishte mundur të peshonte interesat e ndryshëm të palëve të përfshira. Ai nuk kishte pasur as mundësi të verifikonte nëse ky transferim nuk mund të cënonte interesat legjitime të personave të subjekteve të të dhënave" sikurse përcakton Rregullorja e Mbrojtjes së të Dhënave të Institucioneve të Be-së.

Shembull: tek çështja *Client Earth and PAN Europe k. EFSA,* [107] GJDBE-ja shqyrtoi vendimin e Autoritetit Evropian të Ushqimit dhe Sigurisë (EFSA) për t'u refuzuar kërkuesve aksesin e plotë në dokumentet, si domosdoshmëri për të mbrojtur të drejtat për privatësi dhe mbrojtje të të dhënave të personave të cilëve u referoheshin dokumentet. Këto të fundit kishin të bënin me një projekt-raport udhëzues të hartuar nga një grup pune i EFSA-së në bashkëpunim me ekspertë të jashtëm, mbi nxjerrjen në treg të produkteve për mbrojtjen e bimëve. Fillimisht, EFSA u dha kërkuesve akses të pjesshëm, duke u refuzuar aksesin në disa variante të projekt-dokumentit udhëzues. Më pas, ajo autorizoi aksesin në projekt-variantin që përfshinte komentet individuale të ekspertëve të jashtëm. Gjithsesi, ajo redaktoi emrat e ekspertëve, duke iu referuar nenit 4, pika 1, gërma b të Rregullores 45/2001 mbi përpunimin e të dhënave personale nga institucionet dhe organet e BE-së dhe bazuar në nevojën për të mbrojtur privatësinë e ekspertëve të jashtëm. Në shkallë të parë, Gjykata e Përgjithshme e BE-së la në fuqi vendimin e EFSA-s.

Në ankimin në apel, GJDBE-ja ndryshoi vendimin e shkallës së parë. Ajo vendosi se transferimi i të dhënave personale në atë rast ishte i nevojshëm për të vërtetuar paanësinë e secilit ekspert të jashtëm në kryerjen e detyrave të tyre në cilësinë e shkencëtarit dhe për të

[107] GJDBE, C-615/13P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) k. European Food Safety Authority (EFSA), Komisioni Evropian*, 16 korrik 2015.

garantuar që procesi vendimmarrës në EFSA të mbetej transparent. Sipas GJDBE-së, EFSA nuk kishte shpjeguar mënyrën se si publikimi i emrave të ekspertëve të jashtë që kishin bërë komente mbi projekt dokumentin udhëzues do të cënonte interesat legjitimë të ekspertëve. Argumenti i përgjithshëm që publikimi i tyre mund të dëmtojë privatësinë nuk mjafton nëse nuk mbështetet në prova specifike për secilin rast.

Duke iu referuar këtyre gjykimeve, ndërhyrja tek e drejta për mbrojtje të të dhënave në kontekstin e aksesit në dokumente kërkon arsye specifike dhe të justifikuara. E drejta për akses në dokumente nuk mund të prevalojë automatikisht të drejtën për mbrojtje të të dhënave.[108]

Kjo qasje është e ngjashme me atë të GJEDNJ-së për sa i takon prvatësisë dhe aksesit në dokumente, sikurse shihet në gjykimet në vijim. Tek çështja *Magyar Helsinki*, GJEDNJ-ja deklaroi se neni 10 nuk i jepte individit të drejtën për akses në informacionin që disponon autoriteti publik, ose nuk detyron qeverinë t'ia japë këtë lloj informacioni individit. Sidoqoftë, kjo lloj e drejte apo detyrimi mund të lindë – së pari, kur përhapja e informacionit bëhet e detyrueshme me një urdhër gjykate të formës së prerë; së dyti, kur aksesi në informacion është i rëndësishëm për ushtrimin nga ana e një individi të së drejtës së tij apo të saj për lirinë e shprehjes – veçanërisht lirinë për të marrë dhe dhënë informacion – dhe kur refuzimi i tij do të ndërhynte tek ajo e drejtë.[109] Nëse refuzimi i aksesit në informacion dhe shtrirja e tij përbëjnë ndërhyrje tek liria e shprehjes së kërkuesit, diçka e tillë duhet vlerësuar në secilin rast dhe mbi bazën e rrethanave të veçanta, ku përfshihen: (i) qëllimi i kërkesës për informacion; (ii) natyra e informacionit të kërkuar; (iii) roli i kërkuesit; dhe (iv) nëse informacioni është gati dhe i disponueshëm.

Shembull: tek *Magyar Helsinki Bizottság k. Hungarisë*,[110] kërkuesi, një OJQ për të drejtat e njeriut, kërkoi informacion nga policia në lidhje me punën e avokatit mbrojtës kryesisht, për të kryer një studim mbi funksionimin e sistemit të mbrojtjes kryesisht në Hungari. Policia refuzoi të jepte informacionin, me arsyetimin se ishin të dhëna personale, të cilat nuk duheshin përhapur. Duke zbatuar kriteret e mësipërme, GJEDNJ-ja vlerësoi se kishte pasur ndërhyrje tek e drejta e mbrojtur nga neni 10. Më konkretisht, kërkuesi i cili dëshironte të ushtronte të drejtën për të përhapur informacion mbi një çështje me interes publik, kishte kërkuar akses në informacion për atë qëllim dhe informacioni ishte i nevojshëm për ushtrimin e së drejtës së kërkuesit për lirinë e shprehjes. Informacioni mbi caktimin e avokatëve mbrojtës kryesisht ishte me interes për publikun. Nuk kishte asnjë arsye të vihej në dyshim se studimi në fjalë përmbante informacion, të cilin kërkuesi planifikonte t'ia komunikonte publikut dhe të cilin publiku kishte të drejtë ta merrte. Prandaj Gjykata u mjaftua me faktin se aksesi në informacionin e kërkuar i nevojitej kërkuesit për përmbushjen e këtij objektivi. Për më tepër, informacioni ishte i gatshëm.

GJEDNJ-ja doli në përfundimin se refuzimi i aksesit në informacion në atë rast kishte dëmtuar vetë thelbin e lirisë për të marrë informacion. Për të arritur në këtë përfundim, ajo shqyrtoi në mënyrë të veçantë qëllimin e informacionit të kërkuar dhe kontributin e tij për

[108] Shih gjithsesi analizën më të hollësishme të EDPS-së (2011), *Public access to documents containing personal data after the Bavarian Lager ruling*, Bruksel, 24 mars 2011.

[109] GJEDNJ, *Magyar Helsinki Bizottság k. Hungarisë* [ÇB] , nr. 18030/11, 8 nëntor 2016, parag. 148.

[110] *Ibid.,* parag. 181, 187-200.

një interes të rëndësishëm publik, natyrën e informacionit të kërkuar dhe nëse kishte interes publik dhe rolin që luante në shoqëri kërkuesi në këtë çështje.

Në arsyetimin e saj, Gjykata theksoi se studimi i ndërmarrë nga OJQ-ja kishte të bënte me veprimtarinë e drejtësisë dhe me të drejtën për një proces të rregullt gjyqësor, e cila është një e drejtë me rëndësi të madhe referuar KEDNJ-së. Duke qenë se informacioni i kërkuar nuk përfshinte të dhëna jashtë sferës publike, të drejtat për privatësi të subjekteve të të dhënave të përfshirë (avokatët mbrojtës kryesisht) nuk do të rrezikoheshin nëse policia do t'i jepte kërkuesit akses në informacion. Informacioni i kërkuar nga kërkuesi ishte me karakter statistikor, që kishte të bënte më numrin e rasteve kur avokatët mbrojtës kryesisht ishin caktuar për të përfaqësuar të pandehur në një procedim penal.

Për Gjykatën, duke qenë se studimi synonte të jepte kontribut në një debat të rëndësishëm për një çështje me interes të përgjithshëm, çdo kufizim mbi studimin e parashikuar nga OJQ-ja duhej t'i ishte nënshtruar shqyrtimit më të kujdesshëm. Informacioni në fjalë ishte me interes publik, meqenëse interesi për publikun përfshin "çështje që janë në gjendje të krijojnë polemika të konsiderueshme, të cilat kanë të bëjnë me shqetësim shoqëror të rëndësishëm, ose të cilat lidhen me një problematikë për të cilin publiku ka interes të informohet".[111] Kësisoj, ai do të mbulonte me siguri një diskutim në lidhje mbi sjelljen e drejtësisë dhe procesin e rregullt gjyqësor, që ishte tema e studimit të kërkuesit. Duke ekuilibruar të drejtat e ndryshme të përfshira dhe duke zbatuar parimin e proporcionalitetit, GJEDNJ-ja vendosi se kishte pasur shkelje të pajustifikuar të së drejtave të kërkuesit sipas nenit 10 të KEDNJ-së.

1.3.2. Fshehtësia profesionals

Sipas së drejtës kombëtare, disa komunikime mund të jenë subjekt i detyrimit për fshehtësi profesionale. Fshehtësia profesionale mund të kuptohet si një detyrim etik i veçantë, i cili krijon një detyrim ligjor të qenësishëm në disa profesione e funksione, të cilat mbështeten tek besimi. Personat dhe institucionet që kryejnë këto funksione janë të detyruar të mos zbulojnë informacionin konfidencial, që u është bërë me dije gjatë ushtrimit të detyrës. Fshehtësia profesionale kryesisht gjen zbatim tek mjekësia dhe tek privilegji avokat-klient, ku shumë juridiksione njohin gjithashtu një detyrim për fshehtësi profesionale në sektorin financiar. Fshehtësia profesionale nuk është e drejtë themelore, por mbrohet si një formë e së drejtës për respektim të jetës private. Për shembull, GJDBE-ja ka vendosur se në disa raste "mund të jetë e nevojshme të ndalohet përhapja e disa informacioneve të cilat klasifikohen si konfidenciale, me qëllim që të mbrohet e drejta themelore për respektim të jetës private, sanksionuar në nenin 8 të KEDNJ-së dhe në nenin 7 të Kartës".[112] GJEDNJ-së i është kërkuar gjithashtu të përcaktojë nëse kufizimet ndaj fshehtësisë profesionale përbëjnë shkelje të nenit 8 të KEDNJ-së, sikurse ilustrohet në shembujt e paraqitur.

Shembull: tek çështja *Pruteanu k. Rumanisë,*[113] kërkuesi vepronte si jurist i një banke tregtare, të cilës i ishte ndaluar të kryente transaksione bankare pasi akuzohej për mashtrim.

[111] *Ibid.,* parag. 156.
[112] GJDBE, Çështja T-462/12 R, *Pilkington Group Ltd k. Komisionit Evropian*, Order of the President of the General Court, 11 mars 2013, parag. 44.

[113] GJEDNJ, *Pruteanu k. Rumanisë*, nr. 30181/05, 3 shkurt 2015.

Gjatë hetimit të çështjes, gjykatat rumune autorizuan autoritetet e ndjekjes penale të interceptonin dhe regjistronin bisedat telefonike të një bashkëpunëtori të shoqërisë, për një periudhë të caktuar kohore. Regjistrimet dhe interceptimet përfshinin komunikimet me avokatin e tij.

Z. Pruteanu pretendoi se diçka e tillë ndërhynte tek e drejta e tij për respektim të jetës private dhe korrespondencës. Në gjykimin e saj, GJEDNJ-ja nënvizoi statusin dhe rëndësinë e marrëdhënies së një avokati me klientin e tij. Interceptimi i bisedave të një avokati me klientin e tij shkelte padyshim fshehtësinë profesionale, e cila ishte themeli i marrëdhënies midis atyre dy personave. Në këtë rast, avokati mund të ankohej gjithashtu për ndërhyrje tek e drejta e tij për respektim të jetës private dhe të korrespondencës. GJEDNJ-ja vendosi se kishte pasur shkelje të nenit 8 të KEDNJ-së.

Shembull: tek *Brito Ferrinho Bexiga Villa-Nova k. Portugalisë,*[114] kërkuesja, një avokate, refuzoi t'u vinte në dispozicion autoriteteve tatimore vërtetimet bankare personale, bazuar tek konfidencialiteti profesional dhe fshehtësia bankare. Prokuroria nisi hetim për evazion fiskal dhe kërkoi autorizim për pezullim të konfidencialitetit profesional. Gjykatat kombëtare urdhëruan pezullimin e rregullave të konfidencialitetit dhe të fshehtësisë bankare, me arsyetimin se interesi publik duhet të prevalojë mbi interesat private të kërkueses.

Kur çështja iu paraqit GJEDNJ-së, Gjykata vlerësoi se aksesi tek vërtetimet bankare të kërkueses përbënte ndërhyrje tek e drejta e saj për respektim të konfidencialitetit profesional, e cila përshihet tek fushëveprimi i jetës private. Ndërhyrja kishte bazë ligjore, meqenëse mbështetej në kodin e procedurës penale dhe synonte përmbushjen e një objektivi legjitim. Gjithsesi, ndërsa shqyrtonte domosdoshmërinë dhe proporcionalitetit e ndërhyrjes, GJEDNJ-ja vuri në dukje faktin se procedura për shfuqizimin e konfidencialitetit ishte kryer pa pjesëmarrjen, apo dijeninë e kërkueses. Kësisoj, kërkuesja nuk kishte pasur mundësi të parashtronte argumentet e saj. Gjithashtu, paçka se legjislacioni kombëtar parashikonte se në këto lloj procedimesh duhej marrë mendimi i shoqatës së avokatëve, diçka e tillë nuk ishte bërë. Së fundmi, kërkueses nuk i ishte dhënë mundësia të kundërshtonte në mënyrë të efektshme shfuqizimin e konfidencialitetit dhe as ndonjë mjet juridik për të kundërshtuar masën. Për shkak të mungesës së garancive procedurale dhe kontrollit gjyqësor efikas mbi masën e pezullimit të detyrimit të konfidencialitetit, GJEDNJ-ja vendosi se kishte pasur shkelje të nenit 8 të KEDNJ-së.

Shpesh, ndërveprimi i fshehtësisë profesionale me mbrojtjen e të dhënave është i dyanshëm. Nga njëra anë, rregullat dhe masat e sigurisë për mbrojtjen e të dhënave të përcaktuara në legjislacion ndihmojnë në garantimin e fshehtësisë profesionale. Për shembull, rregullat që detyrojnë kontrolluesit dhe përpunuesit të zbatojnë masa të rrepta sigurie të të dhënave, synojnë ndër të tjera, të parandalojnë cënimin e konfidencialitetit të të dhënave personale të mbrojtura nga fshehtësia profesionale. Gjithashtu, Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave të BE-së lejon përpunimin e të dhënave në lidhje me shëndetin, të cilat janë kategori të veçanta të dhënash personale që kërkojnë mbrojtje më të madhe, por me kusht që të jenë marrë masa të përshtatshme dhe specifike për mbrojtjen e të drejtave të subjekteve të të dhënave dhe sidomos të fshehtësisë profesionale.[115]

[114] GJEDNJ, *Brito Ferrinho Bexiga Villa-Nova k. Portugalisë*, nr. 69436/10, 1 dhjetor 2015.
[115] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 9, pika 2, gërma (h) dhe neni 9, pika 3.

Nga ana tjetër, detyrimet për fshehtësi profesionale, që bien mbi kontrolluesit dhe përpunuesit për sa i takon disa llojeve të të dhënave personale, mund të kufizojnë të drejtat e subjekteve të të dhënave, veçanërisht të drejtën për t'u informuar. Megjithëse Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave përmban një listë gjithëpërfshirëse informacioni, që në parim i duhet dhënë subjektit të të dhënave, kur të dhënat nuk janë marrë drejtpërdrejt nga ai ose ajo, ky kriter dhënieje informacioni nuk zbatohet kur të dhënat personale duhet të mbeten konfidenciale për shkak të detyrimit të fshehtësisë profesionale, të përcaktuar qoftë nga e drejta kombëtare, ashtu edhe nga ajo e BE-së.[116]

Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave (GDPR) parashikon mundësinë që Shtetet Anëtare të miratojnë në ligj rregulla specifike për mbrojtjen e detyrimeve për fshehtësi profesionale, ose të barasvlershme me to dhe për të harmonizuar të drejtën për mbrojtjen e të dhënave personale me detyrimin për fshehtësi profesionale.[117]

GDPR-ja përcakton që Shtetet Anëtare mund të miratojnë rregulla specifike për sa i përket kompetencave të autoriteteve mbikëqyrëse, në lidhje me kontrolluesit, apo përpunuesit që i nënshtrohen detyrimit për fshehtësi profesionale. Këto rregulla specifike kanë të bëjnë me kompetencën për të pasur akses në ambientet e një kontrolluesi, apo përpunuesi, tek pajisjet e përpunimit të të dhënave dhe tek të dhënat personale që disponojnë, kur këto të dhëna personale janë përftuar në kuadër të një veprimtarie që përfshihet nga detyrimi për ruajtjen e fshehtësisë. Kësisoj, autoritetet mbikëqyrëse të ngarkuara për mbrojtjen e të dhënave, duhet të respektojnë detyrimet për fshehtësi profesionale, që janë të detyrueshme për kontrolluesit dhe përpunuesit. Gjithashtu, vetë nëpunësit e autoriteteve mbikëqyrëse janë subjekt i detyrimit për fshehtësi profesionale, gjatë dhe pas largimit nga detyra. Gjatë ushtrimit të funksioneve të tyre, nëpunësit e autoriteteve mbikëqyrëse mund të njihen me informacion konfidencial. Neni 54, pika 2 e Rregullores përcakton qartë se ata kanë detyrimin e fshehtësisë profesionale për sa i takon këtij informacioni konfidencial.

GDPR-ja detyron Shtetet Anëtare të njoftojnë Komisionin mbi rregullat që ato miratojnë për të harmonizuar mbrojtjen e të dhënave dhe parimet e përcaktuara në Rregullore me detyrimin për fshehtësi profesionale.

1.3.3. Liria e fesë dhe e besimit

Liria e fesë dhe e besimit mbrohet nga neni 9 i KEDNJ-së (liria e mendimit, ndërgjegjes dhe fesë) dhe nga neni 10 i Kartës së të Drejtave Themelore të BE-së. Të dhënat personale që zbulojnë besimet fetare ose filozofike konsiderohen "të dhëna sensitive" edhe nga e drejta e BE-së, ashtu edhe nga e drejta e KiE-së dhe përpunimi e përdorimi i tyre është subjekt mbrojtjeje të shtuar.

Shembull: kërkuesi tek çështja *Sinak Isik k. Turqisë*[118] ishte anëtar i komunitetit fetar alevit, besimi i të cilit ndikohet nga Sufizmi dhe nga besime të tjera para-islame dhe nga një pjesë

[116] *Ibid.,* Neni 14, pika 5, gërma (d).
[117] *Ibid.,* Paragrafi 164 dhe neni 90.

[118] GJEDNJ, *Sinan Işık k. Turqisë*, nr. 21924/05, 2 shkurt 2010.

e studiuesve konsiderohet si fe më vete, ndërsa nga të tjerë si pjesë e Islamit. Kërkuesi pretendonte se, përkundër dëshirës, karta e tij e identitetit përmbante një seksion ku paraqitej besimi i tij fetar "Islam" dhe jo "Alevi". Gjykatat kombëtare e refuzuan kërkesën e tij për të ndryshuar kartën e identitetit në "Alevi", me arsyetimin se termi përshkruante një nën-grup të Islamit dhe jo një fe të veçantë. Ndaj ai u ankua pranë GJEDNJ-së për faktin se ishte detyruar të zbulonte besimin fetar pa pëlqimin e tij, për shkak se ishte e detyrueshme të paraqitej feja e personit në kartën e identitetit dhe se kjo ishte shkelje e të drejtës së tij për lirinë e fesë dhe të ndërgjegjes, sidomos duke qenë se përkatësia në "Islam" tek karta e tij e identitetit ishte e pasaktë.
GJEDNJ-ja ritheksoi se liria e besimit përcakton lirinë e manifestimit të besimit fetar të personit në komunitet me të tjerët, në publik dhe brenda rrethit të personave që kanë të njëjtin besim fetar, por gjithashtu edhe në vetmi dhe intimitet. Legjislacioni i brendshëm në fuqi në atë kohë i detyronte personat të pajiseshin me kartë identiteti, dokument i cili duhet të paraqitej sipas kërkesës së çdo autoriteti publik apo ndërmarrjeje private, në të cilën duhej të tregohej besimi fetar i tyre. Një detyrim i tillë nuk merrte parasysh se e drejta për të manifestuar besimin fetar përfshin gjithashtu edhe të kundërtën, d.m.th të drejtën për të mos qenë i detyruar të tregosh besimin fetar. Megjithëse qeveria argumentoi se legjislacioni kombëtar ishte ndryshuar në mënyrë të tillë që individët të kërkonin që seksioni i besimit fetar të lihej bosh, në këndvështrimin e Gjykatës edhe thjesht fakti që duhet të bëhej kërkesë për të fshirë besimin fetar, mund të zbulonte informacion në lidhje me qëndrimin e individëve ndaj fesë. Gjithashtu, kur kartat e identitetit përmbajnë një seksion të besimit fetar, lënia e tij bosh ka konotacion të veçantë, meqenëse zotëruesit e një kartë identiteti pa të dhëna mbi fenë do të dalloheshin prej atyre, karta e të cilëve tregonin besimi fetar. GJEDNJ-ja vendosi se legjislacioni i brendshëm shkelte nenin 9 të KEDNJ-së.

Gjithsesi, për funksionimin e kishave dhe shoqatave apo komuniteteve fetare mund të nevojitet përpunimi i informacionit personal të anëtarësisë, për të mundësuar komunikimin dhe organizimin e aktiviteteve brenda bashkësisë. Për këtë, shpesh kishat dhe shoqatat fetare kanë zbatuar rregulla në lidhje me përpunimin e të dhënave personale. Sipas nenit 91 të Rregullores së Përgjithshme të Mbrojtjes së të Dhënave, kur këto rregulla janë gjithëpërfshirëse, ato mund të vijojnë të jenë të vlefshme, me kusht që të harmonizohen me dispozitat e Rregullores. Kishat dhe shoqatat fetare që kanë rregulla të tilla, mund t'i nënshtrohen mbikëqyrjes së një autoritetit të pavarur mbikëqyrës, i cili mund të jetë specifik për to, me kusht që ato të përmbushin kriteret e Rregullores së Përgjithshme të Mbrojtjes së të Dhënave për këto autoritete.[119]

Organizatat fetare mund të kryejnë përpunim të dhënash personale për arsye të ndryshme – për shembull, për të mbajtur lidhje me bashkësinë e tyre, ose për të komunikuar informacion në lidhje me aktivitete dhe festa fetare, apo bamirësie, që organizohen. Në disa shtete, kishat duhet të mbajnë regjistra të anëtarëve të tyre, për qëllime tatimore, meqenëse anëtarësimi në disa institucioneve fetare mund të ketë ndikim në taksat që paguhen nga individët. Sidoqoftë, referuar së drejtës evropiane, të dhënat që tregojnë besimet fetare janë të dhëna sensitive dhe kishat kanë përgjegjësi për menaxhimin dhe përpunimin e këtyre të dhënave, sidomos për shkak se informacioni që përpunojnë organizatat fetare shpesh ka të bëjë me fëmijët, të moshuarit dhe anëtarë të tjerë vulnerabil të shoqërisë.

[119] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 91, pika 2.

1.3.4. Liria e arteve dhe shkencave

Një e drejtë tjetër që duhet ekuilibruar me të drejtat për respektim të jetës private dhe për mbrojtje të të dhënave është liria e arteve dhe shkencave, të mbrojtura qartësisht nga neni 13 i Kartës së të Drejtave Themelore të BE-së. Kjo e drejtë buron kryesisht nga e drejta e lirisë së mendimit dhe shprehjes dhe duhet ushtruar duke pasur në vëmendje nenin 1 të Kartës (dinjitetin njerëzor). GJEDNJ-ja vlerëson se liria e arteve mbrohet nga neni 10 i KEDNJ-së.[120] E drejta e garantuar në nenin 13 të Kartës mund të jetë gjithashtu subjekt i kufizimeve sipas nenit 52, pika 1 të Kartës, i cili mund të interpretohet gjithashtu në optikën e nenit 10, pika 2 të KEDNJ-së.[121]

Shembull: tek çështja *Vereinigung bildender Künstler k. Austrisë*[122] gjykatat austriake ndaluan shoqërinë kërkuese të vijonte të ekspozonte një pikturë, e cila përmbante fotografitë me kokat e disa figurave publike në pozicione seksuale. Një parlamentar austriak, fotografitë e të cilit ishin përdorur në pikturë, paditi shoqërinë kërkuese, duke kërkuar urdhër ndalimi të ekspozimit të pikturës. Gjykata vendase urdhëroi ndalimin. GJEDNJ-ja u shpreh se neni 10 i KEDNJ-së gjen zbatim në rastet e komunikimit të ideve të cilat fyejnë, trondisin, apo shqetësojnë shtetin, ose çfarëdo pjese të popullsisë. Ata të cilët krijojnë, interpretojnë, shpërndajnë, ose ekspozojnë punime artistike, japin kontribut në shkëmbimin e ideve dhe mendimeve dhe shteti ka detyrimin të mos ndërhyjë padrejtësisht në lirinë e tyre të shprehjes. Meqenëse piktura ishte një kolazh dhe në të ishin përdorur vetëm kokat e personave, ndërsa trupat e tyre ishin pikturuar në mënyrë jo realiste dhe të ekzagjeruar, çka qartësisht nuk synonte të pasqyronte, apo të aludonte realitetin, GJEDNJ-ja u shpreh më tej se "vështirë se piktura mund të kuptohej si referim i detajeve të jetës private [të subjektit], por më së shumti qëndrimit të tij publik si politikan" dhe se "në këtë cilësi, [subjekti i pikturuar] duhet të tregonte me tepër tolerancë ndaj kritikës". Duke peshuar interesat e ndryshëm të përfshirë, GJEDNJ-ja vendosi se ndalimi i pakufizuar i ekspozimit të mëtejshëm të pikturës, ishte jo proporcional. Përfundimisht Gjykata vendosi se kishte pasur shkelje të nenit 10 të KEDNJ-së.

E drejta evropiane në fushën e mbrojtjes së të dhënave njeh gjithashtu vlerën e veçantë të shkencës për shoqërinë. Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave dhe Konventa 108 e Modernizuar lejojnë mbajtjen e të dhënave për një kohë më të gjatë, nëse të dhënat personale përpunohen vetëm për qëllim shkencore ose historike. Po ashtu, pavarësisht qëllimit fillestar të një aktiviteti të caktuar përpunimi, përdorimi i mëtejshëm i të dhënave personale për kërkim shkencor nuk konsiderohet si qëllim i papajtueshëm.[123] Njëkohësisht duhen zbatuar masat e duhura të sigurisë për këtë lloj përpunimi, për të mbrojtur të drejtat dhe liritë e subjekteve të të dhënave. Kur bëhet fjalë për përpunimin e të dhënave personale për qëllime të kërkimit shkencor, historik ose statistikor, e drejta e BE-së ose e Shteteve Anëtare mund të parashikojë përjashtime, për sa i përket të drejtave të subjektit të të dhënave, sikurse për

[120] GJEDNJ, *Müller dhe të Tjerët k. Zvicrës*, nr. 10737/84, 24 maj 1988.

[121] Shpjegime në lidhje me Kartën e të Drejtave Themelore, FZ 2007 C 303.

[122] GJEDNJ, *Vereinigung bildender Künstler k. Austrisë*, nr. 68345/01, 25 janar 2007, paragrafët 26 dhe 34.

[123] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5, pika 1, gërma (b) dhe Konventa 108 e Modernizuar, neni 5, pika 4, gërma (b).

shembull për të drejtën e aksesit, korrigjimit, kufizimit të përpunimit dhe kundërshtimit (shih gjithashtu Seksionin 6.1 dhe Seksionin 9.4).

1.3.5. Mbrojtja e pronësisë intelektuale

E drejta për mbrojtjen e pronës sanksionohet nga neni 1 i Protokollit të Parë të KEDNJ-së dhe po ashtu nga neni 17, pika 1 e Kartës së të Drejtave Themelore të BE-së. Një aspekt i rëndësishëm i të drejtës së pronës, që ka rëndësi të veçantë për mbrojtjen e të dhënave, është mbrojtja e pronësisë intelektuale, përmendur qartë në nenin 17, pika 2 të Kartës. Disa direktiva të rendit juridik të BE-së synojnë mbrojtjen e efektshme të pronësisë intelektuale, veçanërisht të së drejtës së autorit. Pronësia intelektuale përfshin jo vetëm pronësisë letrare dhe artistike, por edhe patentat, markat dhe të drejtat e tjera në lidhje me to.

Sikurse është qartësuar në jurisprudencën e GJDBE-së, mbrojtja e së drejtës themelore të pronës, duhet të ekuilibrohet me mbrojtjen e të drejtave të tjera themelore, sidomos me të drejtën për mbrojtje të të dhënave.[124] Ka pasur raste kur institucionet e mbrojtjes së të drejtës së autorit, kanë kërkuar nga operatorët e shërbimeve të internetit, që të bënin të ditur identitetin e përdoruesve të platformave të shkëmbimit të skedarëve në internet. Këto platforma shpesh u mundësojnë përdoruesve që të shkarkojnë pjesë muzikore pa pagesë, edhe pse këto të fundit mbrohen nga e drejta e autorit.

Shembull: *Promusicae k. Telefónica de España*[125] kishte të bënte me refuzimin që i kishte bërë një operatori spanjoll shërbimesh interneti, Telefónica që t'i jepte Promusicae-s, një organizate jo-fitimprurëse producentësh muzikorë dhe audio-vizivë, të dhënat personale të disa personave, të cilëve u kishte siguruar shërbimet e aksesit në internet. Promusicae-ja e kërkonte informacionin, në mënyrë që të niste procedim civil ndaj këtyre personave, për të cilët pretendonte se përdornin një program për shkëmbimin e skedarëve, i cili mundësonte aksesin në fonograme, të drejtat e shfrytëzimit të të cilave i kishin anëtarët e Promusicae-s.

Gjykata spanjolle ia referoi çështjen GJDBE-së, për të verifikuar nëse këto të dhëna personale mund të komunikoheshin, sipas së drejtës së BE-së, në kuadër të procedimit civil për tyë garantuar mbrojtje të efektshme të së drejtës së autorit. Gjykata u mbështet në Direktivat 2000/31, 2001/29 dhe 2004/48, të para në optikën e neneve 17 dhe 47 të Kartës. GJDBE-ja arriti në përfundimin se këto tre direktiva, ashtu si edhe Direktiva mbi privatësinë dhe komunikimet elektronike (Direktiva 2002/58), nuk i pengojnë Shtetet Anëtare që të përcaktojnë detyrimin për të komunikuar të dhëna personale, në kuadër të procedimeve civile, për të garantuar mbrojtje të efektshme të së drejtës së autorit.

GJDBE-ja theksoi se për rrjedhojë çështja ngrinte pikëpyetje në lidhje me nevojën për të harmonizuar normat e mbrojtjes së të drejtave të ndryshme themelore - konkretisht të së drejtës për respektim të jetës private me të drejtat për mbrojtje të pronës dhe për mbrojtje të efektshme gjyqësore.

Gjykata doli në përfundimin se "Shtetet Anëtare, kur transpozojnë direktivat e lartpërmendura, duhet të kujdesen që interpretimi i këtyre direktivave të mundësojë ekuilibrimin e duhur të së drejtave të ndryshme themelore, të cilat mbrohen nga rendi juridik i Komunitetit. Më tej, gjatë zbatimit të masave për transpozimin e këtyre direktivave,

[124] GJDBE, C-275/06, *Productores de Música de España (Promusicae) k. Telefónica de España SAU* [ÇB] , 29 janar 2008, paragrafët 62–68.
[125] *Ibid.*,paragrafët 54 dhe 60.

autoritetet dhe gjykatat e Shteteve Anëtare, nuk duhet të interpretojnë vetëm të drejtën e tyre kombëtare në përputhje me këto direktiva, por duhet gjithashtu të sigurohen se nuk po mbështeten në një interpretim të tyre, i cili do të hynte në konflikt me ato të drejta themelore, ose me parimet e tjera të përgjithshme të së drejtës së Komunitetit, sikurse me parimin e proporcionalitetit."[126]

Shembull: *Bonnier Audio AB dhe të Tjerët k. Perfect Communication Sweden AB*[127] kishte të bënte me ekuilibrimin e të drejtave për pronësinë intelektuale me mbrojtjen e të dhënave personale. Kërkuesit – pesë shoqëri producentësh që kishin të drejtat e autorit për 27 audio-libra – u ankuan në gjykatën suedeze me pretendimin se këto të drejta autori ishin shkelur nëpërmjet një serveri FTP (protokoll transferimi skedarësh, i cili mundëson shkëmbimin e skedarëve dhe transferimin e të dhënave nëpërmjet internetit). Kërkuesit kërkuan që operatori i shërbimit të internetit (ISP) të bënte me dije emrin dhe adresën e personit që përdorte adresën IP nga e cila ishin dërguar skedarët. ISP-ja, ePhone, e kundërshtoi ankesën me pretendimin se shkelte Direktivën 2006/24 (Direktivën e Mbajtjes së të Dhënave – shfuqizuar në 2014-ën).

Gjykata suedeze ia referoi çështjen GJDBE-së, duke shtruar pyetjen nëse Direktiva 2006/24 përjashtonte zbatimin e një dispozite kombëtare mbështetur në nenit 8 të Direktivës 2004/48 (Direktiva e Zbatimit të të Drejtave të Pronësisë Intelektuale), e cila lejon nxjerrjen e një urdhri që i kërkon ISP-ve t'u transmetojnë zotëruesve të së drejtës së autorit, informacion mbi abonentët, adresat IP të së cilëve pretendohej se ishin përdorur për kryerjen e shkeljeve. Pyetja mbështetej në supozimin se kërkuesi kishte paraqitur prova të qarta për shkeljen e një të drejte autori të caktuar dhe se masa ishte proporcionale.

GJDBE-ja theksoi se Direktiva 2006/24 trajtonte ekskluzivisht menaxhimin dhe mbajtjen e të dhënave të gjeneruara nga operatorët e shërbimeve të komunikimit elektronik për qëllime të hetimit, zbulimi dhe ndjekjes së krimeve të rënda dhe komunikimin e tyre tek autoritetet kompetente kombëtare. Kështu, një dispozitë kombëtare që transpozon Direktivën e Zbatimit të të Drejtave të Pronësisë Intelektuale është jashtë fushës së zbatimit të Direktivës 2006/24 dhe për rrjedhojë nuk përjashtohet nga ajo direktivë.[128]

Për sa i përket komunikimit të emrit dhe adresës në fjalë, të kërkuara nga kërkuesit, GJDBE-ja u shpreh se ky veprim përbën përpunim të dhënash personale dhe është brenda fushës së zbatimit të Direktivës 2002/58 (Direktivës së ePrivatësisë). Ajo gjithashtu theksoi se komunikimi i atyre të dhënave kërkohej për një procedim civil, në dobi të zotëruesit të një të drejte autori, me qëllim që të garantohej mbrojtje e efektshme e së drejtës së autorit dhe rrjedhimisht, për shkak të objektit të saj, përfshihet gjithashtu në fushën e zbatimit të Direktivës 2004/48.[129]

GJDBE-ja doli në përfundimin se Direktivat 2002/58 dhe 2004/48 duhen interpretuar si jo përjashtuese të legjislacionit kombëtar, siç është rasti me legjislacionin në pikëpyetje në procedimin kryesor, për aq kohë sa ai legjislacion i mundëson gjykatës kombëtare, të cilës i është drejtuar një ankesë për një urdhër komunikimi të dhënash personale, të ekuilibrojë

[126] *Ibid.*, parag. 65 dhe 68; shih gjithashtu GJDBE, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) k. Netlog NV*, 16 shkurt 2012.
[127] GJDBE, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB k. Perfect Communication Sweden AB*, 19 prill 2012.
[128] *Ibid.*, parag. 40-41.
[129] *Ibid.*, parag. 52-54. Shih gjithashtu GJDBE, C-275/06, *Productores de Música de España (Promusicae) k. Telefónica de España SAU* [ÇB], 29 janar 2008, parag. 58.

interesat në konflikt, bazuar në faktet e secilit rast dhe duke marrë parasysh kriteret e parimit të proporcionalitetit.

1.3.6. Mbrojtja e të dhënave dhe interesave ekonomike

Në epokën digjitale apo në epokën e të dhënave masive, të dhënat janë cilësuar si "nafta e re" e ekonomisë, për nxitjen e inovacionit dhe krijimtarisë.[130] Shumë shoqëri tregtare kanë ndërtuar modele të fuqishme biznesi mbështetur tek përpunimi i të dhënave dhe këto përpunime shpesh përfshijnë të dhëna personale. Disa nga këto shoqëri mund të besojnë se rregullat specifike të mbrojtjes së të dhënave personale, mund të krijojnë në praktikë detyrime të rënda që mund të cënojnë interesat e tyre ekonomike. Në këtë mënyrë, shtrohet pyetja nëse interesat ekonomikë të kontrolluesve dhe përpunuesve, apo të publikut të gjerë, mund të justifikojnë kufizimin e të drejtës për mbrojtje të të dhënave.

Shembull: tek çështja *Google Spain,*[131] GJDBE-ja u shpreh se individët kanë të drejtë t'u kërkojnë motorëve të kërkimit të heqin rezultatet e kërkimit nga indeksi i tyre i kërkimit me disa kushte të caktuara. Në arsyetimin e saj, GJDBE-ja nënvizoi faktin se përdorimi i motorëve të kërkimit dhe rezultateve të radhitura të kërkimit, mund të krijojnë një profil të hollësishëm të një personi. Ky informacion mund të lidhet me një aspekt të gjerë të jetës private të personit, që nuk do të mund të gjendej apo ndërlidhej lehtësisht pa ndihmën e një motori kërkimi. Për pasojë, ky i fundit përbënte ndërhyrje potencialisht të rëndë tek të drejtat themelore për privatësi dhe mbrojtje të të dhënave personale të subjekteve të të dhënave.

Në vijim, GJDBE-ja shqyrtoi nëse ndërhyrja mund të justifikohej. Për sa i përket interesit ekonomik të shoqërisë poseduese të motorit të kërkimit për kryerjen e përpunimit, GJDBE-ja deklaroi se "është e qartë që [ndërhyrja] nuk mund të justifikohet thjesht me interesin ekonomik që ka operatori i këtij lloj motori për këtë përpunim", dhe se "si rregull" të drejtat themelore referuar neneve 7 dhe 8 të Kartës, prevalojnë mbi këtë interes ekonomik dhe mbi interesin e publikut të gjerë për të gjetur informacion me anë të një kërkimi që lidhet me emrin e subjektit të të dhënave.[132]

Një nga normat themelore të së drejtës evropiane në fushën e mbrojtjes së të dhënave, është t'u japë individëve më tepër kontroll mbi të dhënat e tyre personale. në mënyrë të veçantë në epokën digjitale, fuqia e njësive tregtare që përpunojnë dhe kanë akses tek sasi masive të dhënash personale në raport me fuqinë e individëve të cilëve u përkasin ato të dhëna personale për të kontrolluar informacionin e tyre, është në përpjesëtim të zhdrejtë. GJDBE-ja e trajton rast pas rasti ekuilibrimin e mbrojtjes së të dhënave me interesat ekonomikë – sikurse interesat e palëve të treta në lidhje me shoqëritë aksionere dhe me përgjegjësi të kufizuar, sikundër ilustrohet në gjykimin e çështjes *Manni.*

Shembull: çështja *Manni*[133] kishte të bënte me përfshirjen e të dhënave personale të një individi në një regjistër tregtar publik. Z. Manni i kishte kërkuar Dhomës së Tregtisë së Leçes

[130] Shih, për shembull, Financial Times (2016), "Data is the new oil… who's going to own it?", 16 nëntor 2016.
[131] GJDBE, C-131/12, *Google Spain SL, Google Inc. k. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [ÇB] , 13 maj 2014.
[132] *Ibid.,* parag. 81 dhe 97.
[133] GJDBE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce k. Salvatore Manni*, 9 mars 2017.

të fshinte të dhënat e tij personale nga ai regjistër, duke qenë se kishte zbuluar që klientë të mundshëm mund t'i drejtoheshin regjistrit dhe të shihnin se ai kishte qenë administratori i një shoqërie e cila kishte falimentuar më tepër se një dekadë më parë. Ky lloj informacioni do t'i bënte paragjykues klientët e tij të mundshëm dhe mund të kishte ndikim negativ në interesat e tij tregtare.

GJDBE-së iu kërkua të përcaktonte nëse e drejta e BE-së e njihte një të drejtë për fshirje në këtë rast. Për të arritur në një përfundim, ajo vendosi në peshore rregullat e mbrojtjes së të dhënave të BE-së me interesin tregtar të z. Manni për fshirjen e informacionit në lidhje me falimentimin e shoqërisë së tij të mëparshme. Ajo mori mirë parasysh faktin se përhapja tek regjistrimi publik i shoqërive ishte i parashikuar me ligj dhe në mënyrë të veçantë nga një Direktivë e BE-së që kishte për qëllim t'ua lehtësonte palëve të treta gjetjen e informacionit në lidhje me shoqëritë. Përhapja e të dhënave ishte e rëndësishme për mbrojtjen e interesave të palëve të treta, të cilat mund të parashikojnë të bëjnë biznes me një shoqëri të caktuar, për shkak se e vetmja garanci që ofrojnë shoqëritë aksionere dhe ato me përgjegjësi të kufizuar për palët e treta janë asetet e tyre. Për rrjedhojë, "dokumentet bazë të shoqërisë në fjalë duhet të përhapen, me qëllim që palët e treta të kenë mundësi të vërtetojnë përmbajtjen e tyre dhe informacione të tjera në lidhje me shoqërinë, sidomos të dhënat e personave të cilët kanë fuqi detyruese mbi shoqërinë".[134]

Referuar rëndësisë së qëllimit legjitim që kishte regjistri, GJDBE-ja u shpreh se z. Manni nuk kishte të drejtë të kërkonte fshirjen e të dhënave personale të tij, meqenëse nevoja për të mbrojtur interesat e palëve të treta në lidhje me shoqëritë aksionere dhe me përgjegjësi të kufizuar dhe për të garantuar siguri ligjore, tregti të ndershme dhe për rrjedhojë mirëfunksionim të tregut të brendshëm, kishte përparësi ndaj të drejtave të që rrjedhin nga legjislacioni i mbrojtjes së të dhënave. Diçka e tillë përforcohej nga fakti se individët që zgjedhin të angazhohen në tregti, me anë të shoqërive aksionere ose me përgjegjësi të kufizuar, janë të vetëdijshëm se do t'u duhet të përhapin informacion në lidhje me identitetin dhe funksionet e tyre.

Megjithëse doli në përfundimin se në këtë rast nuk kishte bazë ligjore për të kërkuar fshirjen e të dhënave, GJDBE-ja pranoi ekzistencën e të drejtës për të kundërshtuar përpunimin, duke vërejtur se: "nuk mund të përjashtohet [...] që mund të ketë situata të caktuara ku arsyet prevaluese dhe legjitime të personit të përfshirë në lidhje me rastin specifik, mund të justifikojnë në mënyrë përjashtimore që aksesi tek të dhënat personale të mbajtura në regjistër, të kufizohet, pas përfundimit të një periudhe të mjaftueshme të gjatë kohore [...] për palët e treta që kanë interes të caktuar për t'u njohur me to".[135]

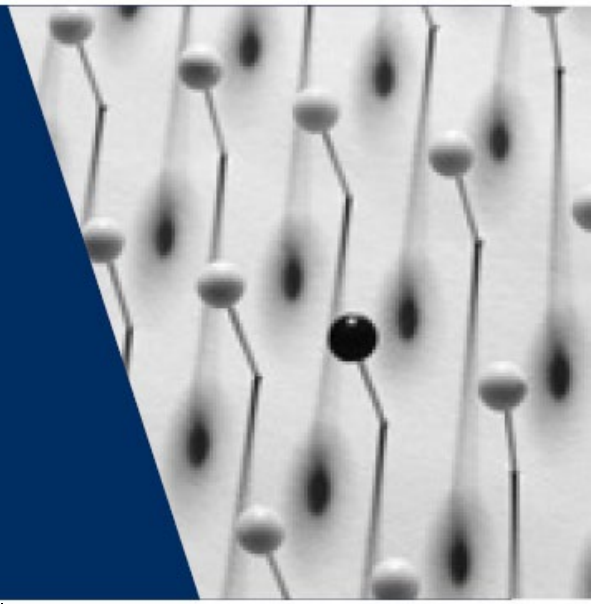
GJDBE-ja deklaroi se ishte në dorë të gjykatave kombëtare të vlerësonin në secilin rast dhe duke marrë parasysh të gjitha rrethanat përkatëse të individit, ekzistencën apo mungesën e arsyeve legjitime dhe prevaluese, të cilat mund të justifikojnë, në mënyrë përjashtimore, kufizimin e aksesit nga palët e treta tek të dhënat personale të mbajtura në regjistrat e shoqërive. Gjithsesi, ajo qartësoi se, në rastin e z. Manni, thjesht fakti se përhapja e të dhënave të tij në regjistër mund të prekte klientelën e tij, nuk mund të konsiderohej si arsye legjitime dhe prevaluese. Klientët e mundshëm të z. Manni kishin interes legjitim për informacionin në lidhje me falimentimin e shoqërisë së tij të mëparshme.

[134] *Ibid.,* parag. 49.
[135] *Ibid.,* parag. 60.

Ndërhyrja tek të drejtat themelore për jetë private dhe mbrojtje të të dhënave personale të z. Manni dhe të personave të tjerë të përfshirë në regjistër, sikurse garantohen nga neni 7 dhe 8 i Kartës, i shërbente një objektivi me interes të përgjithshëm dhe ishte e domosdoshme dhe proporcionale.

Rrjedhimisht, tek çështja *Manni*, GJDBE-ja vendosi se të drejtat për mbrojtjen e të dhënave dhe privatësisë nuk prevalonin ndaj interesit të palëve të treta për të pasur akses në informacionin e regjistrit të shoqërive, në lidhje me shoqëritë aksionere dhe ato me përgjegjësi të kufizuar.

2 Terminologjia e mbrojtjes së të dhënave



BE	Çështje të trajtuara	KiE
Të dhëna personale		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 4, pika 1 Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave,	**Përkufizime ligjore të mbrojtjes së të dhënave**	Konventa 108 e Modernizuar, neni 2, gërma (a) GJEDNJ, *Bernh Larsen Holding AS dhe të Tjerët k.*

nenet 4, pika 5 dhe 5, pika 1, gërma e Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 9 GJDBE, Çështje të bashkuara C-92/09 dhe C-93/09, *Volker und Markus Schecke GbR dhe Hartmut Eifert k. Land Hessen* [GC], 2010 GJDBE, C-275/06, *Productores de Música de España (Promusicae) k. Telefónica de España SAU* [GC], 2008 GJDBE, C-70/10, *Scarlet Extended SA k. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 GJDBE, C-582/14, *Patrick Breyer k. Bundesrepublik Deutschland*, 2016 GJDBE, Çështje të bashkuara C-141/12 dhe C-372/12, *YS k. Minister voor Immigratie, Integratie en Asiel* dhe *Minister voor Immigratie, Integratie en Asiel k. M dhe S*, 2014		*Norvegjisë*, nr. 24117/08, 2013 GJEDNJ, *Uzun k. Gjermanisë*, nr. 35623/05, 2010 GJEDNJ, *Amman k. Zvicrës* [GC], nr. 27798/95, 2000
GJDBE, C-101/01, *Criminal proceedings k. Bodil Lindqvist*, 2003	**Kategori të veçanta të të dhënave personale** **(të dhënat sensitive)**	Konventa 108 e Modernizuar, neni 6, pika 1
GJDBE, C-434/16, *Peter Nowak k. Data Protection Commissioner*, 2017	**Të dhëna personale të Anonimizuara dhe të Pseudonimizuara**	Konventa 108 e Modernizuar, neni 5, pika 4, shkronja e Relacioni Shpjegues i Konventës 108 të Modernizuar, Paragrafi 50

Përpunimi i të dhënave		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 4, pika 2 GJDBE, C-212/13, *František Ryneš k.* Úřad *pro ochranu osobních* údajů, 2014 GJDBE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce k. Salvatore Manni*, 2017 GJDBE, C-101/01, *Criminal proceedings kundër Bodil Lindqvist*, 2003 GJDBE, C-131/12, *Google Spain SL, Google Inc. k. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014	**Përkufizime**	Konventa 108 e Modernizuar, neni 2, shkronja b dhe c
Përdoruesit e të dhënave		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 4, pika 7 GJDBE, C-212/13, *František Ryneš k. Úřad pro ochranu osobních údajů*, 2014 GJDBE, C-1318/12, *Google Spain SL, Google Inc. k. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014	**Kontrolluesi**	Konventa 108 e Modernizuar, neni 2, gërma (d) Rekomandimi për Profilizimin, neni 1, gërma (g)*
Rregullorja e Përgjithshme e Mbrojtjes së të dhënave, neni 4, pika 8	**Përpunuesi**	Konventa 108 e Modernizuar, neni 2, gërma (f) Rekomandimi për Profilizimin, neni 1, gërma (h)

Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 4, pika 9	**Marrësi**	Konventa 108 e Modernizuar, neni 2, gërma (e)
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 4, pika 10	**Pala e tretë**	
Pëlqimi		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 4, pika 11 dhe 7 GJDBE, C-543/09, *Deutsche Telekom AG k. Bundesrepublik Deutschland*, 2011 GJDBE, C-536/15, *Tele2 (Netherlands) BV dhe të Tjerët k. Autoriteit Consument en Markt (AMC)*, 2017	**Përkufizime dhe kritere për pëlqim të vlefshëm**	Konventa 108 e Modernizuar, neni 5, pika 2 Rekomandimi për të Dhënat Mjekësore, neni 6 dhe rekomandime të ndryshme të mëvonshme GJEDNJ, *Elberte k. Letonisë*, nr. 61243/08, 2015

2.1. Të dhënat personale

Pikat kryesore

- Të dhënat janë të dhëna personale kur kanë lidhje me një person të identifikuar ose të identifikueshëm, me "subjektin e të dhënave".
- Për të përcaktuar nëse një person fizik është i identifikueshëm, si kontrolluesi ashtu edhe çdo person tjetër, duhet të parashikojnë të gjitha mjetet e arsyeshme që kanë të ngjarë të përdoren – sikurse veçimin – për të identifikuar drejtpërdrejtë ose tërthorazi personin fizik.
- Autentifikim nënkupton të vërtetuarit nëse një person i caktuar ka një identitet të caktuar dhe/ose është i autorizuar për të kryer veprime të caktuara.
- Në Konventën 108 të Modernizuar dhe në legjislacionin e BE-së për mbrojtjen e të dhënave janë përcaktuar disa kategori të veçanta të dhënash, të ashtuquajturat të dhëna sensitive, për të cilat nevojitet mbrojtje më e madhe dhe për pasojë i nënshtrohen një regjimi të veçantë ligjor.
- Të dhënat janë të anonimizuara nëse nuk lidhen më me një person të identifikuar ose të identifikueshëm.
- Pseudonimizimi është një masë me anë të së cilës të dhënat personale nuk mund t'i atribuohen një subjekti të dhënash pa informacion shtesë, i cili mbahet veçmas. "Çelësi" i cili mundëson ri-identifikimin e subjekteve të të dhënave duhet mbajtur veçmas dhe nën masa sigurie. Të dhënat që u janë nënshtruar procesit të pseudonimizimit, mbeten

të dhëna personale. Në të drejtën e BE-së nuk ekziston koncepti i "të dhënave të pseudonimizuara".
- Parimet dhe rregullat e mbrojtjes së të dhënave nuk gjejnë zbatim për informacionin e anonimizuar. Sidoqoftë, ato gjejnë zbatim për të dhënat e pseudonimizuara.

*Shënim: *Këshilli i Evropës, Komiteti i Ministrave (2010), Rekomandimi Rec(2010)13 i Komitetit të Ministrave drejtuar shteteve anëtare në lidhje me mbrojtjen e personave nga përpunimi automatik i të dhënave personale në kuadër të profilizimit* (Rekomandimi për Profilizimin)*, 23 nëntor 2010.*

2.1.1. Aspektet kryesore të konceptit të të dhënave personale

Tek e **drejta e BE-së** dhe tek e **drejta e KiE-së**, "të dhënat personale" përkufizohen si çdo informacion në lidhje me një person fizik, të identifikuar ose të identifikueshëm,[136] domethënë informacioni në lidhje me një person, identiteti i së cilit është ose haptazi i qartë, ose mund të përcaktohet nëpërmjet informacionit shtesë. Për të përcaktuar nëse një person është i identifikueshëm, kontrolluesi ose një person tjetër duhet të parashikojë të gjitha mjetet e arsyeshme që ka të ngjarë të përdoren drejtpërdrejtë ose tërthorazi për të identifikuar një person, si për shembull, veçimi, i cili bën të mundur që të trajtohet një person ndryshe nga një tjetër.[137]

Nëse të dhënat në lidhje me këtë person përpunohen, ky person emërtohet "subjekt i të dhënave".

Subjekti i të dhënave

Referuar së drejtës së BE-së, personat fizikë janë të vetmet subjekte përfituese nga rregullat e mbrojtjes së të dhënave[138] dhe vetëm personat që jetojnë mbrohen nga legjislacioni evropian i mbrojtjes së të dhënave.[139] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave (GDPR) i përkufizon të dhënat personale si çdo informacion në lidhje me një person fizik të identifikuar ose të identifikueshëm.

E drejta e KiE-së, veçanërisht Konventa 108 e Modernizuar, i referohet gjithashtu mbrojtjes së personave për sa i përket përpunimit të të dhënave të tyre personale. Edhe këtu, të dhënat personale janë çdo informacion në lidhje me një person të identifikuar ose të identifikueshëm.

[136] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 4, pika 1; Konventa 108 e Modernizuar, neni 2, shkronja (a).
[137] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 26 i preambulës.
[138] *Ibid.,* neni 1.
[139] *Ibid.,* paragrafi 27 i preambulës. Shih gjithashtu Grupi i Punës së Nenit 29 (2007), *Opinion 4/2007 on the concept of personal data,* WP 136, 20 qershor 2007, fq. 22.

Ky person fizik, apo individ, sikurse i referohet respektivisht GDPR-ja dhe Konventa 108 e Modernizuar, njihet në legjislacionin e mbrojtjes së të dhënave si subjekt i të dhënave.

Personat juridikë gëzojnë gjithashtu një nivel mbrojtjeje. Jurisprudenca e GJEDNJ-së përfshin gjykime të ankesave nga persona juridikë, për shkelje të pretenduara të së drejtës për mbrojtje nga përdorimi i të dhënave të tyre mbështetur në nenin 8 të KEDNJ-së. Neni 8 i KEDNJ-së mbulon si të drejtën për respektim të jetës private dhe familjare, ashtu edhe të drejtën e banesës e korrespondencës. Rrjedhimisht, Gjykata mund të marrë në shqyrtim çështje referuar kësaj të fundit dhe jo të drejtës për respektim të jetës private.

Shembull: çështja *Bernh Larsen Holding AS dhe të Tjerët k. Norvegjisë*[140] kishte të bënte me ankesën e tre shoqërive norvegjeze në lidhje me vendimin e një autoriteti tatimor, që i urdhëronte t'u vinin në dispozicion inspektorëve tatimorë një kopje të të gjitha të dhënave të një serveri që ata e përdornin bashkërisht.

GJEDNJ-ja vlerësoi se një detyrim i tillë mbi shoqëritë kërkuese, përbënte ndërhyrje tek e drejta e tyre për respektim të "banesës" dhe "korrespondencës" sipas nenit 8 të KEDNJ-së. Gjithsesi, Gjykata vlerësoi se autoritetet tatimore kishin marrë masat e duhura të sigurisë ndaj abuzimit: shoqëritë kërkuese ishin njoftuar paraprakisht

Amann kundër Zvicrës,[50] autoritetet kishin përgjuar një telefonatë pune të kërkuesit. Bazuar në atë telefonatë, autoritetet hetuan kërkuesin dhe plotësuan një formular në lidhje me të, me qëllim skedimin e tij për arsye të sigurisë kombëtare. Edhe pse përgjimi kishte të bënte me një telefonatë pune, GJEDNJ-ja vlerësoi se ruajta e të dhënave në lidhje me atë telefonatë, cenonte jetën private të kërkuesit. Ajo theksoi se termi "jetë private" nuk duhet të interpretohet në mënyrë të kufizuar, veçanërisht duke qenë se respektimi i jetës private përfshin edhe të drejtën për të ndërtuar e zhvilluar marrëdhënie me njerëz të tjerë. Për më tepër, nuk ekzistonte asnjë arsye parimore që të justifikonte përjashtimin e aktiviteteve të natyrës profesionale apo komerciale nga nocioni i "jetës private". Ky interpretim i gjerë përkonte me atë të Konventës 108. GJEDNJ-ja konstatoi më tej se ndërhyrja në rastin e kërkuesit, nuk kishte qenë në përputhje me ligjin, duke qenë se ligji kombëtar nuk përmbante dispozita specifike dhe të hollësishme në lidhje me mbledhjen, regjistrimin dhe ruajtjen e informacionit. Kështu, Gjykata vendosi se ishte shkelur neni 8 i KEDNJ-së.

Sipas Konventës 108 të Modernizuar, mbrojtja e të dhënave trajton kryesisht mbrojtjen e të dhënave të personave fizikë; gjithsesi, Palët Kontraktuese mund të shtrijnë mbrojtjen e të dhënave në legjislacionin e brendshëm edhe tek personat juridikë, si për shembull bizneset dhe shoqatat. Në Relacionin Shpjegues të Konventës së Modernizuar thuhet se legjislacioni kombëtar mund të mbrojë interesat legjitimë të personave juridikë nëpërmjet shtrirjes së fushës së zbatimit të konventës edhe tek këta aktorë.[141] **E drejta e BE-së në fushën e mbrojtjes së të dhënave** nuk mbulon përpunimin e të dhënave në lidhje me personat juridikë dhe veçanërisht

[140] GJEDNJ, *Bernh Larsen Holding AS dhe të Tjerët k. Norvegjisë*, nr. 24117/08, 14 mars 2013. Shih gjithashtu, GJEDNJ, *Liberty dhe të Tjerët k. Mbretërisë së Bashkuar*, nr. 58243/00, 1 korrik 2008.
[141] Relacioni Shpjegues i Konventës 108 të Modernizuar, parag. 30.

sipërmarrjet e krijuara si persona juridikë, përfshirë emrin dhe formën e personit juridik dhe të dhënat e kontaktit të tij.[142] Përkundrazi, Direktiva e Privatësisë Elektronike mbron konfidencialitetin e komunikimeve dhe interesave legjitimë të personave jurikë për sa i përket kapacitetit arkivues dhe përpunues të dhënash në rritje në lidhje me abonentët dhe përdoruesit.[143] Në të njëjtën mënyrë, edhe projekt-Rregullorja e Privatësisë Elektronike shtrin mbrojtjen tek personat juridikë.

Shembull: tek çështja *Volker und Markus Schecke dhe Hartmut Eifert k. Land Hessen-it,*[144] GJDBE-ja, duke iu referuar publikimit të të dhënave personale që kishin të bënin me përfituesit e ndihmës bujqësore, deklaroi se "personat juridikë, për sa i përket këtij lloj identifikimi, mund të kërkojnë mbrojtjen e neneve 7 dhe 8 të Kartës, por vetëm për aq kohë sa emërtimi ligjor i personit juridik identifikon një apo më shumë persona fizikë. [...E] drejta për respektim të jetës private për sa i takon përpunimit të të dhënave personale, e njohur nga nenet 7 dhe 8 të Kartës, ka të bëjë me çdo informacion që lidhet me një individ të identifikuar apo të identifikueshëm [...]".[145]

Duke vendosur në peshore interesin e BE-së për të garantuar transparencë në alokimin e ndihmës nga njëra anë dhe të drejtat themelore për privatësi dhe mbrojtje të të dhënave të individëve që kishin përfituar ndihmën nga ana tjetër, GJDBE-ja vlerësoi se ndërhyrja tek këto të drejta themelore ishte jo proporcionale. Ajo çmoi se objektivi i transparencës mund të ishte përmbushur me efektshmëri me mënyra të tjera më pak cenuese të së drejtave të individëve të përfshirë. Gjithsesi, kur shqyrtoi proporcionalitetin e publikimit të informacionit në lidhje me personat juridikë që kishin përfituar ndihmën, GJDBE-ja arrit një përfundim të ndryshëm, teksa vendosi se publikimi nuk kalonte kufijtë e parimit të proporcionalitetit. Ajo theksoi se "niveli shkeljes së të drejtës për mbrojtje të të dhënave personale e shfaq veten në mënyra të ndryshme për personat juridik nga njëra anë dhe për personat fizikë nga ana tjetër".[146] Personat juridikë i nënshtroheshin detyrimeve më të rënda për sa i përket publikimit të informacionit në lidhje me ta. GJDBE-ja theksoi se nëse do t'u kërkohej autoriteteve kombëtare të shqyrtonin përpara publikimit të të dhënave nëse të dhënat e çdo personi juridik përfitues identifikojnë persona fizikë që kanë lidhje me ta, kjo do të krijonte një ngarkesë administrative të paarsyeshme për ato autoritete. Për rrjedhojë, duke përcaktuar që publikimi i të dhënave në lidhje me personat juridikë duhet të bëhej në mënyrë të përgjithshme, legjislacioni i kishte ekuilibruar drejt interesat e ndryshme të përfshira.

Karakteri i të dhënave

[142] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 14 i preambulës.
[143] Direktiva e-Privatësia, paragrafi 7 dhe neni 1, pika 2.
[144] GJDBE, Çështje të bashkuara C-92/09 dhe C-93/09, *Volker und Markus Schecke GbR dhe Hartmut Eifert k. Land Hessen-it* [ÇB] , 9 nëntor 2010, parag. 53.
[145] *Ibid.,* parag. 52-53.
[146] *Ibid.,* parag. 87.

Çdo lloj informacioni mund të jetë e dhënë personale, me kusht që të lidhet me një person të identifikuar ose të identifikueshëm.

Shembull: vlerësimi i punës së një nëpunësi nga ana e eprorit të tij, i cili ruhet në dosjen personale të nëpunësit, është e dhënë personale në lidhje me nëpunësin, edhe pse ajo mund të pasqyrojë pjesërisht apo plotësisht mendimin personal të eprorit, si për shembull: "nëpunësi nuk punon me përkushtim" dhe jo fakte sikurse: "nëpunësi ka munguar në punë për pesë javë gjatë gjashtë muajve të fundit".

Të dhënat personale përfshijë informacione që i përkasin jetës private të një personi, që përfshin gjithashtu edhe aktivitetet profesionale, ashtu si edhe informacione në lidhje me jetën publike të tij apo të saj.

Tek çështja *Amann,*[147] GJEDNJ-ja e interpretoi termin "të dhëna personale" si jo të kufizuar tek çështje të sferës private të individit. Kjo domethënie e termit "të dhëna personale" është i vlefshëm edhe për GDPR-në.

Shembull: tek çështja *Volker und Markus Schecke dhe Hartmut Eifert kundër Land Hessen-it,*[148] GJDBE-ja theksoi se "sa i përket kësaj, nuk asnjë rëndësi nëse të dhënat e publikuara kanë të bëjnë me aktivitete të karakterit profesional [...]. Gjykata Evropiane e të Drejtave të Njeriut është shprehur në lidhje me këtë pikë, duke iu referuar interpretimit të nenit 8 të Konventës 108, se termi "jetë private" nuk duhet interpretuar në mënyrë të kufizuar dhe se nuk asnjë arsye parimore për të justifikuar përjashtimin e aktiviteteve me karakter [...] profesional nga nocioni i jetës private".

Shembull: tek çështjet e bashkuar *YS k. Minister voor Immigratie, Integratie en Asiel* dhe *Minister voor Immigratie, Integratie en Asiel k. M dhe S,*[149] GJDBE-ja përcaktoi se analiza ligjore që përmbante një projekt-vendim i Shërbimit të Emigracionit dhe Natyralizimit, i cili trajtonte aplikimet për leje qëndrimi, nuk përbënte në vetvete të dhënë personale, edhe pse mund të përmbante disa të dhëna personale.

Jurisprudenca e GJEDNJ-së që ka të bëjë me nenin 8 të KEDNJ-së vërteton se mund të jetë e vështirë të ndahen krejtësisht çështjet e jetës private nga ato profesionale.[150]

Shembull: tek *Bărbulescu k. Rumanisë*,[151] kërkuesi ishte larguar nga puna për shkak se kishte përdorur internetin e punëdhënësit gjatë orarit të punës në shkelje të rregullores së brendshme. Punëdhënësi kishte monitoruar komunikimet dhe të dhënat e regjistruara, të cilat paraqisnin mesazhe me karakter krejtësisht privat, ishin përdorur gjatë procedimit brenda vendit. Teksa vlerësoi se neni 8 gjente zbatim, GJEDNJ-ja e la të hapur çështjen nëse rregullorja kufizuese e punëdhënësit i linte ndonjë pritshmëri të arsyeshme kërkuesit në lidhje me privatësinë, por sidoqoftë ajo doli në përfundimin se rregullat e caktuara nga

[147] Shih GJEDNJ, *Amann k. Zvicrës,* nr. 27798/95, 16 shkurt 2000, parag. 65.
[148] GJDBE, Çështje të bashkuara C-92/09 dhe C-93/09, *Volker und Markus Schecke GbR dhe Hartmut Eifert k. Land Hessen-it* [ÇB] , 9 nëntor 2010, parag. 59.
[149] GJDBE, Çështje të bashkuara C-141/12 dhe C-372/12, *YS k.Minister voor Immigratie, Integratie en Asiel* dhe *Minister voor Immigratie, Integratie en Asiel k. M dhe S,* 17 korrik 2014, parag. 39.
[150] Shih për shembull, GJEDNJ, *Rotaru k. Rumanisë* [ÇB] , nr 28341/95, 4 maj 2000, parag. 43; GJEDNJ, *Niemietz k. Gjermanisë*, nr. 13710/88, 16 dhjetor 1992, parag. 29.
[151] GJEDNJ, *Bărbulescu k. Rumanisë* [ÇB] , nr. 61496/08, 5 shtator 2017, parag. 121.

punëdhënësi nuk mund ta reduktojnë në zero jetën private shoqërore në vendin e punës. Për sa i përket themelit të çështjes, Palëve Kontraktuese u duhej lënë një fushë veprimi e gjerë për të vlerësuar domosdoshmërinë e miratimit të një kuadri ligjor, i cili përcakton kushtet sipas të cilave një punëdhënës mund të rregullojë komunikimet që s'kanë lidhje me punën të punëmarrësve të tij – qofshin elektronike apo të formave të tjera – në vendin e punës. Pavarësisht kësaj, autoritetet vendase duhet të garantonin që masat e marra nga një punëdhënës, për monitorimin e korrespondencës dhe komunikimeve të tjera, pavarësisht shtrirjes dhe kohëzgjatjes së këtyre masave, të shoqëroheshin me masa sigurie të përshtatshme dhe të mjaftueshme për mbrojtje nga abuzimi. Proporcionaliteti dhe garancitë procedurale kundër arbitraritetit janë thelbësore dhe GJEDNJ-ja identifikoi një numër faktorësh që ishin të rëndësishëm në ato rrethana. Në këto faktorë hynin për shembull shtrirja e monitorimit të punëmarrësve nga ana e punëdhënësit dhe shkalla e ndërhyrjes tek privatësia e punëmarrësit, pasojat për punëmarrësit dhe nëse ishin marrë masat e duhura të sigurisë. Gjithashtu, autoritetet vendase duhet të garantonin që një punëmarrës, komunikimet e së cilit ishin monitoruar, të kishte mundësi t'i drejtohej një organi gjyqësor, i cili të kishte juridiksionin për të përcaktuar, së paku në thelb, se si ishin respektuar kriteret e përshkruara dhe nëse masat e kundërshtuara ishin të ligjshme. Në këtë rast, GJEDNJ-ja gjeti shkelje të nenit 8, për shkak se autoritetet vendase nuk kishin siguruar mbrojtje të përshtatshme të së drejtës së kërkuesit për respektim të jetës private dhe korrespondencës dhe për rrjedhojë nuk kishin vendosur një ekuilibër të drejtë midis interesave të përfshira.

Sipas **së drejtës së BE-së**, ashtu si edhe sipas **të drejtës së KiE-së**, informacioni përmban të dhëna në lidhje me një person nëse:

- Individi identifikohet, ose është i identifikueshëm nëpërmjet këtij informacioni; ose
- Individi, megjithëse i paidentifikuar, mund të veçohet me anë të këtij informacioni, në mënyrë të tillë që e bën të mundur të zbulohet kush është subjekti i të dhënave nëpërmjet kërkimit të mëtejshëm.

Të dyja llojet e informacionit mbrohen në të njëjtën mënyrë nga legjislacioni evropian i mbrojtjes së të dhënave. Identifikueshmëria e drejtpërdrejtë, ose e tërthortë e individëve kërkon analizim të vazhdueshëm, "duke marrë parasysh teknologjinë e disponueshme në kohën e kryerjes së përpunimit, ose zhvillimet teknologjike".[152] GJEDNJ ka përcaktuar në mënyrë të përsëritur se nocioni i "të dhënave personale" tek KEDNJ-ja, është i njëjtë me atë tek Konventa 108, sidomos për sa i përket kushtit të lidhjes me persona të identifikuar ose të identifikueshëm.[153]

GDPR-ja përcakton se personi fizik është i identifikueshëm kur ai, ose ajo "mund të identifikohet, drejtpërdrejtë ose tërthorazi, në mënyrë të veçantë duke iu referuar një identifikuesi, sikurse emrit, një numri identifikimi, të dhënave të vendndodhjes, identifikuesit në internet, ose një apo më shume faktorëve të cilët janë specifikë për identitetin fizik, psikologjik, gjenetik, mendor, ekonomik, kulturor, ose shoqëror të atij personi".[154] Kështu, për identifikimin lipsen elemente të cilat përshkruajnë personin, në mënyrë të tillë që e bëjnë atë të dallueshëm nga persona të tjerë dhe që mund të njihet si individ. Emri i personit është shembulli

[152] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 26 i preambulës.
[153] Shih GJEDNJ, *Amann k. Zvicrës* [ÇB] , nr 27798/95, 16 shkurt 2000, parag. 65.
[154] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 4, pika 1.

i dorës së parë për sa i përket këtyre elementeve përshkrues dhe mund të identifikojë drejtpërdrejtë personin. Në disa raste, edhe cilësi të tjera mund të kenë efekt të ngjashëm me atë të emrit, duke e bërë personin të identifikueshëm tërthorazi. Numri i telefonit, numri i sigurimeve shoqërore dhe targa e automjetit janë të gjitha shembuj informacioni që e bën individin të identifikueshëm. Është gjithashtu e mundshme të përdoren atribute – si për shembull skedarë kompjuterikë, *cookies* dhe mjete të monitorimit të trafikut në internet – për të veçuar individë, nëpërmjet identifikimit të sjelljes dhe zakoneve të tyre. Sikurse shpjegohet në një opinion të Grupit të Punës së Nenit 29, "madje edhe pa kërkuar emrin dhe adresën e individit, është e mundur të kategorizohet personi, bazuar në kritere shoqërore-ekonomike, psikologjike, filozofike ose të tjera dhe t'i atribuohen atij, apo asaj disa vendime, meqenëse pika e kontaktit të individit (kompjuteri) nuk kërkon më zbulimin e identitetit të tij, apo të saj në kuptimin e ngushtë të tij".[155] Përkufizimi i të dhënave personale sipas KiE-së ashtu edhe sipas BE-së është mjaftueshëm i gjerë për të përfshirë të gjitha mundësitë e identifikimit (dhe, për rrjedhojë, të gjitha nivelet e identifikueshmërisë).

Shembull: tek çështja *Promusicae k. Telefónica de España*,[156] GJDBE-ja deklaroi se "nuk vihet në kundërshtim se komunikimi i kërkuar nga ana e Promusicae-s i emrave dhe adresave të disa përdoruesve të [një platforme të caktuar shkëmbimit skedarësh në internet] përfshin vënien në dispozicion të të dhënave personale, të cilat janë informacione në lidhje me persona fizikë të identifikuar, ose të identifikueshëm, sipas përkufizimit në nenin 2, gërma (a) e Direktivës 95/46 [aktualisht neni 4, pika 1 e GDPR-së]. Ai komunikim informacioni, i cili, sikurse pretendon Promusicare dhe nuk kundërshtohet nga Telefónica, mbahet nga Telefónica, përbën përpunim të dhënash personale".[157]

Shembull: çështja *Scarlet Extended SA k. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [158] kishte të bënte me refuzimin nga ana e Scarlet-it, një operatori shërbimesh interneti, për të instaluar një sistem filtrimi të komunikimeve elektronike, që përdorin program informatik shkëmbimi skedarësh, për të penguar shkëmbimin e skedarëve që shkelin të drejtat e autorit të mbrojtura nga SABAM-i, një shoqëri menaxhimi që përfaqësonte autorë, kompozitorë dhe producentë. GJDBE-ja deklaroi se adresat IP të përdoruesve "janë të dhëna personale të mbrojtura, për shkak se ato mundësojnë identifikim të saktë të atyre përdoruesve".

Duke qenë se shumë emra nuk janë unikë, mund të nevojiten cilësi shtesë për të përcaktuar identitetin e një personit, për të garantuar që ai person nuk ngatërrohet me dikë tjetër. Ndonjëherë, cilësitë e drejtpërdrejta, ose të tërthorta, mund të duhet të kombinohen, për të identifikuar individin me të cilin lidhet informacioni. Shpesh përdoren data dhe vendi i lindjes. Gjithashtu, në shumë shtete përdoren numrat e personalizuar, për të veçuar më mirë qytetarët. Të dhënat tatimore të transferuara,[159] të dhënat që i përkasin një aplikuesi për leje qëndrimi në një dokument administrativ[160] dhe dokumentet që kanë të bëjnë me marrëdhëniet bankare dhe

[155] Grupi i Punës së Nenit 29, *Opinioni 4/2007 mbi konceptin e të dhënave personale*, WP 136, 20 qershor 2007, fq. 15.
[156] GJDBE, C-275/06, *Productores de Música de España (Promusicae) k. Telefónica de España SAU* [ÇB] , 29 janar 2008, parag. 45.
[157] Direktiva e shfuqizuar 95/46, neni 2, gërma (b), tashmë Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 4, pika 2.
[158] GJDBE, C-70/10, *Scarlet Extended SA k. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 nëntor 2011, parag. 51.
[159] GJDBE,C-201/14, *Smaranda Bara dhe të Tjerët k. Casa Naţională de Asigurări de Sănătate dhe të Tjerët*, 1 tetor 2015.
[160] GJDBE, *YS k. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel k. M and S*, 17 korrik 2014.

ato të besimit[161] mund të jenë të dhëna personale. Të dhënat biometrike, sikurse gjurmët e gishtave, fotografitë digjitale, ose skanimet e irisit, të dhënat e vendndodhjes dhe atributet në internet, përdoren gjithnjë e më shumë për të identifikuar personat në epokën digjitale.

Gjithsesi, që të zbatohet legjislacioni evropian i mbrojtjes së të dhënave, nuk ka nevojë të kryhet identifikimi i subjektit të të dhënave; mjafton që personi i përfshirë të jetë i identifikueshëm. Personi konsiderohet i identifikueshëm nëse ekzistojnë elemente të mjaftueshme në dispozicion, me anë të së cilëve personi të mund të identifikohet drejtpërdrejtë ose tërthorazi.[162] Sipas Paragrafit 26 të Preambulës së GDPR-së, standardi qëndron tek mundësia e përdorimit të mjeteve të arsyeshme për identifikimin, të cilat të jenë në dispozicion dhe të administrohen nga përdoruesit e parashikueshëm të informacionit; këtu përfshihet edhe informacioni që mbahet nga subjektet e treta përfituese (shih Seksionin 2.3.2).

Shembull: Një autoritet lokal vendos të mbledhë të dhëna në lidhje me automjetet që qarkullojnë tej normave të lejuara të shpejtësisë në rrugët lokale. Ai kryen fotografimin e automjeteve, regjistron automatikisht kohën dhe vendndodhjen, me qëllim që t'ia kalojë të dhënat autoritetit kompetent, në mënyrë që ky i fundit të gjobisë ata që kanë shkelur kufizimet e shpejtësisë. Një subjekt të dhënash paraqet një ankesë, në të cilën pretendon se sipas legjislacionit të mbrojtjes së të dhënave, autoriteti lokal nuk ka asnjë bazë ligjore për këtë mbledhje të dhënash. Autoriteti lokal këmbëngul se të dhënat që ai mbledh, nuk janë të dhëna personale. Targat e automjete, thekson ai, janë anonime. Autoriteti lokal nuk zotëron autoritet ligjor për akses në regjistrin e përgjithshëm të automjeteve, për të gjetur identitetin e poseduesve të automjeteve, apo shoferëve.

Ky arsyetim nuk është në përputhje me Paragrafin 25 të GDPR-së. Duke qenë se qëllimi i mbledhjes së të dhënave është qartësisht identifikimi dhe gjobitja e shkelësve të normave të shpejtësisë, është e parashikueshme se do të bëhen përpjekje për identifikim. Megjithëse autoriteti lokal nuk zotëron drejtpërdrejtë mjetet e identifikimit, ai do t'ia përcjellë të dhënat autoritetit kompetent, policisë, e cila i zotëron këto mjete. Paragrafi 26 përfshin gjithashtu në mënyrë të qartë rastin kur është e parashikueshme që subjekte të tjera përfituese, përveç përdoruesit të drejtpërdrejtë të të dhënave, të përpiqen të identifikojnë individin. Referuar Paragrafit 26, veprimi i autoritetit lokal është i barasvlershëm me mbledhjen e të dhënave në lidhje me personat e identifikueshëm dhe për rrjedhojë kërkon bazë ligjore sipas legjislacionit të mbrojtjes së të dhënave.

Për të "krijuar bindjen se ka mundësi të arsyeshme që do të përdoren mjete për të identifikuar personin fizik, duhen marrë parasysh të gjithë faktorët objektivë, sikurse kostoja dhe koha që nevojitet për kryerjen e identifikimit, duke marrë në konsideratë teknologjinë e disponueshme në periudhën e përpunimit dhe zhvillimet teknologjike."[163]

Shembull: tek çështja *Breyer k. Bundesrepublik Deutschland,*[164] GJDBE-ja shqyrtoi nocionin e identifikueshmërisë së tërthortë të subjekteve të të dhënave. Çështja trajtonte adresat IP dinamike, të cilat ndryshojnë sa herë që bëhet një lidhje e re në internet. Faqet e internetit në përdorim nga institucionet federale gjermane regjistronin dhe ruanin adresat IP

[161] GJEDNJ, *M.N. dhe të Tjerët k. San Marinos*, nr. 28005/12, 7 korrik 2015.
[162] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 4, pika 1.
[163] *Ibid.,* Paragrafi 26.
[164] GJDBE, C-582/14, *Patrick Breyer k. Bundesrepublik Deutschland*, 19 tetor 2016, parag. 43.

dinamike, me qëllim parandalimin e sulmeve kibernetike dhe për të nisur procedime penale kur ishte e nevojshme. Vetëm operatori i shërbimit të internetit që përdorte z. Breyer e zotëronte informacionin shtesë që nevojitej për ta identifikuar atë.

GJDBE-ja gjykoi se adresa IP dinamike, të cilën e regjistron një operator i shërbimeve të medias në internet kur një person hyn në faqen në internet, të cilën operatori e ka bërë të aksesueshme për publikun, është e dhënë personale, ku vetëm një palë e tretë – në këtë rast operatori i shërbimit të internetit – zotëron të dhënat shtesë që janë të nevojshme për të identifikuar një person.[165] Ajo u shpreh se "nuk është e nevojshme që i gjithë informacioni që mundëson identifikimin e subjektit të të dhënave të jetë në duart e një personi të vetëm" që informacioni të jetë e dhënë personale. Përdoruesit e adresave IP dinamike të regjistruara nga një operator shërbimi interneti mund të identifikohen në situata të caktuara, për shembull në kuadër të procedimeve penale në rastin e një sulmi kibernetik, me ndihmën e personave të tjerë.[166] Sipas GJDBE-së, kur operatori "disponon mjetet ligjore që i japin mundësinë të identifikojnë subjektin e të dhënave me anë të dhënash shtesë të cilat operatori i internetit i zotëron në lidhje me atë person", kjo përbën "mjet që ka të ngjarë të shfrytëzohet për identifikuar subjektin e të dhënave." Rrjedhimisht, këto të dhëna konsiderohen të dhëna personale.

Sipas së drejtës së KiE-së, identifikueshmëria kuptohet në mënyra të ndryshme. Relacioni Shpjegues i Konventës 108 të Modernizuar përmban një përshkrim të ngjashëm: nocioni "i identifikueshëm" nuk i referohet vetëm identitetit civil apo ligjor si të tillë të individit, por edhe asaj që mundëson që një person të "individualizohet" ose të veçohet nga të tjerët dhe si pasojë të mund të trajtohet në mënyrë të ndryshme. Ky "individualizim" mund të bëhet, për shembull, duke iu referuar atij apo asaj në mënyrë specifike, ose një pajisjeje ose kombinimi pajisjesh (kompjuter, telefoni celular, kamera, pajisjeve të lojërave, etj.) që lidhen me një numër identifikimi, një pseudonim, me të dhëna biometrike ose gjenetike, me të dhëna të vendndodhjes, me adresën IP, ose me një identifikues tjetër.[167] Individi nuk konsiderohet "i identifikueshëm" nëse identifikimi i tij apo i saj kërkon kohë, përpjekje ose burime të paarsyeshme. Një rast i tillë mund të jetë për shembull kur për të identifikuar një subjekt të dhënash do të nevojiteshin operacione tepër të ndërlikuara, të gjata dhe të kushtueshme. Nëse koha, përpjekjet dhe burimet janë të paarsyeshme, diçka e tillë duhet analizuar rast pas rasti, duke marrë parasysh faktorë të tillë si qëllimi i përpunimit, kostoja dhe përfitimet nga identifikimi, lloji i kontrolluesit dhe teknologjia e përdorur.[168]

Për sa i përket formës në të cilën mbahen ose përdoren të dhënat personale, është e rëndësishme të theksohet se nuk kjo është e rëndësishme për sa i takon zbatueshmërisë së legjislacionit të mbrojtjes së të dhënave. Komunikimet me shkrim ose ato verbale mund të përmbajnë të dhëna

[165] Direktiva e shfuqizuar 95/46/EC e Parlamentit Evropian dhe e Këshillit e 24 tetorit 1995 mbi mbrojtjen e personave nga përpunimi i të dhënave personale dhe mbi lëvizjen e lirë të këtyre të dhënave, neni 2, shkronja (a).
[166] GJDBE, C-70/10, *Scarlet Extended SA k. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM),* 24 nëntor 2011, parag. 47–48.
[167] Relacioni Shpjegues i Konventës 108 të Modernizuar, parag. 18.
[168] *Ibid.,* parag. 17.

personale ashtu si edhe imazhet,[169] përfshirë videot[170] dhe audiot[171] e televizionit me qark të shkurtër (CCTV). Informacioni i regjistruar elektronikisht dhe informacioni në letër mund të jenë gjithashtu të dhëna personale. Edhe mostrat qelizore të indeve njerëzore – të cilat regjistrojnë ADN-në e personit – mund të jenë burimi nga ku mund të nxirren të dhëna biometrike,[172] me kusht që të dhënat të lidhen me karakteristikat e trashëguara ose të fituara të individit, të japin informacion unik mbi shëndetin ose fiziologjinë e tij dhe të përftohen si rezultat i analizës së mostrës biologjike të atij personi.[173]

Anonimizimi

Sipas parimit të kufizimit të mbajtjes së të dhënave që përcaktohet si në GDPR, ashtu edhe në Konventën 108 të Modernizuar (e trajtuar më në hollësi në Seksionin 3), të dhënat duhen mbajtur "në formë të tillë që lejon identifikimin e subjekteve të të dhënave për aq kohë sa është e nevojshme për qëllimet për të cilat janë përpunuar të dhënat personale".[174] Rrjedhimisht, nëse kontrolluesi dëshiron t'i mbajë të dhënat pasi ato nuk nevojiten më dhe nuk i shërbejnë më qëllimit të tyre fillestar, ato duhen fshirë ose anonimizuar.

Procesi i anonimizimit të të dhënave nënkupton që të gjithë elementet identifikuese janë eliminuar nga një grup të dhënash personale, në mënyrë të tillë që subjekti i të dhënave të mos jetë më i identifikueshëm.[175] Në Opinion e tij 05/2014, Grupi i Punës së Nenit 29 analizon efektshmërinë dhe kufizimet e teknikave të ndryshme të anonimizimit.[176] Ai pranon vlerën e mundshme të teknikave të tilla, por nënvizon se disa teknika nuk funksionojnë detyrimisht në të gjitha rastet. Për të gjetur zgjidhjen optimale në një situatë të caktuar, procesi i duhur i anonimizimit duhet të përcaktohet rast pas rasti. Pavarësisht teknikës së përdorur, duhet të parandalohet identifikimi, në mënyrë të pakthyeshme. Kjo do të thotë se, që të dhënat të jenë të anonimizuara, asnjë element, i cili duke bërë përpjekje të arsyeshme mund të shërbejë për ri-identifikimin e personit apo personave të përfshirë, nuk duhet lënë tek informacion.[177] Rreziku i ri-identifikimit mund të vlerësohet duke marrë në konsideratë "kohën, përpjekjet, apo burimet që nevojiten, referuar karakterit të të dhënave, kontekstit të përdorimit të tyre, teknologjitë e disponueshme për ri-identifikim dhe kostot përkatëse".[178]

Kur të dhënat janë anonimizuar me sukses, ato nuk janë më të dhëna personale dhe legjislacioni i mbrojtjes së të dhënave nuk gjen më zbatim.

---

[169] GJEDNJ, *Von Hannover k. Gjermanisë*, nr. 59320/00, 24 qershor 2004; GJEDNJ, *Sciacca k. Italisë*, nr. 50774/99, 11 janar 2005; GJDBE, C-212/13, *František Ryneš k. Úřad pro ochranu osobních údajů*, 11 dhjetor 2014.
[170] GJEDNJ, *Peck k. Mbretërisë së Bashkuar*, nr. 44647/98, 28 janar 2003; GJEDNJ, *Köpke k. Gjermanisë* (dec.), nr. 420/07, 5 tetor 2010; EDPS (2010), *The EDPS video-surveillance guidelines*, 17 mars 2010.
[171] GJEDNJ, *P.G. dhe J.H. k. Mbretërisë së Bashkuar*, nr. 44787/98, 25 shtator 2001, parag. 59–60; GJEDNJ, *Wisse k. Francës*, nr. 71611/01, 20 dhjetor 2005 (variant në gjuhën frënge).
[172] Shih Grupi i Punës së Nenit 29 (2007) *Opinion 4/2007 on the concept of personal data*, WP136, 20 qershor 2007, fq. 9; Këshilli i Evropës, Recommendation No. Rec (2006) 4 of the Committee of Ministers to member states on research on biological materials of human origin, 15 mars 2006.
[173] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, Paragrafi 26.
[174] *Ibid.,* neni 5, pika (1), shkronja (e); Konventa 108 e Modernizuar, neni 5, pika (4), gërma (e).
[175] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, Paragrafi 26.
[176] Grupi i Punës së Nenit 29 (2014), *Opinion 05/2014 on Anonymization Techniques*, WP216, 10 prill 2014.
[177] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, Paragrafi 26 i Preambulës.
[178] Këshilli i Evropës, Komiteti i Konventës 108 (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23 janar 2017, parag. 6.2.

GDPR-ja përcakton se personi ose organizata që kontrollon përpunimin e të dhënave personale, nuk mund të detyrohet të mbajë, të sigurojë, apo të përpunojë informacion shtesë për identifikimin e subjektit të të dhënave, për qëllimin e vetëm të zbatimit të legjislacionit. Megjithatë, nga ky rregull bëhet një përjashtimi rëndësishëm: kurdo që subjekti i të dhënave, për qëllime të ushtrimit të së drejtave për akses, korrigjim, fshirje, kufizim të përpunimit dhe transferueshmëri të të dhënave, i jep kontrolluesit informacion shtesë, i cili bën të mundur identifikimin e tij apo të saj, atëherë të dhënat që më parë ishin anonimizuar, bëhen sërish të dhëna personale.[179]

Pseudonimizimi

Informacioni personal përmban atribute sikurse emrin, datëlindjen, gjininë, adresën ose elemente të tjera të cilat bëjnë të mundur identifikimin. Procesi i pseudonimizimit të të dhënave personale nënkupton që këto atribute zëvendësohen me një pseudonim.

E drejta e BE-së e përkufizon "pseudonimizimin" si "përpunimin e të dhënave personale në mënyrë të tillë që të dhënat personale të mos i atribuohen më një subjekti të caktuar të të dhënave pa përdorur informacion shtesë, me kusht që ky informacion shtesë të mbahet veçmas dhe t'i nënshtrohet masave teknike dhe organizative për të garantuar që të dhënat personale të mos i atribuohen një personi fizik të identifikuar ose të identifikueshëm".[180] Ndryshe nga të dhënat e anonimizuara, të dhënat e pseudonimizuara mbeten të dhëna personale dhe për pasojë janë subjekt i legjislacionit të mbrojtjes së të dhënave. Megjithëse pseudonimizimi mund të zvogëlojë rreziqet për sigurinë e subjekteve të të dhënave, ai nuk përjashtohet nga objekti GDPR-së.

GDPR-ja njeh përdorime të ndryshme të pseudonimizimit, si një masë teknike e përshtatshme për rritjen e mbrojtjes së të dhënave dhe përmendet në mënyrë të veçantë për projektimin dhe sigurinë e përpunimit të të dhënave.[181] Ai përbën gjithashtu një masë të përshtatshme sigurie që mund të përdoret për të përpunuar të dhëna personale për qëllime të ndryshme nga ato për të cilat janë mbledhur të dhënat fillimisht.[182]

Pseudonimizimi nuk përmendet shprehimisht në përkufizimin ligjor të Konventës 108 të Modernizuar të **KiE**-së. Sidoqoftë, Relacioni Shpjegues i Konventës 108 të Modernizuar përcakton qartë se "përdorimi i një pseudonimi, ose i çdo lloj identifikuesi digjital/identiteti digjital, nuk çon në anonimizim të të dhënave, duke qenë se subjekti i të dhënave mbetet gjithsesi i identifikueshëm ose i individualizuar".[183] Një mënyrë për të pseudonimizuar të dhënat është nëpërmjet kodimit të të dhënave. Pasi të dhënat janë pseudonimizuar, lidhja me një identitet ekziston në formën e pseudonimit, plus një çelës kodimi. Pa një çelës të tillë, është e vështirë të identifikohen të dhënat e pseudonimizuara. Gjithsesi, për ata që janë të autorizuar të përdorin çelësin e kodimit, ri-identifikimi është i mundshëm pa vështirësi. Mbrojtje e veçantë i duhet kushtuar përdorimit të çelësit të kodimit nga persona të paautorizuar. Për pasojë, "të

[179] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 11.
[180] *Ibid.,* neni 4, pika 5.
[181] *Ibid.,* neni 25, pika 1.
[182] *Ibid.,* neni 6, pika 4.
[183] Relacioni Shpjegues i Konventës 108 të Modernizuar, parag. 18.

dhënat e [p]seudonimizuara duhen [...] konsideruar të dhëna personale [...]" që mbulohen nga Konventa 108 e Modernizuar.[184]

Legjitimimi

Kjo është një procedurë me anë të së cilës personi ka mundësi të vërtetojë se ai apo ajo zotëron një identitet të caktuar dhe/ose është i autorizuar të kryejë veprime të caktuara, sikurse të hyjë në një zonë sigurie, ose të tërheqë para' nga një llogari bankare. Legjitimimi mund të kryhet nëpërmjet krahasimit të të dhënave biometrike, si për shembull fotografisë, ose gjurmëve të gishtave në një pasaportë, me të dhënat e personit që paraqitet vetë, për shembull, në një kontroll kufitar;[185] ose duke kërkuar informacion, për të cilin duhet të jetë në dijeni vetëm personi që zotëron një identitet ose autorizim të caktuar, si për shembull një numër personal identifikimi (PIN) ose një fjalëkalim; ose duke kërkuar paraqitjen e një objekti të veçantë, i cili duhet të zotërohet vetëm nga një person me identitet apo autorizim të caktuar, si për shembull një kartë me çip special, ose një çelës kasaforte banke. Përveç fjalëkalimeve apo kartave me çip, të cilat herë-herë shoqërohen me kode PIN, nënshkrimet elektronike janë gjithashtu një instrument tepër i përshtatshëm për identifikimin dhe legjitimimin e personit në komunikimet elektronike.

2.1.2. Kategoritë e veçanta të të dhënave personale

Sipas së drejtës së BE-së ashtu edhe sipas **së drejtës së KiE-së**, ekzistojnë kategori të veçanta të dhënash personale, të cilat për shkak të natyrës së tyre, mund të përbëjnë rrezik për subjektet e të dhënave kur përpunohen dhe për to duhet mbrojtje më e madhe. Këto të dhëna i nënshtrohen parimit të ndalimit dhe ky lloj përpunimi është i ligjshëm vetëm me një numër të kufizuar kushtesh.

Në kuadrin e Konventës 108 të Modernizuar (neni 6) dhe të GDPR-së (neni 9), kategoritë e mëposhtme konsiderohen të dhëna sensitive:

- Të dhënat personale që zbulojnë origjinën racore apo etnike;
- Të dhënat personale që zbulojnë mendimet politike, besimet fetare ose të tjera, përfshirë edhe besimet filozofike;
- Të dhënat personale që zbulojnë anëtarësimin në sindikata;
- Të dhënat gjenetike dhe të dhënat biometrike të përpunuara për qëllime të identifikimit të personit;
- Të dhënat personale në lidhje me shëndetin, jetën seksuale apo orientimin seksual.

[184] *Ibid.*
[185] *Ibid.,* parag. 56-57.

Shembull: çështja *Bodil Lindqvist*[186] kishte të bënte me referimin që u bëhej personave të ndryshëm nëpërmjet emrit ose mënyrave të tjera, si për shembull numrit të telefonit ose informacionit në lidhje me hobin, në një faqe interneti. GJDBE-ja u shpreh se "referimi që i bëhet faktit se një individ ka plagosur këmbën dhe është me raport mjekësor, përbën të dhënë personale në lidhje me shëndetin".[187]

Të dhënat personale në lidhje me dënimet penale dhe veprat penale

Konventa 108 e Modernizuar i përfshin të dhënat personale në lidhje me veprat penale, procedimet penale dhe dënimet dhe masat e tjera të sigurisë në lidhje me to tek lista e kategorive të veçanta të të dhënave personale.[188] Në kuadrin e GDPR-së, të dhënat personale në lidhje me dënimet penale dhe veprat penale ose masat e tjera të sigurisë në lidhje me to, nuk përmenden si të tilla tek lista e kategorive të veçanta të të dhënave, por trajtohen në një nen të veçantë. Neni 10 i GDPR-së përcakton se përpunimi i këtyre të dhënave mund të bëhet vetëm "nën kontrollin e autoritetit zyrtar, ose kur përpunimi autorizohet nga legjislacioni i Bashkimit ose i Shteteve Anëtare, me kusht që të merren masat e përshtatshme për mbrojtjen e të drejtave dhe lirive të subjekteve të të dhënave". Nga ana tjetër, regjistrat e përgjithshëm që përmbajnë informacion mbi dënimet penale, mund të mbahen vetëm nën kontrollin e autoriteteve zyrtare të caktuara.[189] Në BE, përpunimi i të dhënave personale në kuadër të zbatimit të ligjit rregullohet me një instrument ligjor specifik, që është Direktiva 2016/680/BE.[190] Direktiva përcakton rregulla specifike për mbrojtjen e të dhënave, të cilat janë të detyrueshme për autoritetet kompetente kur përpunojnë të dhëna personale posaçërisht për parandalimin, hetimin, zbulimin dhe ndjekjen e veprave penale (shih Seksionin 8.2.1).

2.2 Përpunimi i të dhënave

Pikat kryesore

- "Përpunimi i të dhënave" ka të bëjë me çdo veprim që kryhet mbi të dhënat personale.
- Termi "përpunim" përfshin përpunimin automatik dhe jo automatik.
- Sipas së drejtës së BE-së, "përpunimi" i referohet gjithashtu edhe përpunimit manual në sisteme të strukturuara arkivimi.
- Sipas së drejtës së KiE-së, kuptimi i termit "përpunim" mund të zgjerohet nga legjislacioni kombëtar, për të përfshirë në të edhe përpunimin manual.

[186] GJDBE, C-101/01, *Criminal proceedings against Bodil Lindqvist*, 6 nëntor 2003, parag. 51.
[187] Direktiva e shfuqizuar 95/46/EC, neni 8, pika 1, tani Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 9, pika 1.
[188] Konventa 108 e Modernizuar, neni 6, pika1.
[189] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 10.
[190] Direktiva (BE) 2016/680 e Parlamentit Evropian dhe e Këshillit e 27 prillit 2016 mbi mbrojtjen e personave fizikë nga përpunimi i të dhënave personale nga autoritetet kompetente për qëllime të parandalimit, hetimit, zbulimit ose ndjekjes së veprave penale ose për ekzekutimin e dënimeve penale dhe mbi lëvizjen e lirë të këtyre të dhënave dhe që shfuqizon Vendimin Kuadër të Këshillit 2008/977/JHA, FZ 2016 L 119.

2.2.1 Koncepti i përpunimit të të dhënave

Koncepti i përpunimit të të dhënave personale është gjithëpërfshirës, qoftë sipas **së drejtës së BE-së**, ashtu edhe sipas asaj të **KiE-së**: " 'përpunim i të dhënave personale' [...] është çdo veprim [...] sikurse mbledhja, regjistrimi, organizimi, strukturimi, ruajtja, përshtatja ose ndryshimi, rikthimi, konsultimi, përdorimi, përhapja nëpërmjet transmetimit, shpërndarja ose ndryshe vënia në dispozicion, përputhja ose kombinimi, kufizimi, fshirja ose shkatërrimi"[191] i të dhënave personale. Konventa 108 e Modernizuar i shton gjithashtu përkufizimit mbajtjen e të dhënave personale.[192]

Shembull: tek çështja *František Ryneš*,[193] z. Ryneš, nëpërmjet sistemit vetjak të vëzhgimit CCTV, të cilin e kishte instaluar për të mbrojtur pronën e tij, kishte regjistruar pamjet e dy individëve të cilët kishin i thyer xhamat e dritareve të banesës. GJDBE-ja vendosi se video-vëzhgimi që përfshin regjistrim dhe mbajtje të të dhënave personale, përbën përpunim automatik të dhënash personale, i cili përfshihet në objektin e legjislacionit për mbrojtjen e të dhënave të BE-së.

Shembull: tek çështja *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce k. Salvatore Manni,*[194] z. Manni kërkoi të hiqeshin të dhënat e tij personale nga regjistri tregtar publik, të cilat e lidhnin atë me likuidimin e një shoqërie të pronave të patundshme, duke pasur kësisoj ndikim negativ në reputacionin e tij. GJDBE-ja u shpreh se "duke regjistruar dhe mbajtur atë informacion në regjistër dhe duke ia komunikuar atë palëve të treta me kërkesë, kur kjo ishte e përshtatshme, autoriteti përgjegjës për mbajtjen e atij regjistri, kryen "përpunim të dhënash personale" për të cilin është "kontrollues".

Shembull: Punëdhënësit mbledhin dhe përpunojnë të dhëna personale në lidhje me të punësuarit e tyre, përfshirë informacionet në lidhje me pagat e tyre. Baza ligjore për ligjshmërinë e kësaj është kontrata e punës.

Punëdhënësit do të jenë të detyruar t'ia përcjellin të dhënat e pagave të stafit të tyre autoriteteve tatimore. Ky transferim të dhënash do të konsiderohet gjithashtu "përpunim", sipas kuptimit të këtij termi në Konventën 108 të Modernizuar dhe në GDPR. Gjithsesi, baza ligjore për këtë përhapje të dhënash nuk është kontrata e punës. Duhet të ketë një bazë ligjore shtesë për operacionet e përpunimit, të cilat përfshijnë transmetimin e të dhënave të pagave nga punëdhënësi tek autoritetet tatimore. Kjo bazë ligjore zakonisht përfshihet në dispozitat e legjislacionit kombëtar fiskal. Në mungesë të këtyre dispozitave – dhe në mungesë të çdo lloj baze tjetër ligjore për përpunimin - transmetimi i të dhënave personale do të përbënte përpunim të paligjshëm.

2.2.2. Përpunimi automatik i të dhënave

Sipas Konventës 108 të Modernizuar dhe GDPR-së, mbrojtja e të dhënave gjen plotësisht zbatim për përpunimin automatik të të dhënave.

---

[191] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 4, pika 2. Shih gjithashtu Konventën 108 të Modernizuar, nenin 2, gërma (b).
[192] Konventa 108 e Modernizuar, neni 2, shkronja (b).
[193] GJDBE, C-212/13, *František Ryneš k. Úřad pro ochranu osobních údajů*, 11 dhjetor 2014, parag. 25.
[194] GJDBE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce k. Salvatore Manni*, 9 mars 2017, parag. 35.

Sipas **së drejtës së BE-së**, përpunimi automatik i të dhënave ka të bëjë me operacionet e kryera tek "të dhënat personale, plotësisht ose pjesërisht me mjete automatike"[195]. Konventa 108 e Modernizuar përmban një përkufizim të ngjashëm.[196] Në terma praktikë, kjo do të thotë se çdo përpunim të dhënash personale me anë të mjeteve automatike, për shembull me ndihmën e një kompjuteri stacionar, një pajisjeve lëvizëse, ose një ruteri, mbulohet si nga rregullat e mbrojtjes së të dhënave të BE-së, ashtu edhe nga ato të KiE-së.

Shembull: *Bodil Lindqvist*[197] kishte të bënte me referimin, në një faqe interneti, të personave të ndryshëm, nëpërmjet emrit ose mënyrave të tjera, si për shembull numrit të telefonit, apo informacioneve në lidhje me hobin. GJDBE-ja u shpreh se "veprimi i referimit në një faqe interneti, të personave të ndryshëm dhe identifikimi i tyre me anë të emrit ose mënyra të tjera, për shembull duke dhënë numrin e telefonit ose informacion në lidhje me kushtet e punës ose hobin, përbën "përpunim të dhënash personale, tërësisht ose pjesërisht me anë të mjeteve automatike" sipas kuptimit të nenit 3, pika 1 të Direktivës 95/46."[198]

Shembull: tek çështja Google Spain SL, Google Inc. k. *Agencia Española de Protección de Datos (AEPD), Mario Costeja González*,[199] z. González kërkoi heqjen ose modifikimin e një lidhjeje midis emrit të tij në motorin e kërkimit Google dhe faqeve të dy gazetave që njoftonin zhvillimin e një ankandi për shitjen e një pasurie të paluajtshme me qëllim kthimin e një borxhi ndaj sigurimeve shoqërore. GJDBE-ja theksoi se "duke kërkuar në internet në mënyrë automatike, të pandërprerë dhe sistematike për të gjetur informacione që publikohen në të, operatori i motorit të kërkimit i "mbledh" këto të dhëna, të cilat më pas i "rikthen", "regjistron" dhe "organizon" në kuadër të programeve të tij të indeksimit, i "ruan" në serverët e tij dhe sipas rastit i "zbulon" dhe i "vë në dispozicion" të përdoruesve të tij në formën e një liste rezultatesh kërkimi".[200] GJDBE-ja vendosi se këto veprime përbëjnë "përpunim", "pavarësisht faktit se operatori i motorit të kërkimit kryen gjithashtu të njëjtat operacione për lloje të tjera informacionesh, pa bërë dallim midis këtyre të fundit nga të dhënat personale".

2.2.3. Përpunimi jo automatik i të dhënave

Edhe për përpunimin manual të të dhënave nevojitet mbrojtje e të dhënave.

Mbrojtja e të dhënave **sipas së drejtës së BE-së** nuk kufizohet në asnjë mënyrë vetëm tek përpunimi automatik i të dhënave. Në këtë kuptim, sipas së drejtës së BE-së, mbrojtja e të dhënave zbatohet për përpunimin e të dhënave personale në një sistem arkivimi manual, e cila është një dosje letre e strukturuar në mënyrë të caktuar.[201] Sistemi i strukturuar i arkivimit është ai që kategorizon një set të dhënash personale, duke i bërë të disponueshme sipas disa kriteresh të caktuara. Për shembull, nëse një punëdhënës mban një dosje fizike me mbishkrimin "lejet vjetore të punonjësve", në të cilën ndodhen të gjitha hollësitë në lidhje me lejet vjetore të stafit gjatë vitit të mëparshëm dhe të renditura në rend alfabetik, atëherë dosja do të konsiderohet

[195] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 2, pika 1 dhe neni 4, pika 2.
[196] Konventa 108 e Modernizuar, neni 2, shkronjat (b) dhe (c); Relacioni Shpjegues i Konventës 108 të Modernizuar, parag. 21.
[197] GJDBE, C-101/01, C-101/01, *Criminal proceedings k. Bodil Lindqvist*, 6 nëntor 2003, parag. 27.
[198] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, Neni 2, pika (1).
[199] GJDBE, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [ÇB], 13 maj 2014.*
[200] *Ibid.,* paragrafi 28.
[201] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, Neni 2, pika (1).

sistem arkivimi manual sipas rregullave të mbrojtjes së të dhënave të BE-së. Shkaku për këtë shtrirje të mbrojtjes së të dhënave mbi të është se:

- Dosjet fizike mund të strukturohen në mënyrë të tillë që mundëson gjetjen e shpejtë dhe me lehtësi të informacionit;
- Mbajtja e të dhënave personale në dosje fizike të strukturuara e bën të lehtë shmangien nga kufizimet e përcaktuara me ligj për përpunimin automatik të të dhënave.[202]

Tek **e drejta e KiE-së**, përkufizimi i përpunimit automatik njeh edhe rastet ku ndërmjet aktiviteteve automatike të përpunimit, mund të nevojiten disa etapa të përdorimit manual të të dhënave personale.[203] Neni 2, gërma (c) e Konventës 108 të Modernizuar thekson se "(k)ur nuk përdoret përpunimi automatik, përpunimi i të dhënave do të thotë një veprim apo grup veprimesh të cilat janë kryer mbi të dhënat personale, brenda një tërësie të strukturuar të dhënash, të cilat janë të aksesueshme apo të cilat gjenden me anë të disa kritereve të caktuara".

2.3. Përdoruesit e të dhënave personale

Pikat kryesore

- Sipas legjislacionit të mbrojtjes së të dhënave, cilido që përcakton mjetet dhe qëllimet e përpunimit të të dhënave personale është "kontrollues"; nëse disa persona e marrin këtë vendim së bashku, ata mund të jenë "kontrollues të përbashkët".
- "Përpunuesi" është një person fizik ose juridik, i cili përpunon të dhëna personale për llogari të një kontrolluesi.
- Përpunuesi bëhet kontrollues nëse vetë ai përcakton mjetet dhe qëllimet e përpunimit.
- Çdo person, të cilit i komunikohen të dhëna personale, është "marrës".
- "Palë e tretë" është një person fizik ose juridik, i ndryshëm nga subjekti i të dhënave, kontrolluesi, përpunuesi dhe personat të cilët janë të autorizuar të përpunojnë të dhëna personale nën autoritetin e drejtpërdrejtë të kontrolluesit apo përpunuesit.
- Pëlqimi si bazë ligjore për përpunimin e të dhënave personale, duhet të jepet lirisht, të jetë i informuar, konkret dhe tregues i dallueshëm i dëshirave, nëpërmjet një veprimi të qartë pohues, që shpreh miratimin e subjektit të të dhënave për përpunimin.
- Për përpunimin e kategorive të veçanta të të dhënave mbi bazë pëlqimi nevojitet pëlqim i qartë.

2.3.1. Kontrolluesit dhe përpunuesit

Pasoja më e rëndësishme për funksionin e kontrolluesit apo përpunuesit është përgjegjësia ligjore për respektimin e detyrimeve përkatëse sipas legjislacionit të mbrojtjes së të dhënave. Në sektorin privat, ai është zakonisht një person fizik ose juridik, ndërsa në sektorin publik zakonisht një autoritet. Ekziston një ndryshim i rëndësishëm ndërmjet kontrolluesit të të

[202] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, Paragrafi 15 i Preambulës.
[203] Konventa 108 e Modernizuar, Neni 2, gërmat (b) dhe (c).

dhënave dhe përpunuesit të të dhënave: i pari është personi fizik apo juridik i cili përcakton qëllimet dhe mjetet e përpunimit, ndërsa i dyti është personi fizik apo juridik i cili përpunon të dhëna për llogari të kontrolluesit, duke zbatuar vetëm udhëzimet e tij. Në parim, është kontrolluesi i të dhënave ai që duhet të kontrollojë përpunimin dhe që është përgjegjës për të edhe në planin ligjor. Megjithatë, në kuadrin e reformimit të rregullave të mbrojtjes së të dhënave, përpunuesit duhet të zbatojnë shumë nga detyrimet që aplikohen për kontrolluesit. Për shembull, sipas GDPR-së, përpunuesit duhet të mbajnë regjistrin e të gjitha kategorive të aktiviteteve përpunuese, me qëllim që të vërtetojnë se janë duke zbatuar detyrimet që u takojnë sipas Rregullores.[204] Përpunuesit janë gjithashtu të detyruar të zbatojnë masat e përshtatshme teknike dhe organizative për garantimin e sigurisë së përpunimit,[205] të caktojnë Nëpunësin e Mbrojtjes së të Dhënave në disa raste të caktuara,[206] dhe të njoftojnë kontrolluesin për çdo shkelje ndaj të dhënave.[207]

Elementet faktike apo rrethanat e secilit rast do të vërtetojnë nëse një person ka aftësinë të vendosë dhe të përcaktojë qëllimet dhe mjetet e përpunimit. Sipas përkufizimit të kontrolluesit në GDPR, të tillë mund të jenë personat fizikë, personat juridikë dhe çdo organ tjetër. Sidoqoftë, Grupi i Punës së Nenit 29 ka nënvizuar se në mënyrë që subjektet e të dhënave të mund t'i drejtohen një njësie më të qëndrueshme kur ushtrojnë të drejtat e tyre, "është më e udhës që të konsiderohet si kontrollues shoqëria apo organizmi sesa një person brenda tij."[208] Për shembull, një shoqëri që u shet produkte të kujdesit shëndetësor specialistëve të fushës, është kontrolluese e përpunimit, që konsiston në hartimin dhe përditësimin e listës së shpërndarjes të të gjithë specialistëve të fushës në një zonë të caktuar dhe jo përgjegjësi i shitjeve i cili në fakt përdor dhe përditëson listën.

> Shembull: Kur seksioni i marketingut të shoqërisë Sunshine planifikon të përpunojë të dhëna për një studim tregu, shoqëria Sunshine dhe jo punonjësit e seksionit tw marketingut, do të jetë kontrolluesi i këtij përpunimi. Seksioni i marketingut nuk mund të jetë kontrolluesi, për shkak se nuk ka identitet ligjor mw vete.

Personat fizikë mund të jenë kontrollues edhe sipas së drejtës së BE-së, ashtu edhe sipas së drejtës së KiE-së. Megjithatë, dispozitat e GDPR-së dhe të Konventës 108 të modernizuar nuk gjejnë zbatim për personat fizikë që përpunojnë të dhëna të të tretëve në kuadër të një aktiviteti krejtësisht personal apo familjar dhe nuk konsiderohen kontrollues përpunimi.[209] Një person i cili mban korrespondencën e tij apo të saj, një ditar personal në të cilin përshkruhen incidente me shokë dhe kolegë dhe dosje shëndetësore të anëtarëve të familjes, mund të përjashtohen nga rregullat e mbrojtjes së të dhënave, meqenëse këto aktivitete mund të jenë krejtësisht personale ose thjesht familjare. GDPR-ja saktëson po ashtu se aktivitetet personal apo familjare mund të përfshijnë gjithashtu përdorimin e rrjeteve sociale dhe aktivitetin në internet që zhvillohet në kuadrin e këtyre aktiviteteve.[210] Nga ana tjetër, rregullat e mbrojtjes së të dhënave gjejnë

[204] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 30, pika 2.
[205] *Ibid.,* neni 32.
[206] *Ibid.,* neni 37.
[207] *Ibid.,* neni 33, pika 2.
[208] Grupi i Punës së Nenit 29 (2010), *Opinioni 1/2010 mbi konceptet e "kontrolluesit" dhe "përpunuesit",* GP 169, Bruksel, 16 shkurt 2010.
[209] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 18 i preambulës dhe neni 2, pika 2, gërma c; Konventa 108 e Modernizuar, neni 3, pika 2.
[210] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 18 i preambulës.

plotësisht zbatim për kontrolluesit dhe përpunuesit të cilët vënë në dispozicion mjetet për përpunimin e të dhënave personale për qëllime vetjake apo familjare (për shembull, platformat e rrjeteve sociale).[211]

Aksesi i qytetarëve në internet dhe mundësia e përdorimit të platformave të e-tregtisë, rrjeteve sociale dhe blogjeve për shkëmbimin e informacioneve personale në lidhje me vetë personat apo me të tretë, e bën gjithnjë e më të vështirë dallimin e përpunimit personal nga ai jo personal.[212] Nëse aktivitetet janë krejtësisht personale apo familjare, kjo varet nga rrethanat.[213] Aktivitetet që kanë aspekte profesionale ose tregtare nuk mund të përfshihen në përjashtimin familjar.[214] Kështu, kur shkalla dhe frekuenca e përpunimit të të dhënave tregon aktivitet profesional ose me kohë të plotë, një person mund të konsiderohet si kontrollues përpunimi. Krahas karakterit profesional apo tregtar të aktivitetit përpunues, një faktor tjetër që duhet marrë parasysh është nëse të dhënat personale u vihen në dispozicion një numri të madh personash, të cilët janë qartazi jashtë sferës private të subjektit të të dhënave. Jurisprudenca në kontekstin e Direktivës së Mbrojtjes së të Dhënave ka përcaktuar se ligji për mbrojtjen e të dhënave gjen zbatim kur një person privat, nëpërmjet përdorimit të internetit, publikon të dhëna në lidhje me të tjerët në një faqe publike interneti. GJDBE-ja nuk ka vendosur ende në lidhje me fakte të ngjashme sipas GDPR-së, e cila përcakton më tepër udhëzime mbi subjektet që mund të konsiderohen jashtë fushës së zbatimit të legjislacionit të mbrojtjes së të dhënave sipas "përjashtimit familjar", sikurse përdorimi i medias sociale për qëllime personale.

Shembull: çështja *Bodil Lindqvist*[215] kishte të bënte me referimin që u ishte bërë personave të ndryshëm me emër ose me mënyra të tjera, si për shembull me numrin e telefonit, apo të dhënave në lidhje me hobin përkatës, në një faqe interneti. GJDBE-ja përcaktoi se "veprimi i të referuarit në një faqe interneti personave të ndryshëm dhe identifikimi i tyre nëpërmjet emrit apo mënyrave të tjera [...] përbënte "përpunim të dhënash personale plotësisht ose pjesërisht me mjete automatike" në kuptim të nenit 3, pika 1 të Direktivës së Mbrojtjes së të Dhënave.[216]
Ky lloj përpunimi të dhënash personale nuk përfshihet tek aktivitetet krejtësisht personale dhe familjare, të cilat janë jashtë fushës së zbatimit të rregullave të BE-së për mbrojtjen e të dhënave, meqenëse ky përjashtim "duhet [...] interpretuar si në lidhje vetëm me aktivitetet të cilat zhvillohen në kuadrin e jetës private apo familjare, ndërsa nuk është qartësisht rasti me përpunimin e të dhënave personale që konsiston në publikimin në internet në mënyrë të tillë që ato të dhëna të jenë të aksesueshme për një numër të papërcaktuar personash."[217]

Sipas GJDBE-së, regjistrimi vizual me anë të kamerave të sigurisë të instaluara në mënyrë private, mund të përfshihet gjithashtu nga legjislacioni i mbrojtjes së të dhënave të BE-së në rrethana të caktuara.

---

[211] *Ibid.,* paragrafi 18 i preambulës; Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 29.
[212] Shih deklaratën e Grupit të Punës së Nenit 29 mbi diskutimet në lidhje me paketën e reformës së mbrojtjes së të dhënave (2013), *Aneksi 2: Propozime dhe ndryshime që kanë të bëjnë me përjashtimin për akivitete personale apo familjare*, 27 shkurt 2013.
[213] Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 28.
[214] Shih Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave, paragrafin 18 të preambulës dhe Raportin Shpjegues të Konventës 108 të Modernizuar, paragrafi 27.
[215] GJDBE, C-101/01, *Criminal proceedings k. Bodil Lindqvist*, 6 nëntor 2003.
[216] *Ibid*., paragrafi 27; Direktiva e shfuqizuar 95/46/EC, neni 3, pika 1, tani Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 2, pika 1.
[217] GJDBE, C-101/01, *Criminal proceedings k. Bodil Lindqvist*, 6 nëntor 2003, paragrafi 47.

Shembull: tek çështja *František Ryneš*, [218] z. Ryneš, me anë të sistemit të mbikëqyrjes CCTV të cilën e kishte instaluar për të mbrojtur pronën e tij, regjistroi pamjet e dy individëve të cilët thyen dritaret e banesës së tij. Regjistrimi iu dorëzua më pas policisë dhe u përdor gjatë procedimit penal.

GJDBE-ja theksoi se "për aq kohë sa ai video survejim [...] mbulon, qoftë edhe pjesërisht, një hapësirë publike dhe rrjedhimisht drejtohet përtej sferës private të personit i cili përpunon të dhënat në këtë mënyrë, diçka e tillë nuk mund të konsiderohet si aktivitet krejtësisht 'personal apo familjar' [...]."[219]

Kontrolluesi

Sipas së drejtës së BE-së, kontrolluesi përkufizohet si dikush i cili "vetëm ose së bashku me të tjerë, përcakton qëllimet dhe mjetet e përpunimit të të dhënave personale".[220] Vendimi i kontrolluesit përcakton përse dhe si duhen përpunuar të dhënat.

Sipas së drejtës së KiE-së, Konventa 108 e Modernizuar përkufizon "kontrolluesin" si "personin fizik ose juridik, autoritetin publik, shërbimin, agjencinë, apo çdo organ tjetër, i cili, i vetëm apo së bashku me të tjerë, ka fuqinë e vendimmarrjes për përpunimin e të dhënave".[221] Kjo fuqi vendimmarrjeje ka të bëjë me qëllimet dhe mjetet e përpunimit, si dhe me kategoritë e të dhënave që duhen përpunuar dhe me aksesin tek të dhënat.[222] Nëse kjo fuqi buron nga një përcaktim ligjor, apo një rrethanë faktike, diçka e tillë duhet përcaktuar rast pas rasti.[223]

Shembull: *Google Spain*[224] u iniciua nga një qytetar spanjoll, i cili kërkonte që të hiqej nga Google-i një lajm i vjetër gazete që kishte të bënte me të shkuarën e tij financiare.

GJDBE-së iu kërkua të vlerësonte nëse Google-i, në cilësinë e operatorit të një motori kërkimi, ishte 'kontrolluesi' i të dhënave në kuptim të nenit 2, pika d të Direktivës së Mbrojtjes së të Dhënave.[225] GJDBE-ja shqyrtoi një përkufizim të zgjeruar të nocionit të "kontrolluesit" për të siguruar "mbrojtje të efektshme dhe të plotë të subjekteve të të dhënave".[226] GJDBE-ja përcaktoi se operatori i motorit të kërkimit përcaktonte qëllimet dhe mjetet e aktivitetit dhe bënte të mundur që të dhënat e ngarkuara në faqet e internetit nga publikuesit e faqeve të ishin të aksesueshme nga çdo përdorues interneti që bën kërkim bazuar në emrin e subjektit të të dhënave.[227] Për rrjedhojë, GJDBE-ja vendosi se Google-i duhej konsideruar 'kontrolluesi'.[228]

---

[218] GJDBE, C-212/13, *František Ryneš k. Úřad pro ochranu osobních údajů*, 11 dhjetor 2014, paragrafi 33.
[219] Direktiva e shfuqizuar 95/46/EC, neni 3, pika 2, paragrafi i dytë, tani Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 2, pika 2, shkronja c.
[220] Rregullorja e Përgjithshme e Mrojtjes së të Dhënave, neni 4, pika 7.
[221] Konventa 108 e Modernizuar, neni 2, pika d.
[222] Relacioni Shpjegues i Konventës 108 të Modernizuar, paragrafi 22.
[223] *Ibid.*
[224] GJDBE, C-131/12, 131/12, *Google Spain SL, Google Inc. k. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [ÇB], 13 maj 2014.
[225] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 4, pika 7; GJDBE, C-131/12, *Google Spain SL, Google Inc. k. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [ÇB], 13 maj 2014, paragrafi 21.
[226] GJDBE, C-131/12, *Google Spain SL, Google Inc. k. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [ÇB], 13 maj 2014, paragrafi 34.
[227] *Ibid.,* paragrafët 35-40.
[228] *Ibid.,* paragrafi 41.

Kur një kontrollues ose përpunues është i vendosur jashtë BE-së, ajo shoqëri duhet të caktojë me shkrim një përfaqësues brenda BE-së.[229] GDPR-ja nënvizon se përfaqësuesi duhet të jetë i vendosur "në një Shtet Anëtar në të cilin ndodhen subjektet e të dhënave, të dhënat personale të të cilëve po përpunohen, me qëllim që t'u ofrohen mallra dhe shërbime, apo sjellja e të cilëve po monitorohet".[230] Nëse nuk caktohet një përfaqësues, mund të ndërmerren veprime ligjore kundër vetë kontrolluesit ose përpunuesit.[231]

Kontrolluesit e përbashkët

GDPR-ja parashikon se kur dy apo më shumë kontrollues përcaktojnë bashkërisht qëllimin dhe mjetet e përpunimit, ata konsiderohen kontrollues të përbashkët. Kjo do të thotë se ata vendosin bashkërisht të përpunojnë të dhëna për qëllimin e përbashkët.[232] Relacioni Shpjegues i Konventës 108 të Modernizuar thekson se është gjithashtu e mundur që të ketë më shumë kontrollues apo kontrollues të përbashkët sipas **kuadrit të KiE-së**.[233]

Grupi i Punës së Nenit 29 vlerëson se kontrollimi i përbashkët mund të marrë forma të ndryshme dhe se pjesëmarrja e kontrolluesve të ndryshëm në aktivitetet kontrolluese mund të jetë i pabarabartë.[234] Ky lloj fleksibiliteti mundëson adresimin e kompleksitetit në rritje të realitetit të përpunimit të të dhënave.[235] Kontrolluesit e përbashkët për rrjedhojë duhet të përcaktojnë në një marrëveshje specifike përgjegjësitë përkatëse për sa i takon zbatimit të detyrimeve që rrjedhin nga rregullorja.[236]

Kontrollimi i përbashkët shkakton përgjegjësi të përbashkët për sa i përket një aktiviteti përpunimi.[237] Referuar kuadrit të **së drejtës së BE-së**, kjo do të thotë se secili kontrollues apo përpunues mund të ngarkohet me përgjegjësi për të gjitha dëmet e shkaktuara nga përpunimi i kryer me kontrollues të përbashkët, për të garantuar që subjekti i të dhënave të kompensohet në mënyrë të efektshme.[238]

Shembull: Një bazë të dhënash e klientëve "të këqij" që përdoret bashkërisht nga disa institucione kreditimi, është një shembull tipik i bashkë-kontrolluesve. Kur dikush aplikon për një kredi nga një bankë e cila është një nga bashkë-kontrolluesit, bankat kontrollojnë bazën e të dhënave që t'i ndihmojë ato të marrin vendimet të informuara në lidhje me besueshmërinë e aplikuesit për kredi.

Dispozitat ligjore nuk shprehen në mënyrë të qartë nëse bashkë-kontrolluesit duhet të kenë secili të njëjtin qëllim të përbashkët, apo mjafton që qëllimet e tyre të përputhen vetëm pjesërisht. Deri më tani, ende nuk ka jurisprudencë përkatëse në nivel evropian. Në Opinion e

[229] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 27, pika 1.
[230] *Ibid.,* neni 27, pika 3.
[231] *Ibid.,* neni 27, pika 5.
[232] *Ibid.,* neni 4, pika 7 dhe neni 26.
[233] Konventa 108 e Modernizuar, neni 2, gërma d; Relacioni Shpjegues i Konventës 108 të Modernizuar, paragrafi 22.
[234] Grupi i Punës së Nenit 29 (2010), *Opinioni 1/2010 mbi konceptet e "kontrolluesit" dhe "përpunuesit",* GP 169, Bruksel 16 shkurt 2010, fq. 19.
[235] *Ibid.*
[236] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 79 i preambulës.
[237] *Ibid*., paragrafi 21.
[238] *Ibid.*, neni 82, pika 4.

2010-ës mbi kontrolluesit dhe përpunuesit, Grupi i Punës së Nenit 29 thekson se kontrolluesit e përbashkët mund të kenë të njëjtat qëllime dhe mjete përpunimi, ose disa qëllime dhe mjete, ose vetëm një pjesë të tyre.[239] Teksa e para nënkupton një marrëdhënie mjaft të ngushtë midis aktorësh të ndryshëm, kjo e dyta tregon një marrëdhënie më të largët.

Grupi i Punës së Nenit 29 anon nga një interpretim më i gjerë i konceptit të kontrollimit të përbashkët, me qëllim që të mundësohet një farë fleksibiliteti për të përballuar kompleksitetin në rritje të realitetit aktual të përpunimit të të dhënave.[240] Një çështje që përfshin Shoqatën Botërore të Telekomunikimit Financiar Ndër-bankar (SWIFT) ilustron qëndrimin e Grupit të Punës.

Shembull: tek e ashtuquajtura çështja e SWIFT-it, institucionet bankare evropiane kishin përdorur SWIFT-in, në fillim si përpunues, për të kryer transferime të dhënash në kuadër të transaksioneve bankare. SWIFT-i ia kishte komunikuar këto të dhëna të transaksioneve bankare, të cilat mbaheshin në një qendër shërbimesh kompjuterike në Shtetet e Bashkuara (SHBA), Departamentit të Thesarit të SHBA-së, pa një kërkesë të shprehur nga institucionet bankare evropiane të cilat i përdornin ato. Gjatë shqyrtimit të ligjshmërisë së kësaj situate, Grupi i Punës së Nenit 29, arriti në përfundimin se institucionet bankare evropiane që përdornin SWIFT-in, ashtu si edhe vetë SWIFT-i, duhet të konsideroheshin si bashkë-kontrollues, përgjegjës ndaj klientëve evropianë për komunikimin e të dhënave të tyre tek autoritetet e Shteteve të Bashkuara.[241]

Përpunuesi

Përpunuesi përkufizohet **në të drejtën e BE-së** si dikush i cili përpunon të dhëna personale për llogari të kontrolluesit.[242] Aktivitetet që i besohen një përpunuesi, mund të kufizohen në një detyrë apo kontekst tepër specifik, ose mund të jenë mjaft të përgjithshme dhe gjithëpërfshirëse.

Sipas së drejtës së KiE-së, përpunuesi ka të njëjtin kuptim me atë të së drejtës së BE-së.[243]

Përpunuesit, përveç përpunimit të të dhënave për të tjerët, do të jenë gjithashtu kontrollues me të drejta të plota për sa i takon përpunimit që ata kryejnë për qëllimet e tyre, p.sh. për menaxhimin e punonjësve të tyre, shitjet dhe kontabilitetin.

Shembull: shoqëria Everready është e specializuar në përpunimin e të dhënave për menaxhimin e të dhënave të burimeve njerëzore të shoqërive të tjera. Në këtë cilësi, Everready është përpunues. Gjithsesi, kur Everready përpunon të dhënat e punonjësve të tij, ai është kontrolluesi i aktiviteteve të përpunimit të të dhënave me qëllimin e përmbushjes së detyrimeve të tij si punëdhënës.

---

[239] Grupi i Punës së Nenit 29 (2010), *Opinioni 1/2010 mbi konceptet e "kontrolluesit" dhe "përpunuesit"*, WP 169, Bruksel, 16 shkurt 2010, fq. 19.
[240] *Ibid.*
[241] *Ibid.*
[242] Grupi i Punës së Nenit 29 (2006), *Opinioni 10/2006 mbi përpunimin e të dhënave personale nga Shoqata Botërore e Telekomunikimit Financiar Ndër-bankar (SWIFT)*, WP 128, Bruksel, 22 nëntor 2006.
[243] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 4, pika 8.

Marrëdhënia midis kontrolluesit dhe përpunuesit

Sikurse e pamë, kontrolluesi përkufizohet si ai që përcakton qëllimet dhe mjetet e përpunimit. GDPR-ja shprehet qartësisht se përpunuesi mund të përpunojë të dhëna personale vetëm sipas udhëzimeve të kontrolluesit, përveçse kur e drejta e BE-së apo e Shtetit Anëtar e detyron përpunuesin ta kryejë atë.[244] Kontrata midis kontrolluesit dhe përpunuesit është një element thelbësor i marrëdhënies së tyre dhe një detyrim ligjor.[245]

Shembull: drejtuesi i shoqërisë Sunshine vendos që shoqëria Cloudy, e specializuar në ruajtjen e të dhënave nëpërmjet shërbimit *cloud*, duhet të menaxhojë të dhënat e klientëve të Sunshine-it. Shoqëria Sunshine mbetet kontrolluese dhe shoqëria Cloudy është thjesht përpunuese, meqenëse sipas kontratës, Cloudy mund të përdorë të dhënat e klientëve të Sunshine-it vetëm për qëllimet e përcaktuara nga Sunshine-i.

Duke qenë se kompetenca për të përcaktuar mjetet e përpunimit i delegohet përpunuesit, gjithsesi duhet që kontrolluesi të jetë i aftë të ushtrojë kontroll në një nivel të përshtatshëm mbi vendimet e përpunuesit në lidhje me mjetet e përpunimit. Përgjegjësia e përgjithshme mbetet ende tek kontrolluesi, i cili duhet të mbikëqyrë përpunuesit, për t'u siguruar se vendimet e tyre përputhen me legjislacionin e mbrojtjes së të dhënave dhe me udhëimet e tij.

Gjithashtu, nëse përpunuesi nuk respekton kushtet e përpunimit të të dhënave sikurse janë përcaktuar nga kontrolluesi, përpunuesi do të shndërrohet në kontrollues, të paktën deri në atë masë sa është shkelja e udhëzimeve të kontrolluesit. Me gjasë, kjo do ta bëntë përpunuesin kontrollues që vepron në mënyrë të paligjshme. Nga ana tjetër, kontrolluesi fillestar është i detyruar të shpjegojë se si ndodhi që përpunuesi të shkelë mandatin e tij.[246] Në fakt, Grupi i Punës së Nenit 29 ka prirjen t'i konsiderojë këto lloj rastesh si situatë kontrolli të përbashkët, duke qenë se diçka e tillë gjeneron mbrojtje më të madhe të interesave të subjekteve të të dhënave.[247]

Mund të ketë gjithashtu problematika në lidhje me ndarjen e përgjegjësisë në rastin kur kontrolluesi është një ndërmarrje e vogël dhe përpunuesi është një korporatë e madhe, e cila ka fuqinë të diktojë kushtet e shërbimeve që ofron. Gjithsesi, në këto rrethana, Grupi i Punës së Nenit 29 këmbëngul se standardi i përgjegjësisë nuk duhet ulur në nivelin e pabarazisë ekonomike dhe se duhet ruajtur i njëjti kuptim i konceptit të kontrolluesit.[248]

Për arsye qartësie dhe transparence, detajet e marrëdhënies midis kontrolluesit dhe përpunuesit, duhet të përshkruhen në një kontratë të shkruar.[249] Kontrata duhet të përmbajë sidomos objektin, karakterin, qëllimin dhe kohëzgjatjen e përpunimit, llojin e të dhënave personale dhe kategoritë e subjekteve të të dhënave. Ajo duhet gjithashtu të përcaktojë detyrimet dhe të drejtat

[244] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 29.
[245] *Ibid*., neni 28, pika 3.
[246] *Ibid*., neni 82, pika 2.
[247] Grupi i Punës së Nenit 29 (2010), Opinioni 1/2010 mbi konceptet e "kontrolluesit dhe "përpunuesit", WP 169, Bruksel, 16 shkurt 2010, fq. 26; Grupi i Punës së Nenit 29 (2006), *Opinioni 10/2006 mbi përpunimin e të dhënave personale nga Shoqata Botërore e Telekomunikimit Financiar Ndër-bankar (SWIFT),* WP 128, Bruksel, 22 nëntor 2006.
[248] Grupi i Punës së Nenit 29 (2010), *Opinioni 1/2010 mbi konceptet e "kontrolluesit" dhe "përpunuesit",* WP 169, Bruksel, 16 shkurt 2010, fq. 26.
[249] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenit 28, pikat 3 dhe 9.

e kontrolluesit dhe të përpunuesit, si për shembull kriteret në lidhje me konfidencialitetin dhe sigurinë. Mungesa e një kontrate të tillë përbën shkelje të detyrimit të kontrolluesit për të vënë në dispozicion dokumentacion me shkrim në lidhje me përgjegjësitë reciproke dhe mund të rezultojë në vendosje sanksionesh. Kur shkaktohen dëme si rezultat i veprimeve që shkojnë përtej, apo janë në kundërshtim me udhëzimet e ligjshme të kontrolluesit, nuk ngarkohet me përgjegjësi vetëm kontrolluesi, por edhe përpunuesi.[250] Përpunuesi duhet të mbajë regjistër për të gjitha kategoritë e aktiviteteve të përpunimit që ai kryen për llogari të kontrolluesit.[251] Këto regjistra duhet t'i vihen në dispozicion autoritetit mbikëqyrës me kërkesën e këtij të fundit, duke qenë se si kontrolluesi, ashtu edhe përpunuesi duhet të bashkëpunojnë me atë autoritet në përmbushjen e detyrave të tij.[252] Kontrolluesit dhe përpunuesit duhet gjithashtu të kenë mundësi të aderojnë në një kod sjelljeje të miratuar, apo në një mekanizëm certifikimi, për të vërtetuar përputhshmërinë e tyre me normat e GDPR-së.[253]

Përpunuesit mund të duan të delegojnë disa detyra tek nën-përpunues të tjerë. Diçka e tillë është ligjërisht e lejueshme, me kusht që të jenë vendosur disa klauzola kontraktuese të përshtatshme midis kontrolluesit dhe përpunuesit, duke përfshirë edhe nëse nevojitet autorizimi i kontrolluesit në secilin rast, apo nëse duhet thjesht të vihet në dijeni. GDPR-ja përcakton se përpunuesi fillestar mbetet plotësisht përgjegjës kundrejt kontrolluesit kur nën-përpunuesi nuk përmbush detyrimet e tij në lidhje me mbrojtjen e të dhënave.[254]

Sipas së drejtës së KiE-së, gjen plotësisht zbatim interpretimi i koncepteve të kontrolluesit dhe përpunuesit sikurse u trajtua më lart.[255]

2.3.2. Marrësit dhe palët e treta

Ndryshimi midis këtyre dy kategorive të personave dhe njësive të cilat u shfaqën nga Direktiva e Mbrojtjes së të Dhënave, konsiston kryesisht në marrëdhënien e tyre me kontrolluesin dhe rrjedhimisht, në autorizimin që ai u jep për të pasur akses në të dhënat personale që zotëron kontrolluesi.

"Palë e tretë" është dikush i cili është i ndryshëm nga kontrolluesi dhe përpunuesi. Sipas nenit 4, pika 10 të GDPR-së, palë e tretë është "çdo person fizik ose juridik, autoritet publik, agjenci apo çdo organizëm përveç subjektit të të dhënave, kontrolluesit, përpunuesit dhe personave të cilët nën autoritetin e drejtpërdrejtë të kontrolluesit ose përpunuesit, janë të autorizuar të përpunojnë të dhëna personale". Kjo do të thotë se personat të cilët punojnë për një organizatë e cila është e ndryshme nga kontrolluesi – edhe nëse i përket të njëjtit grupi apo shoqërie aksionere – do të jetë (ose do t'i përkasë) një "palë e tretë". Nga ana tjetër, degët e një banke

[250] *Ibid*., neni 82, pika 2.
[251] *Ibid*., neni 30, pika 2.
[252] *Ibid*., nenet 30, pika 4 dhe 31.
[253] *Ibid*., nenet 28, pika 5 dhe 42, pika 4.
[254] *Ibid*., neni 28, pika 4.
[255] Shih, për shembull, Konventën 108 të Modernizuar, neni 2, gërmat b dhe f; Rekomandimin mbi Profilizimin, neni 1.

që përpunojnë llogaritë e klientëve, nën autoritetin e drejtpërdrejtë të bankës së saj qendrore, nuk do të konsiderohen "palë të treta".[256]

"Marrësi" është term më i gjerë se sa "pala e tretë". Në kuptimin e nenit 4, pika 9 të GDPR-së, marrës do të thotë "çdo person fizik ose juridik, autoritet publik, agjenci apo çdo organizëm tjetër, të cilit i komunikohen të dhëna, qoftë palë e tretë ose jo". Marrësi mund të jetë ose një person i jashtëm në raport me kontrolluesin apo përpunuesit – në këtë rast është palë e tretë – ose dikush i brendshëm tek kontrolluesi ose përpunuesi, sikundër mund të jetë një punonjës, ose një sektor brenda së njëjtës shoqërie apo autoriteti.

Dallimi ndërmjet marrësve dhe palëve të treta është i rëndësishëm vetëm për shkak të kushteve për komunikim të ligjshëm të të dhënave. Punonjësit e një kontrolluesi apo përpunuesi, pa pasur nevojë për norma të tjera ligjore, mund të jenë marrës të të dhënave personale, nëse janë të angazhuar në aktivitetet përpunuese të kontrolluesit apo përpunuesit. Nga ana tjetër, një palë e tretë, e cila është veçmas nga kontrolluesi apo përpunuesi, nuk është e autorizuar të përdorë të dhëna personale që përpunohen nga kontrolluesi, përveçse kur ka bazë ligjore specifike në raste të caktuara.

Shembull: një punonjës i përpunuesit, i cili përdor të dhëna personale në kuadër të detyrave që i janë caktuar nga punëdhënësi, është marrës i të dhënave, por jo palë e tretë, meqenëse ai përdor të dhënat për llogari të përpunuesit dhe sipas udhëzimeve të tij. Për shembull, nëse një punëdhënës komunikon të dhënat personale të punonjësve të tij tek drejtoria e burimeve njerëzore, me qëllim kryerjen e vlerësimeve të punës, stafi i burimeve njerëzore do të jetë marrësi i të dhënave personale, për shkak se të dhënat u janë komunikuar në kuadër të përpunimit për llogari të kontrolluesit.

Megjithatë, nëse organizata i jep të dhëna në lidhje me punonjësit e saj një shoqërie trajnimi, e cila do t'i përdorë ato për të përshtatur programin e trajnimit për punonjësit, shoqëria trajnuese është palë e tretë. Arsyeja është se shoqëria trajnuese nuk ka legjitimitet apo autorizim specifik (të cilat në rastin e "burimeve njerëzore" burojnë nga marrëdhënia e punësimit me kontrolluesin) për të përpunuar këto të dhëna personale. Me fjalë të tjera, ata nuk i kanë përftuar të dhënat në kuadër të punësimit të tyre pranë kontrolluesit të të dhënave.

2.4. Pëlqimi

Pikat kryesore

- Pëlqimi, si bazë ligjore për përpunimin e të dhënave personale, duhet të jepet në mënyrë të lirë, të informuar dhe specifike dhe të jetë tregues i qartë i dëshirave, nëpërmjet një akti pohues të qartë sipas të cilit kuptohet miratimi për përpunimin.

[256] Grupi i Punës së Nenit 29 (2010), *Opinioni 1/2010 mbi konceptin e "kontrolluesit" dhe "përpunuesit"*, WP 169, Bruksel, 16 shkurt 2010, fq. 31.

- Përpunimi i kategorive të veçanta të të dhënave kërkon pëlqim eksplicit.

Sikurse do të trajtohet më në hollësi në Kapitullin 4, pëlqimi është një nga gjashtë kriteret ligjore për përpunimin e të dhënave personale. Pëlqim do të thotë "një tregues i dhënë lirisht, specifik, i informuar dhe i qartë i dëshirave të subjektit të të dhënave."[257]

E drejta e BE-së përcakton disa elemente për një pëlqim të vlefshëm, të cilët synojnë që të sigurohet se subjektet e të dhënave kanë pasur vërtet qëllim të miratojnë një përdorim të caktuar të të dhënave të tyre:[258]

- Pëlqimi duhet të jepet nëpërmjet një akti të qartë pohues, i cili përcakton një tregues të qartë, të dhënë lirisht, specifik dhe të informuar të miratimit të subjektit të të dhënave për përpunimin e të dhënave personale të tij apo të saj. Ky akt mund të jetë një veprim ose një deklarimi.
- Subjekti i të dhënave duhet të ketë të drejtën të tërheqë pëlqimin në çdo kohë.
- Në kontekstin e një deklarimi me shkrim që ka të bëjë edhe me çështje të tjera, sikurse për "kushtet e shërbimit", kërkesat për pëlqim duhet të paraqitet duke përdorur gjuhë të qartë dhe të thjeshtë dhe në një formë të kuptueshmë dhe lehtësisht të aksesueshme, e cila të dallojë qartësisht pëlqimin nga çështje të tjera; çdo pjesë e një deklarimi të tillë që përbën shkelje të GDPR-së nuk është detyruese.

Pëlqimi do të jetë i vlefshëm në kontekstin e ligjit për mbrojtjen e të dhënave vetëm nëse të gjitha këto kritere janë plotësuar. Përgjegjësia për të demonstruar se subjekti i të dhënave ka dhënë pëlqimin për përpunimin e të dhënave të tij apo të saj i takon kontrolluesit.[259] Elementet për një pëlqim të vlefshëm do të trajtohen më tej në Seksionin 4.1.1 në lidhje me kriteret ligjore për përpunimin e të dhënave personale.

Konventa 108 nuk përmban një përkufizim të pëlqimit; kjo i lihet të drejtës kombëtare. Megjithatë, **në të drejtën e KiE-së**, elementet e pëlqimit të vlefshëm përkojnë me ato të shpjeguara më lart.[260]

Norma të tjera shtesë sipas së drejtës civile, sikurse zotësia juridike, natyrisht që zbatohen edhe në kontekstin e mbrojtjes së të dhënave, duke qenë se këto kritere janë parakushte themelore ligjore. Pëlqimi i pavlefshëm i personave të cilët nuk kanë zotësinë juridike, sjell për rrjedhojë mungesën e një baze ligjore për përpunimin e të dhënave të këtyre personave. Për sa i përket zotësisë juridike të fëmijëve për të qenë palë në marrëveshje, GDPR-ja parashikon se rregullat përkatëse për moshën minimale për të marrë pëlqim të vlefshëm, nuk cënojnë të drejtën e përgjithshme të kontratave të Shteteve Anëtare.[261]

[257] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 4, pika 11. Shih gjithashtu Konventën 108 të Modernizuar, neni 5, pika 2.
[258] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 7.
[259] *Ibid*., neni 7, pika 1.
[260] Konventa 108 e Modernizuar, neni 5, pika 2; Relacioni Shpjegues i Konventës 108 të Modernizuar, paragrafët 42-45.
[261] Rregullorja e Përgjithshme e mbrojtjes së të Dhënave, neni 8, pika 3.

Pëlqimi duhet të jepet në mënyrë të qartë, të tillë që nuk lë dyshime për qëllimin e subjektit të të dhënave.[262] Pëlqimi duhet të jetë eksplicit kur bëhet fjalë për përpunimin e të dhënave sensitive dhe mund të jepet me gojë ose me shkrim.[263] Ky i fundit mund të bëhet edhe me mjete elektronike.[264] Qoftë sipas së drejtës së BE-së, ashtu edhe atë të KiE-së, miratimi për përpunimin e të dhënave personale të një personi duhet të jepet me anë të një deklarimi, ose një veprimi të qartë pohues.[265] Për rrjedhojë, pëlqimi nuk mund të derivojë nga heshtja, fushat e parazgjedhura, formularët e paraplotësuar apo mosveprimi.[266]

3 Parimet themelore të së drejtës evropiane në fushën e mbrojtjes së të dhënave

BE	Çështje të trajtuara	KiE
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, Neni 5, pika 1, gërma a	Parimi i ligjshmërisë	Konventa 108 e Modernizuar, neni 5, pika 3
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5, pika 1, gërma a	Parimi i drejtësisë	Konventa 108 e Modernizuar, neni 5, pika 4, gërma a GJEDNJ, *K.H. dhe të Tjerët k. Sllovakisë*, nr. 32881/04, 2009
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5, pika 1, gërma a GJDBE, C-201/14, *Smaranda Bara dhe të Tjerët k. Casa Naţională de Asigurări de Sănătate dhe të Tjerët*, 2015	Parimi i transparencës	Konventa 108 e Modernizuar, neni 5, pika 4, gërma a dhe neni 8 GJEDNJ, *Haralambie k. Rumanisë*, nr. 21737/03, 2009
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5, pika 1, gërma b	Parimi i kufizimit të qëllimit	Konventa 108 e Modernizuar, neni 5, pika 4, gërma b

[262] *Ibid*., neni 6, pika 1 dhe 9, pika 2, gërma a.
[263] *Ibid*., paragrafi 32 i preambulës.
[264] *Ibid*.
[265] *Ibid*., neni 4, pika 11; Relacioni Shpjegues i Konventës 108 të Modernizuar, paragrafi 42.
[266] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 32 i preambulës; Relacioni Shpjegues i Konventës 108 të Modernizuar, paragrafi 42.

Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5 pika 1, gërma c GJDBE, Çështje të bashkuara C-293/12 and C-594/12, *Digital Rights Ireland dhe Kärntner Landesregierung dhe të Tjerët* [GC], 2014	Parimi i minimizimit të të Dhënave	Konventa 108 e Modernizuar, neni 5, pika 4, gërma c
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5, pika 1, gërma d GJDBE, C-553/07, *College van burgemeester en wethouders van Rotterdam k. M. E. E. Rijkeboer*, 2009	Parimi i saktësisë së të dhënave	Konventa 108 e Modernizuar, neni 5, pika 4, gërma d
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5, pika 1, gërma e GJDBE, Çështje të bashkuara C-293/12 and C-594/12, *Digital Rights Ireland dhe Kärntner Landesregierung dhe të Tjerët* [GC], 2014	Parimi i kufizimit të mbajtjes	Konventa 108 e Modernizuar, neni 5, pika 4, gërma e GJEDNJ, *S. dhe Marper k. Mbretërisë së Bashkuar* [GC], nr. 30562/04 dhe 30566/04, 2008
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 5, pika 1, gërma f, dhe 32	Parimi i sigurisë së të dhënave (integritetit dhe konfidencialitetit	Konventa 108 e Modernizuar, neni 7
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5, pika 2	Parimi i përgjegjshmërisë	Konventa 108 e Modernizuar, neni 10

Neni 5 i Rregullores së Përgjithshme të Mbrojtjes së të Dhënave përcakton parimet që rregullojnë përpunimin e të dhënave personale. Këto parime mbulojnë:

- Ligjshmërinë, drejtësinë dhe transparencën;
- Kufizimin e qëllimit;
- Minimizimin e të dhënave;
- Saktësinë e të dhënave;
- Kufizimin e mbajtjes;
- Integritetin dhe konfidencialitetin.

Parimet shërbejnë si një pikënisje për dispozita më të detajuara në nenet vijuese të rregullores. Ato shfaqen gjithashtu edhe në nenet 5, 7, 8 dhe 10 të Konventës 108 të Modernizuar. I gjithë legjislacioni i mëvonshëm për mbrojtjen e të dhënave në nivel KiE-je dhe BE-je duhet të përputhet me këto parime

dhe ato duhen mbajtur në mendje kur interpretohet ky legjislacion. Sipas së drejtës së BE-së, kufizimet e parimeve të përpunimit janë të lejueshme vetëm në masën që ato korrespondojnë me të drejtat dhe detyrimet e parashikuara në nenet 12 deri 22 dhe ato duhet të respektojnë thelbin e të drejtave dhe lirive themelore. Çdo përjashtim apo kufizim të zbatimit të këtyre parimeve kyçe duhet përcaktuar në nivel BE-je ose kombëtar,[267] të përcaktohet me ligj, të ndjekë një qëllim legjitim dhe të përbëjë një masë proporcionale në një shoqëri demokratike.[268] Të tre këto kushte duhet të plotësohen.

3.1 Parimet e ligjshmërisë, drejtësisë dhe transparencës së përpunimit

Pikat kryesore

- Parimet e ligjshmërisë, drejtësisë dhe transparencës zbatohen për çdo përpunim të dhënash personale.
- Sipas GDPR-së, ligjshmëria kërkon një nga sa më poshtë:
  - Pëlqimin e subjektit të të dhënave;
  - Nevojën për të lidhur një kontratë;
  - Një detyrim ligjor;
  - Nevojën për të mbrojtur interesat jetikë të subjektit të të dhënave ose të një personi tjetër;
  - Nevojën për përmbushjen e një detyre në interes publik;
  - Nevojën për qëllime të interesave legjitime të kontrolluesit apo një pale të tretë, përveçse kur këto interesa tejkalohen nga interesat dhe të drejtat e subjektit të të dhënave.
- Përpunimi i të dhënave personale duhet kryer në mënyrë të drejtë.
  - Subjekti i të dhënave duhet informuar në lidhje me riskun, për të garantuar që përpunimi nuk pasoja negative të paparashikuara.
- Përpunimi i të dhënave personale duhet kryer në mënyrë transparente.
  - Kontrolluesit duhet të informojnë subjektet e të dhënave përpara se nisin përpunimin e të dhënave të tyre, midis së tjerash në lidhje me qëllimin e përpunimit dhe identitetin dhe adresën e kontrolluesit.
  - Informacioni në lidhje me aktivitetet përpunuese duhet të jepet në një gjuhë të qartë dhe të thjeshtë, për t'u mundësuar subjekteve të të dhënave që të kuptojnë lehtësisht rregullat, rreziqet, masat e sigurisë dhe të drejtat e përfshira.
  - Subjektet e të dhënave kanë të drejtën e aksesit në të dhënat e tyre kudo që ato përpunohen.

3.1.1 Ligjshmëria e përpunimit

[267] Konventa 108 e Modernizuar, neni 11, pika 1; Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 23, pika 1.
[268] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 23, pika 1.

E drejta e BE-së dhe e KiE-së në fushën e mbrojtjes së të dhënave përcakton se të dhënat personale duhen përpunuar në mënyrë të ligjshme.[269] Përpunimi i ligjshëm kërkon që pëlqimi i subjektit të të dhënave, ose një kriter tjetër legjitim të jetë i përcaktuar në legjislacionin e mbrojtjes së të dhënave.[270] Neni 6, pika 1 e GDPR-së përfshin 5 kritere ligjore për përpunimin përveç pëlqimit, d.m.th. kur përpunimi i të dhënave personale është i nevojshëm për përmbushjen e një kontrate, për përmbushjen e një detyre që kryhet në ushtrim të autoritetit publik, për përputhshmërinë me një detyrim ligjor, për qëllimin e interesave legjitime të një kontrolluesi ose pale të tretë, ose nëse është i nevojshëm për të mbrojtur interesat jetikë të subjektit të të dhënave. Kjo do të trajtohet më në hollësi në Seksionin 4.1.

3.1.2 Përpunimi i drejtë

Përveç ligjshmërisë së përpunimit, e drejta për mbrojtje të të dhënave e BE-së dhe e KiE-së kërkon edhe që të dhënat personale të përpunohen në mënyrë të drejtë.[271] Parimi i përpunimit të drejtë rregullon kryesisht marrëdhënien midis kontrolluesit dhe subjektit të të dhënave.

Kontrolluesit duhet të njoftojnë subjektet e të dhënave dhe publikun e gjerë se ata do të përpunojnë të dhënat në mënyrë të ligjshme dhe transparente dhe duhet të jenë në gjendje të demonstrojnë përputhshmërinë e aktiviteteve të përpunimit me GDPR-në. Aktivitetet e përpunimit nuk duhen kryer në fshehtësi dhe subjektet e të dhënave duhet të jenë në dijeni të risqeve të mundshme. Gjithashtu, për aq sa është e mundur, kontrolluesit duhet të veprojnë në mënyrë të tillë që dëshirat e subjektit të të dhënave të përmbushen me shpejtësi, sidomos nëse pëlqimi i tij apo i saj përbën bazën ligjore për përpunimin e të dhënave.

Shembull: tek çështja *K.H. dhe të Tjerët kundër Sllovakisë*,[272] kërkueset të cilat ishin gra me origjinë etnike rome, ishin trajtuar në dy spitale në Sllovakinë lindore gjatë shtatzënisë dhe lindjes. Më pas, asnjëra prej tyre nuk mund të mbetej shtatzënë sërish, pavarësisht përpjekjesh të përsëritura. Gjykatat vendase urdhëruan spitalet të lejonin kërkueset dhe përfaqësuesit e tyre të shihnin kartelat mjekësore dhe të bënin kopje me shkrim dore, por rrëzuan kërkesën e tyre për të fotokopjuar ato dokumente, me pretendimin se kishin për qëllim të parandalonin abuzimin me to. Ndër detyrimet pozitive që kanë shtetet sipas nenit 8 të KEDNJ-së, përfshihet domosdoshmërish detyrimi për tí vënë në dispozicion subjektit të të dhënave kopje të kartelës së të dhënave të tij apo të saj. I takonte shtetit të përcaktonte modalitetet e kopjimit të kartelave të të dhënave personale, ose kur ishte e përshtatshme, të bënte me dije arsyet detyruese për refuzimin. Në rastin e kërkueseve, gjykatat vendase e justifikuan ndalimin për të kopjuar kartelat mjekësore, kryesisht me nevojën për të mbrojtur informacionin përkatës nga abuzimi me të. Megjithatë, GJEDNJ-ja nuk gjeti arsye që ta ndihmonin të kuptonte se si këto kërkuese, të cilave gjithsesi u ishte dhënë aksesi në kartelat e plota mjekësore, mund të abuzonin me informacionin që kishte të bënte me to. Për më tepër, risku i një abuzimi mund të parandalohej me mënyra të tjera veç ndalimit të bërjes së kopjes së kartelave të kërkueseve, si për shembull duke kufizuar numrin e personave të autorizuar për të pasur akses në kartela. Shteti nuk kishte

[269] Konventa 108 e Modernizuar, neni 5, pika 3; Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5, pika 1, gërma a.
[270] Karta e të Drejtave Themelore të Bashkimit Evropian, neni 8, pika 2; Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 40 i preambulës dhe nenet 6-9; Konventa 108 e Modernizuar, neni 5, pika 2, Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 41.
[271] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5, pika 1, gërma a; Konventa 108 e Modernizuar, neni 5, pika 4, gërma a.
[272] GJEDNJ, *K.H. dhe të Tjerët k. Sllovakisë*, nr. 32881/04, 28 prill 2009.

vërtetuar ekzistencën e arsyeve bindëse për të refuzuar aksesin efikas të kërkueseve në informacionin në lidhje me shëndetin e tyre. Gjykata vendosi se kishte pasur shkelje të nenit 8.

Për sa i përket shërbimeve të internetit, karakteristikat e sistemeve të përpunimit të të dhënave duhet t'i mundësojnë subjekteve të të dhënave të kuptojnë me të vërtetë se çfarë po ndodh me të dhënat e tyre. Sido që të jetë rasti, parimi i drejtësisë shkon përtej detyrimeve të transparencës dhe mund të lidhet gjithashtu me përpunimin e të dhënave personale në mënyrë etike.

Shembull: Një departament kërkimi shkencor pranë një universiteti zhvillon një eksperiment analizimi të ndryshimit të humorit tek 50 subjekte, të cilëve u kërkohet të regjistrojnë mendimet e tyre çdo një orë në një dosje elektronike, në një orar të caktuar. Të 50 personat kanë dhënë pëlqimin e tyre për këtë projekt të caktuar dhe për përdorimin specifik të të dhënave të tyre nga universiteti. Departamenti kërkimor zbulon shpejt se regjistrimi elektronik i mendimeve do të ishte tepër i dobishëm për një projekt tjetër me fokus në shëndetin mendor, nën koordinimin e një ekipi tjetër. Megjithëse universiteti, në cilësinë e kontrolluesit, mund t'i përdorte të njëjtat të dhëna për punën e një ekipi tjetër pa qenë e nevojshme të ndërmerrte hapa të tjerë për të garantuar ligjshmërinë e përpunimit të atyre të dhënave, duke qenë se qëllimet përputhen, universiteti informoi subjektet dhe u kërkoi pëlqimin të ri, konform kodit të tij etik mbi kërkimin shkencor dhe parimit të përpunimit të drejtë.

3.1.3 Transparenca e përpunimit

Si e drejta e BE-së, ashtu edhe e drejta e KiE-së për mbrojtjen e të dhënave përcaktojnë se përpunimit i të dhënave personale duhet kryer "në mënyrë transparente kundrejt subjektit të të dhënave".[273]

Ky parim përcakton detyrimin për kontrolluesin që të marrë çdo masë të përshtatshme me qëllim që të mbajë të informuar subjektet e të dhënave, të cilat mund të jenë përdorues ose klientë, në lidhje me mënyrës se si do të përdoren të dhënat e tyre.[274] Transparenca mund t'i referohet informacionit që i jepet personit përpara nisjes së përpunimit,[275] informacionit i cili duhet të jetë lehtësisht i aksesueshëm nga subjektet e të dhënave gjatë përpunimit,[276] por gjithashtu edhe informacionit që u jepet subjekteve të të dhënave pas një kërkese për akses tek të dhënat e tyre.[277]

Shembull: tek çështja *Haralambie k. Rumanisë*,[278] kërkuesi kërkoi të kishte akses në dosjen që dispononte shërbimi sekret në lidhje me të, por kërkesa e tij u plotësua vetëm pas pesë vitesh. GJEDNJ-ja ritheksoi se individët të cilët ishin subjekte të dosjeve personale të ruajtura nga autoritetet publike, kishin interes jetik të kishin akses në to. Detyra e autoriteteve publike ishte të ofronin procedura të efektshme, për të mundësuar aksesin në këtë lloj

[273] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5, pika 1, gërma a; Konventa 108 e Modernizuar, neni 5, pika 4, gërma a dhe neni 8.
[274] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 12.
[275] *Ibid*., nenet 13 dhe 14.
[276] Grupi i Punës së Nenit 29, *Opinioni 2/2017 mbi përpunimin e të dhënave në punë*, fq. 23.
[277] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 15.
[278] GJEDNJ, *Haralambie k. Rumanisë*, nr. 21737/03, 27 tetor 2009.

informacioni. GJEDNJ-ja vlerësoi se as sasia e dosjeve të transferuara, as mangësitë e sistemit të arkivimit, nuk justifikonin vonesën pesëvjeçare të plotësimit të kërkesës së këkuesit për akses në dosjen e tij. Autoritet nuk i kishin ofruar kërkuesit procedurë të efektshme dhe të lehtë, që t'i mundësonte atij të kishte akses në dosjen personale brenda një afati kohor të arsyeshëm. Gjykata doli në përfundimin se ishte shkelur neni 8 i KEDNJ-së.

Proceset përpunuese duhet t'i shpjegohen subjekteve të të dhënave në një mënyrë lehtësisht të aksesueshme, e cila të garantojë që ata e kuptojnë se çfarë do t'u ndodhë të dhënave të tyre. Kjo do të thotë se qëllimi specifik i përpunimit të të dhënave personale duhet të jetë i ditur për subjektin e të dhënave në momentin e mbledhjes së të dhënave personale.[279] Transparenca e përpunimit ka si kriter përdorimin e një gjuhe të qartë dhe të thjeshtë.[280] Për personat e përfshirë duhet të jetë e qartë se cilat janë rreziqet, rregullat, masat e sigurisë dhe të drejtat në lidhje me përpunimin e të dhënave personale të tyre.[281]

E drejta e KiE-së përcakton gjithashtu se një informacion thelbësor i caktuar duhet t'u jepet subjekteve të të dhënave në mënyrë të detyrueshme dhe proaktive nga kontrolluesi. Informacioni në lidhje me emrin dhe adresën e kontrolluesit (ose të bashkë-kontrolluesve), bazën ligjore dhe qëllimet e përpunimit të të dhënave, kategoritë e të dhënave të përpunuara dhe të marrësve, si dhe mjetet e ushtrimit të të dhënave mund të jepet në çdo format të përshtatshme (qoftë nëpërmjet një faqeje interneti, mjeteve teknologjike në pajisjet personale, etj.), për sa kohë që informacioni i paraqitet subjektit të të dhënave në mënyrë të drejtë dhe të efektshme. Informacioni i paraqitur duhet të jetë lehtësisht i aksesueshëm, i lexueshëm, i kuptueshëm dhe i përshtatur për subjektet e të dhënave (për shembull në një gjuhë të përshtatshme për fëmijët kur është e nevojshme). Duhet dhënë gjithashtu çdo informacion shtesë që është i nevojshëm për të garantuar përpunim të drejtë të të dhënave, ose që është i nevojshëm për këtë qëllim, sikurse për kohëzgjatjen e ruajtjes së të dhënave, njohjes së arsyetimit që qëndron në themel të përpunimit të të dhënave, apo informacion mbi transferimin e të dhënave drejt një marrësi në një Palë tjetër apo një marrësi që nuk është Palë (përfshirë edhe informacionin nëse marrësi që nuk është Palë ofron nivel të përshtatshëm mbrojtjeje, apo masa të marra nga kontrolluesi për të garantuar atë nivel të përshtatshëm mbrojtjeje të dhënash).[282]

Sipas së drejtës për akses,[283] subjekti i të dhënave ka të drejtë t'i thuhet nga kontrolluesit me kërkesën e tij apo të saj, nëse të dhënat e tij apo të saj janë duke u përpunuar dhe nëse po, cilat të dhëna janë subjekt i këtij përpunimi.[284] Gjithashtu, sipas së drejtës për t'u informuar,[285] personat të dhënat e së cilëve janë përpunuar, duhen informuar nga kontrolluesi apo përpunuesi në mënyrë proaktive, ndër të tjera, për qëllimet, kohëzgjatjen, mënyrat e përpunimit, si parim përpara nisjes së aktivitetit përpunues.

Shembull: çështja *Smaranda Bara dhe të Tjerët k. Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF)* [286] kishte të bënte me transmetimin e të dhënave fiskale në lidhje me të ardhurat e personave të vetëpunësuar nga

[279] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 39.
[280] *Ibid*.
[281] *Ibid*.
[282] Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 68.
[283] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 15.
[284] Konventa 108 e Modernizuar, nenet 8 dhe 9, pika 1, gërma b.
[285] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 13 dhe 14.
[286] GJDBE, C-201/14, *Smaranda Bara dhe të Tjerët k. Casa Naţională de Asigurări de Sănătate dhe të Tjerët*, 1 tetor 2015, paragrafët 28–46.

ana e Agjencisë Kombëtare të Administrimit Fiskal tek Fondi Kombëtar i Sigurimit Shëndetësor në Rumani, bazuar tek të cilat kërkohej shlyerja e pagesave të prapambetura të kontributeve të sigurimit shëndetësor. GJDBE-së iu kërkua të përcaktonte nëse subjekti i të dhënave duhej informuar paraprakisht në lidhje me identitetin e kontrolluesit të të dhënave dhe mbi qëllimin e transmetimit të të dhënave përpara se këto të dhëna të përpunoheshin nga Fondi Kombëtar i Sigurimit Shëndetësor. GJDBE-ja vendosi se kur një organ publik administrativ i një Shteti Anëtar transmeton të dhëna personale tek një organ tjetër publik administrativ i cili i përpunon më tej ato të dhëna, subjektet e të dhënave duhen informuar në lidhje me atë transmetim apo përpunim.

Në disa situata të caktuara, lejohen përjashtime nga detyrimi për të informuar subjektet e të dhënave për përpunimin e të dhënave, të cilat do të trajtohen më në detaje në Seksionin 6.1 mbi të drejtat e subjektit të të dhënave.

3.2 Parimi i kufizimit të qëllimit

Pikat kryesore

- Qëllimi i përpunimit duhet të jetë i përcaktuar përpara se të ketë nisur përpunimi.
- Nuk mund të kryhet përpunim i mëtejshëm i të dhënave në mënyrë tillë që nuk përputhet me qëllimin fillestar, megjithëse Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave parashikon përjashtime nga ky rregull për qëllime arkivore me interes publik, për qëllime kërkimore shkencore ose historike dhe për qëllime statistikore.
- Në thelb, parimi i kufizimit të qëllimit do të thotë se çdo përpunim të dhënash personale duhet kryer për një qëllim të mirë përcaktuar dhe vetëm për qëllime specifike shtesë që janë në përputhje me qëllimin fillestar.

Parimi i kufizimit të qëllimit është një nga parimet themelore të së drejtës evropiane në fushën e mbrojtjes së të dhënave. Ai është ngushtësisht i lidhur me transparencën, parashikueshmërinë dhe kontrollin nga ana e përdoruesit: nëse qëllimi i përpunimit është i saktë dhe i qartë sa duhet, njerëzit dinë çfarë të presin dhe transparenca e siguria ligjore rriten. Njëkohësisht, përcaktimi i qartë i qëllimit është i rëndësishëm për t'u mundësuar subjekteve të të dhënave të ushtrojnë në mënyrë të efektshme të drejtat e tyre, sikurse të drejtën për të kundërshtuar përpunimin.[287]

Parimi ka si kriter që çdo përpunim të dhënash personale të kryhet për një qëllim specifik dhe të mirë përcaktuar dhe vetëm për qëllime shtesë të cilat janë në përputhje me qëllimin fillestar.[288] Përpunimi i të dhënave personale për qëllime të papërcaktuara dhe/ose të pakufizuara është për rrjedhojë i paligjshëm. Përpunimi i të dhënave personale pa një qëllim të sigurt, thjesht mbështetur në vlerësimin se mund të jetë i nevojshëm në një moment të dhënë në të ardhme, po ashtu nuk është i ligjshëm. Legjitimiteti i përpunimit të të dhënave personale do të varet nga qëllimi i përpunimit, i cili duhet të jetë eksplicit, i përcaktuar dhe legjitim.

[287] Grupi i Punës së Nenit 29 (2013), *Opinioni 3/2013 mbi kufizimin e qëllimit*, WP 203, 2 prill 2013.
[288] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5, pika 1, gërma b.

Çdo qëllim i ri për përpunimin e të dhënave që nuk është në përputhje me atë fillestar, duhet të ketë bazën ligjore përkatëse dhe nuk mund të mbështetet në faktin se të dhënat u mblodhën apo u përpunuan fillimisht për një qëllim tjetër legjitim. Nga ana tjetër, përpunimi legjitim kufizohet tek qëllimi i përcaktuar fillimisht dhe çdo qëllim i ri përpunimi do të kërkojë një bazë të re ligjore të veçantë. Për shembull, komunikimi i të dhënave personale tek palë të treta për një qëllim të ri duhet vlerësuar me kujdes, duke qenë se për këtë komunikim të dhënash mund të duhet një bazë ligjore shtesë, veçmas asaj sipas së cilës u mblodhën të dhënat.

Shembull: Një shoqëri udhëtimi ajror mbledh të dhënat e pasagjerëve të saj, për të kryer rezervime, në mënyrë që fluturimi të organizohet në mënyrën e duhur. Shoqëria e fluturimit do të ketë nevojë për të dhëna në lidhje me: numrat e poltronave të pasagjerëve; paaftësitë e mundshme fizike, sikundër nevojat për karrige me rrota; dhe kërkesat e veçanta në lidhje me dietën ushqimore, sikurse ushqimet kosher dhe hallall. Nëse shoqërive të fluturimit do t'u kërkohet që t'ua transferojnë ato të dhëna, të cilat ruhen tek Regjistri i Emrave të Pasagjerëve autoriteteve të emigracionit në aeroportin e mbërritjes, ato të dhëna po përdoren kësisoj për qëllime të kontrollit të emigracionit, çka përbën qëllim të ndryshëm nga ai parësor i mbledhjes së të dhënave. Për këtë, transferimi i këtyre të dhënave tek një autoritet i emigracionit nevojit bazë ligjore të re dhe të ndryshme.

Për të vlerësuar shtrirjen dhe kufizimet e një qëllimi të caktuar, Konventa 108 e Modernizuar dhe Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave mbështeten tek koncepti i pajtueshmërisë: përdorimi i të dhënave për qëllime të pajtueshme lejohet mbështetur në bazën ligjore fillestare. Për rrjedhojë, përpunimi i mëtejshëm i të dhënave nuk mund të bëhet në mënyrë të tillë që subjekti i të dhënave e konsideron të papritur, të papërshtatshme dhe të kundërshtueshme.[289] Për të përcaktuar nëse përpunimi i mëtejshëm duhet konsideruar i pajtueshëm, kontrolluesi duhet të marrë parasysh sa vijon (ndër të tjera):

- "çdo lidhje midis atyre qëllimeve dhe qëllimeve të përpunimin të mëtejshëm të parashikuar";
- Kontekstin në të cilin janë mbledhur të dhënat personale, sidomos sa i përket pritshmërive të arsyeshme të subjekteve të të dhënave në funksion të marrëdhënies së tyre me kontrolluesin për sa i përket përdorimit të mëtejshëm të atyre të dhënave;
- Karakterin e të dhënave personale;
- Pasojat e përpunimit të mëtejshëm të parashikuar për subjektet e të dhënave; dhe
- Ekzistencën e masave të përshtatshme të sigurisë, si në kuadrin e përpunimit fillestar, ashtu edhe në të përpunimit të mëtejshëm të parashikuar."[290] Kjo për shembull mund të bëhet nëpërmjet kriptimit apo pseudonimizimit.

Shembull: Shoqëria Sunshine përfton të dhënat e klientëve në kuadër të menaxhimit të marrëdhënieve me klientin (MMK). Ajo ia transmeton më pas ato të dhëna një shoqërie marketingu të drejtpërdrejtë, shoqërisë Moonlight, e cila dëshiron t'i përdorë këto të dhëna për të kryer fushata marketingu të shoqërive të treta. Transmetimi i të dhënave nga ana e Sunshine-it për marketing nga shoqëri të tjera përbën përdorim të mëtejshëm të të dhënave për një qëllim të ri, i cili nuk përputhet me MMK-në, që

[289] Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 49.
[290] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 50 i preambulës dhe neni 6, pika 4; Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 49.

ishte qëllimi fillestar i shoqërisë Sunshine për mbledhjen e të dhënave të klientëve. Rrjedhimisht, transmetimi i të dhënave tek shoqëria Moonlight ka nevojë për bazën e vetë ligjore.

Nga ana tjetër, përdorimi i të dhënave të MMK-së nga ana e shoqërisë Sunshine për qëllimet e vetë të marketingut, domethënë për dërgimin e mesazheve të marketingut tek klientët e saj në lidhje me produktet e saj, pranohet përgjithësisht si qëllim i pajtueshëm.

Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave dhe Konventa 108 e Modernizuar përcaktojnë se "përpunimi i mëtejshëm për qëllime arkivore në interes publik, për qëllime kërkimi shkencor ose historik apo statistikor" konsiderohet *a priori* i pajtueshëm me qëllimin fillestar.[291] Megjithatë, kur të dhënat personale përpunohen më tej, duhen marrë masat e përshtatshme të sigurisë, si për shembull anonimizimi, kriptimi ose pseudonimizimi i të dhënave dhe kufizimi i aksesit tek të dhënat.[292] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave shton se "kur subjekti i të dhënave ka dhënë pëlqimin, ose kur përpunimi bazohet në të drejtën evropiane ose të shtetit anëtar që përbën një masë të nevojshme dhe proporcionale në një shoqëri demokratike për të garantuar, në veçanti, objektivat e rëndësishëm me interes të përgjithshëm publik, kontrolluesi duhet të lejohet të përpunojë më tej të dhënat personale pavarësisht përputhshmërisë së qëllimeve".[293] Pra, kur kryhet përpunim i mëtejshëm i të dhënave, subjekti i të dhënave duhet të informohet në lidhje me qëllimet, si dhe me të drejtat e tij apo të saj, sikurse për të drejtën për të kundërshtuar.[294]

Shembull: Shoqëria Sunshine ka mbledhur dhe mbajtur të dhënat e Menaxhimit të Marrëdhënieve me Klientin (MMK) në lidhje me klientët e saj. Përdorimi i mëtejshëm i këtyre të hënave nga shoqëria Sunshine për analizim statistikor të sjelljes në lidhje me blerjen nga ana e klientëve të saj, është i lejuar, meqenëse statistikat përbëjnë qëllim të pajtueshëm. Nuk nevojitet bazë ligjore shtesë, si për shembull pëlqimin i subjekteve të të dhënave. Megjithatë, për përpunimin e mëtejshëm të të dhënave personale për qëllime statistikore, shoqëria Sunshine duhet të marrë masat e përshtatshme të sigurisë për të garantuar të drejtat dhe liritë e subjektit të të dhënave. Masat teknike dhe organizative që Sunshine-i duhet të zbatojë mund të përfshijnë pseudonimizimin.

3.3 Parimi i minimizimit të të dhënave

Pikat kryesore

- Përpunimi i të dhënave duhet kufizuar vetëm në atë çka është e nevojshme për të përmbushur qëllimin legjitim.
- Përpunimi i të dhënave personale duhet kryer vetëm atëherë kur qëllimi i përpunimit nuk mund të përmbushet në mënyrë të arsyeshme me mjete të tjera.
- Përpunimi i të dhënave nuk mund të ndërhyjë në mënyrë jo proporcionale tek interesat, të drejtat dhe liritë e tjera të përfshira.

[291] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5, pika 1, gërma b; Konventa 108 e Modernizuar, neni 5, pika 4, gërma b. Një shembull i këtyre dispozitave në nivel kombëtar është Ligji Austriak për Mbrojtjen e të Dhënave (Datenschutzgesetz), Fletorja e Ligjit Federal I, nr. 165/1999, paragrafi 46.
[292] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 6, pika 4; Konventa 108 e Modernizuar, neni 5, pika 4, gërma b; Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 50.
[293] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 50 i preambulës.
[294] *Ibid*.

Duhen përpunuar vetëm të dhënat që janë: "të përshtatshme, të rëndësishme dhe të kufizuara në lidhje me qëllimet për të cilat ato janë mbledhur dhe/ose përpunuar më tej".[295] Kategoritë e të dhënave të zgjedhura për përpunimin duhet të jenë të nevojshme për përmbushjen e objektivit të përgjithshëm të deklaruar të aktiviteteve përpunuese dhe kontrolluesi duhet të kufizojë me rigorozitet në minimumin e mundshëm mbledhjen e të dhënave vetëm në informacionet që janë drejtpërdrejt të rëndësishme për qëllimin specifik që synon të arrijë përpunimi.

Shembull: Tek çështja *Digital Rights Ireland*,[296] GJDBE-ja shqyrtoi vlefshmërinë e Direktivës për Mbajtjen e të Dhënave e cila synonte harmonizimin e dispozitave kombëtare në lidhje me mbajtjen e të dhënave personale të gjeneruara apo përpunuara nga shërbimet ose rrjetet të komunikimeve elektronike të aksesueshme për publikun, për transmetimin e tyre të mundshëm tek autoritetet kompetente për luftën ndaj krimeve të rënda, sikurse krimi i organizuar dhe terrorizmi. Pavarësisht se ky qëllim u vlerësua nga Gjykata si një qëllim që në thelb përmbush një objektiv me interes të përgjithshëm, mënyra e përgjithësuar sipas së cilës Direktiva shtrihej "mbi të gjithë personat dhe mjetet e komunikimit elektronik, si dhe mbi të dhënat e trafikut, pa bërë asnjë dallim, kufizim, apo përjashtim, në funksion të objektivit të luftës kundër krimeve të rënda", u konsiderua problematike.[297]

Gjithashtu, nëpërmjet përdorimit të teknologjive speciale që përforcojnë privatësinë, është ndonjëherë e mundur të shmanget plotësisht përdorimi i të dhënave personale, ose të zbatohen masa që mundësojnë reduktimin e mundësisë për të lidhur të dhënat me subjektin (për shembull nëpërmjet pseudonimizimit), e cila është një zgjidhje që respekton privatësinë. Diçka e tillë është veçanërisht e përshtatshme në kuadrin e sistemeve të përpunimit me shtrirje më të gjerë.

Shembull: këshilli bashkiak i një qyteti vë në dispozicion një kartë me çip për përdoruesit e rregullt të transportit publik qytetas, kundrejt një tarife të caktuar. Karta përmban emrin e përdoruesit në formë të shkruar në sipërfaqe të saj dhe po ashtu në formë elektronike, në çip. Sa herë që udhëtari përdor autobusin apo tramvajin, karta duhet të vendoset përballë pajisjes lexuese të instaluar në autobus apo tramvaj. Të dhënat e lexuara nga pajisja, kontrollohen elektronikisht me një bazë të dhënash që përmban emrat e njerëzve të cilët kanë blerë kartën e udhëtimit.

Ky lloj sistemi nuk përputhet plotësisht me parimin e minimizimit të të dhënave: kontrolli i një individi nëse ai lejohet të përdorë mjetet e transportit, mund të bëhet pa pasur nevojë për krahasim të të dhënave personale të çipit të kartës me bazën e të dhënave. Do të mjaftonte për shembull, pajisja me një imazh elektronik special, sikurse një barkod mbi kartë, e cila kur të kalohej përpara pajisjes lexuese, do të konfirmonte vlefshmërinë e saj. Ky lloj sistemi nuk do të regjistronte se kush dhe kur përdoren mjetet e transportit. Kjo do të ishte zgjidhja optimale në kuptim të parimit të minimizimit, duke qenë se ky parim krijon detyrimin për minimizimin e mbledhjes së të dhënave.

Neni 5, pika 1 e Konventës 108 të Modernizuar përcakton një kriter proporcionalitetit për përpunimin e të dhënave personale në raport me qëllimin legjitim të ndjekur. Të gjithë interesat e përfshirë në të gjithë etapat e përpunimit duhen ekuilibruar në mënyrë të drejtë. Kjo do të thotë se "të dhënat personale të cilat janë të përshtatshme dhe të rëndësishme, por të cilat mund të shkaktojnë ndërhyrje jo proporcionale tek të drejtat dhe liritë themelore të përfshira, duhet të konsiderohen si të tepërta".[298]

[295] Konventa 108 e Modernizuar, neni 5, pika 4, gërma c; Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5, pika 1, gërma c.
[296] GJDBE, Çështje të bashkuara C-293/12 dhe C-594/12, *Digital Rights Ireland Ltd k. Minister for Communications, Marine and Natural Resources dhe të Tjerët* dhe *Kärntner Landesregierung dhe të Tjerët* [ÇB] , 8 prill 2014.
[297] *Ibid*., paragrafët 44 dhe 57.
[298] Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 52; Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5, pika 1, gërma c.

3.4 Parimi i saktësisë së të dhënave

Pikat kryesore

- Parimi i saktësisë së të dhënave duhet zbatuar nga kontrolluesi në të gjitha aktivitetet përpunuese.
- Të dhënat e pasakta duhen fshirë ose korrigjuar pa vonesë.
- Të dhënat mund të jetë e nevojshme të kontrollohen dhe të përditësohen rregullisht për të garantuar saktësinë e tyre.

Kontrolluesi i cili mban informacione personale nuk t'i përdorë ato pa marrë masa për të garantuar me një siguri të arsyeshme se të dhënat janë të sakta dhe të përditësuara.[299]

Detyrimi për të garantuar saktësinë e të dhënave duhet vlerësuar në kontekstin e qëllimit të përpunimit të të dhënave.

Shembull: Tek çështja *Rijkeboer*,[300] GJDBE-ja shqyrtoi kërkesën e një shtetasi holandez për të marrë informacion nga administrata vendore e qytetit të Amsterdamit, në lidhje me identitetin e personave të cilëve u ishin komunikuar gjatë dy viteve paraardhëse të dhënat në lidhje me të nga ana e autoritetit vendor, si dhe mbi përmbajtjen e të dhënave të komunikuara. GJDBE-ja deklaroi se "e drejta për privatësi nënkupton që subjekti i të dhënave të mund të jetë i bindur se të dhënat e tij personale janë përpunuar në mënyrë korrekte dhe të ligjshme, që do të thotë sidomos se të dhënat bazë në lidhje me të janë të sakta dhe se ato u komunikohen marrësve të autorizuar". Gjykata iu referua në vijim preambulës së Direktivës së Mbrojtjes së të Dhënave, e cila përcakton se subjektet e të dhënave duhet të gëzojnë të drejtën e aksesit tek të dhënat e tyre personale, me qëllim që të verifikojnë nëse të dhënat janë të sakta.[301]

Në disa raste, përditësimi i të dhënave të mbajtura është i ndaluar me ligj, për shkak se qëllimi i mbajtjes së të dhënave është kryesisht për të dokumentuar ngjarje si "imazhe" historike.

Shembull: Kartela shëndetësore e një operacioni nuk mund të ndryshohet, ose thënë ndryshe 'përditësohet', edhe sikur konkluzionet që përmenden në kartelë të dalin më vonë si të gabuara. Në rrethana të tilla, mund të bëhen vetëm shtesa të shënimeve të mbajtura në kartelë, me kusht që ato të etiketohen qartë si shtesa të bëra në një fazë të mëvonshme.

Nga ana tjetër, ka edhe situata ku është absolutisht e nevojshme të përditësohen e të kontrollohet rregullisht saktësia e të dhënave, për shkak të dëmtimit që ka mundësi t'i shkaktohet subjektit të të dhënave nëse të dhënat do të mbeteshin të pasakta.

Shembull: Nëse një person dëshiron të lidhë një kontratë kredie me një institucion bankar, zakonisht banka do të verifikojë përshtatshmërinë e kreditorit për klientin e saj të mundshëm. Për këtë qëllim, ekzistojnë baza të dhënash që përmbajnë të dhëna në lidhje me historikun e kreditimit të individëve. Nëse kjo bazë të dhënash përmban të dhëna të pasakta apo të pa përditësuara në lidhje me një person, ky i fundit mund të ketë pasoja të dëmshme. Rrjedhimisht, kontrolluesit e këtyre bazave të të dhënave duhet të angazhohen në mënyrë të veçantë për të përmbushur parimin e saktësisë

[299] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5, pika 1, gërma d.
[300] GJDBE, C-553/07, *College van burgemeester en wethouders van Rotterdam k. M. E. E. Rijkeboer*, 7 maj 2009.
[301] Paragrafi 41 i preambulës së Direktivës 95/46/EC.

3.5 Parimi i kufizimit të mbajtjes së të dhënave

Pikat kryesore

- Parimi i kufizimit të mbajtjes së të dhënave do të thoë se të dhënat personale duhen fshirë, ose duhen anonimizuar menjëherë sapo ato të mos jenë më të nevojshme për qëllimet për të cilat ishin mbledhur.

Në nenin 5, pika 1, gërma "e" të GDPR-së dhe po ashtu edhe në nenin 5, pika 4, gërma "e" të Konventës 108 të Modernizuar përcaktohet se të dhënat personale "duhen mbajtur në formë të tillë që lejon identifikimin e subjekteve të të dhënave për një kohë jo më të gjatë se sa është e nevojshme për qëllimet për të cilat të dhënat janë përpunuar". Si pasojë, të dhënat duhen fshirë ose anonimizuar kur këto qëllime janë përmbushur. Për këtë qëllim, "kontrolluesi duhet të përcaktojë afatet kohore për fshirjen apo vlerësimin periodik të tyre", për t'u siguruar që të dhënat nuk po mbahen më gjatë se sa është e nevojshme.[302]

Tek çështja *S. And Marper*, GJEDNJ-ja vendosi se parimet themelore të instrumenteve përkatëse të Këshillit të Evropës, ashtu si dhe të legjislacionit e praktikës së Palëve Kontraktuese, përcaktojnë se mbajtja e të dhënave duhet të jetë proporcionale në raport me qëllimin e mbledhjes dhe të kufizuara në kohë, sidomos në sektorin e policisë.[303]

Shembull: Tek çështja *S. and Marper*,[304] GJEDNJ-ja vendosi se mbajtja e pakufizuar e gjurmëve të gishtave, kampioneve qelizore dhe profileve të ADN-së të dy kërkuesve, ishte jo proporcionale dhe e panevojshme në një shoqëri demokratike, duke pasur parasysh se procedimi penal kundër të dy kërkuesve kishte përfunduar respektivisht me një vendim pafajësie dhe një pushim çështjeje.

Kufizimi kohor për mbajtjen e të dhënave personale gjen zbatim vetëm për të dhënat të cilat mbahen në formë të tillë që lejon identifikimin e subjekteve të të dhënave. Për rrjedhojë, mbajtja e ligjshme e të dhënave të cilat nuk nevojiten më, mund të arrihet me anë të anonimizimit të të dhënave.

Arkivimi i të dhënave në interesin publik, për qëllime shkencore apo historike, ose për përdorim statistikor, mund të bëhet për periudha të gjata kohore, me kusht që këto të dhëna të përdoren vetëm për qëllimet e mësipërme.[305] Me qëllim mbrojtjen e të drejtave dhe lirive të subjektit të të dhënave, për mbajtjen dhe përdorimin e vijueshëm të të dhënave personale, duhen zbatuar masat e përshtatshme teknike dhe organizative.

Konventa 108 e Modernizuar lejon gjithashtu përjashtime nga parimi i kufizimit të mbajtjes, me kusht që ato të jenë të përcaktuara me ligj, të respektojnë thelbin e të drejtave dhe lirive themelore dhe të jenë të nevojshme dhe proporcionale për përmbushjen e një numri të kufizuar qëllimesh legjitime.[306] Ndër të tjera, përfshihen në to mbrojtja e sigurisë kombëtare, hetimi dhe ndjekja e veprave penale, ekzekutimi i dënimeve penale, mbrojtja e subjektit të të dhënave dhe mbrojtja e të drejtave dhe lirive themelore të të tjerëve.

Shembull: tek çështja *Digital Rights Ireland*,[307] GJDBE-ja shqyrtoi vlefshmërinë e Direktivës për Mbajtjen e të Dhënave, e cila synonte harmonizimin e dispozitave kombëtare në lidhje me mbajtjen e

[302] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 39 i preambulës.
[303] GJEDNJ, *S. and Marper k. Mbretërisë së Bashkuar*, [ÇB] , nr. 30562/04 dhe 30566/04, 4 dhjetor 2008; shih gjithashtu për shembull: GJEDNJ, *M.M. k. Mbretërisë së Bashkuar*, nr. 24029/07, 13 nëntor 2012.
[304] GJEDNJ, *S. and Marper k. Mbretërisë së Bashkuar* [ÇB] , nr. 30562/04 dhe 30566/04, 4 dhjetor 2008.
[305] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 5, pika 1, gërma "e"; Konventa 108 e Modernizuar, neni 5, pika 4, gërma "b" dhe 11, pika 2.
[306] Konventa 108 e Modernizuar, neni 11, pika 1; Raporti Shpjegues i Konventës 108 të Modernizuar, neni 5, pika 4, gërma b dhe 11, pika 2.
[307] GJDBE, Çështje të bashkuara C-293/12 dhe C-594/12, *Digital Rights Ireland Ltd k. Minister for Communications, Marine and Natural Resources dhe të Tjerët* dhe *Kärntner Landesregierung dhe të Tjerët* [ÇB] , 8 prill 2014.

të dhënave personale të gjeneruara ose përpunuara nëpërmjet shërbimeve ose rrjeteve të komunikimeve elektronike të aksesueshme për publikun, për të luftuar krimet e rënda, sikurse krimin e organizuar dhe terrorizmin. Direktiva për Mbajtjen e të Dhënave detyronte mbajtjen e të dhënave për "të paktën gjashtë muaj, pa bërë dallim ndërmjet kategorive të të dhënave të parashikuara në nenin 5 të kësaj Direktive, për shkak të dobisë së mundshme të tyre për qëllime të objektivit të ndjekur apo sipas personave të përfshirë".[308] GJDBE-ja ngriti gjithashtu çështjen e mungesës së kritereve objektive në Direktivën për Mbajtjen e të Dhënave, mbi të cilët të përcaktohej afati kohor i saktë i mbajtjes së të dhënave – i cili mund të shkonte nga një minimum prej gjashtë muajsh, tek maksimumi 24 muaj – për të garantuar që ai afat kohor të kufizohej vetëm në nevojën absolute.[309]

3.6 Parimi i sigurisë së të dhënave

Pikat kryesore

- Siguria dhe konfidencialiteti i të dhënave personale janë thelbësore për parandalimin e pasojave negative ndaj subjektit të të dhënave.
- Masat e sigurisë mund të jenë të natyrës teknike dhe/ose organizative.
- Pseudonimizimi është një proces i cili mund të mbrojë të dhënat personale.
- Përcaktimi nëse masat e sigurisë janë të përshtatshme, duhet bërë rast pas rasti dhe me rishikimin periodik.

Parimi i sigurisë së të dhënave përcakton se duhen zbatuar masa të përshtatshme teknike dhe organizative kur përpunohen të dhëna personale, për të mbrojtur të dhënat nga aksesi rastësor, u paautorizuar ose i paligjshëm, përdorimi, modifikimi, përhapja, humbja, shkatërrimi ose dëmtimi.[310] GDPR-ja përcakton se kontrolluesi dhe përpunuesi duhet të marrin parasysh "gjendjen e teknologjisë, shpenzimet e zbatimit dhe natyrën, objektin, kontekstin dhe qëllimet e përpunimit si dhe riskun e probabilitetit të ndryshueshëm dhe ashpërsisë ndaj të drejtave dhe lirive të personave fizikë" kur zbatojnë këto masa.[311] Në varësi të rrethanave specifike në secilin rast, masat e përshtatshme teknike dhe organizative duhet të përfshijnë, për shembull, pseudonimizimin dhe kriptimin e të dhënave personale dhe/ose testimin periodik dhe vlerësimin e efektshmërisë së masave, për të garantuar sigurinë e përpunimit të të dhënave.[312]

Sikurse shpjegohet në Seksionin 2.1.1, pseudonimizim të dhënash do të thotë zëvendësimi i cilësive tek të dhënat personale – të cilat bëjnë të mundur identifikimin e subjektit të të dhënave – me pseudonim dhe mbajtja e këtyre cilësive të veçuara, me masa teknike ose organizative. Procesi i pseudonimizimit nuk duhet ngatërruar me procesin e anonimizimit, ku të gjitha fijet që identifikojnë personin janë të shkëputura.

Shembull: për shembull, fjalia "Charles Spencer, lindur më 3 prill 1967, është babai i një familjeje me katër fëmijë, dy djem dhe dy vajza" mund të pseudonimizohet si vijon:

"C.S. 1967 është babai i një familjeje me katër fëmijë, dy djem dhe dy vajza"; ose

[308] *Ibid.,* paragrafi 63.
[309] *Ibid*., para. 64.
[310] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 39 i preambulës dhe neni 5, pika 1, gërma f; Konventa 108 e Modernizuar, neni 7.
[311] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 32, pika 1.
[312] *Ibid*.

"324 është babai i një familjeje me katër fëmijë, dy djem dhe dy vajza"; ose

"YESz320l është babai i një familjeje me katër fëmijë, dy djem dhe dy vajza".

Përdoruesit të cilët aksesojnë të dhënat e pseudonimizuara zakonisht nuk do të mund të identifikojnë "Charles Spencer-in, lindur më 3 prill 1967" nëpërmjet "324" apo "YESz3201". Rrjedhimisht, këto të dhëna kanë më shumë të ngjarë të jenë të sigurta nga keqpërdorimi.

Megjithatë, shembulli i parë ofron më pak siguri. Nëse fjalia "C. S. 1967 është babai i një familjeje me katër fëmijë, dy djem dhe dy vajza" përdoret brenda fshatit të vogël në të cilin jeton Charles Spencer-i, z. Spencer mund të identifikohet lehtësisht. Metoda e përdorur për pseudonimizimin mund të cënojë efektshmërinë e mbrojtjes së të dhënave.

Të dhënat personale me cilësi të kriptuara ose të mbajtura të veçuara përdoren në shumë kontekste si një mënyrë për të mbajtur sekret identitetet personale. Diçka e tillë është veçanërisht e dobishme kur kontrolluesit e të dhënave duhet të sigurohen se janë duke trajtuar të njëjtët subjekte të të dhënave, por nuk kanë nevojë, apo nuk duhet të kenë identitetet reale të subjekteve të të dhënave. Një rast për shembull është kur një shkencëtar studion zhvillimin e një sëmundjeje tek pacientët, identiteti i së cilëve dihet vetëm nga spitali ku ata trajtohen dhe nga i cili studiuesi merr kartelat e pseudonimizuara. Për rrjedhojë, pseudonimizimi është një lidhje e fortë në arsenalin e teknologjive përforcuese të privatësisë. Ai mund të funksionojë si një element i rëndësishëm kur zbatohet privatësia që në fazën e konceptimit (*privacy by design*), e cila do të thotë të kesh mbrojtje të të dhënave të integruar në strukturën e sistemeve të përpunimit të të dhënave.

Neni 25 i GDPR-së, i cili trajton mbrojtjen e të dhënave që në fazën e konceptimit, i referohet shprehimisht pseudonimizimit si shembull i një mase të përshtatshme teknike dhe organizative që kontrolluesit duhet të zbatojnë për të respektuar parimet e mbrojtjes së të dhënave dhe për të integruar masat e nevojshme të sigurisë. Duke vepruar kësisoj, kontrolluesit do të zbatojnë kriteret e rregullores dhe do të mbrojnë të drejtat e subjekteve të të dhënave kur përpunojnë të dhënat e tyre personale.

Angazhimi në një kod të miratuar sjelljeje, ose në një mekanizëm të miratuar certifikimi do t'i ndihmonte të demonstronin përputhshmërinë me kriterin e sigurisë së përpunimit.[313] Në Opinionin e saj mbi problematikat për mbrojtjen e të dhënave nga përpunimi i Regjistrit të Emrave të Pasagjerëve, Këshilli i Evropës ofron shembuj të tjerë masash të përshtatshme sigurie për mbrojtjen e të dhënave personale në sistemet e regjistrit të emrave të pasagjerëve. Të tilla përfshijnë mbajtjen e të dhënave në një mjedis fizik të sigurt, kufizimin e aksesit nëpërmjet identifikimit të shtresëzuar dhe mbrojtjen e komunikimit të të dhënave nëpërmjet kriptografimit rigoroz.[314]

Shembull: rrjetet sociale dhe operatorët e shërbimeve të postës elektronik bëjnë të mundur [ër përdoruesit që të shtojnë një shtresë tjetër sigurie të dhënash për shërbimet që ata ofrojnë, nëpërmjet përdorimit të autentifikimit me dy nivele. Përveç vendosjes së një fjalëkalimi personal, përdoruesit duhet të kryejnë një identifikim të dytë në mënyrë që të aksesojnë llogarinë e tyre personale. Ky identifikim i dytë mund të jetë për shembull një kod sigurie që dërgohet tek telefoni celular i cili është i lidhur me llogarinë personale. Kësisoj, verifikimi në dy kohë ofron mbrojtje më të mirë të informacionit personal ndaj aksesit të paautorizuar tek llogaritë personale nëpërmjet piraterisë kompjuterike.

Raporti Shpjegues i Konventës 108 të Modernizuar paraqet shembuj të tjerë masash të përshtatshme sigurie, si për shembull zbatimi i detyrimit për sekret profesional, apo miratimi i masave të veçanta të sigurisë teknike, sikurse është kriptimi i të dhënave.[315] Për të zbatuar masa specifike sigurie, kontrolluesi, ose përpunuesi sipas rastit, duhet të marrë parasysh disa elemente, sikurse karakterin dhe vëllimin e të dhënave personale të përpunuara, pasojat e mundshme negative tek subjektet e të dhënave

[313] *Ibid*., neni 32, pika 3.
[314] Këshilli i Evropës, Komiteti i Konventës 108, *Opinion mbi problematikat për mbrojtjen e të dhënave nga përpunimi i Regjistrit të Emrave të Pasagjerëve*, T-PD(2016)18rev, 19 gusht 2016, fq. 9.
[315] Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 56.

dhe nevojën për kufizim të aksesit tek të dhënat.[316] Kur zbatohen masat e përshtatshme të sigurisë, duhen pasur parasysh metodat dhe teknikat bashkëkohore të sigurisë së të dhënave për përpunimin e të dhënave. Kostot e këtyre masave duhet të jenë proporcionale në raport me seriozitetin dhe probabilitetin e rreziqeve të mundshme. Është i nevojshëm rishikimi periodik i tyre, në mënyrë që të përditësohen nëse duhet.[317]

Në rastet kur ndodhin shkelje ndaj të dhënave personale, si Konventa 108 e Modernizuar, ashtu edhe GDPR-ja përcaktojnë se kontrolluesi duhet të njoftojë pa vonesa të panevojshme autoritetin kompetent mbikëqyrës në lidhje me shkeljen e cila paraqet rrezik për të drejtat dhe liritë e personave.[318] Ekziston një detyrim i ngjashëm njoftimi të subjektit të të dhënave, kur shkelja ndaj të dhënave personale ka gjasa të rezultojë në risk të lartë për të drejtat dhe liritë e tij apo të saj.[319] Njoftimi i subjekteve të të dhënave për këtë lloj shkeljeje duhet bërë me një gjuhë të qartë dhe të thjeshtë.[320] Nëse përpunuesi merr dijeni për një shkelje ndaj të dhënave, duhet të njoftojë kontrolluesin menjëherë.[321] Në situata të caktuara, mund të bëhen përjashtime nga detyrimi për njoftim. Për shembull, kontrolluesi nuk është i detyruar të njoftojë autoritetin mbikëqyrës kur "shkelja ndaj të dhënave nuk ka gjasa të rezultojë në risk për të drejtat dhe liritë e personave fizikë".[322] Po ashtu, nuk është e nevojshme të njoftohet subjekti i të dhënave kur masat e sigurisë që janë marrë i kanë bërë të dhënat të pakuptueshme për personat e paautorizuar, ose kur masat vijuese të ndërmarra se risku i lartë nuk ka më gjasa të realizohet.[323] Nëse komunikimi i një shkeljeje ndaj të dhënave drejtuar subjekteve të të dhënave do të kërkonte nga kontrolluesi përpjekje jo proporcionale, një komunikim publik apo një masë e ngjashme mund të garantojnë që "subjektet e të dhënave janë informuar në një mënyrë njëlloj të efektshme".[324]

3.7 Parimi i përgjegjshmërisë

Pikat kryesore

- Përgjegjshmëria detyron kontrolluesit dhe përpunuesit të zbatojnë në mënyrë aktive dhe të pandërprerë masa për të nxitur dhe garantuar mbrojtjen e të dhënave në aktivitetet e tyre të përpunimit.
- Kontrolluesit dhe përpunuesit janë përgjegjës për përputhshmërinë e aktiviteteve të tyre përpunuese me legjislacionin e mbrojtjes së të dhënave dhe detyrimeve të tyre përkatëse.
- Kontrolluesit duhet të jenë në gjendje në çdo moment t'u demonstrojnë subjekteve të të dhënave, publikut të gjerë dhe autoriteteve mbikëqyrëse përputhshmërinë e tyre me dispozitat e mbrojtjes së të dhënave. Përpunuesit duhet gjithashtu të zbatojnë disa detyrime që lidhen ngushtë me përgjegjshmërinë (sikurse mbajtja e regjistrit të aktiviteteve të përpunimit dhe caktimin e një Nëpunësi për Mbrojtjen e të Dhënave).

GDPR-ja dhe Konventa 108 e Modernizuar përcaktojnë se kontrolluesi është përgjegjës dhe duhet të jetë në gjendje të demonstrojë respektimin e parimeve që zbatohen për përpunimin e të dhënave personale të përshkruara në këtë kapitull.[325] Për këtë qëllim, kontrolluesi duhet të zbatoj masat e përshtatshme teknike dhe organizative.[326] Pavarësisht se parimi i përgjegjshmërisë së parashikuar në nenin 5, pika 2 të GDPR-së i drejtohet vetëm kontrolluesve, edhe nga përpunuesit pritet përgjegjshmëri, duke qenë se ata duhet të respektojnë shumë detyrime dhe sepse kanë një marrëdhënie të drejtpërdrejtë me përgjegjshmërinë.

---

[316] *Ibid*., paragrafi 62.
[317] *Ibid., paragrafi 63.*
[318] Konventa 108 e Modernizuar, neni 7, pika 2; Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 33, pika 1.
[319] Konventa 108 e Modernizuar, neni 7, pika 2; Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 34, pika 1.
[320] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 34, pika 2.
[321] *Ibid.,* neni 33, pika 1.
[322] *Ibid*.
[323] *Ibid*., neni 34, pika 3, gërmat a dhe b.
[324] *Ibid*., neni 34, pika 3, gërma c.
[325] *Ibid*., neni 5, pika 2; Konventa 108 e Modernizuar, neni 10, pika 1.
[326] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 24.

E drejta e BE-së dhe e KiE-së në fushën e mbrojtjes së të dhënave përcakton se kontrolluesi është përgjegjës dhe duhet të jetë në gjendje të garantojë përputhshmërinë me parimet e mbrojtjes së të dhënave të trajtuara në Seksionet 3.1 dhe 3.6.[327] Grupi i Punës së Nenit 29 thekson se "lloji i procedurave dhe mekanizmave ndryshon në përputhje me rreziqet që paraqet përpunimi dhe karakteri i të dhënave".[328]

Kontrolluesit mund të lehtësojnë plotësimin e këtij kriteri në mënyra të ndryshme, përfshirë:

- Mbajtjen e një regjistri të aktiviteteve të përpunimit dhe ia paraqet autoritetit mbikëqyrës me kërkesë;[329]
- Në situata të caktuara, caktimi i një nëpunësi për mbrojtjen e të dhënave i cili është i përfshirë në të gjitha çështjet që lidhen me mbrojtjen e të dhënave;[330]
- Kryen vlerësime të ndikimit tek mbrojtja e të dhënave për llojet e përpunimit të cilat ka gjasa të paraqesin risk të lartë për të drejtat dhe liritë e personave fizikë;[331]
- Garantimin e mbrojtjes së të dhënave që në fazën e konceptimit dhe me parapërzgjedhje;[332]
- Zbatimin e modaliteteve dhe procedurave për ushtrimin e të drejtave të subjekteve të të dhënave;[333]
- Angazhimin në një kod të miratuar sjelljeje apo mekanizëm certifikimi.[334]

Pavarësisht se parimi i përgjegjshmërisë së nenit 5, pika 2 të GDPR-së nuk i drejtohet specifikisht përpunuesve, disa dispozita që lidhen me përgjegjshmërinë përcaktojnë detyrime për ta, si për shembull mbajtjen e regjistrit të aktiviteteve përpunuese dhe caktimin e Nëpunësit të Mbrojtjes së të Dhënave për të gjitha aktivitet përpunuese për të cilat duhet një i tillë.[335] Përpunuesit duhet po ashtu të garantojnë që janë zbatuar të gjitha masat e nevojshme për të garantuar sigurinë e të dhënave.[336] Kontrata ligjërisht detyruese e lidhur midis kontrolluesit dhe përpunuesit duhet të përcaktojë që përpunuesi duhet të ndihmojë kontrolluesin në përmbushjen e disa detyrimeve, si për shembull kur kryen vlerësimin e ndikimit tek mbrojtja e të dhënave, apo të njoftojë kontrolluesin për çdo shkelje ndaj të dhënave personale menjëherë pasi konstatohet një e tillë.[337]

Organizata për Bashkëpunim dhe Zhvillim Ekonomik (OECD) ka miratuar në 2013-ën udhëzuesin mbi privatësinë, i cili thekson se kontrolluesit kanë rol të rëndësishëm në funksionimin e mbrojtjes së të dhënave në praktikë. Ky udhëzues përmban një parim të përgjegjshmërisë, në masën që "kontrolluesi i të dhënave duhet të jetë përgjegjës për respektimin e masave të cilat u japin efekt parimeve [materiale] të përcaktuara më lart."[338]

Shembull: Amendimi në vitin 2009[339] i Direktivës së e-Privatësisë 2002/58/EC është një shembull legjislativ që thekson parimin e përgjegjshmërisë. Sipas nenit 4 të variantit të ndryshuar, direktiva përcakton detyrimin për të "garantuar zbatimin e një politike sigurie për përpunimin e të dhënave

[327] *Ibid*., neni 5, pika 2; Konventa 108 e Modernizuar, neni 10, pika 1.
[328] Grupi i Punës së Nenit 29, *Opinioni 3/2010 mbi parimin e përgjegjshmërisë*, WP 173, Bruksel, 13 korrik 2010, paragrafi 12.
[329] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 30.
[330] *Ibid*., nenet 37-39.
[331] *Ibid*., neni 35; Konventa 108 e Modernizuar, neni 10, pika 2.
[332] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 25; Konventa 108 e Modernizuar, neni 10, pikat 2 dhe 3.
[333] *Ibid*., nenet 12 dhe 24.
[334] *Ibid*., nenet 40 dhe 42.
[335] *Ibid*., nenet 5, pika 2, 30 dhe 37.
[336] *Ibid*., neni 28, pika 3, gërma c.
[337] *Ibid*., neni 28, pika 3, gërma d.
[338] OECD (2013), Udhëzuesi në lidhje me mbrojtjen e privatësisë dhe qarkullimeve ndërkufitare të të dhënave personale, neni 14.
[339] Direktiva 2009/136/EC e Parlamentit Evropian dhe e Këshillit e 25 nëntorit 2009, që ndryshon Direktivën 2002/22/EC mbi shërbimin universal dhe të drejtat e përdoruesve në lidhje me rrjetet dhe shërbimet e komunikimeve elektronike; Direktivën 2002/58/EC e përpunimit të të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike dhe Rregulloren (EC) nr. 2006/2004 e bashkëpunimit ndërmjet autoriteteve kombëtare përgjegjëse për zbatimin e ligjeve të mbrojtjes së konsumatorëve, FZ 2009 L 337, fq. 11

personale". Kësisoj, për sa i përket dispozitave të direktivës në lidhje me sigurinë, legjislatori ka gjykuar të nevojshme përfshirjen e një kriteri të qartë për ekzistencën dhe zbatimin e politikës së sigurisë.

Sipas opinionit të Grupit të Punës së Nenit 29[340], thelbi i përgjegjshmërisë është detyrimi i kontrolluesit:

- Për të zbatuar masa të cilat, në rrethana normale, garantojnë respektimin e rregullave të mbrojtjes së të dhënave në kontekstin e aktiviteteve përpunuese; dhe
- Për të pasur gati dokumentacionin që u vërteton subjekteve të të dhënave dhe autoriteteve mbikëqyrëse se çfarë masash janë marrë për respektimin e rregullave të mbrojtjes së të dhënave.

Në këtë mënyrë, parimi i përgjegjshmërisë detyron kontrolluesit të demonstrojnë në mënyrë aktive zbatimin e ligjit dhe jo thjesht të presin që subjektet e të dhënave apo autoritetet mbikëqyrëse t'u sinjalizojnë parregullsitë.

4 Rregullat e së drejtës evropiane në fushën e mbrojtjes së të dhënave

BE	Çështje të trajtuara	KiE
Rregullat në lidhje me përpunimin e ligjshëm të të dhënave		

[340] *Opinioni 3/2010 mbi parimin e përgjegjshmërisë* i Grupit të Punës së Nenit 29, WP 173, Bruksel, 13 korrik 2010.

Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 6, pika 1, gërma a GJDBE, C-543/09, *Deutsche Telekom AG k. Bundesrepublik Deutschland*, 2011 GJDBE, C-536/15, *Tele2 (Netherlands) BV dhe të Tjerët k. Autoriteit Consument en Markt (AMC)*, 2017	Pëlqimi	Rekomandimi mbi Profilizimin, nenet 3.4 (b) dhe 3.6 Konventa 108 e Modernizuar, nenet 5 (2)
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 6, pika 1, gërma b	Marrëdhënia (para-) kontraktuese	Rekomandimi mbi Profilizimin, neni 3.4, gërma b
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 6, pika 1, gërma c	Detyrimet ligjore të kontrolluesit	Rekomandimi mbi Profilizimin, neni 3.4, gërma a
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 6, pika 1, gërma d	Interesat jetikë të subjektit të të dhënave	Rekomandimi mbi Profilizimin, neni 3.4, gërma b
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 6, pika 1, gërma e GJDBE, C-524/06, *Huber k. Bundesrepublik Deutschland* [GC], 2008	Interesi public dhe ushtrimi i autoritetit publik	Rekomandimi mbi Profilizimin, neni 3.4, gërma b
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 6, pika 1, gërma f GJDBE, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde k. Rīgas pašvaldības SIA 'Rīgas satiksme'*, 2017 GJDBE, Çështje të bashkuara C-468/10 dhe C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) dhe Federación de Comercio Electrónico y Marketing Directo (FECEMD) k. Administración del Estado*, 2011	Interesat legjitimë të të tjerëve	Rekomandimi mbi Profilizimin, neni 3.4, gërma b GJEDNJ, *Y k. Turqisë*, nr. 648/10, 2015
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 6, pika 4	Përjashtimi nga kufizimi i qëllimit: përpunimi i mëtejshëm për qëllime të tjera	Konventa 108 e Modernizuar, neni 5, pika 4, gërma b
Rregullat në lidhje me përpunimin e ligjshëm të të dhënave sensitive		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 9, pika 1	Ndalimi i përgjithshëm i përpunimit	Konventa 108 e Modernizuar, neni 6
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 9, pika 2	Përjashtime nga ndalimi i përgjithshëm	Konventa 108 e Modernizuar, neni 6

Rregullat në lidhje me sigurinë e përpunimit		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 32	Detyrimi për të garantuar sigurinë e përpunimit	Konventa 108 e Modernizuar, neni 7, pika 1 ECtHR, *I k. Finlandës*, nr. 20511/03, 2008
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 28 dhe 32, pika 1, gërma b	Detyrimi për konfidencialitetin	Konventa 108 e Modernizuar, neni 7, pika 1
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 34 Direktiva mbi privatësinë dhe komunikimet elektronike, neni 4, pika 2	Njoftimet për shkeljen ndaj të dhënave	Konventa 108 e Modernizuar, neni 7, pika 2
Rregullat në lidhje me përgjegjshmërinë dhe nxitjen e përputhshmërisë		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 12, 13 dhe 14	Transparenca në përgjithësi	Konventa 108 e Modernizuar, neni 8
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 37, 38 dhe 39	Nëpunësit e Mbrojtjes së të Dhënave	Konventa 108 e Modernizuar, neni 10, pika 1
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 30	Regjistrat e aktiviteteve të përpunimit	
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 35 dhe 36	Vlerësimi i ndikimit dhe konsultimi paraprak	Konventa 108 e Modernizuar, neni 10, pika 2
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 33 dhe 34	Njoftimet e shkeljeve ndaj të dhënave	Konventa 108 e Modernizuar, neni 7, pika 2
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 40 dhe 41	Kodet e sjelljes	
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 42 dhe 43	Certifikimi	
Mbrojtja e të dhënave që në fazën e konceptimit dhe me parapërzgjedhje		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 25, pika 1	Mbrojtja e të dhënave që në fazën e konceptimit	Konventa 108 e Modernizuar, neni 10, pika 2

Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 25, pika 2	Mbrojtja e të dhënave me parapërzgjedhje	Konventa 108 e Modernizuar, neni 10, pika 3

Parimet kanë domosdoshmërish karakter të përgjithshëm. Zbatimi i tyre në situata konkrete lë një farë hapësire interpretimi dhe mundësi zgjedhjeje të mënyrave. Në **të drejtën e KiE-së**, u lihet palëve të Konventës 108 të Modernizuar të qartësojnë këtë hapësirë interpretimi në të drejtën e tyre të brendshme. Situata në **të drejtën e BE-së** është e ndryshme: për përfshirjen e mbrojtjes së të dhënave në tregun e brendshëm, u gjykua e nevojshme të përcaktohen rregulla më të hollësishme në nivel BE-je, me qëllim harmonizimin e nivelit të mbrojtjes së të dhënave në legjislacionet kombëtare të Shteteve Anëtare. Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave përcakton një shtresë rregullash të hollësishme, nën drejtimin e parimeve të nenit 5, të cilat janë drejtpërdrejt të zbatueshme në rendin juridik kombëtar. Për rrjedhojë, vlerësimet në vijim në lidhje me rregullat e hollësishme të mbrojtjes së të dhënave në nivel evropian trajtojnë kryesisht të drejtën e BE-së.

4.1 Rregullat në lidhje me përpunimin e ligjshëm

Pikat kryesore

- Të dhënat personale mund të përpunohen në mënyrë të ligjshme nëse ato përmbushin nja nga kriteret e mëposhtme:
  - Përpunimi mbështetet tek pëlqimi i subjektit të të dhënave;
  - Çdo marrëdhënie kontraktuese përfshin përpunim e të dhënave personale;
  - Përpunimi është i nevojshëm për përmbushjen e një detyrimi ligjor të cilit i nënshtrohet kontrolluesi;
  - Interesi jetik i subjekteve të të dhënave apo të një personi tjetër e bën të nevojshëm përpunimin e të dhënave të tyre;
  - Përpunimi është i nevojshëm për përmbushjen e një detyre në interes publik;
  - Interesat legjitimë të kontrolluesve apo të palëve të treta janë arsyeja për përpunimin, por vetëm në masën që ato nuk tejkalohen nga interesat ose të drejtat themelore të subjekteve të të dhënave.
- Përpunimi i ligjshëm i të dhënave personale sensitive i nënshtrohet një regjimi të veçantë dhe më të rreptë.

4.1.1 Bazat ligjore për përpunimin e të dhënave

Kreu II i Rregullores së Përgjithshme të Mbrojtjes së të Dhënave, i titulluar "Parimet" parashikon se çdo përpunim të dhënash personale duhet pikë së pari të përputhet me një nga parimet që kanë të bëjnë me cilësinë e të dhënave të përcaktuara në nenin 5 të GDPR-së. Një nga këto parime parashikon se të dhënat personale duhen "përpunuar në mënyrë të ligjshme, të drejtë dhe transparente". Së dyti, që të dhënat të përpunohen në mënyrë të ligjshme, përpunimi duhet të përputhet me një nga bazat ligjore, të cilat i japin legjitimitet përpunimit të të dhënave dhe që renditen në nenin 6[341] për të dhënat personale jo sensitive, ndërsa në nenin 9 për

[341] GJDBE, Çështje të bashkuara C-465/00, C-138/01 dhe C-139/01, *Rechnungshof . Österreichischer Rundfunk dhe të Tjerët dhe Christa Neukomm dhe Jospeh Lauermann k. Österreichischer Rundfunk*, 20 maj 2003, parag. 65; GJDBE, C-524/06, *Heinz Huber k. Bundesrepublik Deutschland* [ÇB] , 16 dhjetor 2008, parag. 48; GJDBE, Çështje të bashkuara C-468/10 dhe C-469/10, *Asociación Nacional de*

kategoritë e veçanta të të dhënave (ose të dhënat sensitive). Në të njëjtën mënyrë, Kreu II i Konventës 108 të Modernizuar i cili parashikon "parimet bazë për mbrojtjen e të dhënave personale", përcakton se, që të jetë i ligjshëm, përpunimi i të dhënave duhet të jetë "proporcional me qëllimin legjitim të ndjekur".

Pavarësisht bazës ligjore për përpunimin, mbi të cilën mbështetet kontrolluesit për të ndërmarrë një aktivitet përpunimi të dhënash personale, ai duhet gjithashtu të zbatojë masat e sigurisë e parashikuara në regjimit juridik të përgjithshëm të mbrojtjes së të dhënave.

PËLQIMI

Në të drejtën e KiE-së, pëlqimi përmendet në nenin 5, pika 2 të Konventës 108 të Modernizuar. Ai përmendet gjithashtu në jurisprudencën e GJEDNJ-së në disa rekomandime të KiE-së.[342] **Në të drejtën e BE-së,** pëlqimi si bazë për përpunim të ligjshëm të të dhënave përcaktohet në mënyrë solide në nenin 6 të GDPR-së dhe përmendet shprehimisht në nenin 8 të Kartës. Karakteristikat për pëlqim të vlefshëm shpjegohen në përkufizimin e pëlqimit në nenin 4, ndërsa kushtet për përftimin e një pëlqimi të vlefshëm jepen në hollësi në nenin 7 dhe normat e veçanta për pëlqimin e fëmijës në lidhje me shërbimet e shoqërisë së informacionit përcaktohen në nenin 8 të GDPR-së.

Sikurse shpjegohet në Seksionin 2.4, pëlqimi duhet dhënë në mënyrë të lirë, të informuar dhe të qartë. Pëlqimi duhet të jetë një deklaratë apo veprim pohues i qartë, që tregon qartësisht miratimin për përpunimin dhe personi ka të drejtën të tërheqë pëlqimin e dhënë në çdo kohë. Kontrolluesit kanë detyrimin të mbajnë një regjistër të verifikueshëm të pëlqimit.

Pëlqimi i lirë

Në kuadrin e Konventës 108 të Modernizuar të **KiE-së**, pëlqimi i subjektit të të dhënave duhet të "përfaqësojë shprehjen e lirë të një zgjedhjeje të qëllimshme".[343] Ekzistenca e pëlqimit të lirë është e vlefshme vetëm "kur subjekti i të dhënave është vërtet në gjendje të bëjë një zgjedhje dhe kur nuk ka rrezik mashtrimi, frikësimi, detyrimi apo pasoja negative domethënëse në rast se ai apo ajo nuk e jep pëlqimin".[344] Në këtë aspekt, e drejta e BE-së saktëson se pëlqimi nuk konsiderohet i dhënë lirisht "nëse subjekti i të dhënave nuk ka liri zgjedhjeje të mirëfilltë, apo nëse nuk është në gjendje të kundërshtojë apo të tërheqë pëlqimin pa pësuar dëmtim".[345] GDPR-ja thekson se "kur gjykohet nëse pëlqimi është dhënë lirisht, i duhet kushtuar shumë rëndësi faktit nëse, ndër të tjera, përmbushja e një kontrate, përfshirë edhe dhënien e një shërbimi, është kusht për dhënien e pëlqimit për përpunimin e të dhënave personale i cili nuk është i nevojshëm për përmbushjen e kontratës".[346] Raporti Shpjegues i Konventës 108 të Modernizuar thekson se "mbi subjektin e të dhënave nuk mund të ushtrohet asnjë ndikim apo presion (qoftë ekonomik, apo i një lloji tjetër), qoftë të drejtpërdrejtë ose të tërthortë dhe pëlqimi nuk duhet konsideruar i dhënë lirisht nëse subjekti i të dhënave nuk mundësi të vërtetë

Establecimientos Financieros de Crédito (ASNEF) dhe Federación de Comercio Electrónico y Marketing Directo (FECEMD) k. Administración del Estado, 24 nëntor 2011, parag. 26.

[342] Shih për shembull, Këshilli i Evropës, Komiteti i Ministrave (2010), Rekomandimi CM/Rec(2010)13 i Komitetit të Ministrave për Shtetet Anëtare në lidhje me mbrojtjen e personave nga përpunimi automatik i të dhënave personale në kontekstin e profilizimit, 23 nëntor 2010, neni 3, pika 4, gërma b.

[343] Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 42.

[344] Shih gjithashtu *Opinionin 15/2011 mbi përkufizimin e pëlqimit* të Grupit të Punës së Nenit 29 (2011), WP 187, 13 korrik 2011, fq. 12.

[345] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 42 i preambulës.

[346] *Ibid*., neni 7, pika 4.

zgjedhjeje, apo nëse nuk është në gjendje të kundërshtojë, apo të tërheqë pëlqimin pa pasoja negative".[347]

Shembull: disa bashki në Shtetin A vendosën të krijojnë karta banimi me një çip të integruar. Nuk është e detyrueshme për banorët që të pajisen me këto karta. Megjithatë, banorët që nuk disponojnë kartën, nuk kanë akses në një numër shërbimesh administrative të rëndësishme, si për shembull mundësinë e pagesës së taksave nëpërmjet internetit, paraqitjen e ankesave në rrugë elektronike që të përfitojnë nga afati kohor tre-ditor për të marrë përgjigje nga autoriteti dhe madje edhe për të shmangur radhët, për të blerë bileta me çmime të reduktuara për hyrje në sallën e koncerteve të bashkisë dhe për të përdorur skanerët në hyrje.

Përpunimi i të dhënave personale nga ana e bashkive në këtë shembull nuk mund të jetë i mbështetur tek pëlqimi. Meqenëse ka të paktën një trysni të tërthortë për banorët që të pajisen me karta elektronike dhe të miratojnë përpunimin, pëlqimi nuk është dhënë lirisht. Për pasojë, zhvillimi nga ana e bashkive të një sistemi kartash elektronike duhet të mbështetet në një bazë tjetër ligjore për të justifikuar përpunimin. Për shembull, ato mund të argumentojnë se përpunimi është i nevojshëm për përmbushjen e një detyre të kryer në interes publik, çka përbën bazë ligjore për përpunimin në përputhje me nenin 6, pika 1, gërma (e) të GDPR-së.[348]

Pëlqimi i lirë mund të vihet gjithashtu në dyshim në situata varësie, kur ekziston shpërpjesëtim midis kontrolluesit që merr pëlqimin dhe subjektit të të dhënave që jep pëlqimin.[349] Një rast tipik i këtij shpërpjesëtimi dhe varësie është përpunimi i të dhënave personale nga një punëdhënës, në kontekstin e marrëdhënies së punësimit. Sipas Grupit të Punës së Nenit 29, "punëmarrësit nuk janë pothuajse kurrë në gjendje të japin, kundërshtojnë apo tërheqin lirisht pëlqimin, për shkak të varësisë që rrjedh nga marrëdhënia punëdhënës/punëmarrës. Duke pasur parasysh pabarazinë e fuqisë, punëmarrësit mund të japin pëlqim të lirë vetëm në raste të pazakonta, kur nuk ka asnjë pasojë në lidhje me pranimin ose kundërshtimin e një propozimi."[350]

Shembull: një shoqëri e madhe planifikon të krijojë një repertor me emrat e të gjithë punonjësve, funksionet e tyre brenda shoqërisë dhe adresën profesionale, me qëllimin e vetëm të përmirësimit të komunikimit të brendshëm të shoqërisë. Drejtuesi i personelit propozon të shtohet në repertor një fotografi për secilin punonjës, për të lehtësuar njohjen e kolegëve pjesëmarrës në mbledhje. Përfaqësuesit e punonjësve kërkojnë që kjo të bëhet vetëm me pëlqimin e secilit punonjës.

Në një situatë të tillë, pëlqimi i punonjësit duhet konsideruar si baza ligjore për përpunimin e fotografive në atë repertor, për shkak se mendohet se punonjësi nuk do të përballet me ndonjë pasojë nëse pranon apo jo t'i publikohet fotografia e tij apo e saj në repertor.

[347] Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 42.
[348] Grupi i Punës së Nenit 29 (2011), *Opinioni 15/2011 mbi përkufizimin e pëlqimit*, WP 187, Bruksel, 13 korrik 2011, fq. 16. Shembuj të tjerë rastesh kur përpunimi i të dhënave nuk mund të bazohet tek pëlqimi, por kërkon një bazë tjetër ligjore për të legjitimuar përpunimin, mund të gjenden në fq. 14 dhe 17 të opinionit.
[349] Shih gjithashtu *Opinionin 8/2001 mbi përpunimin e të dhënave personale në kuadrin e punësimit*, WP 48, Bruksel, 13 shtator 2001, të Grupit të Punës së Nenit 29 (2001); Dokumentin e punës mbi interpretimin e përbashkët të nenit 26, pika 1 të Direktivës 95/46 të 24 tetorit 1995, WP 114, Bruksel, 25 nëntor 2005, të Grupit të Punës së Nenit 29 (2005); *Opinionin 2/2017 mbi përpunimin e të dhënave në punë*, WP 249, Bruksel, 8 qershor 2017, të Grupit të Punës së Nenit 29 (2017).
[350] Grupi i Punës së Nenit 29, *Opinioni 2/2017 mbi përpunimin e të dhënave në punë*, WP 249, Bruksel, 8 qershor 2017.

Shembull: shoqëria A planifikon një takim të tre punonjësve të saj me drejtuesit e shoqërisë B, për të diskutuar bashkëpunimin e mundshëm në të ardhmen për një projekt. Takimi do të zhvillohet në mjediset e shoqërisë B, e cila i kërkon shoqërisë A tí dërgojë me postë elektronike emrat, CV-të dhe fotografitë e pjesëmarrësve në takim. Shoqëria B argumenton se emrat dhe fotografitë e pjesëmarrësve i duhen në mënyrë që stafi në hyrje të godinës të verifikojë nëse ata janë personat e duhur, ndërsa CV-të u duhen drejtuesve për t'u përgatitur më mirë për takimin. Në këtë rast, transmetimi nga ana e shoqërisë A të të dhënave personale të punonjësve të saj nuk mund të mbështetet tek pëlqimi. Pëlqimi nuk mund të konsiderohet si 'i dhënë lirisht', për shkak se është e mundur që punonjësit të përballen me pasoja negative në rast se ata kundërshtojnë propozimin (për shembull ata mund të zëvendësohen nga kolegë të tjerë, jo vetëm për të marrë pjesë në mbledhje, por gjithashtu edhe për të mbajtur lidhjet me shoqërinë B dhe për t'u angazhuar në projekt në përgjithësi). Për pasojë, përpunimi duhet të mbështetet në një bazë tjetër të ligjshme për përpunimin.

Sidoqoftë, kjo nuk do të thotë se pëlqimi nuk mund të jetë kurrë i vlefshëm në rrethana kur mosdhënia e pëlqimit mund të ketë pasoja negative. Për shembull, nëse mosdhënia e pëlqimit për t'u pajisur me një kartë klienti në supermarket sjell si rezultat mos përfitimin e një uljeje të vogël çmimi në disa mallra, pëlqimi mund të jetë një bazë e vlefshme ligjore për përpunimin e të dhënave personale të klientëve të cilët kanë dhënë pëlqimin për t'u pajisur me një kartë të tillë. Nuk ka ndërvarësi midis shoqërisë dhe klientit dhe pasojat e mosdhënies së pëlqimit nuk janë aq të rënda sa për të penguar zgjedhjen e lirë të subjektit të të dhënave (me kusht që ulja e çmimit të jeë aq modeste sa të mos ndikojë zgjedhjen e lirë).

Nga ana tjetër, nëse mallrat apo shërbimet mund të përftohen vetëm nëse i komunikohen disa të dhëna personale kontrolluesit apo në vijim palëve të treta, pëlqimi i subjektit të të dhënave për përhapjen e të dhënave të tij, të cilat nuk janë të nevojshme për kontratën, nuk mund të konsiderohet si vendim i lirë dhe për rrjedhojë nuk është i vlefshëm sipas së të drejtës për mbrojtje të të dhënave.[351] GDPR-ja ndalon rreptësishtë lidhjen e pëlqimit me dhënien e mallrave dhe shërbimeve.[352]

Shembull: miratimi i dhënë nga pasagjerët një shoqërie udhëtimi ajror për transmetimin e të ashtuquajturave të dhëna të regjistrit të emrave të pasagjerëve (d.m.th. të të dhënave në lidhje me identitetin e tyre, mënyrës së të ushqyerit, apo problemeve me shëndetin) tek autoritetet e emigracionit të një shteti të huaj të caktuar, nuk mund të konsiderohet si pëlqim i vlefshëm nga e drejta për mbrojtjen e të dhënave, meqenëse pasagjerët që janë duke udhëtuar nuk kanë zgjedhje tjetër në rast se duan të vizitojnë atë shtet. Që këto të dhëna të transferohen në mënyrë të ligjshme, nevojitet një bazë ligjore tjetër në vend të pëlqimit, me shumë gjasa një ligj specifik.

Pëlqimi i informuar

Përpara se të marrë vendimin e tij apo të saj, subjekti i të dhënave duhet të pajiset me informacione të mjaftueshme. Përgjithësisht, pëlqimi i informuar do të përfshijë një përshkrim të saktë dhe lehtësisht të kuptueshëm në lidhje me çështjen për të cilën kërkohet pëlqimi.

[351] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 7, pika 4.
[352] *Ibid*.

Sikurse shpjegon Grupi i Punës së Nenit 29, pëlqimi duhet të mbështetet mbi të vlerësuarit dhe të kuptuarit të fakteve dhe të pasojave të pëlqimit për përpunimin nga ana e subjektit të të dhënave. Për këtë shkak, "personit të përfshirë duhet t'i jepet informacion në mënyrë të qartë dhe të kuptueshme, të saktë dhe të plotë mbi të gjitha elementet e rëndësishme [...] si për shembull mbi karakterin e të dhënave të përpunuara, qëllimet e përpunimit, marrësit e transferimeve të mundshme dhe të drejtat e subjektit të të dhënave."[353] Në mënyrë që qëllimi të jetë i informuar, personat duhet gjithashtu të jenë të vetëdijshëm për pasojat në rast se nuk japin pëlqimin për përpunimin.

Duke pasur parasysh rëndësinë që ka pëlqimi i informuar, GDPR-ja dhe Raporti Shpjegues i Konventës 108 të Modernizuar kanë synuar të qartësojnë këtë nocion. Paragrafët e preambulës së GDPR-së përcaktojnë se pëlqim i informuar do të thotë "se subjekti i të dhënave duhet të jetë në dijeni të paktën për identitetin e kontrolluesit dhe qëllimet e përpunimit për të cilat janë të destinuara të dhënat personale.[354]

Në rastin përjashtimor kur pëlqimi përdoret për të siguruar bazën ligjore për një transferim ndërkombëtar të dhënash, kontrolluesi duhet të informojë subjektin e të dhënave për rreziqet e mundshme që mund të shkaktojë ky transferim, për shkak të mungesës së një vendimi mbi nivelin e përshtatshëm të mbrojtjes dhe masave të përshtatshme të sigurisë, që ai pëlqim të konsiderohet i vlefshëm.[355]

Raporti Shpjegues i Konventës 108 të Modernizuar saktëson se duhet dhënë informacion në lidhje me pasojat për subjektin e të dhënave nga vendimi i tij për dhënien e pëlqimit, domethënë "çfarë nënkupton fakti i dhënies së pëlqimit dhe shtrirjen e këtij të fundit".[356]

Cilësia e informacionit është e rëndësishme. Cilësi e informacionit do të thotë se gjuha e përdorur duhet të përshtatet me marrësit e parashikueshëm të tij. Informacioni duhet dhënë pa përdorur zhargone, me një gjuhë të qartë dhe të thjeshtë, që përdoruesi i zakonshëm duhet të jetë i aftë ta kuptojë.[357] Po ashtu informacioni duhet të jetë lehtësisht i aksesueshëm nga subjektet e të dhënave, qoftë verbalisht, ashtu edhe me shkrim. Aksesueshmëria dhe vizibiliteti i informacionit janë elemente të rëndësishme: informacioni duhet të jetë qartësisht i dukshëm dhe i dallueshëm në mjedisin digjital njoftimet e shtresëzuara informuese mund të jenë një zgjidhje e mirë, meqenëse ato u mundësojnë subjekteve të të dhënave të zgjedhin nëse duan të lexojnë variante më të përmbledhura informacionesh apo më të zgjeruara.

Pëlqimi specifik

Në mënyrë që pëlqimi të jetë i vlefshëm, ai duhet gjithashtu të jetë specifik për qëllimin e përpunimit. Ky i fundit duhet të përshkruhet qartësisht dhe me terma që nuk lenë vend për keqkuptime. Kjo shkon paralelisht me cilësinë e informacionit që jepet në lidhje me qëllimin e pëlqimit. Në këtë kontekst, marrin rëndësi pritshmëritë e arsyeshme të një subjekti mesatar të dhënash. Subjekti i të dhënave duhet pyetur sërish për pëlqimin, kur duhen shtuar apo ndryshuar aktivitetet përpunuese që nuk mund të parashikoheshin në mënyrë të arsyeshme në momentin kur u dha pëlqimi fillestar dhe të cilat sjellin ndryshim të qëllimit. Kur përpunim ndjek disa qëllime, duhet dhënë pëlqimi për secilin prej tyre.[358]

Shembuj: tek çështja *Deutsche Telekom AG*,[359] GJDBE-ja shqyrtoi nëse një operator shërbimesh telekomunikacioni i cili do të transmetonte të dhënat personale të abonentëve të tij për t'u publikuar në

[353] Grupi i Punës së Nenit 29 (2007), Dokument Pune mbi përpunimin e të dhënave personale në lidhje me shëndetin në Regjistrin Elektronik të Shëndetit (RESH), WP 131, Bruksel, 15 shkurt 2007.
[354] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 42 i preambulës.
[355] *Ibid*., neni 49, pika 1, gërma a.
[356] Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 42.
[357] Grupi i Punës së Nenit 29 (2011), *Opinioni 15/2011 mbi përkufizimin e pëlqimit*, WP187, Bruksel, 13 korrik 2011, fq. 19.
[358] Rregullorja e Pëgjithshme e Mbrojtjes së të Dhënave, paragrafi 32
[359] GJDBE, C-543/09, *Deutsche Telekom AG k. Bundesrepublik Deutschland*, 5 maj 2011. Shih sidomos paragrafët 53 dhe 54.

numëratorë, duhej të merrte sërish pëlqimin nga subjektet e të dhënave,[360] për shkak se në momentin kur ishte dhënë pëlqimi, nuk ishin bërë të ditur marrësit e të dhënave.

GJDBE-ja u shpreh se sipas nenit 12 të Direktivës mbi privatësinë dhe komunikimet elektronike, rimarrja e pëlqimit nuk ishte e nevojshme përpara transmetimit të të dhënave. Duke qenë se subjektet e të dhënave kishin vetëm alternativën e dhënies së pëlqimit për qëllimin e përpunimit – i cili ishte publikimi i të dhënave – ata nuk mund të zgjidhnin se në cilin numërator mund të publikoheshin të dhënat e tyre.

Sikurse nënvizoi GJDBE-ja "nga një interpretim kontekstual dhe sistematik i nenit 12 të Direktivës mbi privatësinë dhe komunikimet elektronike, rezulton se pëlqimi, sipas nenit 12, pika 2, lidhet me qëllimin e publikimit të të dhënave personale në një numërator publik dhe jo me identitetin e një operatori të caktuar numëratori."[361] Gjithashtu se "është vetë publikimi i të dhënave personale në një numërator publik me një qëllim të caktuar i cili mund të rezultojë i dëmshëm për abonentin",[362] se sa thjesht çështja e identitetit të publikuesit.

Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV k. Autoriteit Consument en Markt (AMC)[363] kishte të bënte me kërkesën e një shoqërie belge që ofronte shërbime informacioni telefonik dhe numëratori, e cila u kishte kërkuar shoqërive që caktojnë numra telefonikë në Vendet e Ulëta t'i jepnin akses tek të dhënat e abonentëve të tyre. Shoqëria belge bazohej mbi një detyrim që rridhte nga Direktiva e Shërbimeve Universale.[364] Kjo e fundit i detyronte shoqëritë të cilat caktojnë numrat e telefonit t'ua vinin numëratoret në dispozicion atyre që i kërkonin, me kusht që abonentët të kishin dhënë pëlqimin që numrat e tyre të publikoheshin. Shoqëritë holandeze refuzuan ta bënin këtë, duke u shprehur se nuk ishin të detyruar t'ua jepnin këto të dhëna një shoqërie të vendosur në një Shtet tjetër Anëtar. Argumenti i tyre ishte se përdoruesit kishin dhënë pëlqimin për publikimin e numrave të tyre duke menduar se ato do të publikoheshin në një numërator holandez. GJDBE-ja u shpreh se Direktiva e Shërbimeve Universale përfshinte të gjitha kërkesat nga shoqëri të shërbimeve të numëratorit, pavarësisht Shtetit Anëtar ku janë të vendosur. GJDBE-ja doli gjithashtu në përfundimin se transmetimi i po këtyre të dhënave tek një shoqëri tjetër, e cila synonte të publikonte një numrator publik, pa marrë sërish pëlqimin nga abonentët, nuk mund të dëmtonte thelbin e së drejtës për mbrojtje të të dhënave personale.[365] Për rrjedhojë, nuk është e nevojshme që shoqëria e cila cakton numrat e telefonit për abonentët e saj, të formulojë kërkesën për pëlqim drejtuar abonentëve të saj në mënyrë të dallueshme, në varësi të Shtetit Anëtar drejt së cilit të dhënat e tyre mund të transmetohen.[366]

Pëlqimi i qartë

Çdo pëlqim duhet dhënë në mënyrë të qartë.[367] Kjo do të thotë se nuk duhet të ketë asnjë dyshim të arsyeshëm që subjekti i të dhënave dëshiron të shprehë miratimin për përpunimin e të dhënave të tij apo të saj. Për shembull, mosveprimi i subjektit të të dhënave nuk nënkupton një pëlqim të qartë.

[360] Direktiva 2002/58/EC e Parlamentit Evropian dhe e Këshillit e 12 korrikut 2002 në lidhje me përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike, FZ 2002 L 201 (Direktiva mbi privatësinë dhe komunikimet elektronikes).
[361] GJDBE, C-543/09, *Deutsche Telekom AG k. Bundesrepublik Deutschland*, 5 maj 2011; paragrafi 61.
[362] *Ibid*., parag. 62.
[363] GJDBE, C-536/15, *Tele2 (Netherlands) BV dhe të Tjerët k. Autoriteit Consument en Markt (AMC)*, 15 mars 2017.
[364] Direktiva 2002/22/EC e Parlamentit Evropian dhe e Këshillit e 7 marsit 2002 mbi shërbimin universal dhe të drejtat e përdoruesve në lidhje me rrjetet dhe shërbimet e komunikimeve elektronike (Direktiva e Shërbimeve Universale), FL 2002 L 108, fq. 51, ndryshuar me Direktivën 2009/136/EC e Parlamentit Evropian dhe e Këshillit e 25 nëntorit 2009 (Direktiva e Shërbimeve Universale), FZ 2009 L 337, fq. 11.
[365] GJDBE, C-536/15, *Tele2 (Netherlands) BV dhe të Tjerët k. Autoriteit Consument en Markt (AMC)*, 15 mars 2017, paragrafi 36.
[366] *Ibid*., paragrafët 40-41.
[367] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, *neni* 4 pika 11.

Një rast i tillë mund të jetë kur kontrolluesi merr pëlqimin me anë të deklaratave në politikat e privatësisë, si për shembull "duke përdorur shërbimin tonë, ju miratoni përpunimin e të dhënave tuaja personale". Në këtë rast, kontrolluesit mund të kenë detyrimin të sigurohen se përdoruesit japin pëlqimin manualisht dhe individualisht për këto politika.

Nëse pëlqimi jepet në formën e shkruar, në kuadër të një kontrate, pëlqimi për përpunimin e të dhënave personale duhet të individualizohet dhe në të gjitha rastet "duhet të merren masat që të garantohet se subjekti i të dhënave është i ndërgjegjshëm për pëlqimin e dhënë dhe për shtrirjen e tij."[368]

Kriteret e pëlqimit të fëmijëve

GDPR-ja parashikon mbrojtje specifike për fëmijët në kontekstin e dhënies së shërbimeve të shoqërisë së informacionit, për shkak se "ata mund të jenë më pak të ndërgjegjshëm për rreziqet, pasojat dhe garancitë përkatëse dhe të drejtat e tyre në lidhje me përpunimin e të dhënave personale".[369] Për rrjedhojë, sipas së drejtës së BE-së, kur operatorët e shërbimeve të shoqërisë së informacionit përpunojnë të dhëna personale të fëmijëve nën moshën 16 vjeç mbi bazën e pëlqimin, ky përpunim do të jetë i ligjshëm "vetëm nëse dhe në masën që pëlqimi jepet ose autorizohet nga zotëruesi i përgjegjësisë prindërore për atë fëmijë."[370] Shtetet anëtare mund të parashikojnë në ligjin kombëtar një moshë më të ulët, me kusht që të mos jetë nën 13 vjeç.[371] Pëlqimi nga zotëruesi i përgjegjësisë prindërore nuk është i nevojshëm "në kontekstin e shërbimeve parandaluese ose këshillimore që i ofrohen drejtpërdrejt një fëmije."[372] Informacioni dhe komunikimi kur përpunimi i drejtohet një fëmije, duhet të jetë në një gjuhë të thjeshtë dhe të qartë, lehtësisht të kuptueshme nga fëmija.[373]

E drejta për të tërhequr pëlqimin në çdo kohë

GDPR-ja përmban një të drejtë të përgjithshme për të tërhequr pëlqimin në çdo kohë.[374] Subjekti i të dhënave duhet të informohet për këtë të drejtë përpara se të japë pëlqimin dhe ai ose ajo mund ta ushtrojë këtë të drejtë sipas gjykimit të tij apo të saj. Nuk duhet të ekzistojë asnjë kriter për shpjegim të arsyeve për tërheqjen e pëlqimit dhe asnjë rrezik pasojash negative, përveç ndërprerjes së përfitimeve që rridhnin nga përdorimi i mëparshëm i të dhënave për të cilin ishte dhënë pëlqimi. Tërheqja e pëlqimit duhet të jetë aq e lehtë sa ç'ishte dhënia e tij.[375] Nuk mund të ketë pëlqim të lirë nëse subjekti i të dhënave nuk mund të tërheqë pëlqimin e tij apo të saj pa pasoja të dëmshme, ose nëse tërheqja e pëlqimit nuk është aq e lehtë sa ç'ishte dhënia e tij.[376]

Shembull: një klient pranon t'i dërgohen letra promocioni në një adresë që ai ose ajo i kanë dhënë kontrolluesit të të dhënave. Në rast se klienti tërheq pëlqimin, kontrolluesi duhet të ndalojë menjëherë dërgimin e letrave promocionale. Asnjë pasojë ndëshkuese, si për shembull një tarifë financiare, nuk duhet të vendoset. Sidoqoftë tërheqja ushtrohet për të ardhmen dhe nuk ka efekt prapaveprues. Periudha gjatë së cilës të dhënat personale të klientit ishin përpunuar në mënyrë të ligjshme, falë pëlqimit të dhënë, është legjitime. Tërheqja parandalon çdo përpunim të mëtejshëm të këtyre të dhënave, përveçse nëse përpunimi është në përputhje me të drejtën e fshirjes.[377]

---

[368] Ibid., paragrafi 42 i preambulës.
[369] *Ibid*., paragrafi 38 i preambulës.
[370] *Ibid*, neni 8, pika 1, paragrafi i parë. Nocioni i shërbimeve të shoqërisë së informacionit përcaktohet në nenin 4, pika 25 të Rregullores së Përgjithshme të Mbrojtjes së të Dhënave.
[371] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 8, pika 1, paragrafi i dytë.
[372] *Ibid*., paragrafi 38 i preambulës.
[373] *Ibid*., paragrafi 58 i preambulës. Shih po ashtu Konventën 108 të Modernizuar, neni 15, pika 2, shkronja e. Raportin Shpjegues të Konventës 108 të Modernizuar, paragrafët 68 dhe 125.
[374]
[375] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 7, pika 3.
[376] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 42 i preambulës; Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 42.
[377] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 17, pika 1, gërma b.

Nevoja për përmbushjen e një kontrate

Në të drejtën e BE-së, neni 6, pika 1, shkronja b e GDPR-së parashikon një bazë tjetër për përpunimin e ligjshëm, konkretisht nëse është "i nevojshëm për përmbushjen e një kontrate, ku subjekti i të dhënave është palë". Kjo dispozitë përfshin gjithashtu marrëdhëniet para-kontraktore. Për shembull, në rastet kur një palë ka për qëllim të lidhë një kontratë, por ende nuk e ka bërë këtë, ndoshta pasi duhen bërë ende disa verifikime. Nëse njëra palë ka nevojë të përpunojë të dhëna për këtë qëllim, ku përpunim është i ligjshëm në masën që është "i nevojshëm me qëllim ndërmarrjen e hapave me kërkesën e subjektit të të dhënave përpara se të lidhet një kontratë".[378]

Nocioni i përpunimit të të dhënave si një "bazë legjitime e përcaktuar me ligj" në nenin 5, pika 2 të Konventës 108 të Modernizuar përfshin gjithashtu "përpunimin e të dhënave për përmbushjen e një kontrate (ose të masave para-kontraktore me kërkesën e subjektit të të dhënave) ku subjekti i të dhënave është palë".[379]

Detyrimet ligjore të kontrolluesit

E drejta e BE-së përcakton edhe një kriter tjetër për legjitimimin e përpunimit të të dhënave, konkretisht nëse "është i nevojshëm për përputhshmërinë me një detyrim ligjor të cilit i nënshtrohet kontrolluesi" (GDPR, neni 6, pika 1, gërma (c)). Kjo dispozitë i referohet si kontrolluesve të sektorit privat ashtu edhe atij të sektorit publik; detyrimet ligjore të kontrolluesve të sektorit publik mund të mbulohen gjithashtu nga neni 6, pika 1, gërma (e) e GDPR-së. Ka shumë shembuj situatash ku ligji detyron kontrolluesit e sektorit privat to përpunojnë të dhëna për subjekte specifike të dhënash. Për shembull, punëdhënësit duhet të përpunojnë të dhëna në lidhje me punëmarrësit e tyre për qëllime të sigurimeve shoqërore e fiskale dhe ndërmarrjet tregtare duhet të përpunojnë të dhëna në lidhje me klientët e tyre për qëllime fiskale.

Detyrimi ligjor mund të burojë nga e drejta e Bashkimit, ose nga e drejta e një Shteti Anëtar, e cila mund të shërbejë si bazë për një ose më shumë aktivitete përpunimi. I takon ligjit të përcaktojë qëllimin e përpunimit, kriteret për identifikimin e kontrolluesit, llojin e të dhënave personale objekt përpunimi, subjektet e të dhënave, subjektet të cilëve u përhapen të dhënat personale, kufizimet e qëllimit, afatet e mbajtjes së të dhënave dhe masat e tjera për të garantuar përpunim të ligjshëm dhe të drejtë[380] Ky ligj që shërben si bazë për përpunimin e të dhënave personale duhet të përputhet si me nenet 7 dhe 8 të Kartës, ashtu edhe me nenin 8 të KEDNJ-së.

Detyrimet ligjore të kontrolluesit duhet gjithashtu të shërbejnë si bazë për përpunim të ligjshëm të të dhënave **sipas së drejtës së KiE-së.**[381] Sikurse u theksua më herët, detyrimet ligjore të një kontrolluesi të sektorit privat janë thjesht një rast specifik i interesave legjitimë të të tjerëve, parashikuar në nenin 8, pika 2 të KEDNJ-së. Për pasojë, shembulli i punëdhënëse që përpunojnë të dhëna në lidhje me të punësuarit e tyre është me rëndësi edhe për të drejtën e KiE-së.

---

[378] *Ibid*., neni 6, pika 1, gërma (b).

[379] Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 46; Këshilli i Evropës, Komiteti i Ministrave (2010), Rekomandimi CM/Rec(2010)13 i Komitetit të Ministrave për Shtetet Anëtare mbi mbrojtjen e personave nga përpunimi automatik i të dhënave personale në kontekstin e profilizimit, 23 nëntor 2010, neni 3, pika 4, gërma (b).

[380] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 45 i preambulës.

[381] Këshilli i Evropës, Komiteti i Ministrave (2010), Rekomandimi CM/Rec(2010)13 i Komitetit të Ministrave për Shtetet Anëtare mbi mbrojtjen e personave nga përpunimi automatik i të dhënave personale në kontekstin e profilizimit, 23 nëntor 2010, neni 3, pika 4, gërma (a).

Interesat jetikë të subjektit të të dhënave ose personave të tjerë fizikë

Në të drejtën e BE-së, neni 6, pika 1, shkronja (d) e GDPR-së përcakton se përpunimi i të dhënave personale është i ligjshëm nëse "është i nevojshëm me qëllim që të mbrohen interesat jetike të subjektit të të dhënave ose personave të tjerë fizikë". Tek kjo bazë ligjore mund të mbështetet vetëm për përpunimin e të dhënave personale në bazë të interesave jetikë të një personi tjetër vetëm nëse përpunimi "qartazi nuk mund të mbështetet në një bazë tjetër ligjore".[382] Ndonjëherë, disa lloje përpunimi mund të justifikohen njëkohësisht me arsyet e interesit publik dhe të interesave jetikë të subjektit të të dhënave ose personave të tjerë. Një rast i tillë për shembull është kur monitorohet një epidemi dhe përhapja e saj, ose në rastin e një emergjence humanitare.

Në të drejtën e KiE-së, interesat jetikë të subjektit të të dhënave nuk përmenden në nenin 8 të KEDNJ-së. Megjithatë, interesat jetikë të subjektit të të dhënave konsiderohen si të nënkuptuara në nocionin e 'bazës legjitime' të përmendur në nenin 5, pika 2 të Konventës 108 të Modernizuar, i cili trajton legjitimitetin e përpunimit të të dhënave personale.[383]

Interesi publik dhe ushtrimi i autoritetit zyrtar

Duke pasur parasysh mënyrat e ndryshme të organizimit të çështjeve publike, neni 6, pika 1, shkronja (e) e GDPR-së parashikon se të dhënat personale mund të përpunohen në mënyrë të ligjshme nëse "është e nevojshme për përmbushjen e një detyre të kryer në interes publik ose në ushtrim të autoritetit zyrtar të veshur kontrolluesit [...]".[384]

Shembull: tek çështja *Huber k. Bundesrepublik Deutschland*,[385] z. Huber, një shtetas austriak me qëndrim në Gjermani, i kërkoi Zyrës Federale të Migracionit dhe Refugjatëve të fshinte të dhënat në lidhje me të nga Regjistri Qendror i Shtetasve të Huaj ('AZR-ja'). Ky regjistër i cili përmban të dhënat personale të shtetasve jo-gjermanë nga BE-ja me qëndrim në Gjermani për më shumë se tre muaj, përdoret për qëllime statistikore dhe nga autoritetet policore dhe gjyqësore kur hetojnë dhe ndjekin penalisht aktivitete kriminale dhe ata që kërcënojnë sigurinë publike. Gjykata referuese kërkoi të dinte nëse përpunimi i të dhënave personale që kryhej në regjistra, si për shembull tek Regjistri Qendror i Shtetasve të Huaj, tek i cili kishin akses edhe autoritete të tjera publike, ishte në përputhje me të drejtën e BE-së, duke pasur parasysh se nuk ekzistonte një regjistër i tillë për shtetasit gjermanë.

GJDBE theksoi se sipas nenit 7, gërma (e) e Direktivës 95/46,[386] të dhënat personale mund të përpunohen ligjërisht nëse është e nevojshme për përmbushjen e një detyre që kryhet në interes publik, ose në ushtrim të autoritetit publik.

Sipas GJDBE-së, "duke pasur parasysh objektivin për të arritur mbrojtje të barasvershme në të gjitha Shtetet Anëtare, koncepti i domosdoshmërisë i përcaktuar në nenin 7, gërma (e) të Direktivës 95/46[387] [...] nuk mund të ketë kuptim të ndryshëm midis Shteteve Anëtare. Rrjedhimisht, ai është një koncept autonom i së drejtës së Komunitetit, i cili duhet interpretuar në mënyrë të tillë që të reflektojë plotësisht objektivin e kësaj direktive, sikurse përcaktohet në nenin 1, pika 1 të saj".[388]

[382] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 46 i preambulës.
[383] Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 46.
[384] Shih Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave, paragrafin 45 të preambulës.
[385] GJDBE, C-524/06, *Heinz Huber k. Bundesrepublik Deutschland* [ÇB] , 16 dhjetor 2008.
[386] Direktiva e shfuqizuar e Mbrojtjes së të Dhënave, neni 7, gërma (e), tani Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 6, pika 1, gërma (e).
[387] *Ibid*.
[388] GJDBE, C-524/06, *Heinz Huber k. Bundesrepublik Deutschland* [ÇB] , 16 dhjetor 2008, paragrafi 52.

GJDBE-ja theksoi se e drejta e lëvizjes së lirë të jë qytetari të Bashkimit në territorin e Shtetit Anëtar, në të cilin ai apo ajo nuk është shtetar, nuk është e pakushtëzuar dhe mund t'i nënshtrohet kufizimeve dhe kushteve të parashikuara nga Traktati i Themelimit të Komunitetit Evropian dhe nga masat e marra për zbatimin e tij. Kësisoj, në parim, është legjitime që Shteti Anëtar të përdorë një regjistër të tillë sikurse AZR-ja, i cili ka për qëllim të ndihmojë autoritetet kompetente për zbatimin e legjislacionit në lidhje me të drejtën e vendosjes, megjithatë ky regjistër nuk mund të përmbajë asnjë informacion i cili nuk është i nevojshëm për këtë qëllim. GJDBE-ja doli në përfundimin se një sistem i tillë për përpunimin e të dhënave personale është në përputhje me të drejtën e BE-së vetëm nëse përmban të dhënat e nevojshme për zbatimin e atij legjislacioni dhe nëse karakteri i tij i centralizuar e bën më efikas zbatimin e atij legjislacioni. I takonte gjykatave kombëtare të verifikonin nëse këto kushte janë përmbushur në rastin konkret. Nëse jo, mbajtja dhe përpunimi i të dhënave personale në një regjistër të tillë si AZR-ja për qëllim statistikore, nuk mund të konsiderohet në asnjë rast si e domosdoshme në kuptim të nenit 7, gërma (e) [389] të Direktivës 95/46.[390]

Së fundi, për sa i përket çështjes së përdorimit të të dhënave të regjistrit për qëllime të luftës kundër krimit, GJDBE-ja vlerësoi se një objektiv i tillë "përfshin domosdoshmërish ndjekjen penale të krimeve dhe veprave penale të kryera, pavarësisht kombësisë së autorëve të tyre". Regjistri konkret nuk përmbante të dhëna personale të shtetasve të Shtetit Anëtar në fjalë dhe ky trajtim i ndryshëm përbënte diskriminim, i cili ndalohet nga neni 18 i TFBE-së. Për rrjedhojë, GJDBE-ja vendosi se kjo dispozitë "ndalon ngritjen nga ana e një Shteti Anëtar të një sistemi për përpunimin e të dhënave personale për qëllime të luftës kundër krimit të qytetarëve të Bashkimit që nuk janë shtetas të atij Shteti Anëtar."[391]

Përdorimi i të dhënave personale nga autoritetet që veprojnë në sferën publike është gjithashtu subjekt i nenit 8 të **KEDNJ**-së dhe kur është rasti, mbulohet nga neni 5, pika 2 e Konventës 108 të Modernizuar.[392]

Interesat legjitime që ndjek kontrolluesi ose pala e tretë

Në të **drejtën e BE**-së, subjekti i të dhënave nuk është i vetmi që ka interesa legjitime. Neni 6, pika 1, gërma (f) e GDPR-së parashikon se të dhënat personale mund të përpunohen në mënyrë të ligjshme "nëse përpunimi është i nevojshëm për qëllimet e interesave legjitime të ndjekura nga kontrolluesi, një ose disa palë të treta, [përveç autoriteteve publike në ushtrim të detyrave të tyre] tek të cilët përhapen të dhënat, përveçse kur këto interesa tejkalohen nga interesat ose të drejtat dhe liritë themelore të subjektit të të dhënave që kërkojnë mbrojtje [...].[393]

Ekzistenca e një interesi legjitim duhet vlerësuar me kujdes në secilin rast.[394] Nëse janë identifikuar interesat legjitimë të kontrolluesit, atëherë duhen vendosur në peshore ato interesa me interesat, ose të drejtat dhe liritë themelore, të subjektit të të dhënave.[395] Pritshmëritë e arsyeshme të subjektit të të dhënave duhen marrë parasysh gjatë kryerjes së këtij vlerësimi, për të verifikuar nëse interesat e kontrolluesit prevalojnë mbi interesat, apo të drejtat themelore të

[389] Direktiva e shfuqizuar e Mbrojtjes së të Dhënave, neni 7 pika (e), tani Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 6, pika 1, gërma (e).
[390] GJDBE, C-524/06, *Heinz Huber k. Bundesrepublik Deutschland* [ÇB] , 16 dhjetor 2008, parag. 54, 58–59 dhe 66–68.
[391] *Ibid*., parag. 78 dhe 81.
[392] Raporti Shpjegues i Konventës 108 të Modernizuar, parag. 46 dhe 47.
[393] Krahasuar me Direktivën 95/46, Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave jep më tepër shembull rastesh që duhen konsideruar si të tilla që përbëjnë interes legjitim.
[394] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, Preambula, Paragrafi 47.
[395] Grupi i Punës së Nenit 29 (2014), Opinioni 06/2014 mbi nocionin e interesave legjitimë të kontrolluesit të të dhënave sipas nenit 7 të Direktivës 95/46/EC, 4 prill 2014.

subjektit të të dhënave.[396]Nëse të drejtat e subjektit të të dhënave tejkalojnë interesat legjitimë të kontrolluesit, atëherë kontrolluesi mund të marrë masa sigurie për të garantuar minimizimin e ndikimit tek të drejtat e subjektit të të dhënave (si për shembull pseudonimizimin e të dhënave) dhe të kthejë anën e "peshores" përpara se të ketë mundësi të mbështetet ligjërisht tek kjo bazë legjitime për përpunimin. Në Opinionin e tij mbi nocionin e interesave legjitimë të kontrolluesit të të dhënave, Grupi i Punës së Nenit 29 nënvizoi rolin vendimtar të përgjegjshmërisë dhe transparencës dhe të të drejtave të subjektit të të dhënave për të kundërshtuar përpunimin e të dhënave të tij, për të aksesuar, ndryshuar, fshirë ose transferuar, kur vendosen në peshore interesat legjitimë të kontrolluesit me interesat e të drejtave themelore të subjektit të të dhënave.[397]

Në paragrafët e preambulës së GDPR-së, jepen disa shembull mbi atë çka përbën interes legjitim të kontrolluesit të të dhënave. Për shembull, përpunimi i të dhënave personale lejohet pa pëlqimin e subjektit të të dhënave kur bëhet për qëllime të marketingut të drejtpërdrejtë, ose kur një përpunim i tillë është "tepër i nevojshëm për qëllime të parandalimit të mashtrimit".[398]

GJDBE-ja ka zgjeruar në jurisprudencën e saj kriterin e përcaktimit të asaj çka përbën interes legjitim.

Shembull: çështja *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*[399] kishte të bënte me dëmtimin e një autobusi elektrik të Shoqërisë së Transportit Rīgas, shkaktuar nga hapja e papritur e një dere taksie nga ana e një pasagjeri. Rīgas satiskme donte të padiste pasagjerin për dëmet. Megjithatë, policia donte të jepte vetëm emrin e pasagjerit dhe kundërshtonte dhënien e numrit të kartës së identitetit dhe adresën e pasagjerët, me arsyetimin se përhapja do të ishte e paligjshme referuar të drejtës kombëtare për mbrojtje të të dhënave.

Gjykata referuese letone i kërkoi GJDBE-së të jepte një vendim paragjyqësor, kur të sqaronte nëse legjislacioni i mbrojtës së të dhënave të BE-së përcaktonte detyrimin për të përhapur të gjitha të dhënat personale të nevojshme për nisjen e një procedimi civil kundër personit të dyshuar si përgjegjës për një shkelje administrative.[400]

GJDBE-ja qartësoi se e drejta e BE-së në fushën e mbrojtjes së të dhënave përfshinte mundësinë – jo detyrimin – për të komunikuar të dhëna tek një palë e tretë për qëllime të interesave legjitimë të ndjekur nga ajo palë.[401] GJDBE-ja përcaktoi tre kushte përmbledhëse të cilat duhen përmbushur në mënyrë që përpunimi i të dhënave personale të jetë i ligjshëm bazuar në "interesat legjitimë'.[402] Së pari, pala e tretë, tek të cilat janë përhapur të dhënat, duhet të ndjekë një interes legjitim. Në rastin konkret, kjo do të thotë se kërkesa për informacione personale, për të paditur një person pasi ka shkaktuar dëmtim prone, përbën interes legjitim të një pale të tretë. Së dyti, përpunimi i të dhënave personale duhet të jetë i nevojshëm për qëllime të interesave legjitimë të ndjekur. Në këtë rast, marra e informacioni personal, sikurse është adresa dhe/ose numri i kartës së identitetit, është i domosdoshëm për identifikimin e atij personi. Së treti, të drejtat dhe liritë themelore të subjektit të të dhënave nuk duhet të mbizotërojnë interesat legjitimë të kontrolluesit ose palës së tretë. Vendosja në ekuilibër të interesave duhet bërë rast pas rasti, duke marrë parasysh elemente të tillë si ashpërsinë e shkeljes së të drejtave të subjektit të të dhënave, ose edhe moshën e subjektit të të dhënave në rrethana të caktuara. Megjithatë, në rastin konkret, GJDBE-ja nuk e vlerësoi si të justifikueshëm refuzimin për përhapje thjesht sepse subjekti i të dhënave ishte i mitur.

[396] *Ibid*.
[397] *Ibid*.
[398] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, Preambula, Paragrafi 47.
[399] GJDBE, C-13/16, -13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde k. Rīgas pašvaldības SIA 'Rīgas satiksme'*, 4 maj 2017.
[400] *Ibid*., parag. 23.
[401] *Ibid*., parag. 26.
[402] *Ibid*., parag. 28-34.

Tek vendimi i gjykimit të çështjes *ASNEF dhe FECEMD*, GJDBE-ja vendosi shprehimisht në lidhje me përpunimin e të dhënave bazuar në 'interesat legjitimë' për arsye të ligjshme, që ishte në atë kohë e përcaktuar në nenin 7, gërma (f) të Direktivës së Mbrojtjes së të Dhënave.[403]

Shembull: tek çështja *ASNEF dhe FECEMD*,[404] GJDBE-ja qartësoi se e drejta kombëtare nuk lejohej të shtonte kushte përtej atyre të përmendura në nenin 7, gërma (f) të Direktivës në lidhje me përpunimin e ligjshëm të të dhënave.[405] Diçka e tillë i referohej një situate ku ligji spanjoll i mbrojtjes së të dhënave përmbante një dispozitë sipas së cilës palët private mund të pretendonin një interes legjitim për përpunimin e të dhënave personale vetëm nëse informacioni ishte shfaqur më parë në burime publike.

GJDBE-ja vërejti fillimisht se Direktiva 95/46[406] kishte për qëllim të garantonte që mbrojtja e të drejtave dhe lirive të personale në lidhje me përpunimit e të dhënave personale të ishte e barasvlershme në të gjitha Shtetet Anëtare. As përafrimi i ligjeve kombëtare të fushës nuk duhet të shkaktojë dobësim të mbrojtjes që ato ofrojnë. Përkundrazi, ai duhet të synojë të garantojë nivel të lartë mbrojtjeje në BE[407]. Për rrjedhojë, GJDBE-ja vlerësoi se "për shkak të objektivit që konsiston në garantimin e një niveli mbrojtjeje të barasvlershëm në të gjitha Shtetet Anëtare, neni 7 i Direktivës 95/46[408] përcakton një listë shteruese dhe të kufizuar rastesh në të cilat përpunimi i të dhënave personale mund të konsiderohet si i ligjshëm" . Gjithashtu "Shtetet Anëtare nuk mund t'i shtojnë nenit 7 të Direktivës 95/46[409] parime të reja në lidhje me ligjshmërinë e përpunimit të të dhënave personale, as të parashikojnë kritere shtesë të cilat do të modifikonin fushën e zbatimit të një prej gjashtë parimeve të parashikuara në këtë nen"[410]. GJDBE-ja pranoi se, kur bëhet fjalë për vendosjen në ekuilibër sipas nenit 7, gërma (f) të Direktivës 95/46/EC, është e mundur që të merret parasysh se ashpërsia e shkeljes së të drejtave themelore të subjektit të të dhënave nga përpunimi mund të variojë, në varësi të faktit nëse të dhënat në fjalë kanë qenë më parë ose jo në burime publike.

Megjithatë, neni 7, gërma (f) e Direktivës "ia ndalon Shtetit Anëtar të përjashtojë, në mënyrë kategorike dhe përgjithësuese, mundësinë e përpunimit të disa kategorive të të dhënave personale, pa lejuar që të drejtat dhe interesat e kundërta të vendosen në peshore në një rast të caktuar."

Referuar këtyre vlerësimeve, GJDBE-ja vendosi se neni 7, gërma (f) e Direktivës 95/46[411] duhet interpretuar si i tillë që "ndalon vendosje rregullash kombëtare, të cilat, në mungesë të pëlqimit të subjektit të të dhënave dhe me qëllim që të lejojnë këtë përpunim të dhënash personale të subjektit të të dhënave, meqenëse është i nevojshëm për ndjekjen e një interesi legjitim të subjektit të të dhënave, ose të një apo disa palëve të treta tek të cilat përhapen të dhënat, kërkojnë jo vetëm që të drejtat dhe liritë themelore të subjektit të të dhënave të respektohen, por gjithashtu edhe që të dhënat të jenë shfaqur në burime publike, duke përjashtuar kësisoj, në mënyrë kategorike dhe përgjithësuese, çdo lloj përpunimi të dhënash të cilat figurojnë në burime të tilla."[412]

---

[403] Direktiva e shfuqizuar e Mbrojtjes së të Dhënave, neni 7, gërma (f), tani Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 6, pika 1, gërma (f).

[404] GJDBE, Çështje të bashkuara C-468/10 dhe C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) dhe Federación de Comercio Electrónico y Marketing Directo (FECEMD) k. Administración del Estado*, 24 nëntor 2011.

[405] Direktiva e shfuqizuar e Mbrojtjes së të Dhënave, neni 7, gërma (f), tani Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 6, pika (1), gërma (f).

[406] Direktiva e shfuqizuar e Mbrojtjes së të Dhënave, tani Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave.

[407] GJDBE, Çështje të bashkuar C-468/10 dhe C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) dhe Federación de Comercio Electrónico y Marketing Directo (FECEMD) k. Administración del Estado*, 24 nëntor 2011, parag. 28. Shih Direktivën e Mbrojtjes së të Dhënave, Paragrafët 8 dhe 10 të Preambulës.

[408] Direktiva e shfuqizuar e Mbrojtjes së të Dhënave, neni 7, tani Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 6, pika (1), gërma (f).

[409] Direktiva e shfuqizuar e Mbrojtjes së të Dhënave, neni 7, tani Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 6.

[410] *Ibid.*

[411] Direktiva e shfuqizuar e Mbrojtjes së të Dhënave, neni 7, gërma (f), tani Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 6, pika (1), gërma (f).

[412] GJDBE, Çështje të bashkuara C-468/10 dhe C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) dhe Federación de Comercio Electrónico y Marketing Directo (FECEMD) k. Administración del Estado*, 24 nëntor 2011, parag. 40, 44 dhe 48–49.

Kurdo që të dhënat personale përpunohet bazuar në "interesat legjitimë", personi ka të drejtën ta kundërshtojë në çdo moment përpunimin, për shkaqe që lidhen me situatën e veçantë të tij apo të saj, në përputhje me nenin 21, pika 1 të GDPR-së. Kontrolluesit duhet të ndalë përpunimin, përveçse kur demonstron shkaqe detyruese legjitime për ta vijuar atë.

Për sa i përket **së drejtës së KiE-së,** në Konventën 108 të Modernizuar[413] dhe në rekomandimet e KiE-së gjenden formulime të ngjashme. Rekomandimi në lidhje me Profilizimin e njeh përpunimin e të dhënave personale për qëllime profilizimi si legjitim, nëse është i nevojshëm për interesat legjitimë të të tjerëve, "përveçse kur këto interesa tejkalohen nga të drejtat dhe liritë themelore të subjekteve të të dhënave".[414] Gjithashtu, "mbrojtja e të drejtave dhe lirive të të tjerëve" përmendet në nenin 8, pika 2 të KEDNJ-së, si një prej arsyeve legjitime për kufizimin e së drejtës për mbrojtje të të dhënave.

Shembull: Tek *Y k. Turqisë,*[415] kërkuesi ishte sieropozitiv. Meqenëse ai ishte pa ndjenja teksa mbërriti në spital, stafi i ambulancës informoi stafin e spitalit që pacienti ishte pozitiv me HIV. Kërkuesi pretendoi përballë GJEDNJ-së se përhapja e këtij informacioni kishte shkelur të drejtën e tij për respektim të jetës private. Megjithatë, duke pasur parasysh nevojën për të mbrojtur sigurinë e stafit të spitalit, transmetimi i këtij informacioni nuk u konsiderua si shkelje e të drejtave të tij.

4.1.2 Përpunimi i kategorive të veçanta të të dhënave (të dhënat sensitive)

E drejta e KiE-së ngarkon të drejtën kombëtare për përcaktimin e masave të përshtatshme të sigurisë për përdorimin e të dhënave sensitive, për sa kohë që përmbushen kushtet e nenit 6 të Konventës 108 të Modernizuar, konkretisht që masat e përshtatshme që plotësojnë dispozitat e tjera të Konventës të jenë të përcaktuara me ligj. E drejta e BE-së, në nenin 9 të GDPR-së, parashikon një sistem të hollësishëm për përpunimin e kategorive të veçanta të të dhënave (të quajtura gjithashtu 'të dhëna sensitive'). Këto të dhëna zbulojnë origjinën racore apo etnike, opinionet politike, besimet fetare ose filozofike dhe anëtarësinë ne sindikata, ashtu si edhe përpunimin e të dhënave gjenetike dhe biometrike, për qëllime të identifikimit unik të një personi fizik dhe për të dhënat në lidhje me shëndetin, jetën seksuale apo prirjen seksuale të një personi. Në parim, përpunimi i të dhënave sensitive është i ndaluar.[416]

Megjithatë, ekziston një listë shteruese përjashtimesh nga ky ndalim, e cila gjendet në nenin 9, pika 2 të Rregullores dhe të cilat përbëjnë arsye të ligjshme për përpunimin e të dhënave sensitive. Këto përjashtime përfshijnë situata ku:

- Subjekti i të dhënave ka dhënë shprehimisht pëlqimin për përpunimin e të dhënave;
- Përpunimi kryhet nga një organ jo-fitimprurës me qëllime politike, filozofike, fetare, ose sindikaliste në vazhdën e aktiviteteve të tij legjitime dhe ka të bëjë vetëm anëtarët, ish-anëtarët, ose personat që kanë kontakt të rregullt me të për qëllimet e saj:
- Përpunimi ka të bëjë me të dhëna të bëra haptazi publike nga subjekti i të dhënave;

[413] Raporti Shpegues i Konventës 108 të Modernizuar, parag. 46
[414] Këshilli i Evropës, Komiteti i Ministrave (2010), Rekomandimi CM/Rec(2010)13 dhe memorandumi shpjegues mbi mbrojtjen e personave në lidhje me përpunimin automatik të të dhënave personale në kontekstin e profilizimit , 23 nëntor 2010, neni 3, pika 4, gërma (b) (Rekomandimi mbi Profilizimin).
[415] ECtHR, *Y v. Turkey*, No. 648/10, 17 February 2015.
[416]

- Përpunimi është i nevojshëm për:
    - Për përmbushjen e detyrimeve dhe ushtrimin e të drejtave specifike, të kontrolluesit apo të subjektit të të dhënave në kontekstin e punësimit, sigurimeve shoqërore dhe mbrojtjes sociale;
    - Për mbrojtjen e interesave jetikë të subjektit të të dhënave apo të një personi tjetër fizik (kur subjekti i të dhënave nuk mund të japë pëlqimin;
    - Për të ngritur, ushtruar ose mbrojtur pretendime ligjore, ose kurdoherë që gjykatat veprojnë në cilësinë e tyre gjyqësore;
    - Për qëllime të shërbimit dhe parandalimit mjekësor: "për vlerësimin e kapacitetit të punës së punonjësit, diagnozës mjekësore, ofrimin e kujdesit shëndetësor dhe social, trajtimin, menaxhimin e sistemeve të kujdesit shëndetësor ose social dhe shërbimet mbi bazën e së drejtës evropiane ose të shtetit anëtar, ose në zbatim të kontratës me një profesionist shëndeti";
    - Për qëllime arkivore në interes publik, për qëllime të kërkimit shkencor ose historik apo për qëllime statistikore.
    - Për arsye të interesave publike në sferën e shëndetit publik;
    - Për shkaqe të interesit thelbësor publik.

Rrjedhimisht, për përpunimin e kategorive të veçanta të të dhënave, një marrëdhënie kontraktuese me subjektin e të dhënave nuk konsiderohet si bazë ligjore për përpunim legjitim të të dhënave sensitive, përveçse në zbatim të një kontrate me një profesionist shëndeti që i nënshtrohet detyrimit të fshehtësisë profesionale.[417]

Pëlqimi i dhënë shprehimisht nga subjekti i të dhënave

Në **të drejtën e BE-së**, arsyeja e parë e mundshme për përpunim të ligjshëm të dhënash, pavarësisht nëse janë apo jo të dhëna sensitive, është pëlqimi i subjektit të të dhënave. Në rastin e të dhënave sensitive, ky pëlqim duhet të jepet shprehimisht. E drejta e Bashkimit ose e Shtetit Anëtar mundet gjithsesi të parashikojë që ndalimi i përpunimit të kategorive të veçanta të të dhënave të mund të mos anulohet nga subjekti i të dhënave.[418] Një rast i tillë, për shembull, mund të jetë kur përpunimi përfshin risqe të pazakonta për subjektin e të dhënave.

E drejta e punësimit dhe e drejta e sigurimeve shoqërore dhe mbrojtjes sociale

Sipas **së drejtës së BE-së**, ndalesa e parashikuar në nenit 9, paragrafi 1, mund të hiqet, nëse përpunimi është i nevojshëm për zbatimin e detyrimeve apo të drejtave të kontrolluesit ose të subjektit të të dhënave në sferën e punësimit apo sigurimeve shoqërore. Megjithatë, përpunimi duhet të autorizohet nga e drejta e BE-së, e drejta kombëtare, apo një marrëveshje kolektive sipas së drejtës së brendshme, e cila të parashikojë garancitë e përshtatshme të mbrojtjes së të drejtave themelore dhe interesave të subjektit të të dhënave.[419] Dosjet e punësimit që mbajnë organizatat, mund të përmbajnë të dhëna personale sensitive sipas disa kushteve të specifikuara në GDPR dhe në të drejtën përkatëse kombëtare. Shembuj të dhënash sensitive mund të përfshijnë informacionin në lidhje me anëtarësimin në sindikata, ose në lidhje me shëndetin.

[417] Rregullorja e Përgjithshme e mbrojtjes së të Dhënave, neni 9, pika (2), gërmat (h) dhe (i).
[418] *Ibid.,* neni 9, pika (2), gërma (a).
[419] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 9, pika (2), gërma (b).

Interesat jetikë të subjektit të të dhënave apo të një personi tjetër

Sipas së drejtës së BE-së, ashtu si në rastin e të dhënave jo-sensitive, të dhënat sensitive mund të përpunohen për shkaqe të interesave jetikë të subjektit të të dhënave, ose të një personi tjetër fizik.[420] Kur përpunimi mbështetet tek interesat jetikë të një personi tjetër, kjo arsye legjitime mund të përdoret vetëm nëse përpunimi "qartazi nuk mund të mbështetet tek një bazë tjetër ligjore".[421] Në disa rast, përpunimi i të dhënave personale mund të mbrojë edhe interesat individualë ashtu edhe ato publikë, për shembull kur përpunimi është i nevojshëm për qëllime humanitare.[422]

Në mënyrë që përpunimi i të dhënave sensitive të jetë legjitim mbështetur tek kjo arsye, duhet që pëlqimi të ketë qenë i pamundur të kërkohej prej subjektit, për shkak se, për shembull, subjekti i të dhënave ka qenë pa ndjenja, ose nuk ka qenë prezent dhe nuk mund të kontaktohej. Me fjalë të tjera, personi ka qenë fizikisht ose ligjërisht i paaftë për të dhënë pëlqimin.

Organizatat bamirëse ose jo-fitimprurëse

Përpunimi i të dhënave personale është gjithashtu i lejuar gjatë aktiviteteve legjitime të fondacioneve, shoqatave, ose organeve të tjera jo-fitimprurëse me qëllime politike, filozofike, fetare ose sindikaliste. Megjithatë, përpunimi duhet të mbështetet vetëm tek anëtarët ose ish-anëtarët e organit, ose tek ata me të cilët organi ka kontakte të rregullta.[423] Të dhënat sensitive nuk mund të përhapen jashtë këtyre organeve pa pëlqimin e subjekteve të të dhënave.

Të dhënat e bëra publike haptazi nga subjekti i të dhënave

Neni 9, pika (2), gërma (e) e GDPR-së parashikon se përpunimi nuk është i ndaluar nëse ai ka të bëjë me të dhëna të cilat janë bërë haptazi publike nga subjekti i të dhënave. Pavarësisht se kuptimi i "të bërit publike haptazi nga subjekti i të dhënave" nuk është i përcaktuar në rregullore, për shkak se është një përjashtim nga ndalimi i përpunimit të të dhënave sensitive, ai duhet interpretuar në mënyrë shteruese dhe të kushtëzuar me faktin që subjekti i të dhënave t'i ketë bërë qëllimisht të dhënat e veta publike. Kështu, nëse një televizion transmeton një video të marrë nga një kamerë sigurie, ku tregohet, ndër të tjera, një zjarrfikës i cili plagoset teksa mundohet të largojë njerëzit nga një godinë, nuk mund të konsiderohet se zjarrfikësi i ka bërë publike qëllimisht të dhënat. Përkundrazi, nëse zjarrfikësi vendos të përshkruajë incidentin dhe të publikojë videon dhe fotografi në një faqe publike interneti, ai ose ajo ka kryer një veprim të qëllimshëm, pohues për publikimin e të dhënave personale. Është e rëndësishme të theksohet se bërja publike e të dhënave nga dikush, nuk përbën pëlqim, por një leje tjetër për përpunimin e kategorive të veçanta të të dhënave.

Fakti që subjekti i të dhënave ka bërë publike të dhënat personale të përpunuara, kjo nuk i përjashton kontrolluesit nga detyrimet sipas së drejtës për mbrojtje të të dhënave personale. Për shembull, parimi i kufizimit të qëllimit vijon të gjejë zbatim për të dhënat personale, edhe nëse ato të dhëna janë bërë publike.[424]

Pretendimet ligjore

Përpunimi i kategorive të veçanta të të dhënave "i cili është i nevojshëm për ngritjen, ushtrimin ose mbrojtjen e pretendimeve ligjore", qoftë në procedime gjyqësore, apo në një procedurë

[420] *Ibid*., neni 9, pika (2), gërma (c).
[421] *Ibid*., Paragrafi 46 i Preambulës.
[422] *Ibid.*
[423] *Ibid.,* neni 9, pika (2), gërma (d).
[424] Grupi i Punës së Nenit 29 (2013), *Opinioni 3/13 mbi kufizimin e qëllimit*, WP 203, Bruksel, 2 prill 2013, fq. 14.

administrative ose jashtë-gjyqësore,[425] është gjithashtu i lejuar sipas GDPR-së.[426] Në një rast të tillë, përpunimi duhet të jetë i rëndësishëm në lidhje me një pretendim ligjor të caktuar dhe në ushtrimin apo mbrojtjen përkatëse të tij dhe mund të kërkohet nga një prej palëve.

Kur veprojnë në cilësinë e tyre gjyqësore, gjykatat mund të përpunojnë kategori të veçanta të dhënash brenda kuadrit të zgjidhjes së një çështjeje ligjore.[427] Shembuj kategorish të tilla të veçanta të të dhënave të përpunuara në këtë kontekst mund të përfshijnë për shembull, të dhënat gjenetike kur përcaktohet prindi, apo të dhënat në lidhje me gjendjen shëndetësore kur një pjesë e provave përmban hollësi që lidhen me plagosjen e viktimës së një krimi.

Arsyet e interesit të rëndësishëm publik

Sipas nenit 9, pika 2, gërma (g) të GDPR-së, Shtetet Anëtare mund të parashikojnë edhe rrethana të tjera kur përpunohen të dhëna sensitive, me kusht që:

- Përpunimi i të dhënave të bëhet për arsye të interesit të rëndësishëm publik;
- Të jetë e parashikuar nga e drejta e BE-së apo ajo kombëtare;
- E drejta e BE-së apo e drejta kombëtare të jetë proporcionale, të respektojë të drejtën për mbrojtje të të dhënave dhe të parashikojë masa të përshtatshme dhe specifike për mbrojtjen e të drejtave dhe interesave të subjektit të të dhënave.[428]

Një shembull i njohur janë sistemet e dosjeve shëndetësore elektronike. Këto sisteme mundësojnë që të dhënat e shëndetit, të cilat janë mbledhur nga operatorët e kujdesit shëndetësor gjatë trajtimit të një pacienti, t'u vihen në dispozicion operatorëve të tjerë të kujdesit shëndetësor të këtij pacienti në shkallë të gjerë, zakonisht në mbarë vendin.

Grupi i Punës së Nenit 29 doli në përfundimin se ngritja e sistemeve të tilla nuk ishte e mundur sipas rregullave ligjore të atëhershme për përpunimin e të dhënave të pacientëve.[429] Megjithatë, sistemet e dosjeve shëndetësore elektronike mund të ngrihen nëse ato bazohen tek "arsyet e interesit të rëndësishëm publik".[430] Për ngritjen e tyre mund të nevojitet një bazë ligjore e qartë, e cila të parashikojë gjithashtu masat e nevojshme për të garantuar që sistemi të menaxhohet në mënyrë të sigurt.[431]

Arsye të tjera për përpunimin e të dhënave sensitive

GDPR-ja parashikon se të dhënat sensitive mund të përpunohen kur përpunimi është i nevojshëm:[432]

- për qëllimet e mjekësisë parandaluese ose të punës, për vlerësimin e kapacitetit të punës së punonjësit, diagnozës mjekësore, ofrimin e kujdesit shëndetësor dhe social, trajtimin, menaxhimin e sistemeve të kujdesit shëndetësor ose social dhe shërbimet mbi bazën e së drejtës së BE-së ose të Shtetit Anëtar, ose në zbatim të kontratës me një profesionist shëndeti;
- për shkaqe të interesit publik në sferën e shëndetit publik, si mbrojtja ndaj kërcënimeve të rënda ndërkufitare për shëndetin ose garantimin e standardeve të larta të cilësisë dhe sigurisë të kujdesit shëndetësor dhe të produkteve mjekësore ose pajisjeve mjekësore,

[425] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, Paragrafi 52 i Preambulës.
[426] *Ibid*., neni 9, pika (2), gërma (f).
[427] *Ibid*.
[428] *Ibid*., neni 9, pika (2), gërma (g).
[429] Grupi i Punës së Nenit 29 (2007), *Dokument Pune në lidhje me përpunimin e të dhënave personale të shëndetit në dosjet mjekësore elektronike (EHR)*, WP 131, Bruksel, 15 shkurt 2007. Shih gjithashtu nenin 9, pika 3 të Rregullores së Përgjithshme të Mbrojtjes së të Dhënave.
[430] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 9, pika 2, gërma (g).
[431] Grupi i Punës së Nenit 29 (2007), *Dokument Pune në lidhje me përpunimin e të dhënave personale të shëndetit në dosjet mjekësore elektronike (EHR)*, WP 131, Bruksel, 15 shkurt 2007.
[432] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 9, pika 2, gërmat (h), (i) dhe (j).

mbi bazën e së drejtës së BE-së ose të Shtetit Anëtar. E drejta duhet të parashikojë masa të përshtatshme dhe specifike për të garantuar të drejtat e subjektit të të dhënave;

- për qëllime arkivore, të kërkimit shkencor apo statistikore bazuar në të drejtën e Bashkimit apo të Shtetit Anëtar. E drejta duhet të jetë proporcionale me qëllimin e ndjekur, të respektojë thelbin e së drejtës së mbrojtjes së të dhënave dhe të parashikojë masa të përshtatshme dhe specifike për të garantuar të drejtat dhe interesat e subjektit të të dhënave.

Kushtet shtesë sipas së drejtës kombëtare

GDPR-ja u lejon gjithashtu Shteteve Anëtare të shtojnë ose mbajnë kushte të tjera, përfshirë edhe kufizime për përpunimin e të dhënave gjenetike, biometrike dhe të shëndetit.[433]

4.2 Rregullat në lidhje me sigurinë e përpunimit

Pikat kryesore

- Rregullat në lidhje me sigurinë e përpunimit detyrojnë kontrolluesin dhe përpunuesin të marrë masat e përshtatshme teknike dhe organizative për të parandaluar çdo ndërhyrje të paautorizuar tek aktivitetet e përpunimit të të dhënave.
- Niveli i nevojshëm i sigurisë së të dhënave përcaktohet nga:
  - Karakteristikat e sigurisë të disponueshme në treg për çdo lloj përpunimi;
  - Kostot;
  - Rreziqet që paraqet përpunimi i të dhënave për të drejtat dhe liritë themelore të subjekteve të të dhënave.
- Garantimi i konfidencialitetit të të dhënave personale është pjesë e një parimi të përgjithshëm të njohur nga Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave.

Qoftë në të drejtën e **BE-së**, ashtu edhe të **KiE-së**, kontrolluesit kanë detyrimin e përgjithshëm të jenë transparentë dhe të përgjegjshëm kur përpunojnë të dhëna personale dhe sidomos për sa i përket shkeljeve ndaj të dhënave, kur shkelje të tilla ndodhin. Në rast shkeljeve ndaj të dhënave personale, kontrolluesit duhet të njoftojnë autoritetet mbikëqyrëse, përveç rastit kur shkelja nuk ka të ngjarë të krijojë rrezik për të drejtat dhe liritë e personave fizikë. Subjektet e të dhënave duhet të informohen gjithashtu për shkeljen ndaj të dhënave personale, kur ajo ka të ngjarë të krijojë rrezik të lartë për drejtat dhe liritë e personave fizikë.

4.2.1. Elementet e sigurisë së të dhënave

Sipas dispozitave përcaktuese në të **drejtën e BE-së**:

> *"Duke marrë parasysh gjendjen e teknologjisë, shpenzimet e zbatimit dhe natyrën, objektin, kontekstin dhe qëllimet e përpunimit si dhe riskun e probabilitetit të ndryshueshëm dhe ashpërsinë për të drejtat dhe liritë e personave fizikë, kontrolluesi dhe përpunuesi zbatojnë masa të përshtatshme teknike dhe organizative për të siguruar një nivel sigurie të përshtatshëm për riskun [...]."*[434]

[433] *Ibid*., neni 9, pika 2, gërma (h) dhe 9, pika 4.
[434] *Ibid*., neni 32, pika 1.

Këto masa përfshijnë ndër të tjera:

- Pseudonimizimin dhe kodimin e të dhënave personale;[435]
- Aftësinë për të siguruar konfidencialitetin, integritetin, disponueshmërinë dhe aftësinë ripërtëritëse;[436]
- aftësinë për të rivendosur disponibilitetin dhe aksesin tek të dhënat personale në kohën e duhur;[437]
- një proces të testimit, vlerësimit të rregullt të efektivitetit të masave teknike dhe organizative për të garantuar sigurinë e përpunimit.[438]

Një dispozitë të ngjashme e gjejmë edhe tek **e drejta e KiE-së**:

"*Secila Palë duhet të sigurojë që kontrolluesi dhe kur gjen zbatim edhe përpunuesi të marrin masat e përshtatshme të sigurisë kundër rreziqeve të tilla si aksesi aksidental apo i autorizuar, shkatërrimi, humbja, përdorimi, modifikimi apo përhapja e të dhënave personale*."[439]

Në të drejtën e BE-së dhe në të drejtën e KiE-së, një shkelje ndaj të dhënave e cila mund të ketë ndikim tek të drejtat dhe liritë e personave, e detyron kontrolluesin të njoftojë autoritetin mbikëqyrës për shkeljen (shih Seksionin 4.2.3).

Shpesh janë hartuar norma sektoriale, kombëtare dhe ndërkombëtare, për të garantuar sigurinë e përpunimit të të dhënave. Vula Evropiane e Privatësisë (EuroPrise), për shembull, është një projekt i eTEN-it (Rrjetet Trans-Evropiane të Telekomunikacioneve) të BE-së, i cili studion mundësitë e certifikimin të produkteve, sidomos të programeve kompjuterike, me qëllim lehtësimin e përputhshmërisë me të drejtën evropiane të mbrojtjes së të dhënave. Agjencia Evropiane për Sigurinë e Rrjeteve dhe të Informacionit (ENISA) u krijua me qëllim përmirësimin e kapacitetit të BE-së, të shteteve të saj anëtare dhe të ndërmarrjeve për të parandaluar, trajtuar dhe për t'iu përgjigjur problemeve të sigurisë së rrjeteve dhe të informacionit.[440] ENISA publikon rregullisht analiza në lidhje me kërcënimet aktuale të sigurisë, si dhe këshilla për t'iu përgjigjur atyre.[441]

Siguria e të dhënave nuk përftohet thjesht duke pasur pajisjet e duhura (fizike dhe softuerë), por duhen gjithashtu edhe rregulla të brendshme organizimi të përshtatshme, të cilat duhet të përfshijnë problematikat e mëposhtme:

- informim periodik të të gjithë të punësuarve për rregullat e sigurisë së të dhënave dhe për detyrimet sipas kuadrit ligjor të mbrojtjes së të dhënave, sidomos në lidhje me detyrimet e konfidencialitetit;
- ndarje e qartë e përgjegjësive dhe përcaktim i qartë i kompetencave në çështje të përpunimit të të dhënave, sidomos për sa i përket vendimeve për përpunimin e të dhënave personale dhe transferimin e të dhënave tek palë të treta;
- përdorim i të dhënave personale në përputhje me udhëzimet e personit kompetent, apo sipas rregullave të përgjithshme të përcaktuara;

[435] *Ibid*., neni 32, pika 1, gërma (a).
[436] *Ibid*, neni 32, pika 1, gërma (b).
[437] *Ibid*., neni 32, pika 1, gërma (c).
[438] *Ibid*., neni 32, pika 1, gërma (d).
[439] Konventa 108 e modernizuar, neni 7, pika 1.
[440] Rregullorja (BE) nr. 526/2013 e Parlamentit Evropiane dhe e Këshillit e 21 majit 2013 për sa i përket Agjencisë së Bashkimit Evropian për Sigurinë e rrjeteve dhe të Informacionit (ENISA) dhe që shfuqizon Rregulloren (KE) nr. 460/2004, FZ 2013 L 165.
[441] Për shembull, ENISA (2016), Cyber Security and Resilience of smart cars. Good practices and recommendations; ENISA (2016), Security of Mobile Payments and Digital Wallets.

- mbrojtje e aksesit në mjedise, pajisje fizike dhe softuerë të kontrolluesit ose të përpunuesit, përfshirë kontrollin e autorizimit të aksesit;
- garantimin se autorizimet e aksesit tek të dhënat personale janë lëshuar nga personi kompetent dhe mbi bazën e dokumentacionit të duhur;
- protokolle automatike të aksesit elektronik tek të dhënat personale dhe kontrolle periodike të këtyre protokolleve nga zyra e kontrollit të brendshëm (çka kërkon që të gjitha aktivitetet e përpunimit të të dhënave të jenë të regjistruara);
- dokumentim të kujdeshëm të formave të tjera të përhapjes të ndryshme nga aksesi automatik i të dhënave, me qëllim që të vërtetohet se nuk kanë ndodhur transmetime të paligjshme të dhënash.

Trajnimi dhe edukimi i duhur i të gjithë personelit në lidhje sigurinë e të dhënave, është gjithashtu një aspekt i rëndësishëm i masave efikase të sigurisë. Po ashtu duhen marrë edhe masa verifikimi për të siguruar që masat e përshtatshme të mos jenë thjesht në letër, por të zbatohen e të funksionojnë në praktikë (si për shembull me auditime të brendshme ose të jashtme).

Masat që synojnë përmirësimin e nivelit të sigurisë së një kontrolluesi apo përpunuesi përfshijnë instrumente të tilla si nëpunësit e mbrojtjes së të dhënave personale, edukimin e punonjësve në lidhje me sigurinë, auditimet periodike, testimin e penetrimit dhe vulat e sigurisë.

Shembull: tek çështja *I. kundër Finlandës*,[442] kërkuesja nuk kishte qenë në gjendje të provonte se kartela e saj mjekësore ishte aksesuar në mënyrë të paligjshme nga punonjës të tjerë të spitalit në të cilin ajo punonte. Për rrjedhojë, pretendimi i saj për shkelje të së drejtës për mbrojtje të të dhënave ishte rrëzuar nga gjykatat kombëtare. GJEDNJ-ja doli në përfundimin se ishte shkelur neni 8 i KEDNJ-së, pasi sistemi i kartelave mjekësore të spitalit "nuk mundësonte verifikimin retroaktiv të përdorimit të kartelave të pacientëve, duke qenë se shfaqte vetëm pesë shikimet më të fundit dhe se ky informacion fshihej sapo kartela zëvendësohej në arkiva". Për GJEDNJ-në, mospërputhja e sistemit të arkivimit dhe aksesit në kartela të këtij spitali me kriteret ligjore të së drejtës kombëtare, ishte element përcaktues, të cilin gjykatat kombëtare nuk e kishin marrë si duhet në konsideratë.

BE-ja ka miratuar Direktivën mbi sigurinë e rrjeteve dhe sistemeve të informacionit (Direktiva NIS),[443] e cila është instrumenti i parë ligjor në lidhje me sigurinë kibernetike që mbulon të gjithë BE-në. Direktiva synon nga njëra anë të përmirësojë sigurinë kibernetike në nivel kombëtar dhe të përforcojë bashkëpunimin brenda BE-së në anën tjetër. Ajo përcakton gjithashtu detyrime për operatorët e shërbimeve thelbësore (përfshirë operatorët e sektorit të energjisë, shëndetësisë, sistemit bankar, transportit, infrastrukturës digjitale, etj.) dhe për operatorët e shërbimeve digjitale për të menaxhuar rreziqet, për të garantuar sigurinë e rrjeteve dhe sistemeve të tyre të informacion, si dhe për të raportuar incidentet e sigurisë.

Perspektivat

Në shtator 2017, Komisioni Evropian propozoi një projekt-rregullore që synon ndryshimin e mandatit të ENISA-s, me qëllim që të përfshiheshin kompetencat dhe përgjegjësitë e reja të agjencisë sipas Direktivës NIS. Objektivi i kësaj projekt-rregulloreje është të zgjerojë detyrat e ENISA-s dhe të përforcojë rolin e saj si "pikë referimi në ekosistemin e sigurisë kibernetike

[442] GJEDNJ, *I. kundër Finlandës*, nr. 20511/03, 17 korrik 2008.
[443] Direktiva (BE) 2016/1148 e Parlamentit Evropian dhe e Këshillit e 6 korrikut 2016 në lidhje me masat për një nivel të përbashkët të lartë sigurie të rrjeteve dhe sistemeve të informacionit në Bashkim, FZ 2016 L 194.

në BE”.[444] Projekt-rregullorja nuk cënon parimet e GDPR-së dhe nëpërmjet qartësimit të elementeve të nevojshme që përbëjnë sistemet evropiane të certifikimit të sigurisë kibernetike, ajo do të përforcojë gjithashtu sigurinë e të dhënave personale. Paralelisht, në shtator 2017, Komisioni Evropian propozoi një projekt-rregullore që saktëson elementet të cilat duhen marrë parasysh nga operatorët e shërbimeve digjitale, për të garantuar sigurinë e rrjeteve dhe sistemeve të tyre të informacionit, sikurse kërkohet në nenin 16, pika 8 të Direktivës NIS. Në momentin e hartimit të këtij manuali, vijojnë ende diskutimet në lidhje me këto dy propozime.

4.2.2. Konfidencialiteti

Sipas së drejtës së BE-së, GDPR-ja njeh konfidencialitetin e të dhënave personale si një parim të përgjithshëm[445]. Operatorët e shërbimeve të komunikimeve elektronike të disponueshme për publikun, duhet të garantojnë konfidencialitetin. Ata i nënshtrohet gjithashtu detyrimit për të ruajtur sigurinë e shërbimeve të tyre.[446]

Shembull: Një punonjës i një shoqërie sigurimesh, merr një telefonatë në vendin e punës nga dikush që paraqitet si klient, i cili i kërkon informacion në lidhje me kontratën e tij të sigurimit.

Detyrimi për të ruajtur konfidencialitetin e të dhënave të klientëve, përcakton që punonjësi duhet të zbatojë të paktën masat minimale të sigurisë, përpara se të përhapë të dhënat personale. Kjo mund të bëhet për shembull duke propozuar që t’ia kthejë telefonatën në numrin e telefonit të regjistruar në dosjen e klientit.

Sipas nenit 5, pika 1, gërma (f), të dhënat personale duhen përpunuar në mënyrë të tillë që të garantohet siguri e përshtatshme e të dhënave personale, përfshirë mbrojtje nga përpunimi i paautorizuar apo i paligjshëm dhe nga humbja aksidentale, shkatërrimi, ose dëmtimi, me anë të masave teknike ose organizative (“integriteti dhe konfidencialiteti”).

Sipas nenit 32, kontrolluesi dhe përpunuesi duhet të marrin masa teknike dhe organizative për të garantuar nivel të lartë sigurie. Këto masa mund të përfshijnë ndër të tjera pseudonimizimin dhe kodimin e të dhënave personale, aftësinë për të garantuar konfidencialitetin, integritetin, disponueshmërinë dhe qëndrueshmërinë e vazhdueshme të përpunimit, vlerësimin dhe testimin e efektshmërisë së masave dhe aftësinë për të rikuperuar përpunimin në rast incidenti fizik apo teknik. Gjithashtu, aderimi në një kod të miratuar sjelljeje, apo në një mekanizëm të miratuar certifikimi mund të përdoret si element për të provuar respektimin e parimit të integritetit dhe konfidencialitetit. Nga ana tjetër, sipas nenit 28 të GDPR-së, kontrata e lidhur mes kontrolluesit dhe përpunuesit duhet të përcaktojë që përpunuesi garanton se personat e autorizuar për

[444] Propozim për një Rregullore të Parlamentit Evropian dhe të Këshillit në lidhje me ENISA-n, “Agjencinë e BE-së për Sigurinë Kibernetike” dhe që shfuqizon Rregulloren (BE) 526/2013 dhe mbi Certifikimin e Sigurisë Kibernetike të Teknologjisë së Informacionit dhe Komunikimit (Akti i Sigurisë Kibernetike), COM(2017)477, 13 shtator 2017, fq. 6.
[445] GDPR, neni 5, pika 1, gërma (f).
[446] Direktiva mbi privatësinë dhe komunikimet elektronike, neni 5, pika 1.

përpunimin e të dhënave personale janë angazhuar të respektojnë konfidencialitetin, ose i nënshtrohen një detyrimi të përshtatshëm ligjor për konfidencialitetin.

Detyrimi për ruajtjen e konfidencialitetit nuk mbulon edhe situatat ku një person merr dijeni për të dhënat në cilësinë e tij si person privat dhe jo si punonjës i kontrolluesit apo i përpunuesit. Në këtë rast, nenet 32 dhe 28 të GDPR-së nuk gjejnë zbatim, për shkak se përdorimi i të dhënave personale nga personat privatë përjashtohet krejtësisht nga fusha e zbatimit të rregullores, kur një përdorim i tillë është në kufijtë e përjashtimit të të ashtuquajturit aktivitet familjar.[447] Përjashtimi i aktivitetit familjar është përdorimi i të dhënave personale "nga ana e një personi fizik në vazhdën e një aktiviteti thjesht personal ose familjar".[448] Që prej vendimit të GJDBE-së për çështjen Bodil Lindqvist,[449] ky përjashtim duhet sidoqoftë të interpretohet ngushtësisht, sidomos për sa i përket përhapjes së të dhënave. Veçanërisht përjashtimi i aktiviteti familjar nuk shtrihet tek publikimi i të dhënave personale për një numër të pakufizuar marrësish në internet, apo tek një përpunim që ka aspekte profesionale apo tregtare (për më shumë hollësi në lidhje me çështjen shih Seksionet 2.1.2, 2.2.2 dhe 2.3.1).

"Konfidencialiteti i komunikimeve" është një aspekt tjetër i konfidencialitetit, i cili është objekt i një *lex specialis*. Rregullat e veçanta për garantimin e konfidencialitetit të komunikimeve elektronike sipas Direktivës e-Privatësia detyrojnë Shtetet Anëtare që të ndalojnë çdo person, përveç përdoruesve, apo pa pëlqimin e përdoruesve, që të dëgjojnë, regjistrojnë, ruajnë apo të kryejnë çdo lloj interceptimi, apo përgjimi të komunikimeve dhe të dhënave të trafikut të tyre.[450] E drejta kombëtare mund të lejojë përjashtime nga ky parim vetëm për qëllime të sigurisë kombëtare, mbrojtjes, parandalimit apo zbulimit të krimeve dhe vetëm nëse masa të tilla janë të nevojshme dhe proporcionale me qëllimet e ndjekura.[451] Të njëjtat rregulla do të zbatohen sipas Rregullores së ardhshme të e-Privatësisë, por fusha e zbatimit të instrumentit juridik në këtë fushë do të shtrihet edhe tek shërbimet e komunikimeve elektronike të aksesueshme nga publiku, me qëllim që të përfshihen gjithashtu komunikimet që kalojnë nëpërmjet shërbimeve të aksesit të drejtpërdrejtë ("over-the-top"), sikurse janë aplikacionet e telefonave celularë.

Sipas së drejtës së KiE-së, kriteri i konfidencialitetit nënkuptohet nga nocioni i sigurisë së të dhënave në nenin 7, pika 1 të Konventën 108 të Modernizuar, i cili trajton sigurinë e të dhënave.

Për përpunuesit, konfidencialiteti nënkupton se ata nuk mund të përhapin të dhëna tek palët e treta apo tek marrësit e tjerë pa autorizim. Për punonjësit e kontrolluesit apo përpunuesit, konfidencialiteti detyron që ata t'i përdorin të dhënat personale vetëm në përputhje me udhëzimet e eprorëve të tyre kompetentë.

Detyrimi i konfidencialitetit duhet përfshirë në çdo kontratë të lidhur midis kontrolluesve dhe përpunuesve. Gjithashtu, kontrolluesit dhe përpunuesit janë të detyruar të marrin masat

[447] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 2, pika 2, gërma (c).
[448] *Ibid.*
[449] GJDBE, C-101/01, *Procedimi penal kundër Bodil Lindqvist*, 6 nëntor 2003.
[450] Direktiva mbi privatësinë dhe komunikimet elektronike, neni 5, pika 1.
[451] *Ibid.*, neni 15, pika 1.

konkrete për të përcaktuar detyrim ligjor konfidencialiteti për punonjësit e tyre, e cila normalisht bëhet duke përfshirë klauzola konfidencialiteti në kontratën e punësimit.

Shkelja e detyrimit profesional për ruajtjen e konfidencialitetit ndëshkohet sipas së drejtës penale të shumë Shteteve Anëtare të BE-së dhe Palëve të Konventës 108.

4.2.3. Njoftimet për shkeljet ndaj të dhënave personale

Nje shkelje ndaj të dhënave personale nënkupton një shkelje sigurie që sjell shkatërrimin aksidental ose të paligjshëm, humbjen, ndryshimin apo përhapjen e paautorizuar, ose aksesin në të dhënat personale të përpunuara.[452] Paçka se teknologjitë e reja, sikurse kodimi, tashmë ofrojnë më shumë mundësi për të garantuar sigurinë e përpunimit, shkeljet ndaj të dhënave mbeten fenomen i zakonshëm. Shkaqet e shkeljeve ndaj të dhënave mund të variojnë nga gabimet aksidentale të njerëzve që punojnë brenda një organizate, tek kërcënimet e jashtme, sikurse janë piratët informatikë dhe organizatat kriminale kibernetike.

Shkeljet ndaj të dhënave mund të shkaktojnë dëme të mëdha për privatësinë dhe të drejtat për mbrojtje të të dhënave të personave të cilët, si rezultat i shkeljes, humbin kontrollin tek të dhënat e tyre personale. Shkeljet mund të sjellin vjedhje identiteti apo mashtrim, humbje financiare apo dëme materiale, humbje konfidencialiteti të të dhënave personale që mbrohen nga sekreti profesional dhe dëmtim të reputacionit të subjektit të të dhënave. Tek Udhëzuesi në lidhje me njoftimin e shkeljes ndaj të dhënave personale sipas Rregullores 2016/679, Grupi i Punës së Nenit 29 shpjegon se shkeljet mund të shkaktojnë tre lloje ndikimesh tek të dhënat personale: përhapje, humbje dhe/ose modifikim të tyre.[453] Gjithashtu detyrimi për të marrë masa me qëllim garantimin e sigurisë së përpunimit, sikurse shpjegohet në Seksionin 4.2, ka rëndësi edhe për të garantuar që në rast shkeljeje, kontrolluesit t'i menaxhojnë ato në mënyrën dhe kohën e duhur.

Autoritetet mbikëqyrëse dhe personat shpesh nuk janë në dijeni që një shkelje ka ndodhur dhe diçka e tillë pengon personat që të marrin masa për t'u mbrojtur nga pasojat negative të saj. Për të konfirmuar të drejtat e personave dhe për të kufizuar ndikimin e shkeljeve ndaj të dhënave, **BE-ja dhe KiE-ja** kanë përcaktuar detyrimin për kontrolluesit që të kryejnë njoftim në rrethana të caktuara.

Sipas Konventës 108 të Modernizuar të **KiE-së**, Palët Kontraktuese duhet minimalisht të detyrojnë kontrolluesit të njoftojnë autoritetin mbikëqyrës kompetent për shkeljet ndaj të dhënave të cilat mund të cënojnë rëndë të drejtat e subjekteve të të dhënave. Ky njoftim duhet bërë "pa vonesë të panevojshme".[454]

E drejta e BE-së përcakton një sistem të hollësishëm rregullimi të afateve dhe përmbajtjes së njoftimeve.[455] Kështu, kontrolluesit duhet të njoftojnë autoritetet mbikëqyrëse për disa shkelje ndaj të dhënave pa vonesë dhe kur është e mundur, brenda 72 orëve nga momenti i marrjes

[452] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave Personale, neni 4, pika 12; Shih gjithashtu Grupi i Punës së Nenit 29 (2017), *Guidelines on Personal data breach notification under Regulation 2016/679*, WP250, 3 tetor 2017, fq. 8.
[453] Grupi i Punës së Nenit 29 (2017), *Guidelines on Personal data breach notification under Regulation 2016/679*, WP250, 3 tetor 2017, fq. 6.
[454] Konventa 108 e Modernizuar, neni 7, pika 2; Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafët 64-66.
[455] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 33 dhe 34.

dijeni për shkeljen. Nëse ata nuk njoftojnë brenda afatit prej 72 orësh, atëherë njoftimi duhet të përmbajë edhe shpjegime në lidhje me vonesën. Kontrolluesit përjashtohen nga detyrimi për njoftim vetëm nëse ata janë në gjendje të vërtetojnë se shkelja ndaj të dhënave nuk ka gjasa të shkaktojë rrezik për të drejtat dhe liritë e subjekteve.

Rregullorja përcakton edhe minimumin e informacionit që duhet të përmbajë njoftimi, i tillë që t'i mundësojë autoritetit mbikëqyrës të ndërmarrë veprimet e nevojshme.[456] Njoftimi duhet të përmbajë të paktën një përshkrim të natyrës së shkeljes ndaj të dhënave dhe të kategorive e numrit të përafërt të subjekteve të të dhënave që janë prekur, një përshkrim të pasoja të mundshme të shkeljes dhe të masave që ka marrë kontrolluesi për të zbutur dhe adresuar pasojat e saj. Gjithashtu, duhen dhënë emri dhe adresa e nëpunësit të mbrojtjes së të dhënave, ose të çdo personi tjetër kontakti, në mënyrë që autoriteti mbikëqyrës kompetent të ketë mundësi të marrë më shumë informacion nëse është e nevojshme.

Nëse shkelja ndaj të dhënave ka të ngjarë të shkaktojë cënim të rëndë të të drejtave dhe lirive të personale, kontrolluesit duhet t'i informojnë ato persona (subjekte të dhënash) për shkeljen pa vonesë të panevojshme.[457] Informacioni që u duhet dhënë subjekteve të të dhënave, sikurse dhe përshkrimi i shkeljes ndaj të dhënave, duhet të jetë në gjuhë të thjeshtë dhe qartë dhe të përmbajë informacion të ngjashëm me atë që nevojitet për njoftimin e autoriteteve mbikëqyrëse. Në rrethana të caktuara, kontrolluesit mund të përjashtohen nga detyrimi për të njoftuar subjektet e të dhënave për disa lloj shkeljesh. Përjashtimet janë kur kontrolluesi ka marrë masat e përshtatshme teknike dhe organizative të mbrojtjes dhe këto masa janë zbatuar për të dhënat personale që janë prekur nga shkelja ndaj të dhënave, sidomos ato që i bëjnë të dhënat personale të palexueshme për askënd që nuk është i autorizuar të ketë akses në to, sikurse është kodimi. Veprimet e ndërmarra nga kontrolluesi në vijim të një shkeljeje, që kanë si qëllim të garantojnë se risku për të drejtat e subjekteve të të dhënave nuk ka më të ngjarë të materializohet, mund të përjashtojnë gjithashtu kontrolluesin nga detyrimi për të njoftuar subjektet e të dhënave. Së fundmi, nëse njoftimi kërkon përpjekje jo proporcionale nga ana e kontrolluesit, subjektet e të dhënave mund të informohen në lidhje me shkeljen në mënyra të tjera, si për shembull me komunikim publik apo me mënyra të ngjashme.[458]

Detyrimi për të njoftuar autoritetet mbikëqyrëse dhe subjektet e të dhënave për shkeljet ndaj të dhënave i ngarkohet kontrolluesve. Megjithatë, shkeljet ndaj të dhënave mund të ndodhin pavarësisht nëse përpunimi kryhet nga një kontrollues apo një përpunues. Për këtë arsye, është thelbësore të garantohet që përpunuesi të jetë gjithashtu i detyruar të njoftojë shkeljet ndaj të dhënave. Në këtë rast, përpunuesit duhet t'ia njoftojnë shkeljet ndaj të dhënave kontrolluesit pa vonesa të paarsyeshme.[459] Më pas është kontrolluesi përgjegjës për të njoftuar autoritetet mbikëqyrëse dhe subjektet e të dhënave të prekur, në respekt të rregullave dhe afateve të sipërcituara.

[456] *Ibid*., neni 33, pika 3.
[457] *Ibid*., neni 34.
[458] *Ibid*., neni 34, pika 3, gërma (c).
[459] Ibid., neni 33, pika 2.

4.3. Rregullat në lidhje me përgjegjshmërinë dhe nxitjen e përputhshmërisë

Pikat kryesore

- Për të garantuar përgjegjshmërinë e përpunimit të të dhënave personale, kontrolluesit dhe përpunuesit duhet të mbajnë regjistrat e aktiviteteve përpunuese që kryhen nën përgjegjësinë e tyre dhe t'ua paraqesin ato autoriteteve mbikëqyrëse me kërkesën e tyre.
- Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave përcakton instrumente të ndryshëm për nxitjen e përputhshmërisë:
  - Caktimin e nëpunësit të mbrojtjes së të dhënave në disa situate të caktuara;
  - Zhvillimin e një vlerësimi të ndikimit përpara nisjes së aktiviteteve përpunuese të cilat kanë gjasa të shkaktojnë risqe të mëdha për të drejtat dhe liritë e personave;
  - Konsultimin paraprak me autoritetin përkatës mbikëqyrës nëse vlerësimi i ndikimit tregon se përpunimi paraqet risqe që nuk mund të adresohen;
  - Kodet e sjelljes për kontrolluesit dhe përpunuesit, të cilët të saktësojnë zbatimin e rregullores në sektorë të ndryshëm të përpunimit;
  - Mekanizmat e certifikimit, vulat dhe shenjat.
- E drejta e KiE-së propozon instrumente të ngjashëm për nxitjen e përputhshmërisë më Konventës 108 të Modernizuar

Parimi i përgjegjshmërisë ka rëndësi të veçantë për garantimin e zbatimit të rregullave të mbrojtjes së të dhënave në Evropë. Kontrolluesi është përgjegjës dhe duhet të jetë në gjendje të vërtetojë përputhshmërinë me rregullat e mbrojtjes së të dhënave. Përgjegjshmëria nuk duhet të hyjë në lojë vetëm kur ndodh shkelja. Përkundrazi, kontrolluesit kanë detyrimin proaktiv të ndjekin politikat e përshtatshme të menaxhimit të të dhënave në të gjitha fazat e përpunimit të të dhënave. Legjislacioni evropian në fushën e mbrojtjes së të dhënave detyron kontrolluesit të zbatojnë masa teknike dhe organizative për të garantuar dhe për të qenë në gjendje të vërtetojnë se përpunimi është duke u kryer në përputhje me ligjin. Ndërmjet këtyre masave është caktimi i nëpunësve të mbrojtjes së të dhënave, mbajtja e regjistrave dhe dokumentacionit në lidhje me përpunimit dhe zhvillimi i vlerësimeve të ndikimit tek privatësia.

4.3.1. Nëpunësit e Mbrojtjes së të Dhënave

Nëpunësit e Mbrojtjes së të Dhënave (DPO-të) janë personat të cilët këshillojnë në lidhje me përputhshmërinë me rregullat e mbrojtjes së të dhënave të organizatave që kryejnë përpunim të dhënash. Ata janë 'gur-themeli i përgjegjshmërisë' meqenëse ata lehtësojnë pajtueshmërinë, gjithë duke shërbyer edhe si ndërmjetës midis autoriteteve mbikëqyrëse, subjekteve të të dhënave dhe organizatës e cila i ka caktuar.

Sipas së drejtës së KiE-së, neni 10, pika 1 e Konventës 108 të Modernizuar përcakton një detyrim të përgjithshëm për përgjegjshmëri nga ana e kontrolluesve dhe përpunuesve. Kjo dispozitë detyron kontrolluesit dhe përpunuesit të marrin të gjitha masat e përshtatshme për zbatimin e rregullave të mbrojtjes së të dhënave të përcaktuara në konventë dhe të jenë në gjendje të vërtetojnë se përpunimi i të dhënave nën kontrollin e tyre pajtohet me dispozitat e konventës. Paçka se konventa nuk saktëson masat konkrete që kontrolluesi dhe përpunuesit duhet të marrin, Raporti Shpjegues i Konventës 108 të Modernizuar parashikon se caktimi i një DPO-je mund të jetë një nga masat e mundshme që ndihmojnë në vërtetimin e përputhshmërisë. Nëpunësit e Mbrojtjes së të Dhënave duhet të disponojnë të gjitha mjetet e nevojshme për përmbushjen e detyrës së tyre.[460]

Përkundër së drejtës së KiE-së, **në të drejtën e BE-së,** caktimi i Nëpunësit të Mbrojtjes së të Dhënave nuk lihet gjithnjë në diskrecionin e kontrolluesve dhe përpunuesit, porse është e detyrueshme në disa kushte të caktuara. GDPR-ja e njeh rolin kyç të DPO-së në sistemin e ri të qeverisjes dhe përmban dispozita të hollësishme në lidhje me caktimin e nëpunësit, funksionin dhe detyrat e tij.[461]

GDPR-ja e bën të detyrueshëm caktimin e DPO-së në tre raste specifike: kur autoriteti ose organi publik kryen përpunim; kur aktiviteti kryesor i kontrolluesit apo përpunuesit konsiston në operacione përpunimi të cilat kërkojnë monitorim të rregullt dhe sistematik të subjekteve të të dhënave në një shkallë të gjerë, ose kur aktivitetet kryesore konsistojnë në përpunim në shkallë të gjerë të kategorive të veçanta të të dhënave, apo të të dhënave personale lidhur me dënimet dhe veprat penale.[462] Megjithëse nocione të tilla si 'monitorimi sistematik në shkallë të gjerë' dhe 'aktivitetë kryesore' nuk përcaktohen në rregullore, Grupi i Punës së Nenit 29 ka miratuar udhëzues në lidhje me mënyrës se si duhen interpretuar ato.[463]

[BOX TYPE 2]

Shembull: disa shoqëri të rrjeteve sociale dhe motorëve të kërkimit ka të ngjarë të konsiderohet kontrolluese, kur operacionet e përpunimit kërkojnë monitorim të rregullt dhe sistematik të subjekteve të të dhënave në shkallë të gjerë. Modeli tregtar i këtyre shoqërive mbështetet tek përpunimi i sasive të mëdha të të dhënave personale dhe ato gjenerojnë të ardhura të konsiderueshme nëpërmjet ofrimit të shërbimeve të reklamave të shënjestruara, si dhe duke lejuar shoqëri tregtare të bëjnë marketing në faqet e tyre. Marketingu i shënjestruar është një mënyrë publikimi reklamash bazuar në demografi dhe në historikun e blerjeve apo sjelljen e mëparshme të konsumatorëve. Për rrjedhojë, ato kanë nevojë të kryejnë monitorim sistematik të zakoneve dhe sjelljeve të subjekteve të të dhënave në internet.

Shembull: një spital dhe një shoqëri sigurimi shëndetësor janë shembull tipik kontrolluesish, aktivitetet e së cilëve konsistojnë në përpunimin në shkallë të gjerë të kategorive të veçanta të të dhënave personale. Të dhënat që zbulojnë informacion në lidhje me shëndetin e një personi, përbëjnë kategori të veçanta të dhënash qoftë sipas së drejtës së KiE-së, ashtu edhe në atë të BE-së, të cilat rrjedhimisht kërkojnë mbrojtje më të madhe. E drejta e BE-së njeh për më tepër edhe të dhënat gjenetike dhe biometrike si kategori të veçanta. Për aq kohë sa institucionet

[460] Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 87.
[461] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 37–39.
[462] *Ibid*., neni 37, pika 1.
[463] Grupi i Punës së Nenit 29 (2017), *Guidelines on Data Protection Officers ('DPOs')*, WP 243 rev.01, rishikimi i fundit dhe miratuar më 5 prill 2017.

mjekësore dhe shoqëritë e sigurimeve përpunojnë të dhënat të tilla në shkallë të gjerë, ato janë të detyruara në pajtim më GDPR-së të caktojnë një nëpunës të mbrojtjes së të dhënave.

Gjithashtu, neni 37 pika 4 e GDPR-së parashikon se në raste të tjera përveç atyre të përcaktuara në nenin 37, pika 1, kontrolluesi, përpunuesi, ose shoqatat dhe organet e tjera që përfaqësojnë kategoritë e kontrolluesve ose përpunuesve, mund ose duhet, në rast se e drejta e Bashkimit apo Shtetit Anëtar e përcakton si detyrim, të caktojnë një nëpunës për mbrojtjen e të dhënave.

Të gjitha organizatat e tjera nuk janë ligjërisht të detyruara të caktojnë një DPO. Megjithatë, GDPR-ja parashikon se kontrolluesit dhe përpunuesit mund të zgjedhin vullnetarisht të caktojnë një DPO, duke i lejuar ndërkohë mundësinë Shteteve Anëtare ta bëjnë të detyrueshëm caktimin e tij për më shumë lloje organizatash përtej atyre të parashikuara nga rregullorja.[464]

Me caktimin nga ana e kontrolluesit të një DPO-je, ai duhet të garantojë që ai apo ajo "të përfshihet në mënyrën dhe kohën e duhur, në të gjitha çështjet që kanë të bëjnë me mbrojtjen e të dhënave personale." Brenda organizatës.[465] Për shembull, DPO-të duhet të përfshihen në dhënien e këshillave në lidhje me zhvillimin e vlerësimeve të ndikimit tek mbrojtja e të dhënave dhe në krijimin dhe mbajtjen e regjistrave të aktiviteteve përpunuese të organizimit. Për t'u mundësuar DPO-ve që të përmbushin në mënyrë të efektshme detyrat e tyre, kontrolluesit dhe përpunuesit duhet t'u sigurojnë atyre burimet e nevojshme, përfshirë ato financiare, infrastrukturën dhe pajisjet. Kërkesa të tjera që duhen plotësuar përfshijnë edhe që DPO-ve t'u jepet koha e nevojshme për përmbushjen e funksioneve të tyre dhe trajnimi i vazhdueshëm i cili u mundëson zhvillimin e ekspertizës dhe përditësimin me të gjitha zhvillimet e legjislacionit të mbrojtjes së të dhënave.[466]

GDPR-ja përcakton disa garanci bazë për të siguruar që DPO-të veprojnë në mënyrë të pavarur. Kontrolluesit dhe përpunuesit duhet të garantojnë që gjatë ushtrimit të detyrave të tyre në lidhje me mbrojtjen e të dhënave, DPO-të të mos marrin udhëzime nga shoqëria, përfshirë personat në nivelin më të lartë të menaxhimit. Gjithashtu, ata nuk duhen pushuar nga puna apo ndëshkuar në asnjë lloj mënyre për shkak të ushtrimit të funksioneve së tyre.[467] Marrim për shembull rastin kur një DPO këshillon kontrolluesin apo përpunuesin që të kryejë një vlerësim të ndikimit tek të dhënat, për shkak se ai apo vlerëson se përpunimi ka gjasa të shkaktojë risqe të larta për subjektet e të dhënave. Shoqëria nuk është dakord me këshillën e DPO-së, nuk e konsideron atë të bazuar dhe për pasojë vendos të mos vijojë me zhvillimin e vlerësimit të ndikimit. Shoqëria mund të injorojë sugjerimin, por nuk mund ta shkarkojë apo ndëshkojë DPO-në për këtë.

Së fundmi, misioni dhe detyrat e DPO-së parashikohen hollësisht në nenin 39 të GDPR-së. Në to përfshihen detyrimet për të informuar dhe këshilluar shoqëritë dhe punonjësit që kryejnë përpunim në lidhje me detyrimet e tyre sipas legjislacionit dhe të monitorojnë përputhshmërinë me rregullat e BE-së dhe ato kombëtare për mbrojtjen e të dhënave, nëpërmjet zhvillimit të auditimeve dhe trajnimit të stafit të përfshirë në operacione përpunimi. DPO-të duhet gjithashtu

[464] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 37, pikat 3 dhe 4.
[465] *Ibid*., neni 38, pika 1.
[466] Grupi i Punës së Nenit 29 (2017), *Guidelines on Data Protection Officers ('DPOs')*, ËP 243 rev.01, varianti i fundit i rishikuar dhe miratuar më 5 prill 2017, parag. 3.1.
[467] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 38, pikat 2 dhe 3.

të bashkëpunojnë me autoritetin mbikëqyrës dhe të veprojnë si pikë kontakti me këtë të fundit, për çështje që kanë të bëjnë me përpunimin e të dhënave, sikurse për shembull për një shkelje ndaj të dhënave.

Për sa i takon të dhënave personale që administrohen nga institucionet dhe organet e BE-së, Rregullorja 45/2001 përcakton se çdo institucion dhe organ i Bashkimit duhet të caktojë një DPO. DPO-ja ka për detyrë të garantojë zbatimin e saktë të rregullores brenda institucioneve dhe organeve të BE-së dhe që subjektet e të dhënave dhe kontrolluesit e të dhënave të informohen në lidhje me të drejtat dhe detyrimet e tyre.[468] Ai apo ajo ka gjithashtu përgjegjësinë për t'iu përgjigjur kërkesave të EDPS-së dhe të bashkëpunojnë me të kur është e nevojshme. Në mënyrë të ngjashme me GDPR-në, Rregullorja 45/2001 përmban dispozita në lidhje me pavarësinë e DPO-ve gjatë ushtrimit të detyrës dhe detyrimin për t'u siguruar atyre stafin dhe burimet e nevojshme.[469] DPO-të duhet gjithashtu të njoftohen përpara se një institucion apo organ i BE-së (apo departamentet e këtyre organizatave) të nisë operacione përpunimi dhe duhet të mbajnë regjistrin e të gjitha operacioneve të përpunimit që janë njoftuar.[470]

4.3.2 Regjistrat e aktiviteteve të përpunimit

Shoqëritë janë shpesh ligjërisht të detyruara të dokumentojnë dhe regjistrojnë aktivitetet e tyre, në mënyrë që të jenë në gjendje të vërtetojnë përputhshmërinë dhe për t'u vënë përpara përgjegjësisë. Një rast i rëndësishëm është e drejta fiskale dhe auditi, për të cilat të gjitha shoqëritë janë të detyruara të mbajnë dokumentacion të gjerë dhe regjistra. Përcaktimi i kritereve të ngjashme në fusha të tjera juridike, sidomos në legjislacionin e mbrojtjes së të dhënave, është po aq e rëndësishme, meqenëse mbajtja e regjistrave është një mënyrë e rëndësishme për të lehtësuar përputhshmërinë me rregullat e mbrojtjes së të dhënave. Për rrjedhojë, **e drejta e BE-së** përcakton se kontrolluesit, apo përfaqësuesit e tyre duhet të mbajnë një regjisër të aktiviteteve përpunuese që kryhen nën përgjegjësinë e tyre.[471] Ky detyrim ka për qëllim të garantojë që nëse është e nevojshme, autoritetet mbikëqyrëse të disponojnë dokumentacionin e nevojshëm që u mundëson të verifikojnë ligjshmërinë e përpunimit.

Informacioni që duhet dokumentuar është si vijon:

- Emri dhe të dhënat e kontaktit të kontrolluesit dhe kur është rasti të kontrolluesit të përbashkët, përfaqësuesit të kontrolluesit dhe të nëpunësit të mbrojtjes së të dhënave;
- Qëllimet e përpunimit;
- Përshkrimin e kategorive të subjekteve të të dhënave dhe të kategorive të të dhënave personale që lidhen me përpunimin;
- informacion mbi kategoritë e marrësve të cilëve u janë komunikuar ose do t'u komunikohen të dhënat personale;
- informacion nëse janë kryer apo do të kryhen transferime të dhënash personale drejt vendeve të treta apo organizatave ndërkombëtare;

[468] Shih nenin 24, pika 1 të Rregullores (KE) nr. 45/2001 për listën e plotë të detyrave të DPO-së.
[469] Rregullorja (KE) nr. 45/2001, neni 24, pikat 6 dhe 7.
[470] *Ibid*., nenet 25 dhe 26.
[471] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 30.

- kur është e mundur, afatet kohore të parashikuara për fshirjen e kategorive të ndryshme të të dhënave personale, si dhe një përshkrim të masave teknike të marra me qëllim garantimin e sigurisë së përpunimit.[472]

Detyrimi për të mbajtur regjistra të aktiviteteve përpunuese sipas GDPR-së nuk bie vetëm mbi kontrolluesit, por edhe mbi përpunuesit. Ky është një zhvillim i rëndësishëm, pasi përpara miratimit të rregullores, kontrata e lidhur midis kontrolluesit dhe përpunuesit mbulonte kryesisht detyrimet përpunuesit. Tashëm detyrimi i tyre për të mbajtur regjistrat është drejtpërdrejt i parashikuar me lig.

GDPR-ja përcakton një përjashtim nga ky detyrim. Kriteri për mbajtjen e regjistrave nuk gjen zbatim për një ndërmarrje apo organizatë (kontrolluese apo përpunuese) e cila ka të punësuar më pak se 250 persona. Megjithatë, ky përjashtim i nënshtrohet kriterin që organizata në fjalë të mos ndërmarrë përpunim që ka të ngjarë të shkaktojë risk të lartë për të drejtat dhe liritë e subjekteve të të dhënave, që përpunimi të jetë vetëm i rastësishëm dhe të mos përfshijë kategori të veçanta të dhënash sikurse janë referuar në nenin 9 pika 1, apo të dhëna personale në lidhje me dënimet dhe veprat penale të referuara në nenin 10.

Mbajtja e regjistrave të aktiviteteve përpunuese duhet t'i mundësojë kontrolluesve dhe përpunuesve të vërtetojnë përputhshmërinë me rregulloren. Ajo u mundëson gjithashtu autoriteteve mbikëqyrëse të monitorojnë ligjshmërinë e përpunimit. Kur një autoritet mbikëqyrës kërkon akses në ato regjistra, kontrolluesit dhe përpunuesit janë të detyruar të bashkëpunojnë dhe t'ua vënë ato në dispozicion.

4.3.3 Vlerësimi i ndikimit tek mbrojtja e të dhënave dhe konsultimi paraprak

Operacionet përpunuese paraqesin disa risqe të qenësishme për të drejtat e personave. Të dhënat personale mund të humbasin, t'u komunikohen palëve të paautorizuara, apo të përpunohen në mënyrë të paligjshme. Natyrisht, risqet variojnë në varësi të natyrës dhe qëllimit të përpunimit. Për shembull, operacionet në shkallë të gjerë që përfshijnë përpunimin e të dhënave sensitive, kanë një nivel shumë më të lartë risku për subjektet e të dhënave krahasuar me risqet e mundshme kur një shoqëri e vogël përpunon adresat dhe numrat personalë të telefonave të punonjësve të saj.

Meqenëse lindin teknologji të reja dhe përpunimi bëhet gjithnjë e më i ndërlikuar, kontrolluesit duhet t'i shmangin këto risqe nëpërmjet verifikimit të ndikimit të mundshëm të përpunimit të synuar përpara nisjes së operacionit të përpunimit. Diçka e tillë u mundëson organizatave të identifikojnë, trajtojnë dhe zgjidhin paraprakish në mënyrën e duhur risqet, duke kufizuar në mënyrë të konsiderueshme gjasat e një ndikimi negativ tek personat për shkak të përpunimit.

Vlerësimet e ndikimit tek mbrojtja e të dhënave janë të parashikuara edhe **në të drejtën e KiE-së**, ashtu edhe **në të drejtën e BE-së**. Në kuadrin ligjor të KiE-së, neni 10, pika 2 e Konventës 108 të Modernizuar detyron Palët Kontraktuese të garantojnë që kontrolluesit dhe përpunuesit "të verifikojnë ndikimin e mundshëm që përpunimi i synuar i të dhënave mund të ketë tek të drejtat dhe liritë themelore të subjekteve të të dhënave, përpara nisjes së atij përpunimi" dhe pas kryerjes së vlerësimit, ta konceptojnë përpunimin në mënyrë të tillë që të parandalohen, apo minimizohen risqet që lidhen me përpunimin.

Legjislacioni i BE-së përcakton një detyrim të ngjashëm, më të hollësishëm, për kontrolluesit që përfshihen në fushën e zbatimit të GDPR-së. Neni 35 parashikon se duhet kryer një vlerësim ndikimi kur përpunimi mund të rezultojë në një risk të lartë për të drejtat dhe liritë e personave. Rregullorja nuk përcakton se si duhet vlerësuar mundësia e riskut, por përkundrazi tregon se cilat mund të jenë ato risqe.[473] Ajo rendit një listë operacionesh përpunimi të konsideruara me risk të lartë dhe për të cilat vlerësimi paraprak i ndikimit është veçanërisht i rëndësishëm, konkretisht në rastet kur:

[472] *Ibid*., neni 30, pika 1.
[473] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, Preambula, Paragrafi 75.

- Të dhënat personale përpunohen për të marrë vendime në lidhje me personat fizikë, pas një analize sistematike dhe të gjerë të aspekteve personale që lidhen me personat (profilizimi);
- Kur të dhënat sensitive dhe të dhënat personale në lidhje me dënimet dhe veprat penale përpunohen në shkallë të gjerë;
- Përpunimi përfshin monitorimin në shkallë të gjerë dhe sistematik të zonave me akses publik.

Autoritetet mbikëqyrëse duhet të miratojnë dhe publikojnë një listë të llojeve të operacioneve përpunuese të cilat nevojitet të jenë subjekt i vlerësimit të ndikimit. Ato mund të përcaktojnë gjithashtu një listë operacionesh përpunimi që përjashtohen nga ky detyrim.[474]

Kur një vlerësim ndikimi është i detyrueshëm, kontrolluesit duhet të analizojnë domosdoshmërinë dhe propocionalitetin e përpunimit, si dhe risqet e mundshme për të drejtat e individëve. Vlerësimi i ndikimit duhet gjithashtu të përmbajë masat e planifikuara të sigurisë për të adresuar risqet e identifikuara. Në mënyrë që të përcaktojnë listat, autoritetet mbikëqyrëse janë të detyruara të bashkëpunojnë me njëra-tjetrën dhe me Bordin Evropian të Mbrojtjes së të Dhënave. Në këtë mënyrë do të garantohet qasje njëtrajtshme në të gjithë BE-në për ato operacione për të cilat nevojitet kryerja e vlerësimit të ndikimit dhe kontrolluesit do të përballen me kërkesa të ngjashme, pavarësisht vendndodhjes së tyre.

Nëse pas kryerjes së një vlerësimi ndikimi duket se përpunimi mund të krijojë risk të lartë për individët dhe asnjë masë nuk është marrë për zgjidhjen e këtij risku, kontrolluesi duhet të konsultohet me autoritetin mbikëqyrës përkatës përpara nisjes së operacionit të përpunimit.[475]

Grupi i Punës së Nenit 29 ka miratuar udhëzime në lidhje me vlerësimet e ndikimit tek mbrojtja e të dhënave dhe mbi mënyrën nëpërmjet së cilës përcaktohet nëse përpunimi ka të ngjarë ose jo të krijojë një risk të lartë.[476] Ai ka hartuar nëntë kritere për të përcaktuar nëse vlerësimi i ndikimit është i nevojshëm në një rast të caktuar:[477] (1) analizim ose pikëzim; (2) vendimmarrje automatike me pasojë ligjore ose të ngjashme me të; (3) monitorim sistematik; (4) të dhëna sensitive; (5) përpunim të dhënash në shkallë të gjerë; (6) struktura të dhënash që korrespondojnë ose janë kombinuar; (7) të dhëna që kanë të bëjnë me subjekte vulnerabil të dhënash; (8) përdorim inovativ ose aplikim zgjidhjesh teknologjike ose organizative; (9) kur përpunim në vetvete "pengon subjektet e të dhënave në ushtrimin e një të drejte apo përdorimin e një shërbimi ose kontrate". Grupi i Punës së Nenit 29 ka krijuar rregullin që operacionet e përpunimit të cilat plotësojnë më pak se dy kritere, paraqesin nivele risku të ulëta dhe nuk nevojiten vlerësimet e ndikimit tek mbrojtja e të dhënave, ndërsa ato që plotësojnë dy ose më shumë kritere, kërkojnë një vlerësim të tillë. Në rastet kur është e paqartë nëse nevojitet një vlerësim ndikimi tek mbrojtja e të dhënave, Grupi i Punës së Nenit 29 rekomandon kryerjen e këtij vlerësimi, pasi ai është "një mjet i dobishëm që ndihmon kontrolluesit e të dhënave të jenë në përputhje me legjislacionin e mbrojtjes së të dhënave".[478] Kur përdoret një teknologji e re përpunimi të dhënash, është e rëndësishme që të kryhet vlerësimi i ndikimit tek mbrojtja e të dhënave.[479]

4.3.4 Kodet e sjelljes

Kodet e sjelljes kanë si qëllim të përdoren në sektorë të ndryshëm të industrisë, për të përvijuar dhe saktësuar zbatimin e GDPR-së në sektorët specifikë. Për kontrolluesit dhe përpunuesit e të dhënave personale, krijimi i kodeve të tilla përmirëson përputhshmërinë dhe zbatimin e rregullave të BE-së për mbrojtjen e të dhënave. Ekspertiza e aktorëve të sektorit do të mundësojë gjetjen e zgjidhjeve me karakter praktik dhe që për rrjedhojë janë më të prira të zbatohen nga të tjerët. Duke pranuar rëndësinë e këtyre kodeve për zbatimin efikas të legjislacionit të mbrojtjes së të dhënave,

[474] Ibid., neni 36, pika 1; Grupi i Punës së Nenit 29 (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, Bruksel, 4 tetor 2017.
[475] *Ibid*., neni 36, pika 1; Grupi i Punës së Nenit 29 (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, Bruksel, 4 tetor 2017.
[476] Grupi i Punës së Nenit 29 (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, Bruksel, 4 tetor 2017.
[477] *Ibid*., fq. 9–11.
[478] *Ibid*., fq. 9.
[479] *Ibid*.

GDPR-ja fton Shtetet Anëtare, autoritetet mbikëqyrëse, Komisionin dhe Bordin Evropian të Mbrojtjes së të Dhënave që të nxisin hartimin e kodeve të sjelljes, të cilat kanë si qëllim të kontribuojnë në zbatimin e duhur të rregullores në BE.[480] Kodet mund të saktësojnë zbatimin e rregullores në sektorë specifikë, përfshirë edhe për çështje të tilla si mbledhja e të dhënave personale, informacioni që u duhet dhënë subjekteve të të dhënave dhe publikut dhe ushtrimi i të drejtave të subjekteve të të dhënave.

Në mënyrë që kodet e sjelljes të jenë në përputhje me rregullat që përcakton GDPR-ja, kodet duhet të depozitohen tek autoriteti mbikëqyrës përpara miratimit të tyre. Autoriteti mbikëqyrës në vijim jep mendim në lidhje me përputhshmërinë e projekt-kodit me rregulloren dhe nëse mendon se kodi përmban garancitë e duhura, ai e miraton atë.[481] Autoritetet mbikëqyrëse duhet të publikojnë kodet e sjelljes që janë miratuar, bashkë me kriteret mbi të cilat është mbështetur miratimi i tyre. Kur një projekt-kod sjelljeje ka të bëjë me aktivitete përpunimi në disa Shtete Anëtare, autoriteti mbikëqyrës kompetent përpara se të miratojë projekt-kodin, të bëjë ndryshime ose shtesa, duhet ta depozitojë pranë Bordit Evropian të Mbrojtjes së të Dhënave, i cili duhet të japë mendim për pajtueshmërinë e kodit me GDPR-në. Komisioni, nëpërmjet procedurës së miratimit të akteve, mund të vendosë që kodi i sjelljes i miratuar që i është përcjellë, ka vlefshmëri të përgjithshme brenda Bashkimit.

Angazhimi në një kod sjelljeje ofron përparësi të rëndësishme, si për subjektet e të dhënave, ashtu edhe për kontrolluesit dhe përpunuesit. Këto kode përmbajnë udhëzime të hollësishme, të cilat përshtatin kërkesat ligjore për sektorët specifikë dhe rrisin transparencën e aktiviteteve të përpunimit. Kontrolluesit dhe përpunuesit mund të përdorin angazhimin në kode si provë që vërteton përputhshmërinë e tyre me legjislacionin e BE-së dhe si mjet për forcimin e imazhit të tyre publik si organizata që i japin përparësi dhe respektojnë mbrojtjen e të dhënave në operacionet e tyre. Kodet e sjelljes së miratuar, së bashku me angazhimet e detyrueshme dhe të zbatueshme, mund të përdoren si masa të përshtatshme sigurie për transferimin e të dhënave tek shtete të treta. Për të garantuar që organizatat që janë të angazhuara në kode sjelljeje i zbatojnë vërtet ato, një organ special (i akredituar nga autoriteti përkatës mbikëqyrës) mund të caktohet për të mbikëqyrur dhe për të garantuar përputhshmërinë. Për të përmbushur detyrat e tij me efektshmëri, organi duhet të jetë i pavarur, të ketë ekspertizë të provuar për çështje që janë objekt rregullimi nga kodi i sjelljes dhe të kenë procedura transparente dhe struktura që i mundësojnë menaxhimin e ankesave në lidhje me shkeljet e këtij kodi.[482]

Sipas së drejtës së KiE-së, Konventa 108 e Modernizuar parashikon se niveli i mbrojtjes së të dhënave që garantohet nga legjislacioni kombëtar, mund të përforcohet në mënyrë të dobishme nga masa rregullues vullnetare, siç janë kodet e praktikave të mira ose kodet e sjelljes profesionale. Megjithatë, këto përbëjnë vetëm masa vullnetare sipas Konventës 108 të Modernizuar: nuk mund të nxirret asnjë detyrim ligjor për miratimin e këtyre masave, paçka se janë të kështillueshme dhe edhe vetë këto masa nuk janë të mjaftueshme për të garantuar përputhshmëri të plotë me konventën.[483]

4.3.5 Certifikimi

Përveç kodeve të sjelljes, edhe mekanizmat e certifikimit, si dhe vulat e shenjat e mbrojtjes së të dhënave, janë mjete të tjera nëpërmjet të cilave kontrolluesit dhe përpunuesit mund të vërtetojnë

[480] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 40, pika 1.
[481] *Ibid*., neni 40, pika 5.
[482] *Ibid*., neni 41, pikat 1 dhe 2.
[483] Raporti Shpjegues i Konventës 108 të Modernizuar, parag. 33.

përputhshmërinë me GDPR-në. Për këtë qëllim, rregullorja parashikon një sistem vullnetar certifikimi, nëpërmjet të cilit disa organe apo autoritete mbikëqyrëse mund të japin certifikime. Kontrolluesit dhe përpunuesit që zgjedhin të angazhohen në mekanizma certifikimi, mund të përftojnë më shumë shikueshmëri dhe besueshmëri, meqenëse certifikimet, vulat dhe shenjat u mundësojnë subjekteve të të dhënave të vlerësojnë me shpejtësi nivelin e mbrojtjes së përpunimit të të dhënave të organizatave. Duhet nënvizuar se fakti që një kontrollues apo përpunues zotëron një certifikim të tillë, nuk zvogëlon detyrimet dhe përgjegjësitë e tij për respektimin e të gjitha kërkesave të rregullores.

4.4 Mbrojtja e të dhënave që në fazën e konceptimit dhe me parapërzgjedhje

Mbrojtja e të dhënave që në fazën e konceptimit

E drejta e BE-së kërkon që kontrolluesit të marrin masa për të zbatuar në mënyrë të efektshme parimet e mbrojtjes së të dhënave dhe për të integruar garancitë e nevojshme në mënyrë që të plotësojnë kriteret e rregullores dhe të mbrojnë të drejtat e subjekteve të të dhënave.[484] Këto masa duhen zbatuar si në momentin e përpunimit, ashtu edhe kur përcaktohen mjetet e përpunimit. Për të zbatuar këto masa, kontrolluesi duhet të marrë në konsideratë nivelin e zhvillimit, kostot e zbatimit, natyrën, qëllimin dhe objektivat e përpunimit të të dhënave, si dhe risqet dhe ashpërsinë e tyre për të drejtat dhe liritë e subjektit të të dhënave.[485]

E drejta e KiE-së përcakton se kontrolluesit dhe përpunuesit duhet të analizojnë efektin e mundshëm të përpunimit të të dhënave personale tek të drejtat dhe liritë e subjekteve të të dhënave përpara nisjes së përpunimit. Gjithashtu, kontrolluesit dhe përpunuesit janë të detyruar të konceptojnë përpunimin e të dhënave në mënyrë të tillë që të parandalojnë, apo të minimizojnë riskun e ndërhyrjes tek këto të drejta e liri dhe të zbatojnë masa teknike dhe organizative që marrin në konsideratë ndërlikimet për të drejtën e mbrojtjes së të dhënave personale në të gjitha etapat e përpunimit të të dhënave.[486]

Mbrojtja e të dhënave me parapërzgjedhje

E drejta e BE-së kërkon që kontrolluesi të zbatojnë masat e përshtatshme për të garantuar që do të përpunohen me parapërcaktim vetëm të dhënat personale që janë të nevojshme për qëllimet. Ky detyrim zbatohet për sasinë e të dhënave të mbledhura, shtrirjes së përpunimit të tyre, afateve të mbajtjes dhe aksesueshmërisë së tyre.[487] Një masë e tillë duhet të garantojë, për shembull, që jo të gjithë punonjësit e kontrolluesve të kenë akses tek të dhënat personale të subjekteve. EDPS-ja ka dhënë orientime të mëtejshme tek *Udhëzuesi për vlerësimin e domosdoshmërisë së masave që kufizojnë të drejtën themelore për mbrojtje të të dhënave personale*.[488]

E drejta e KiE-së kërkon që kontrolluesit dhe përpunuesit të zbatojnë masa teknike dhe organizative që marrin në konsideratë ndërlikimet për të drejtën e mbrojtjes së të dhënave dhe të zbatojnë masa

[484] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 25, pika 1.
[485] Shih Grupi i Punës së Nenit 29 (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP248 rev.01, 4 tetor 2017. Shih gjithashtu ENISA (2015), Privacy and Data Protection by Design-from policy to engineering, 12 janar 2015.
[486] Konventa 108 e Modernizuar, neni 10, pikat 2 dhe 3, Raporti Shpjegues i Konventës 108 të Modernizuar, parag. 89.
[487] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 25, pika 2.
[488] Mbikëqyrësi Evropian i Mbrojtjes së të Dhënave (EDPS), (2017), *Necessity Toolkit*, Bruksel, 11 prill 2017.

teknike dhe organizative duke marrë parasysh ndërlikimet për të drejtën e mbrojtjes së të dhënave personale në të gjitha etapat e përpunimit të të dhënave.[489]

Në vitin 2016, ENISA publikoi një raport në lidhje me mjetet dhe shërbimet e disponueshme për mbrojtjen e privatësisë.[490] Ndër parashtrime të tjera, ky vlerësim ofron një listë kriteresh dhe parametrash që shërbejnë si indikatorë të praktikave të mira, apo të këqija në fushën e privatësisë. Ndërsa disa kritere lidhen drejtpërdrejtë me dispozitat e GDPR-së – sikurse përdorimi i pseudonimizimi dhe i mekanizmave të miratuara të certifikimit – të tjerat kanë të bëjnë me iniciativa inovative për të garantuar privatësinë që në fazën e konceptimit dhe me parapërzgjedhje. Për shembull, kriteri i përdorueshmërisë, megjithëse nuk lidhet drejtpërdrejt me privatësinë, mund ta përforcojë atë, për shkak se ai mund të bëjë të mundur që të përdoret në një shkallë më të gjerë një pajisje apo shërbim mbrojtjeje privatësie. Në fat, pajisjet e mbrojtjes së privatësisë që janë të vështira të zbatohen në praktikë, mund të kenë nivel përdorimi shumë të ulët nga publiku i gjerë, pavarësisht nëse ofrojnë garanci tepër të forta për mbrojtjen e privatësisë. Për më tepër, kriteri i pjekurisë dhe qëndrueshmërisë së një pajisjeje të mbrojtjes së privatësisë, d.m.th. mënyra se si pajisja zhvillohet me kalimin e kohës dhe u përgjigjet sfidave aktuale, ose të reja për privatësinë, është me rëndësi thelbësore. Teknologji të tjera që përforcojnë privatësinë, për shembull në kontekstin e komunikimeve të sigurta, përfshijnë kodimin nga skaji në skaj (komunikim ku personat e vetëm që mund të lexojnë mesazhet janë personat që komunikojnë); kodimin klient-server (kodimi i kanalit të komunikimit midis klientit dhe një serveri), autentifikimi (verifikimi i identiteteve të palëve që komunikojnë) dhe komunikimi anonim (asnjë palë e tretë nuk mund të identifikojë palët që komunikojnë).

[489] Konventa 108 e Modernizuar, neni 10, pika 3, Raporti Shpjegues i Konventës 108 të Modernizuar, parag. 89.
[490] ENISA, PETs controls matrix: A systematic approach for assessing online and mobile privacy tools, 20 dhjetor 2016.

5 Mbikëqyrja e pavarur

BE	Çështje të trajtuara	KiE
Karta, neni 8, pika 3 Traktati për Funksionimin e BE-së, neni 16, pika 2 Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 51–59 GJDBE, C-518/07, *Komisioni Evropian k. Republikës Federale të Gjermanisë* [GC], 2010 GJDBE, C-614/10, *Komisioni Evropian k. Republikës së Austrisë* [GC], 2012 GJDBE, C-288/12, *Komisioni Evropian k. Hungarisë* [GC], 2014 GJDBE, C-362/14, *Maximillian Schrems k. Komisionerit për Mbrojtjen e të Dhënave* [GC], 2015 Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 60–67 Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 68–76	Autoritetet mbikëqyrëse Bashkëpunimi ndërmjet autoriteteve mbikëqyrëse Bordi Evropian i Mbrojtjes së të Dhënave	Konventa 108 e Modernizuar, neni 15 Konventa 108 e Modernizuar, nenet 16–21

Pikat kryesore

- Mbikëqyrja e pavarur është një komponent thelbësor i legjislacionit evropian të mbrojtjes së të dhënave, përcaktuar në nenin 8, pika 3 të Kartës.
- Për të garantuar mbrojtje të efektshme të të dhënave, e drejta kombëtare duhet të përcaktojë ngritjen autoriteteve të pavarura të mbrojtjes së të dhënave.

- Autoritetet mbikëqyrëse duhet të veprojnë në pavarësi të plotë, e cila duhet të garantohet nga ligji organic dhe të pasqyrohet në strukturën specifike organizative të autoritetit mbikëqyrës.
- Autoritetet mbikëqyrëse kanë kompetenca dhe detyra specifike, ndër të cilat përfshihen:
    - Mbikëqyrja dhe promovimi i mbrojtjes së të dhënave në nivel kombëtar;
    - Këshillimi i subjekteve të të dhënave dhe kontrolluesve, sikurse edhe i qeverisë, apo publikut të gjerë;
    - Të dëgjojnë ankesat dhe të ndihmojnë subjektet e të dhënave në raste shkeljesh të pretenduara të së drejës për mbrojtje të të dhënave;
    - Mbikëqyrja e kontrolluesve dhe përpunuesve.
- Autoritetet mbikëqyrëse kanë gjithashtu kompetencën të ndërhyjnë nëse është e nevojshme duke:
    - Paralajmëruar, udhëzuar, deri edhe gjobitur kontrolluesit dhe përpunuesit;
    - Urdhëruar korrigjimin, bllokimin apo fshirjen;
    - Vendosur ndalimin e përpunimit ose të gjobës administrative;
    - Referuar çështje në gjykatë.
- Meqenëse përpunimi i të dhënave personale shpesh përfshin kontrollues, përpunues dhe subjekte të dhënash që ndodhen në shtete të ndryshme, autoritetet mbikëqyrëse janë të detyruara të bashkëpunojnë me njëra-tjetrën për çështje ndërkufitare, për të garantuar mbrojtje të efektshme të personave në Evropë.
- Në BE, Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave përcakton një mekanizëm të sportelit unik për çështje që kanë të bëjnë me përpunim ndërkufitar. Disa shoqëri kryejnë aktivitete përpunimi ndërkufitar, për shkak se përpunojnë të dhëna personale në kontekstin e aktiviteteve të strukturave që ndodhen në më shumë se një Shtet Anëtar, ose në kontekstin e një strukture të vetme në Bashkim, por të cilat prekin në mënyrë domethënëse subjekte të dhënash në më shumë se një Shtet Anëtar. Në kuadrin e këtij mekanizmi, këto shoqëri do të kenë të bëjnë vetëm me një autoritet mbikëqyrës kombëtar për mbrojtjen e të dhënave.
- Mekanizmi i bashkëpunimit dhe njëtrajtshmërisë do të mundësojë një qasje të koordinuar të të gjitha autoriteteve mbikëqyrëse të përfshira në një çështje. Autoriteti mbikëqyrës drejtues, ai që mbulon strukturën kryesore ose unike, do të konsultohet dhe do të depozitojë projekt-vendimin e tij tek autoritetet e tjera mbikëqyrëse të përfshira.
- Ashtu si Grupi i Punës së Nenit 29, autoritetet mbikëqyrëse të çdo Shteti Anëtar, si dhe Mbikëqyrësi Evropian i Mbrojtjes së të Dhënave (EDPS-ja) do të jenë pjesë Bordit Evropian të Mbrojtjes së të Dhënave.
- Detyrat e Bordit Evropian të Mbrojtjes së të Dhënave përfshijnë për shembull monitorimin e zbatimit të rregullores, të këshillojë Komisionin për çështje përkataëse dhe të nxjerrë opinione, udhëzues, ose praktika të mira për një shumëllojshmëri tematikash.
- Ndryshimi kryesor është që Bordi Evropian i Mbrojtjes së të Dhënave nuk do të miratojë vetëm opinione, sikurse bëhej gjatë Direktivës 95/46/EC. Ai do të marrë gjithashtu vendime detyruese për rastet kur një autoritet mbikëqyrës ka bërë vërejtje të rëndësishme dhe të arsyetuara për çështje të sportelit unik, kur ka mendime të kundërta se kush do të jetë autoriteti mbikëqyrës kryesor dhe së fundmi kur autoriteti mbikëqyrës kompetent nuk kërkon ose nuk ndjek opinionin e EDPB-së. Objektivi është të garantohet zbatim i njëtrajtshëm i rregullores në të gjitha Shtetet Anëtare.

Mbikëqyrja e pavarur është komponent thelbësor i legjislacionit evropian të mbrojtjes së të dhënave. Qoftë e drejta e BE-së, ashtu edhe ajo e KiE-së e shohin ekzistencën e autoriteteve të pavarura mbikëqyrëse si të domosdoshme për mbrojtje të efektshme të të drejtave dhe lirive të personave në lidhje me përpunimin e të dhënave të tyre personale. Meqenëse përpunimi i të dhënave është tashmë i kudondodhur dhe gjithnjë e më i komplikuar për t'u kuptuar nga individët, këto autoritete janë rojtaret e epokës digjitale. Në BE, ekzistenca e autoriteteve mbikëqyrëse të pavarura konsiderohet si një nga

elementet më thelbësore të së drejtës për mbrojtje të të dhënave personale, sanksionuar në legjislacionin parësor të BE-së. Neni 8, pika 3 e Kartës së të Drejtave Themelore të BE-së dhe neni 16, pika 2 e TFBE-së e njohin mbrojtjen e të dhënave personale si të drejtë themelore dhe pohojnë se përputhshmëria me rregullat e mbrojtjes së të dhënave duhet t'i nënshtrohet kontrollit nga ana e autoritetit mbikëqyrës.

Rëndësia e mbikëqyrjes së pavarur për legjislacionin e mbrojtjes së të dhënave është pranuar gjithashtu edhe nga jurisprudenca.

[BOX TYPE 1]

Shembull: tek çështja *Schrems*,[491] GJDBE-ja shqyrtoi nëse transferimi i të dhënave personale në Shtetet e Bashkuara (SHBA-të) sipas Marrëveshjes së parë të Portit të Sigurt BE-SHBA ishte në përputhje me legjislacionin e mbrojtjes së të dhënave të BE-së, referuar sinjalizimeve të Edward Snowden-it për survejimin masiv që zhvillonte Agjencia e Sigurisë Kombëtare të SHBA-ve. Transfermi i të dhënave personale drejt SHBA-ve mbështetej në një vendim të Komisionit Evropian të miratuar në vitin 2000, i cili lejonte transferimin e të dhënave personale nga BE-ja drejt organizatave të SHBA-ve që ishin të vetë-certifikuara sipas skemës së Portit të Sigurt, duke qenë se ky mekanizëm garantonte nivel të përshtatshëm mbrojtjeje të të dhënave personale. Kur iu kërkua që të hetonte ankesën e subjektit në lidhje me ligjshmërinë e transferimeve të të dhënave pas zbulimeve të Snowden-it, autoriteti mbikëqyrës irlandez refuzoi ankesën me arsyetimin se ekzistenca e vendimit të Komisionit për nivelin e përshtatshëm të regjimit amerikan të mbrojtjes së të dhënave, i pasqyruar në parimet e Portit të Sigurt ('Vendimi i Portit të Sigurt'), e pengonte atë të vijonte hetimin e ankesës.

Megjithatë, GJDBE-ja u shpreh se ekzistenca e vendimit të Komisionit, që lejonte transferimet e të dhënave drejt vendeve të treta të cilat garantojnë nivel të përshtatshëm mbrojtjeje të dhënash, nuk eliminon apo zvogëlon kompetencat e autoriteteve mbikëqyrëse kombëtare. GJDBE-ja theksoi se kompetencat e këtyre autoriteteve për të monitoruar dhe garantuar zbatimin e rregullave të BE-së për mbrojtjen e të dhënave burojnë nga legjislacioni parësor i BE-së, veçanërisht nga neni 8, pika 3 e Kartës dhe neni 16, pika 2 e TFBE-së. "Ngritja e autoriteteve mbikëqyrëse të pavarura është për rrjedhimisht […] element thelbësor i mbrojtjes së personave në lidhje me përpunimin e të dhënave personale."[492]

Kështu, GJDBE-ja vendosi se edhe kur transferimi i të dhënave personale i nënshtrohej një vendimi të Komisionit për nivel të përshtatshëm, kur autoritetit mbikëqyrës kombëtar i paraqitet një ankesë, autoriteti duhet ta shqyrtojë ankesën me rigorozitet. Autoriteti mbikëqyrës mund të refuzojë ankesën nëse ajo është e pabazuar. Në këtë rast, GJDBE-ja theksoi se e drejta për mjete juridike të efektshme përcakton se personave duhet t'u mundësohet ta kundërshtojnë një vendim të tillë në një gjykatë kombëtare, e cila mund t'ia përcjellë GJDBE-së për një vendim paragjyqësor në lidhje me vlefshmërinë e vendimit të Komisionit. Kur autoriteti mbikëqyrës e konsideron të bazuar ankesën, ai duhet të ketë të drejtën të përfshihet në procedim ligjor dhe ta përcjellë çështjen në gjykatat kombëtare. Gjykatat kombëtare mund ta referojnë çështjen tek GJDBE-ja, në cilësinë e të vetmit organ me kompetencë për të vendosur për vlefshmërinë e një vendimi të Komisionit për nivel të përshtatshëm.[493]

GJDBE-ja më pas shqyrtoi vlefshmërinë e Vendimit të Portit të Sigurt, për të përcaktuar nëse sistemi i transferimeve ishte në përputhje me rregullat e BE-së për mbrojtjen e të dhënave. Ajo konstatoi se neni 3 i Vendimit të Portit të Sigurt kufizonte kompetencat e autoriteteve mbikëqyrëse kombëtare (që buronin nga Direktiva e Mbrojtjes së të Dhënave) për të vepruar me qëllim ndalimin e transferimit të të

[491] GJDBE, C-362/14, *Maximilliam Schrems k. Komisionerit të Mbrojtjes së të Dhënave* [ÇB] , 6 tetor 2015.
[492] GJDBE, C-362/14, *Maximillian Schrems k. Komisionerit të Mbrojtjes së të Dhënave* [ÇB] , 6 tetor 2015, parag. 41.
[493] *Ibid*., paragrafët 53–66.

dhënave në rastin e një niveli të papërshtatshëm mbrojtjeje të të dhënave personale në SHBA. Duke pasur parasysh rëndësinë që kanë autoritetet mbikëqyrëse të pavarura për të garantuar respektimin e legjislacionit të mbrojtjes së të dhënave, GJDBE-ja vendosi se sipas Direktivës së Mbrojtjes së të Dhënave, lexuar njëkohësisht me Kartën, Komisioni nuk kishte kompetencën të kufizonte në atë mënyrë kompetencat e autoriteteve mbikëqyrëse të pavarura. Kufizimi i kompetencave të autoriteteve mbikëqyrëse ishte një nga arsyet për të cilat GJDBE-ja e shpalli të pavlefshëm Vendimin e Portit të Sigurt.

E drejta evropiane e përcakton kësisoj mbikëqyrjen e pavarur si një mekanizëm të rëndësishëm për të garantuar mbrojtje të dhënash të efektshme. Autoritetet mbikëqyrëse kombëtare janë pika e parë e kontaktit për subjektet e të dhënave rastet e shkeljeve ndaj të dhënave.[494] Sipas së drejtës së BE-së dhe asaj të KiE-së, ngritja e një autoriteteve mbikëqyrëse është e detyrueshme. Të dy kuadrot ligjorë e përshkruajnë detyrat dhe kompetencat e këtyre autoriteteve në mënyrë të ngjashme me atë që përcakton GDPR-ja. Për rrjedhojë, parimisht, autoritetet mbikëqyrëse duhet të funksionojnë në të njëjtën mënyrë sipas së drejtës së BE-së dhe të drejtës së KiE-së.[495]

5.1 Pavarësia

E drejta e BE-së dhe **e drejta e KiE-së** kërkojnë që çdo autoritet mbikëqyrës të veprojë në pavarësi të plotë në ushtrimin e detyrave dhe kompetencave të tij.[496] Pavarësia e autoritetit mbikëqyrës, anëtarëve të tij dhe stafit nga ndikimi i jashtëm i drejtpërdrejtë apo i tërthortë, është themelore për të garantuar objektivitet të plotë në vendime për çështje të mbrojtjes së të dhënave. Ligji që krijon autoritetin e mbrojtjes së të dhënave nuk duhet vetëm të përmbajë dispozita konkrete që garantojnë pavarësinë, por edhe struktura organizative e autoritetit duhet të demonstrojë pavarësinë e tij. Për herë të parë në vitin 2010, GJDBE-ja shqyrtoi shkallën e pavarësisë së nevojshme të autoriteteve mbikëqyrëse të mbrojtjes së të dhënave.[497] Shembujt e mëposhtëm ilustrojnë mënyrën me të cilën GJDBE-ja përkufizon shprehjen "pavarësi e plotë".

[BOX TYPE 1]

Shembull: Tek *Komisioni Evropian k. Republikës Federale të Gjermanisë*,[498] Komisioni Evropian i kërkoi GJDBE-së të shprehej se Gjermania nuk e kishte transpozuar në mënyrë të saktë kriterin e 'pavarësisë së plotë' të autoriteteve mbikëqyrëse përgjegjëse për garantimin e mbrojtjes së të dhënave dhe kësisoj nuk kishte përmbushur detyrimet e saj që rrjedhin nga neni 28, pika 1 e Direktivës së Mbrojtjes së të Dhënave. Sipas mendimit të Komisionit, fakti që Gjermania i kishte vendosur autoritetet mbikëqyrëse për monitorimin e përpunimit të të dhënave personale të shteteve të ndryshme federale (*Landeve*) nën monitorim shtetëror, për të garantuar zbatimin e legjislacionit të mbrojtjes së të dhënave, shkelte kriterin e pavarësisë.

GJDBE-ja nënvizoi se shprehja 'me pavarësi të plotë' duhet interpretuar mbështetur në vetë formulimin e dispozitës dhe në qëllimet e sistemin e legjislacionit të BE-së për mbrojtjen e të dhënave.[499] GJDBE-ja theksoi se autoritetet mbikëqyrëse janë 'rojtarët' e të drejtave në lidhje me përpunimin e të dhënave

[494] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 13, pika 2, gërma (d).
[495] *Ibid*., neni 51; Konventa 108 e Modernizuar, neni 15.
[496] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 52, pika 1; Konventa 108 e Modernizuar, neni 15, pika 5.
[497] FRA (2010), *Fundamental rights: challenges and achievements in 2010*, Annual report 2010, fq. 59; FRA (2010), *Data protection in the European Union: the role of National Data Protection Authorities*, maj 2010.
[498] GJDBE, C-518/07, *Komisioni Evropian k. Republikws Federale tw Gjermanisw* [ÇB] , 9 mars 2010, parag. 27.
[499] *Ibid*., paragrafët 17 dhe 29.

personale. Për rrjedhojë, krijimi i tyre në Shtetet Anëtare konsiderohet "si element thelbësor i mbrojtjes së personale në lidhje me përpunimin e të dhënave personale".[500] GJDBE-ja vendosi se "gjatë ushtrimit të detyrave të tyre, autoritetet mbikëqyrëse duhet të veprojnë me objektivitet dhe paanësi. Për këtë qëllim, ato duhet të jenë të lira nga çdo ndikim i jashtëm, përfshirë edhe ndikimin e drejtpërdrejtë, apo të tërthortë të autoriteteve publike".[501]

GJDBE-ja u shpreh gjithashtu se kuptimi i 'pavarësisë së plotë' duhet interpretuar duke iu referuar pavarësisë së EDPS-së, sikurse përkufizohet në Rregulloren e Mbrojtjes së të Dhënave të Institucioneve të BE-së. Në këtë rregullore, koncepti i pavarësisë përcakton se EDPS-ja nuk mund të kërkojë, apo të pranojë udhëzime nga askush.

Rrjedhimisht, GJDBE-ja vendosi se autoritetet mbikëqyrëse në Gjermani, për shkak të monitorimin që u bëhej nga autoritetet publike, nuk ishin plotësisht të pavarura në kuptim të legjislacionit të mbrojtjes së të dhënave të BE-së.

Shembull: Tek *Komisioni Evropian k. Republikës së Austrisë*,[502] GJDBE-ja nënvizoi probleme të ngjashme në lidhje me pavarësinë e disa anëtarëve dhe stafit të Autoritetit Austriak të Mbrojtjes së të Dhënave (Komisioni i Mbrojtjes së të Dhënave, DSK). GJDBE-ja doli në përfundimin se fakti që personeli i autoritetit mbikëqyrës vihej në dispozicion nga Kancelaria Federale, cënonte kriterin e pavarësisë së përcaktuar në legjislacionin e BE-së për Mbrojtjen e të Dhënave. Gjithashtu, GJDBE-ja u shpreh se kriteri sipas së cilit duhej të informonte Kancelarinë në çdo moment për aktivitetin e zhvilluar, kompromotonte pavarësinë e plotë të autoritetit mbikëqyrës.

Shembull: Tek *Komisioni Evropian k. Hungarisë*,[503] u ndaluan praktika të ngjashme kombëtare që cënonin pavarësinë e personelit. GJDBE-ja nënvizoi se "detyrimi [...] për të garantuar që çdo autoritet mbikëqyrës të ushtrojë në pavarësi të plotë funksionet që i janë ngarkuar, mbart detyrimin që Shteti Anëtar i përfshirë të respektojë kohëzgjatjen e parashikuar të mandatit të tij". Gjykata vlerësoi gjithashtu se "duke ndërprerë para kohe mandatin e autoritetit mbikëqyrës të mbrojtjes së të dhënave personale, Hungaria nuk kishte përmbushur detyrimet e saj sipas Direktivës 95/46/EC [...]."

Nocioni dhe kriteret e 'pavarësisë së plotë' janë tashmë të përcaktuara qartësisht në GDPR, në të cilën janë integruar parimet e përcaktuara nga vendimet e sipërpërmendura të GJDBE-së. Sipas rregullores, pavarësia e plotë në ushtrimin e detyrave dhe funksioneve të tyre nënkupton:[504]

- Anëtarët e çdo autoriteti mbikëqyrës, duhet të mbeten të lirë nga ndikimi i jashtëm, i drejtpërdrejtë ose jo, dhe nuk duhet të marrin udhëzime nga askush;
- Anëtarët e çdo autoriteti mbikëqyrës duhet të distancohen nga çdo veprim që nuk është në pajtim me detyrat e tyre, për të parandaluar konfliktin e interesit;
- Shtetet Anëtare duhet t'i vënë në dispozicion çdo autoriteti mbikëqyrës burimet e nevojshme njerëzore, teknike dhe financiare dhe infrastrukturën për përmbushjen e efektshme të detyrave të tyre;
- Shtetet Anëtare duhet të garantojnë që çdo autoritet mbikëqyrës të zgjedhë vetë personelin e tij;

[500] *Ibid*., parag. 23.
[501] *Ibid*., parag. 25.
[502] GJDBE, C-614/10, *Komisioni Evropian k. Republikës së Austrisë* [ÇB] , 16 tetor 2012, parag. 59 dhe 63.
[503] GJDBE, C-288/12, *Komisioni Evropian k. Hungarisë* [ÇB] , 8 prill 2014, parag. 50 dhe 67.
[504] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 52.

- Kontrolli financiar të cilit i nënshtrohet çdo autoritet mbikëqyrës sipas legjislacionit kombëtar, nuk duhet të prekë pavarësinë e tij. Autoritetet mbikëqyrëse duhet të kenë bugjetin e tyre publik vjetor, i cili t'u mundësojë të funksionojnë në mënyrën e duhur.

Pavarësia e autoriteteve mbikëqyrëse konsiderohet gjithashtu si kriter thelbësor në të drejtën e KiE-së. Konventa 108 e Modernizuar kërkon nga autoritetet mbikëqyrëse që "të veprojnë në pavarësi dhe paanësi të plotë gjatë përmbushjes së detyrave dhe ushtrimit të kompetencave të tyre", pa kërkuar ose pa marrë udhëzime.[505] Në këtë mënyrë, konventa pranon se këto autoritete mund të mbrojnë me efektshmëri të drejtat dhe liritë e personave në lidhje me përpunimin e të dhënave vetëm nëse ushtrojnë funksionet e tyre në pavarësi të plotë. Raporti Shpjegues i Konventës 108 të Modernizuar përcakton një sërë elementesh që ndihmojnë në ruajtjen e pavarësisë. Të tilla elemente janë mundësia që autoritetet mbikëqyrëse të punësojnë vetë personelin e tyre dhe të miratojnë vendime pa iu nënshtruar ndërhyrjes së jashtme, ashtu si edhe faktorët që kanë të bëjnë me kohëzgjatjen e ushtrimit të funksioneve të tyre dhe kushteve sipas të cilave mund të ndërpriten funksionet e tyre.[506]

5.2 Kompetencat dhe tagrat

Sipas së drejtës së BE-së, GDPR-ja përcakton kompetencat dhe strukturën organizative të autoriteteve mbikëqyrëse dhe sanksionon që ato të jenë kompetente e të zotërojnë tagrat për përmbushjen e detyrave që u ngarkon rregullorja. Autoriteti mbikëqyrës është organi kryesor në të drejtën kombëtare, i cili siguron respektimin e legjislacionit të BE-së për mbrojtjen e të dhënave. Autoritetet mbikëqyrëse kanë një gamë të gjerë detyrash e kompetencash, që shkojnë përtej monitorimit, ku përfshihen aktivitete kontrolli proaktiv dhe parandalues. Për kryerjen e këtyre detyrave, autoritetet mbikëqyrëse duhet të kenë kompetenca të përshtatshme hetimore, korrigjuese dhe këshilluese, sikurse renditen në nenet 57 dhe 58 të GDPR-së, sikurse:[507]

- Për të këshilluar kontrolluesit dhe subjektet e të dhënave për të gjitha çështjet që lidhen me mbrojtjen e të dhënave;
- Për të autorizuar modelin e klauzolave kontraktuese, rregullat e detyrueshme të korporatave ose rregullimet administrative;
- Për të hetuar operacionet e përpunimit dhe për të ndërhyrë përkatësisht;
- Për të kërkuar t'i jepet çdo informacion me rëndësi për mbikëqyrjen e aktiviteteve të kontrolluesit;
- Për të paralajmëruar ose për të marrë masa ndaj kontrolluesve dhe të urdhërojë t'u komunikohen subjekteve të të dhënave shkeljet ndaj të dhënave personale;
- Për të urdhëruar korrigjimin, bllokimin, fshirjen ose shkatërrimin e të dhënave;
- Për të vendosur një kufizim të përkohshëm ose të përhershëm të përpunimit, ose për të vendosur gjoba administrative;
- Për ta dërguar një çështje në gjykatë.

Për të ushtruar funksionet e tij, autoriteti mbikëqyrës duhet të ketë akses tek të gjitha të dhënat personale dhe informacioni i nevojshëm për një hetim, ashtu si edhe tek çdo mjedis ku kontrolluesi mban informacionet e rëndësishme. Sipas GJDBE-së, kompetencat e autoritetit mbikëqyrës duhet të

[505] Konventa 108 e Modernizuar, neni 15, pika 5.
[506] Raporti Shpjegues i Konventës 108 të Modernizuar.
[507] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 57 dhe 58. Shih gjithashtu Protokollin Shtesë të Konventës 108, nenin 1.

interpretohen gjerësisht, me qëllim që të garantohet efektshmëri e plotë e mbrojtjes së të dhënave për subjektet e të dhënave në BE.

[BOX TYPE 1]

Shembull: Tek çështja *Schrems*, GJDBE-ja shqyrtoi nëse transferimi i të dhënave drejt SHBA-ve nëpërmjet Marrëveshjes së Portit të Sigurt BE-SHBA ishte në përputhje me të drejtën e BE-së në fushën e mbrojtjes së të dhënave, duke pasur parasysh zbulimet e bëra nga Edward Snowden-i. Arsyetimi i GJDBE-së ishte se autoritetet mbikëqyrëse kombëtare, të cilat vepronin në cilësinë e tyre monitoruese të pavarur të përpunimit të të dhënave nga ana e kontrolluesve, mund të ndalojnë transferimin e të dhënave personale drejt një shteti të tretë, pavarësisht ekzistencës së një vendimi niveli të përshtatshëm, në rast se ka prova të arsyeshme se mbrojtja e përshtatshme nuk sigurohet më në shtetin e tretë.[508]

Çdo autoritet mbikëqyrës është kompetent për ushtrimin e kompetencave hetimore dhe të ndërhyrjes brenda territorit të tij. Megjithatë, duke qenë se aktivitetet e kontrolluesve dhe përpunuesve janë shpesh ndërkufitare dhe përpunimi i të dhënave prek subjekte të dhënash të vendosur në shumë Shtete Anëtare, ngrihet çështja që ka të bëjë me ndarjen e kompetencave midis autoriteteve të ndryshme mbikëqyrëse. GJDBE-ja ka pasur rastin të shqyrtojë këtë problem tek çështja *Weltimmo*.

[BOX TYPE 1]

Shembull: Tek çështja *Weltimmo,*[509] GJDBE-ja shqyrtoi kompetencën e autoriteteve m bikëqyrëse kombëtare për të trajtuar çështje që përfshijnë organizata që nuk janë të vendosura brenda juridiksionit të tyre. Weltimmo ishte një shoqëri e regjistruar në Sllovaki, e cila shfrytëzonte një faqe interneti me njoftime për pasuri të patundshme që ndodheshin në Hungari. Reklamuesit depozituan një ankesë pranë autoritetit mbikëqyrës hungarez për mbrojtjes e të dhënave me objekt shkeljen e ligjit hungarez të mbrojtjes së të dhënave dhe ky autoriteti gjobiti Weltimmo-n. Shoqëria kundërshtoi gjobën në gjykatat kombëtare dhe çështja iu përcoll GJDBE-së për të përcaktuar nëse Direktiva e BE-së e Mbrojtjes së të Dhënave lejonte autoritetet mbikëqyrëse të një Shteti Anëtar të zbatonin legjislacionin e tyre kombëtar të mbrojtjes së të dhënave për një shoqëri të regjistruar në një Shtet tjetër Anëtar.

GJDBE-ja e interpretoi nenin 4, pika 1, gërma (a) të Direktivës së Mbrojtjes së të Dhënave si të tillë që e lejonte zbatimin e së drejtës së mbrojtjes së të dhënave të një Shteti Anëtar të ndryshëm nga Shteti Anëtar në të cilin është i regjistruar kontrolluesi, "në masën që kontrolluesi ushtron, nëpërmjet një strukture të qëndrueshme në territorin e atij Shteti Anëtar, një aktivitet real dhe të efektshëm, qoftë ky edhe minimal, në kuadër të të cilit kryhet ai përpunim". GJDBE-ja vërejti se, bazuar në informacionin që dispononte, Weltimmo-ja zhvillonte aktivitet real dhe të efektshëm në Hungari, meqenëse shoqëria kishte një përfaqësues në Hungari, i cili ishte i regjistruar në regjistrin sllovak të shoqërive me adresë në Hungari, si dhe me një llogari bankare dhe adresë postare hungareze, si dhe zhvillonte aktivitetet në Hungari duke përdorur gjuhën hungareze. Këto të dhëna tregonin se ekzistonte një strukturë, e cila e bënte aktivitetin e Weltimmo-s t'i nënshtrohej së drejtës hungareze për mbrojtjen e të dhënave dhe juridiksionit të autoritetit mbikëqyrës hungarez. Gjithsesi, GJDBE-ja ia la gjykatës kombëtare për të verifikuar informacionin dhe për të vendosur nëse Weltimmo-ja kishte në fakt një strukturë në Hungari.

Nëse ajo gjykatë do të konsideronte se Weltimmo-ja kishte një strukturë në Hungari, autoriteti mbikëqyrës hungarez do të kishte kompetencën të vendoste gjobë. Megjithatë, nëse gjykata kombëtare do të vendoste për të kundërtën, d.m.th. që Weltimmo-ja nuk kishte strukturë në Hungari, rrjedhimisht ligji i zbatueshëm do të ishte ai i Shtetit apo Shteteve Anëtare në të cilat ishte e regjistruar shoqëria. Në

[508] GJDBE, C-362/14, *Maximilian Schrems k. Komisionerit të Mbrojtjes së të Dhënave* [ÇB] , 6 tetor 2015, parag. 26–36 dhe 40–41.
[509] GJDBE, C-230/14, *Weltimmo s.r. o. k. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 tetor 2015.

këtë rast, meqenëse kompetencat e autoriteteve mbikëqyrëse duhen ushtruar në përputhje me sovranitetin territorial të Shteteve të tjera Anëtare, autoriteti hungarez nuk do të kishte mundësi të vendoste sanksione. Meqenëse Direktiva e Mbrojtjes së të Dhënave përcaktonte një detyrim për bashkëpunim midis autoriteteve mbikëqyrëse, autoriteti hungarez mundej gjithsesi t'i kërkonte autoritetit homolog sllovak të shqyrtonte çështjen, të konstante shkeljen e ligjit sllovak dhe të vendoste sanksion sipas parashikimeve të legjislacionit sllovak.

Me miratimin e GDPR-së, ekzistojnë tashmë rregulla të hollësishme në lidhje me kompetencat e autoriteteve mbikëqyrëse për praktika ndërkufitare. Rregullorja përcakton një 'mekanizëm të sportelit unik' dhe dispozita që detyrojnë bashkëpunimin midis autoriteteve mbikëqyrëse të ndryshme. Për bashkëpunim efikas për çështje ndërkufitare, GDPR-ja kërkon që një autoritet mbikëqyrës epror të jetë i vendosur si autoriteti mbikëqyrës i strukturës kryesore ose i të vetmes strukturë të kontrolluesit apo përpunuesit. [510] Autoriteti mbikëqyrës epror është përgjegjës për çështjet ndërkufitare, është interlokutori unik i kontrolluesit ose përpunuesit dhe koordinon bashkëpunimin me autoritetet e tjera mbikëqyrëse me qëllim që të arrihet konsensusi. Bashkëpunimi përfshin shkëmbimin e informacionit, mbështetjen e ndërsjellë në monitorim dhe hetim dhe miratimin e vendimeve detyruese.[511]

Tek e drejta e KiE-së, kompetencat dhe tagrat e autoriteteve mbikëqyrëse janë të përcaktuara në nenin 15 të Konventës 108 të Modernizuar. Këto kompetenca përkojnë me ato që u jepen autoriteteve mbikëqyrëse nga e drejta e BE-së, përfshirë kompetencat hetimore dhe të ndërhyrjes, kompetenca për të dalë me vendime dhe për të vendosur sanksione administrative për shkelje të dispozitave të konventës, si dhe kompetenca iniciative gjyqësore. Autoritetet mbikëqyrëse të pavarura kanë gjithashtu kompetencën të trajtojnë kërkesa dhe ankesa të depozituara nga subjekte të dhënash, të bëjnë ndërgjegjësim publik në lidhje me legjislacionin e mbrojtjes së të dhënave dhe të japin këshillojnë vendimmarrësit kombëtarë për çdo iniciativë legjislative apo administrative që rregullon përpunimin e të dhënave personale.

5.3 Bashkëpunimi

GDPR-ja përcakton një kuadër të përgjithshëm për bashkëpunimin midis autoriteteve mbikëqyrëse dhe parashikon rregulla më të hollësishme në lidhje me bashkëpunimin e autoriteteve mbikëqyrëse për aktivitetet ndërkufitare të përpunimit të të dhënave.

Sipas GDPR-së, autoritetet mbikëqyrëse duhet të japin ndihmë të ndërsjellë dhe të shkëmbejnë informacion të rëndësishëm për zbatimin e rregullores në mënyrë koherente. [512] Këtu përfshihet autoriteti mbikëqyrës të cilit i është kërkuar kryerja e konsultimeve, inspektimeve dhe hetimeve. Autoritetet mbikëqyrëse mund të kryejnë operacione të përbashkëta, si dhe hetime të përbashkëta dhe të marrin masa ligj-zbatuese të përbashkëta, në të cilat përfshihen anëtarë të stafeve të të gjitha autoriteteve mbikëqyrëse.[513]

Në BE, kontrolluesit dhe përpunuesit zhvillojnë gjithnjë e më tepër aktivitet trans-nacional. Kësisoj, nevojitet bashkëpunim i ngushtë midis autoriteteve mbikëqyrëse kompetente të Shteteve Anëtare, për të garantuar që përpunimi i të dhënave personale të respektojë kriteret e GDPR-së. Referuar mekanizmit të 'sportelit unik', nëse një kontrollues apo përpunues ka struktura në disa Shtete Anëtare, ose nëse ka një strukturë të vetme, por aktivitetet e përpunimit prekin thelbësisht subjekte të dhënash në më shumë se një Shtet Anëtar, autoriteti mbikëqyrës i strukturës kryesore (ose të vetme) është autoriteti epror për aktivitetet ndërkufitare të kontrolluesit ose përpunuesit. Autoriteti epror ka kompetencën të ndërmarrë veprime ligj-zbatuese ndaj kontrolluesit ose përpunuesit. Mekanizmi i sporteli unik synon të përmirësojë harmonizimin dhe zbatimin e njëtrajtshëm të legjislacionit të BE-së për mbrojtjen e të

[510] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 56, pika 1.
[511] *Ibid.,* neni 60.
[512] *Ibid*., neni 61, pikat 1–3 dhe 62, pika 1.
[513] *Ibid*., neni 62, pika 1.

dhënave në të gjitha Shtetet Anëtare. Diçka e tillë është e dobishme edhe për shoqëritë tregtare, pasi do të kenë të bëjnë vetëm me autoritetin epror në vend të disa autoriteteve mbikëqyrëse. Kjo rrit sigurinë ligjore për biznesin dhe në praktikë duhet të sjellë edhe që vendimet të merren më shpejt dhe që biznesi nuk përballet me autoritete të ndryshme mbikëqyrëse që i ngarkojnë atij detyrime kontradiktore.

Identifikimi i autoritetit epror kërkon që të përcaktohet vendndodhja e strukturës kryesore të një biznesi në BE. Nocioni 'strukturë kryesore' përkufizohet në GDPR. Gjithashtu, Grupi i Punës së Nenit 29 ka miratuar udhëzues për identifikimin e autoritetit mbikëqyrës epror në lidhje me një kontrollues ose përpunues, i cili parashikon kriteret për identifikimin e strukturës kryesore.[514]

Për të garantuar nivel të lartë mbrojtjeje të dhënash në të gjithë BE-së, autoriteti mbikëqyrës epror nuk vepron i vetëm. Ai duhet të bashkëpunojë me autoritetet e tjera mbikëqyrëse për të miratuar vendime në lidhje me përpunimin e të dhënave personale nga kontrolluesit dhe përpunuesit, duke u përpjekur të arrijë konsensusin dhe të garantojë koherencë. Bashkëpunimi ndërmjet autoriteteve përkatëse mbikëqyrëse përfshin shkëmbimin e informacionit, ndihmën e ndërsjellë, kryerjen e hetimeve të përbashkëta dhe të aktiviteteve të kontrollit.[515] Teksa ndihmojnë njëra-tjetrën, autoritetet mbikëqyrëse duhet të trajtojnë në mënyrë të saktë kërkesat për informacion që paraqiten nga autoritetet e tjera mbikëqyrëse dhe të ushtrojnë masa kontrolli, sikurse për shembull kërkesat për autorizim dhe konsultim paraprak me kontrolluesin e të dhënave në lidhje me aktivitetet e tij të përpunimit, inspektime ose hetime. Ndihma e ndërsjellë midis autoriteteve mbikëqyrëse në Shtete të tjera Anëtare duhet dhënë me kërkesë, pa vonesë të panevojshme dhe jo më vonë se një muaj nga marrja e kërkesës.[516]

Kur kontrolluesi ka struktura në disa Shtete Anëtare, autoritetet mbikëqyrëse mund të kryejnë operacione të përbashkëta, duke përfshirë hetime dhe masa ekzekutive në të cilat angazhohen anëtarë të personelit të autoriteteve mbikëqyrëse të Shteteve të tjera Anëtare.[517]

Bashkëpunimi midis autoriteteve të ndryshme mbikëqyrëse është po ashtu një kriter I rëndësishëm në të drejtën e KiE-së. Konventa 108 e Modernizuar parashikon se autoritetet mbikëqyrëse duhet të bashkëpunojnë me njëra-tjetrën në masën që është e nevojshme për përmbushjen e detyrave të tyre.[518] Ky bashkëpunim mund të jetë për shembull në formën e shkëmbimit të informacioneve të rëndësishme e të dobishme, duke koordinuar hetimet dhe duke kryer veprime të përbashkëta.[519]

5.4 Bordi Evropian i Mbrojtjes së të Dhënave

Rëndësia e autoriteteve mbikëqyrëse të pavarura dhe kompetencat kryesore që u jep legjislacioni evropian i mbrojtjes së të dhënave, është përshkruar më herët në këtë kapitull. Bordi Evropian i Mbrojtjes së të Dhënave është një aktor i rëndësishëm për garantimin e zbatimit efikas dhe të njëtrajtshëm të rregullave të mbrojtjes së të dhënave në të gjithë BE-së.

GDPR-ja e ka përcaktuar Bordin si organ të BE-së me personalitet juridik.[520] Ai është pasuesi i Grupit të Punës së Nenit 29,[521] i cili u ngrit me Direktivën e Mbrojtjes së të Dhënave për të këshilluar Komisionin në lidhje me çdo masë të BE-së që prekte të drejtat e personave në lidhje me përpunimin e të dhënave personale dhe privatësinë, për të nxitur zbatimin e njëtrajtshëm të direktivës dhe për të t'i ofruar Komisionit opinion eksperti për çështje që lidhen me mbrojtjen e të dhënave. Grupi i Punës së Nenit 29 përbëhej nga përfaqësues të autoriteteve mbikëqyrëse të Shteteve Anëtare të BE-së, bashkë me përfaqësues të Komisionit dhe të EDPS-së.

---

[514] Grupi i Punës së Nenit 29 (2016), *Guidelines for identifying a controller or processor's lead supervisory authority*, WP 244, Bruksel, 13 dhjetor 2016, rishikuar më 5 prill 2017.
[515] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 60, pikat 1–3.
[516] *Ibid*., neni 61, pikat 1 dhe 2.
[517] *Ibid*., neni 62, pika 1.
[518] Konventa 108 e Modernizuar, nenet 16 dhe 17.
[519] *Ibid*., neni 17.
[520] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 68.
[521] Sipas Direktivës 95/46/EC, Grupi i Punës së Nenit 29 duhej të këshillonte Komisionin për çdo masë të BE-së që prekte të drejtat e personave në lidhje me përpunimin e të dhënave personale dhe privatësinë, të nxiste zbatimin e njëtrajtshëm të Direktivës dhe t'i jepte Komisionit opinion eksperti për çështje që lidhen me mbrojtjen e të dhënave. Grupi i Punës së Nenit 29 përbëhej nga përfaqësues të autoriteteve mbikëqyrëse të Shteteve Anëtare të BE-së, bashkë me përfaqësues të Komisionit dhe të EDPS-së.

Ashtu si Grupi i Punës, EDPB-ja përbëhet nga drejtuesit e autoriteteve mbikëqyrëse të secilit Shtet Anëtar dhe të EDPS-së, ose përfaqësuesit e tyre.[522] EDPS-ja gëzon të drejtë vote të barabartë, me përjashtim të rasteve që lidhen me zgjidhjen e mosmarrëveshjeve, ku mund të votojë vetëm për vendime që kanë të bëjnë me parimet dhe rregullat e zbatueshme në institucionet e BE-së, që përkojnë në thelb me ato të GDPR-së. Komisioni ka të drejtë të marrë pjesë në aktivitetet dhe mbledhjet e EDPB-së, por nuk ka të drejtë vote.[523] Bordi zgjedh Kryetarin (të cilit i ngarkohet edhe ta përfaqësojë atë) dhe dy Zëvendës-kryetarë nga anëtarësia e tij, me shumicë të thjeshtë, për një mandat pesëvjeçar. Gjithashtu, Bordi ka edhe një sekretariat, të cilin e vendos në dispozicion EDPS-ja, në mënyrë që Bordi të ketë mbështetje analitike, administrative dhe logjistike.[524]

Detyrat e EDPB-së parashikohen hollësisht në nenet 64, 65 dhe 70 të GDPR-së dhe përfshijnë detyrime shteruese të cilat mund të ndahen në tre aktivitete kryesore:

- **Njëtrajtshmëria:** EDPB-ja mund të miratojë vendime ligjërisht të detyrueshme në tre raste: kur një autoritet mbikëqyrës ka ngritur kundërshtime të rëndësishme dhe të motivuara në rastet e sportelit unik, kur ka mendime të kundërta se cili autoritet mbikëqyrës është 'epror' si dhe kur autoriteti mbikëqyrës kompetent nuk kërkon, ose nuk ndjek opinionin e EDPB-së.[525] Përgjegjësia kryesore e EDPB-së është të garantojë zbatim të njëtrajtshëm të GDPR-së në të gjithë BE-në dhe luan rol thelbësor në mekanizmin e njëtrajtshmërisë, sikurse përshkruhet në Seksionin 5.5.
- **Konsultimi:** detyrat e EDPB-së përfshijnë këshillimin e Komisioni për çdo çështje që ka të bëjë me mbrojtjen e të dhënave personale në Bashkim, sikurse për ndryshimin e GDPR-së, rishikimet e legjislacionit të BE-së që kanë të bëjnë me përpunimin e të dhënave dhe që mund të jenë në kundërshtim me rregullat e BE-së për mbrojtjen e të dhënave, ose miratimin nga Komisioni të vendimeve për nivelin e përshtatshëm, të cilat autorizojnë transferimin e të dhënave personale tek një shtet i tretë ose organizatë ndërkombëtare.
- **Orientimi:** Bordi gjithashtu miraton udhëzues, rekomandime dhe praktika të mira, për të nxitur zbatimin e njëtrajtshëm të rregullores dhe promovon bashkëpunimin dhe shkëmbimin e njohurive midis autoriteteve mbikëqyrëse. Gjithashtu, ai duhet të nxisë shoqatat e kontrolluesve apo përpunuesve që të hartojnë kode sjelljeje, si dhe të zbatojnë mekanizma certifikimi dhe vula të mbrojtjes së të dhënave.

Vendimet e EDPB-së mund të kundërshtohen në GJDBE.

5.5 Mekanizmi i Njëtrajtshmërisë sipas GDPR-së

GDPR-ja parashikon një mekanizëm njëtrajtshmërie për të garantuar që rregullorja zbatohet në mënyrë koherente nga të gjitha Shtetet Anëtare, me anë të së cilit autoritetet mbikëqyrëse bashkëpunojnë me njëra-tjetrën dhe nëse është rasti edhe me Komisionin. Mekanizmi i njëtrajtshmërisë përdoret në dy situata. Rasti i parë lidhet me opinionet e EDPB-së kur një autoritet mbikëqyrës kompetent synon të miratojë masa, të tilla si listën e operacioneve të përpunimit për të cilat nevojitet kryerja e Vlerësimit të Ndikimit tek Mbrojtja e të Dhënave (DPIA), ose për të përcaktuar modelin e klauzolave kontraktuese. Rasti i dytë ka të bëjë me vendimet detyruese të EDPB-së për autoritetet mbikëqyrëse në çështjet që lidhen me sportelin unik dhe kur një autoritet mbikëqyrës nuk ndjek, ose nuk kërkon opinionin e EDPB-së.

[522] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 68, pika 3.
[523] *Ibid*., neni 68, pikat 4 dhe 5.
[524] *Ibid*., nenet 73 dhe 75.
[525] *Ibid*., neni 65.

6 Të drejtat e subjekteve të të dhënave dhe zbatimi i tyre

BE	Çështje të trajtuara	KiE
E drejta për t'u informuar		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 12 GJDBE, C-473/12, *Institut professionnel des agents immobiliers (IPI) k. Englebert*, 2013 GJDBE, C-201/14, *Smaranda Bara dhe të Tjerët k. Casa Naţională de Asigurări de Sănătate dhe të Tjerët*, 2015	Transparenca e informacionit	Konventa 108 e Modernizuar, neni 8
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 13, pikat 1 dhe 2 dhe neni 14, pikat 1 dhe 2	Përmbajtja e informacionit	Konventa 108 e Modernizuar, neni 8, pika 1
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 13, pika 1 dhe neni 14, pika 3	Momenti i dhënies së informacionit	Konventa 108 e Modernizuar, neni 9, pika 1, gërma (b).
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 12, pikat 1, 5 dhe 7	Mënyrat e dhënies së informacionit	Konventa 108 e Modernizuar, neni 9, pika 1, gërma (b).
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 13, pikat 2, gërma (d) dhe neni 14, pika 2, gërma (e), nenet 77, 78 dhe 79	E drejta për t'u ankuar	Konventa 108 e Modernizuar, neni 9, pika 1, gërma (f)
E drejta e aksesit		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 15, pika 1 GJDBE, C-553/07, *College van burgemeester en wethouders van Rotterdam k. M. E. E. Rijkeboer*, 2009 GJDBE, Çështje të bashkuara C-141/12 dhe C-372/12, *YS k. Minister voor Immigratie, Integratie en Asiel* dhe *Minister voor Immigratie, Integratie en Asiel k. M dhe S*, 2014 GJDBE, C-434/16, *Peter Nowak k. Data Protection Commissioner*, 2017	E drejta e aksesit të një subjekti tek të dhënat që kanë të bëjnë me të	Konventa 108 e Modernizuar, neni 9, pika 1, gërma (b) GJEDNJ, *Leander k. Suedisë*, nr. 9248/81, 1987
E drejta e korrigjimit		

Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 16	Korrigjimi i të dhënave personale të pasakta	Konventa 108 e Modernizuar, neni 9, pika 1, gërma (e) GJEDNJ, *Cemalettin Canli k. Turqisë*, nr. 22427/04, 2008 GJEDNJ, *Ciubotaru k. Moldavisë*, nr. 27138/04, 2010
E drejta e fshirjes		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 17, pika 1	Fshirja e të dhënave personale	Konventa 108 e Modernizuar, neni 9, pika 1, gërma (e) GJEDNJ, *Segerstedt-Wiberg dhe të Tjerët k. Suedisë*, nr. 62332/00, 2006
GJDBE, C-131/12, *Google Spain SL, Google Inc. k. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 GJDBE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce k. Salvatore Manni*, 2017	E drejta për t'u harruar	
E drejta për kufizimin e përpunimit		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 18, pika 1	E drejta për të kufizuar përdorimin e të dhënave personale	
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 19	Detyrimi për të njoftuar	
E drejta e transferueshmërisë së të dhënave		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 20	E drejta për transferueshmërinë e të dhënave	
E drejta për të kundërshtuar		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 21, pika 1 GJDBE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce k. Salvatore Manni*, 2017	E drejta për të kundërshtuar për shkak të situatës së veçantë të subjektit të të dhënave	Rekomandimi në lidhje me profilizimin, neni 5.3 Konventa 108 e Modernizuar, neni 9, pika 1, gërma (d)

Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 21, pika 2	E drejta për të kundërshtuar përdorimin e të dhënave për qëllime marketingu	Rekomandimi në lidhje me marketingun e drejtpërdrejtë, neni 4.1
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 21, pika 5	E drejta për të kundërshtuar me anë të mjeteve automatike	
Të drejtat në lidhje me vendimmarrjen automatike dhe profilizimin		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 22	Të drejtat në lidhje me vendimmarrjen automatike dhe profilizimin	Konventa 108 e Modernizuar, neni 9, pika 1, gërma (a)
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 21	E drejta për të kundërshtuar vendimmarrjen automatike E drejta për të marrë shpjegim të qartë	
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 13, pika 2, gërma (f)		Konventa 108 e Modernizuar, neni 9, pika 1, gërma (c)
Mjetet e ankimit, përgjegjësia, sanksionet dhe kompensimi		
Karta, neni 47 CJEU, C-362/14, *Maximillian Schrems k. Data Protection Commissioner* [GC], 2015 Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 77–84	Për shkeljet e së drejtës kombëtare për mbrojtjen e të dhënave	KEDNJ, neni 13 (vetëm për Shtetet Anëtare të KiE-së) Konventa 108 e Modernizuar, nenet 9, pika 1, gërma (f), 12, 15, 16-21 GJEDNJ, *K.U. k. Finlandës*, nr. 2872/02, 2008 GJEDNJ, *Biriuk k. Lituanisë*, nr. 23373/03, 2008
Rregullorja e Mbrojtjes së të Dhënave të Institucioneve të BE-së, nenet 34 dhe 49 GJDBE, C-28/08 P, *Komisioni Evropian k. The Bavarian Lager Co. Ltd* [GC], 2010	Për shkeljet e legjislacionit të BE-së nga institucionet dhe organet e BE-së	

Efektshmëria e rregullave ligjore në përgjithësi dhe e të drejtave të subjekteve të të dhënave në veçanti, varet në një masë të madhe nga ekzistenca e mekanizmave të përshtatshme për zbatimin e tyre. Në epokën digjitale, përpunimi i të dhënave është i kudondodhur dhe gjithnjë e më i vështirë për t'u kuptuar nga personat. Me qëllim që të reduktohet disbalanca e fuqisë midis subjekteve të të dhënave dhe kontrolluesve, personave u janë dhënë disa të drejta, në mënyrë që të ushtrojnë kontroll më të madh mbi përpunimin e të dhënave të tyre personale. E drejta e aksesit të subjektit tek të dhënat që i përkasin dhe e drejta për t'i korrigjuar ato, janë të përcaktuara në nenin 8, pika 2 të Kartës së të Drejtave Themelore

të BE-së, dokument i cili buron nga e drejta parësore e BE-së dhe ka vlerë themelore në rendin juridik të BE-së. E drejta dytësore, veçanërisht Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, ka përcaktuar një kuadër ligjor të njëtrajtshëm, i cili fuqizon subjektet e të dhënave duke u dhënë atyre të drejta në raport me kontrolluesit e të dhënave. Përveç së drejtave të aksesit dhe korrigjimit, GDPR-ha njeh një sërë të drejtash të tjera, sikurse të drejtën për fshirje ('e drejta për t'u harruar'), të drejtën për të kundërshtuar, ose për të kufizuar përpunimin e të dhënave dhe të drejta në lidhje me vendimmarrjen automatike dhe profilizimin. Masa të ngjashme mbrojtjeje, të cilat u mundësojnë subjekteve të të dhënave të ushtrojnë kontroll efikas mbi të dhënat e tyre, janë parashikuar gjithashtu edhe në Konventën 108 të Modernizuar. Neni 9 rendit të drejtat që personat duhet të kenë mundësi t'i ushtrojnë për sa i përket përpunimit të të dhënave të tyre personale. Palët Kontraktuese duhet të garantojnë që këto të drejta të jenë të disponueshme për çdo subjekt të dhënash në juridiksionin e tyre dhe të shoqërohen me mjete të efektshme ligjore dhe praktike, të cilat u mundësojnë subjekteve të të dhënave që t'i ushtrojnë ato.

Krahas dhënies së këtyre të drejtave për subjektet, është po aq e rëndësishme të përcaktohen mekanizma që u mundësojnë subjekteve të të dhënave të kundërshtojnë shkeljet e të drejtave të tyre, të vënë para përgjegjësisë kontrolluesit dhe të kërkojnë kompensim. E drejta për mjete ankimi të efektshme, sikurse garantohet nga KEDNJ-ja dhe nga Karta, kërkon që mjetet gjyqësore mbrojtëse të jenë të disponueshme për çdo person.

6.1 Të drejtat e subjekteve të të dhënave

Pikat kryesore

- Çdo subjekt ka të drejtën të informohet në lidhje me çdo përpunim të të dhënave të tij personale që kryen kontrolluesi i të dhënave, me disa përjashtime të kufizuara.
- Subjektet e të dhënave kanë të drejtën e:
  - Aksesit tek të dhënat që kanë të bëjnë me ta dhe të marrin informacione të caktuara në lidhje me përpunimin;
  - Korrigjimit të të dhënave nga kontrolluesi i cili përpunon të dhënat e tyre, nëse këto të dhëna janë të pasakta;
  - Fshirjes së të dhënave të tyre nga ana e kontrolluesit, sipas rastit, nëse kontrolluesi kryen përpunim të paligjshëm të të dhënave të tyre;
  - Kufizimit të përkohshëm të përpunimit;
  - Transferimit të të dhënave të tyre tek një kontrollues tjetër, sipas disa kushteve të caktuara.
- Gjithashtu, subjektet e të dhënave duhet të kenë të drejtën të kundërshtojnë përpunimin:
  - Për arsye që lidhen me situatën e tyre të veçantë;
  - Përdorimin e të dhënave të tyre për qëllime marketingu të drejtpërdrejtë.
- Subjektet e të dhënave kanë të drejtën të mos i nënshtrohen vendimeve që mbështeten vetëm në përpunimin automatik, përfshirë profilizimin, të cilat sjellin pasoja ligjore, ose që e cënojnë atë në mënyrë domethënëse. Subjektet e të dhënave kanë gjithashtu të drejtën të:
  - Kërkojnë ndërhyrje njerëzore nga ana e kontrolluesit;
  - Shprehin mendimet e tyre dhe të kundërshtojnë një vendim të mbështetur tek përpunimi automatik.

6.1.1 E drejta për t'u informuar

Si në të drejtën e KiE-së, ashtu edhe në atë të BE-së, kontrolluesit e operacioneve të përpunimit janë të detyruar të informojnë subjektin e të dhënave në momentin e mbledhjes së të dhënave personale, për përpunimin e parashikuar. Ky detyrim nuk varet nga kërkesa e subjektit të të dhënave, përkundrazi

kontrolluesi duhet të zbatojë këtë detyrim në mënyrë proaktive, pavarësisht nëse subjekti i të dhënave shfaq interes ose jo për këtë informacion.

Sipas së drejtës së KiE-së, në përputhje me nenin 8 të Konventës 108 të Modernizuar, Palët Kontraktuese duhet të përcaktojnë që kontrolluesit të informojnë subjektet e të dhënave në lidhje me identitetin e tyre dhe adresën e zakonshme, bazën ligjore dhe qëllimin e përpunimit, kategoritë e të dhënave personale të përpunuara, marrësit e të dhënave të tyre personale (nëse ka) dhe mbi mënyrën se si ata mund t'i ushtrojnë të drejtat e tyre që burojnë nga neni 9, ku përfshihen e drejta e aksesit, korrigjimit dhe mjetet juridike. Subjekteve të të dhënave u duhet komunikuar çdo informacion tjetër shtesë që çmohet i nevojshëm me qëllim garantimin e një përpunimi të dhënash personale të drejtë dhe transparent. Raporti Shpjegues i Konventës 108 të Modernizuar qartëson se informacioni që u paraqitet subjekteve të të dhënave "duhet të jetë lehtësisht i aksesueshëm, i qartë, i kuptueshëm dhe i përshtatur për subjektet përkatëse të të dhënave".[526]

Në të drejtën e BE-së, parimi i transparencës përcakton se çdo përpunim të dhënash personale duhet të jetë përgjithësisht transparent për personat. Këta të fundit kanë të drejtën të dinë se në çfarë mënyre dhe cilat të dhëna personale janë mbledhur, përdorur ose ndryshe përpunuar, si dhe t'u bëhen me dije risqet, masat e sigurisë dhe të drejtat e tyre në lidhje me përpunimin.[527] Kështu, neni 12 i GDPR-së përcakton një detyrim të gjerë e të plotë për kontrolluesit, që të japin informacion transparent dhe/ose të bëjnë me dije mënyrën se si subjektet e të dhënave mund të ushtrojnë të drejtat e tyre.[528] Informacioni duhet të jetë konciz, transparent, i qartë dhe lehtësisht i aksesueshëm, në një gjuhë të qartë dhe të thjeshtë. Ai duhet dhënë me shkrim, përfshirë edhe në mënyrë elektronike kur është e përshtatshme dhe deri edhe verbalisht me kërkesë të subjektit të të dhënave, me kusht që të jetë provuar identiteti i tij apo i saj përtej çdo dyshimi. Informacioni duhet dhënë pa vonesa e shpenzime të tepruara.[529]

Nenet 13 dhe 14 të GDPR-së trajtojnë të drejtën e subjekteve të të dhënave për t'u informuar, qoftë në situatat ku të dhënat janë mbledhur drejtpërdrejtë prej tyre, ashtu edhe në situatat në të cilat të dhënat nuk janë marrë prej tyre respektivisht.

Qëllimi i së drejtës për t'u informuar dhe kufizimet e saj sipas së drejtës së BE-së, janë qartësar në jurisprudencën e GJDBE-së.

[BOX TYPE 1]

Shembull: tek *Institut professionnel des agents immobiliers (IPI) k. Englebert*,[530] GJDBE-së iu kërkua të interpretonte nenin 13, pika të 1 të Direktivës 95/46. Ky nen u jepte Shteteve Anëtare të drejtën për të zgjedhur të miratonin ose jo masa legjislative për të kufizuar objektin e së drejtës së subjekteve të të dhënave për për t'u informuar kur nevojitet për të mbrojtur, ndër të tjera, të drejtat dhe liritë e të tjerëve dhe për të parandaluar dhe hetuar krimet apo shkeljet e etikës për profesionet e rregulluara. IPI është një organ profesional agjentësh të pasurive të paluajtshme në Belgjikë, i cili është përgjegjës për të garantuar respektimin e praktikave të mira të profesionit të agjentit të pasurive të paluajtshme. IPI i kërkoi një gjykate kombëtare të shpallte se të paditurit kishin shkelur rregullat profesionale dhe të urdhëronte që ata të ndalnin kryerjen e disa aktiviteteve të ndryshme në lidhje me pasuritë e patundshme. Ky pretendim mbështetej mbi prova të siguruara nga detektivë privatë të angazhuar nga IPI.

[526] Raporti Shpjegues i Konventës 108 të Modernizuar, parag. 68.
[527] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 39 i preambulës.
[528] *Ibid*., nenet 13 dhe 14; Konventa 108 e Modernizuar, neni 8, pika 1, gërma (b).
[529] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 12, pika 5; Konventa 108 e Modernizuar, neni 9, pika 1, gërma (b).
[530] GJDBE, C-473/12, *Institut professionnel des agents immobiliers (IPI) k. Geoffrey Englebert dhe të Tjerët*, 7 nëntor 2013.

Gjykata ishte në mëdyshje për sa i përket vlerës së provave të siguruara nga detektivët, për shkak të mundësisë që ato të ishin përftuar në shkelje të kritereve të legjislacionit belg, sidomos të detyrimit për të informuar subjektet e të dhënave për përpunimin e të dhënave të tyre personale përpara se informacion të mblidhet. GJDBE-ja theksoi se neni 13, pika 1 përcaktonte se Shtetet Anëtare 'mund', por nuk janë të detyruara, të përcaktojnë në të drejtën e tyre kombëtare përjashtime nga detyrimi për të informuar subjektet e të dhënave në lidhje me përpunimin e të dhënave të tyre. Duke qenë se neni 13, pika 1 përfshin parandalimin, hetimin zbulimin dhe ndjekjen e veprave penale, apo shkeljeve të etikës si shkaqe për të cilat Shtetet Anëtare mund të kufizojnë të drejtat e individëve, aktiviteti i një organi të tillë si IPI dhe detektivëve privatë që vepronin për llogari të tij, mund të mbështetej tek kjo dispozitë. Megjithatë, nëse një Shtet Anëtar nuk ka përcaktuar një përjashtim të tillë, subjektet e të dhënave duhet të informohen.

Shembull: Tek *Smaranda Bara dhe të Tjerët k. Casa Naţională de Asigurări de Sănătate dhe të Tjerët*,[531] GJDBE-ja qartësoi nëse e drejta e BE-së ia ndalonte një organi administrativ publik kombëtar të transferonte të dhëna personale tek një tjetër organ administrativ publik për përpunim të mëtejshëm, pa informuar subjektet e të dhënave për transferimin dhe përpunimin. Në këtë rast, Agjencia Administrative Kombëtare nuk kishte informuar kërkuesit për transferimin e të dhënave të tyre tek Fondi Kombëtar i Sigurimit Shëndetësor përpara kryerjes së transferimit.

GJDBE-ja vlerësoi se kriteri në të drejtën e BE-së për të informuar subjektin e të dhënave në lidhje me përpunimin e të dhënave personale të tyre, është "edhe më i rëndësishëm për shkak se cënon ushtrimin e të drejtave nga ana e subjekteve të të dhënave në lidhje me aksesin tek të dhënat që përpunohen dhe të drejtën për t'i korrigjuar […] dhe të drejtën e tyre për të kundërshtuar përpunimin e atyre të dhënave". Parimi i përpunimit të drejtë kërkon që subjektet e të dhënave të informohen në lidhje me transferimin e të dhënave të tyre tek një organ tjetër publik për përpunim të mëtejshëm nga ky i fundit. Sipas nenit 13, pika 1 të Direktivës 95/46, Shtetet Anëtare mund të kufizojnë të drejtën për t'u informuar nëse vlerësohet se është e nevojshme për të mbrojtur një interes të rëndësishëm ekonomik shtetëror, përfshirë atë në lidhje me taksat. Megjithatë, këto kufizime duhet të përcaktohen me mjete ligjore. Duke qenë se as përcaktimi i të dhënave që duheshin transferuar, e as rregullimet e hollësishme për transferimin nuk ishin përcaktuar me mjete ligjore, por thjesht me anë të një protokolli midis dy autoriteteve publike, kushtet për përjashtim që përcakton e drejta e BE-së, nuk ishin përmbushur. Kërkuesit duhet të ishin informuar paraprakisht për transferimin e të dhënave të tyre tek Fondi Kombëtar i Sigurimit Shëndetësor dhe për përpunimin e mëtejshëm të të dhënave të tyre nga ky organ.

Përmbajtja e informacionit

Sipas nenit 8, pika 1 të Konventës 108 të Modernizuar, kontrolluesi është i detyruar të informojnë subjektin e të dhënave dhe të garantojë përpunim të drejtë dhe transparent të të dhënave personale, përfshirë:

- Identitetin e kontrolluesit dhe vendndodhjen ose adresën e përhershme;
- Bazën ligjore dhe qëllimet e përpunimit të planifikuar;
- Kategoritë e të dhënave personale të përpunuara;
- Marrësit ose kategoritë e marrësve të të dhënave personale, nëse ka;
- Mënyrat me të cilat mund të ushtrojnë të drejtat e tyre subjektet e të dhënave.

[531] GJDBE, C-201/14, *Smaranda Bara Dhe tw Tjerwt k. Casa Naţională de Asigurări de Sănătate dhe tw Tjerwt*, 1 tetor 2015.

Sipas GDPR-së, kur të dhënat personale janë mbledhur nga subjekti i të dhënave, kontrolluesi ka për detyrë ta informojë subjektin e të dhënave në momentin e përftimit të të dhënave personale për sa vijon:[532]

- Identitetin e kontrolluesit dhe adresën e kontaktit, përfshirë edhe ato të Nëpunësit të Mbrojtjes së të Dhënave, nëse ka;
- Qëllimin dhe bazën ligjore për përpunimin, për shembull kontratën ose detyrimin ligjor;
- Interesin legjitim të kontrolluesit, nëse përdoret si bazë për përpunimin;
- Marrësit apo kategoritë e marrësve të mundshëm të të dhënave personale;
- Nëse të dhënat do të transferohen tek një shtet i tretë, apo organizatë ndërkombëtare dhe nëse dika e tillë mbështetet tek një vendim përshtatshmërie, apo tek garancitë e përshtatshme;
- Periudhën në të cilën do të mbahen të dhënat personale dhe në rast se periudha nuk mund të përcaktohet, kriteret që do të përdoren për të përcaktuar afatet e mbajtjes së të dhënave;
- Të drejtat e subjekteve të të dhënave në lidhje me përpunimin, sikurse të drejtat e aksesit, korrigjimit, fshirjes dhe të kufizimit apo kundërshtimit të përpunimit;
- Nëse dhënia e të dhënave personale përcaktohet me ligj ose një kontratë, nëse subjekti i të dhënave është i detyruar t'i japë të dhënat personale të tij apo të saj, si dhe pasojat në rast mosdhënieje të të dhënave personale;
- Ekzistencën e vendimmarrjes automatike, përfshirë profilizimit;
- Të drejtën për të paraqitur ankesë pranë autoritetit mbikëqyrës;
- Ekzistencën e së drejtës për të anuluar pëlqimin.

Në rastet e vendimmarrjes automatike, përfshirë profilizimin, subjektet e të dhënave duhen informuar në mënyrë të qenësishme për logjikën e përdorur për profilizimin, rëndësinë e tij dhe pasojat e parashikuara nga ky përpunim për subjektin e të dhënave.

Në rastet kur të dhënat personale nuk janë marrë drejtpërdrejtë nga subjekti i të dhënave, kontrolluesi i të dhënave duhet të njoftojë personin për origjinën e të dhënave personale. Në çdo rast, kontrolluesi duhet që ndër të tjera, të informojë subjektet e të dhënave për ekzistencën e vendimmarrjes automatike, përfshirë profilizimin.[533] Së fundmi, nëse kontrolluesi synon të përpunojë të dhëna personale për një qëllim të ndryshëm nga ai të cilin i ka bërë të ditur fillimisht subjektit të të dhënave, parimet e kufizimit të qëllimit dhe transparencës përcaktojnë se kontrolluesi duhet ta informojë subjektin e të dhënave në lidhje me qëllimin e ri. Kontrolluesit duhet të japin këtë informacion përpara çdo përpunimi të mëtejshëm. Me fjalë të tjera, në rastet ku subjekti i të dhënave ka dhënë pëlqimin për përpunimin e të dhënave personale, kontrolluesi duhet të marrë një pëlqim të ri nga subjekti i të dhënave nëse qëllimi i përpunimit të të dhënave ndryshon ose nëse janë shtuar qëllime të tjera.

[532] Rregullorja e Pwrgjithshme e Mbrojtjes sw tw Dhwnave, neni 13, pika 1.
[533] Rregullorja e Pwrgjithshme e Mbrojtjes sw tw Dhwnave, nent 13, pika 2 dhe 14, pika 2, gwrma (f).

Momenti i komunikimit të informacionit

GDPR-ja bën dallim midis dy skenarëve dhe dy momenteve kohore në të cilat kontrolluesi i të dhënave duhet të informojë subjektin e të dhënave:

- Kur të dhënat personale janë marrë drejtpërdrejtë nga subjekti i të dhënave, kontrolluesi duhet t'i japë subjektit të të dhënave të gjitha informacionet në lidhje me të dhe mbi të drejtat sipas GDPR-së në momentin e përftimit të të dhënave.[534]
  Nëse kontrolluesi synon të kryejë përpunim të mëtejshëm të të dhënave personale për një qëllim të ndryshëm, kontrolluesi duhet të komunikojë të gjithë informacionin përkatës përpara se përpunimi të nisë.
- Kur të dhënat personale nuk janë përftuar drejtpërdrejtë nga subjekti i të dhënave, kontrolluesi është i detyruar të inforjmë subjektin e të dhënave për përpunimin "brenda një periudhe të arsyeshme kohore pas përftimit të të dhënave personale, por e shumta brenda një muaji", ose përpara se të dhënat personale t'u komunikohen palëve të treta.[535]

Raporti Shpjegues i Konventës 108 të Modernizuar përcakton se nëse informimi i subjekteve të të dhënave nuk është i mundur në nisje të përpunimit, aim und të bëhet në një moment të mëvonshëm, për shembull kur kontrolluesi ka kontaktuar subjektin e të dhënave për çfarëdo arësye.[536]

Mënyrat e ndryshme të informimit

Si në të drejtën e KiE-së, ashtu edhe në atë të BE-së, informacioni që kontrolluesi duhet t'i japë subjekteve të të dhënave duhet të jetë konciz, transparent, i kuptueshëm dhe lehtësisht i aksesueshëm. Ai duhet dhënë me shkrim ose në mënyrë të tjera, përfshirë në rrugë elektronike, duke përdorur gjuhë të qartë, të thjeshtë dhe lehtësisht të kuptueshme. Kur jep informacion, kontrolluesi mund të përdorë ikona të standardizuara, në mënyrë që informacioni të jepet në mënyrë lehtësisht të dallueshme dhe të kuptueshme.[537] Për shembull, një ikonë që paraqet një dryn mund të përdoret për të sinjalizuar se të dhënat mblidhen dhe/ose kodohen në mënyrë të sigurt. Subjektet e të dhënave mund të kërkojnë që informacioni t'u jepet në mënyrë verbale. Informacioni duhet të jepet pa pagesë, përjashtuar rastet kur kërkesat e subjektit të të dhënave janë qartësisht të pabazuara ose të tepruara (p.sh. kanë karakter përsëritës).[538] Aksesi i lehtë në informacionin e dhënë është me rëndësi thelbësore që subjekti i të dhënave të ketë mundësi të ushtrojë të drejtat e tij, apo të saj të sanksionuara në të drejtën e BE-së për mbrojtjen e të dhënave.

Parimi i përpunimit të drejtën kërkon që informacioni të jetë lehtësisht i kuptueshëm për subjektet e të dhënave. Duhet përdorur ajo lloj gjuhe që është e përshtatshme për ata të cilëve u drejtohet. Niveli dhe lloji i gjuhës së përdorur do të duhet të jetë i ndryshëm në varësi të audiencës, për shembull, për një të rritur apo për një fëmijë, për publikun e gjerë, apo për një ekspert akademik. Çështja se si mund të ekuilibrohet ky aspekt i informacionit të kuptueshëm, trajtohet në Opinionin e Grupit të Punës së Nenit

[534] *Ibid*., neni 13, pikat 1 dhe 2, introductory ëording ëhere the General Data Protection Regulation refers to the information on the obligation to apply at "the time ëhen personal data are obtained".
[535] *Ibid*., nenet 13, pika 3 dhe 14, pika 3; shih gjithashtu referencën për intervalet e arsyeshme dhe pa vonesë të panevojshme sipas Konventës 108 të Modernizuar, nenit 8, pika 1, gërma (b).
[536] Raporti Shpjegues i Konventës 108 të Modernizuar, parag. 70.
[537] Komisioni Evropian do të zhvillojë më tej informacionin që do të paraqitet me anë të ikonave dhe procedurat për krijimin e ikonave standarde nëpërmjet akteve të deleguara; shih Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave, neni 12, pika 8.
[538] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni12, pikat 1, 5 dhe 7 dhe Konventa 108 e Modernizuar, neni 9, pika 1, gërma (b).

29 mbi Informimin e Harmonizuar, i cili nxit idenë e të ashtuquajturave njoftime të shtresëzuara[539] të cilat i mundësojnë subjektit të të dhënave të vendosë se në çfarë niveli i preferon hollësitë. Gjithësesi, kjo mënyrë paraqitjeje informacioni nuk e përjashton kontrolluesin nga detyrimi që buron nga nenet 13 dhe 14 të GDPR-së. Kontrolluesi duhet sidoqoftë t'i japë subjektit të të dhënave informacion të plotë.

Një nga mënyrat më të efektshme për të informuar është vendosja e njoftimeve informuese në faqen kryesore të faqes së internetit të kontrolluesit, si për shembull politikat e privatësisë. Ekziston megjithatë një pjesë e konsiderueshme e popullatës e cila nuk e përdor internetin dhe në politikat e informimit të një shoqërie apo autoriteti publik duhet marrë parasysh diçka e tillë.

[BOX TYPE 2]

Deklarata e privatsisë në lidhje me përpunimin e të dhënave personale në një faqe interneti mund të ketë përmbajtjen e mëposhtme:

Kush jemi ne?

'Kontrolluesi' i përpunimit të të dhënave është Bed and Breakfast C&U, me seli në [Adresa: xxx], Tel: xxx; Faks: xxx; Email: info@c&u.com; Adresa e kontaktit të Nëpunësit të Mbrojtjes së të Dhënave: [xxx].

Njoftimi në lidhje me të dhënat personale bën pjesë në kushtet e përgjithshme që rregullojnë shërbimet tona të hotelerisë.

Çfarë të dhënash mbledhin me prej jush?

Ne mbledhim nga jut ë dhënat personale në vijim: emrin tuaj, adresën postare, numrin e telefonit, adresën e postës elektronike, informacion mbi akomodimin tuaj, numrin e kartës së kreditit dhe të debitit dhe adresën e IP-së, ose emrat e domain-it të kompjuterëve që keni përdorur për t'u lidhur me faqen tonë të internetit.

Përse i mbledhim të dhënat tuaja?

Ne përpunojmë të dhënat tuaja me pëlqimin tuaj dhe për qëllime të kryerjes së rezervimeve, për lidhjen dhe përmbushjen e kontratave që kanë të bëjnë me shërbimet që ne ju ofrojnë dhe për të zbatuar kriteret e përcaktuara me ligj, për shembull të ligjit për taksat vendore, i cili na detyron të mbledhim të dhëna personale për të mundësuar pagesën e taksës së qytetit për akomodimin.

Si i përpunojmë të dhënat tuaja?

Të dhënat tuaja personale do të mbahen për një periudhë prej tre muajsh. Të dhënat tuaja nuk I nënshtrohen vendimmarrjes automatike.

Bed and Breakfast C&U ndjek procedura strikte sigurie, për të garantuar që informacioni juaj personal të mos dëmtohet, shkatërrohet apo përhapet tek palë të treat pa lejen tuaj dhe për të parandaluar aksesin e paautorizuar. Kompjuterët që mbajnë informacionin ruhen në një mjedis të sigurt, me akses fizik të kufizuar. Ne përdorim firewall-ë të sigurt dhe masa të tjera për të kufizuar aksesin elektronik. Nëse të dhënat duhen transferuar tek një palë e tretë, ne e detyrojmë atë që të zbatojë masa të ngjashme për mbrojtjen e të dhënave tuaja personale.

[539] Grupi i Punës së Nenit 29 (2004), *Opinion 10/2004 on More Harmonised Information Provisions*, WP 100, Bruksel, 25 nëntor 2004.

I gjithë informacioni që ne mbledhim apo regjistrojmë, është vetëm për përdorimin tonë të brendshëm. Vetëm personave të cilëve u nevojitet informacioni për të përmbushur detyrimet e tyre që burojnë nga kjo kontratë, u jepet akses tek të dhënat personale. Ne do t'ju pyesim qartësisht jur të kemi nevojë për informacion për t'ju identifikuar. Ne mund t'ju kërkojmë të bashkëpunoni me kontrollet tona të sigursë përpara se t'ju komunikojmë informacione. Ju mund të përditësoni informacionin personal që na jepni në çdo moment duke na kontaktuar drejtpërdrejtë.

Cilat janë të drejtat tuaja?

Ju keni të drejtën e aksesit tek të dhënat tuaja, të merrni një kopje të të dhënave tuaja, të kërkoni fshirjen apo korrigjimin e tyre, ose të kërkoni që të dhënat tuaja të transferohen tek një kontrollues tjetër.

Ju mund të na drejtoni kërkesat tuaja tek info@c&u.com. Ne duhet t'u përgjigjemi kërkesave tuaja brenda një muaji, por nëse kërkesa juaj është tepër e ndërlikuar, apo nëse marrim shumë kërkesa të tjera, ne do t'ju informojmë që kjo periudhë mund të zgjatet edhe me dy muaj të tjerë.

Aksesi tek të dhënat tuaja

Ju keni të drejtën e aksesit tek të dhënat tuaja, t'ju bëhet e ditur me kërkesë arsyeja për përpunimin e të dhënave, të kërkoni fshirjen ose korrigjimin e tyre dhe të drejtën të mos i nënshtroheni një vendimmarrjeje krejtësisht automatike pa u marrë parasysh mendimet tuaja. Ju mund të komunikoni kërkesat tuaja tek info@c&u.com. Ju keni gjithashtu të drejtën të kundërshtoni përpunimin, të anuloni pëlqimin dhe të ankoheni tek autoriteti kombëtar mbikëqyrës, nëse vlerësoni se ky përpunim të dhënash është në shkelje të ligjit dhe të kërkoni kompensim për dëmtimet e pësuara si rrjedhojë e përpunimit të paligjshëm.

E drejta për të paraqitur ankesë

GDPR-ja detyron kontrolluesin të informojë subjektet e të dhënave në lidhje me mekanizmat ligjzbatuese sipas së drejtën kombëtare dhe asaj të BE-së për rastet e shkeljeve ndaj të dhënave personale. Kontrolluesi duhet të informojë subjektet e të dhënave për të drejtën e tyre për të paraqitur ankesë në lidhje me një shkelje ndaj të dhënave personale tek autoriteti mbikëqyrës dhe nëse është e nevojshme, në një gjykatë kombëtare.[540] E drejta e KiE-së parashikon gjithashtu të drejtën e subjekteve të të dhënave për t'u informuar për mënyrat e ushtrimit të të drejtave të tyre, përfshirë të drejtën për mjet mbrojtjeje të përcaktuar në nenin 9, pika 1, gërma (f).

Përjashtimet nga detyrimi për të informuar

GDPR-ja përcakton përjashtime nga detyrimi për të informuar. Sipas nenit 13, pika 4 dhe nenit 14, pika 5 të GDPR-së, detyrimi për të informuar subjektet e të dhënave nuk zbatohet nëse subjekti i të dhënave e disponon të gjithë informacionin përkatës.[541] Po ashtu, kur të dhënat personale nuk janë përftuar nga subjekti i të dhënave, detyrimi për të informuar nuk gjen zbatim, nëse dhënia e informacionit është e

[540] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 13, pika 2, gërma (d) dhe 14, pika 2, gërma (e); Konventa 108 e Modernizuar, neni 8, pika 1, gërma (f).
[541] *Ibid*., nenet 13, pika 4 dhe 14, pika 5, gërma (a).

pamundur apo jo proporcionale, sidomos kur të dhënat personale janë përpunuar për qëllime arkivore në interesin publik, për qëllime të kërkimit shkencor ose historik, apo për qëllime statistikore.[542]

Gjithashtu, Shteteve Anëtare u jep GDPR-ja një hapësirë për të kufizuar detyrimet dhe të drejtat që u njeh rregullorja personave, nëse kjo përbën një masë të nevojshme dhe proporcionale në një shoqëri demokratike, për shembull për mbrojtjen e sigurisë kombëtare dhe publike, mbrojtjen e vendit, mbrojten e hetime dhe procedimeve gjyqësore, apo për mbrojtjen e interesave ekonomike dhe financiare, ashtu si edhe të interesave private, të cilat prevalojnë mbi interesat në lidhje me mbrojtjen e të dhënave.[543]

Çdo përjashtim apo kufizim duhet të jetë i nevojshëm në një shoqëri demokratike dhe të jetë në përpjestim me qëllimin e ndjekur. Vetëm në disa raste përjashtimore, për shembull për shkak të indikacioneve mjekësore, mbrojtja e subjektit të të dhënave mund të kërkojë në vetvete kufizim të transparencës; kjo ka të bëjë sidomos me kufizimin e së drejtës për akses të çdo subjekti të dhënash.[544] Gjithësesi, si nivel minimal mbrojtjeje, e drejta kombëtare duhet të respektojë thelbin e së drejtave dhe lirive themelore që mbrohen nga e dreja e BE-së.[545] Për këtë duhet që e drejta kombëtare të përmbajë dispozita specifike që qartësojnë qëllimin e përpunimit, kategoritë e të dhënave personale të përfshira, masat e mbrojtjes dhe kritere të tjera proceduriale.[546]

Kur të dhënat janë mbledhur për qëllime të kërkimit shkencor, apo historik, për qëllime statistikore, apo për qëllime arkivore në interesin public, e drejta e Bashkimit apo e Shteteve Anëtare mund të përcaktojë përjashtime nga detyrimi për të informuar, nëse ka të ngjarë të pamundësojë, ose të dëmtojë rëndë arritjen e qëllimeve specifike.[547]

Kufizime të ngjashme ekzistojnë edhe në të drejtën e KiE-së, kur të drejtat që i njihen subjekteve të të dhënave në nenin 9 të Konventës 108 të Modernizuar, mund t'u nënshtrohen kufizimeve të mundshme në pajtim me nenin 11 Konventës 108 të Modernizuar, sipas disa kushteve strikte. Gjithashtu, sipas nenit 8, pika 2 të Konventës 108 të Modernizuar, detyrimi për transparencë të përpunimit që u ngarkohet kontrolluesve, nuk gjen zbatim kur subjekti i të dhënave është i informuar.

E drejta e personit për akses tek të dhënat e veta

Sipas së drejtës së KiE-së, e drejta për akses e personit tek të dhënat e veta njihet qartësisht nga neni 9 i Konventës 108 të Modernizuar, i cili përcakton se çdo person ka të drejtën që, me kërkesën e tij, t'i jepet informacion i kuptueshëm në lidhje me përpunimin e të dhënave personale që kanë të bëjnë me të. E drejta për akses nuk njihet vetëm nga dispozitat e Konventës 108 të Modernizuar, por edhe nga jurisprudenca e GJEDNJ-së. GJEDNJ-ja është shprehur në mënyrë të përsëritur se personat kanë të drejtën e qasjes në informacion në lidhje me të dhënat e tyre personale dhe se kjo e drejtë buron nga nevoja për respektimin e jetës private.[548] Gjithësesi, e drejta për akses tek të dhënat personale që mbahen nga organizatat publike ose private mund të kufizohet në disa rrethana të caktuara.[549]

Sipas së drejtës së BE-së, e drejta për akses e dikujt tek të dhënat që kanë të bëjnë me të, pranohet qartësisht në nenin 15 të GDPR-së dhe përcaktohet gjithashtu si një element i së drejtës themelore për mbrojtje të të dhënave personale në nenin 8, pika të të Kartës së të Drejtave Themelore të BE-së.[550] E

[542] *Ibid*., neni 14, pika 5, gërmat (b)–(e).
[543] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 23, pika 1.
[544] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 15.
[545] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 23, pika 1.
[546] *Ibid*., neni 23, pika 2.
[547] *Ibid*., neni 89, pikat 2 dhe 3.
[548] GJEDNJ, *Gaskin k. Mbretërisë së Bashkuar*, nr. 10454/83, 7 korrik 1989; GJEDNJ, *Odièvre k. Francës* [ÇB], nr. 42326/98, 13 shkurt 2003; GJEDNJ, *K.H. dhe të Tjerët k. Sllovakisë*, nr. 32881/04, 28 prill 2009; GJEDNJ, *Godelli k. Italisë*, nr. 33783/09, 25 shtator 2012.
[549] GJEDNJ, *Leander k. Suedisë*, nr. 9248/81, 26 mars 1987.
[550] Shih gjithashtu GJDBE, Çështje të bashkuara C-141/12 dhe C-372/12, *YS k. Minister voor Immigratie, Integratie en Asiel* dhe *Minister voor Immigratie, Integratie en Asiel k. M dhe S*, 17 korrik 2014; GJDBE, C-615/13 P, *ClientEarth, Pesticide Action Netëork Europe (PAN Europe) k. Autoriteti Evropian i Sigurisë Ushqimore (EFSA), Komisioni Evropian*, 16 korrik 2015.

drejta e personit për të pasur akses në të dhënat personale të tij apo të saj, është një element kyç i së drejës evopriane në fushën e mbrojtjes së të dhënave.[551]

GDPR-ja parashikon se çdo subjekt të dhënash ka të drejtën e aksesit tek të dhënat personale të tij apo të saj dhe në disa informacione në lidhje me përpunimin, të cilat kontrolluesi duhet t'ia japë.[552] Në mënyrë të veçantë, çdo subjekt të dhënash ka të drejtën t'i konfirmohet (nga ana e kontrolluesit) nëse të dhënat që kanë të bëjnë me të, janë duke u përpunuar apo jo, si dhe informacion për të paktën me sa më poshtë vijon:

- Qëllimet e përpunimit;
- Kategoritë e të dhënave të përfshira;
- Marrësit apo kategoritë e marrësve, të cilëve u komunikohen të dhënat;
- Afatete e parashikuara të mbajtjes së të dhënave, ose nëse kjo nuk është e mundur, kriteret e përdorura për të përcaktuar afatet;
- Ekzistencën e të drejtave për të korrigjuar apo për të fshirë të dhënat personale, ose të kufizimit të përpunimit të të dhënave personale;
- Të drejtën për të bërë ankesë pranë autoritetit mbikëqyrës;
- Çdo informacion të disponueshëm në lidhje me origjinën e të dhënave që u nënshtrohen përpunimit, nëse këto të dhëna nuk janë mbledhur drejtpërdrejtë nga subjekti i të dhënave;
- Në rast vendimesh automatike, logjikën e përdorur për çdo përpunim automatic të dhënash.

Kontrolluesi i të dhënave duhet t'i vërë në dispozicion subjektit të të dhënave një kopje të të dhënave personale që përpunohen. Çdo informacion që i komunikohet subjektit të të dhënave, duhet të jetë i qartë, çka nënkupton se kontrolluesi duhet të sigurohet që subjekti i të dhënave e kupton informacionin që i jepet. Për shembull, përfshirja e shkurtesave teknike, termave të koduar, apo akronimeve tek përgjigjja kundrejt një kërkese për akses, zakonisht nuk mjafton, përjashto rastin kur shpjegohet kuptimi i këtyre termave. Kur kryhet vendimmarrje automatike, përfshirë profilizimin, logjika e përgjithshme e përdorur do të duhet gjithashtu të shpjegohet, duke përfshirë edhe kriteret që janë marrë parasysh kur është vlerësuar subjekti i të dhënave. Kritere të ngjashme ekzistojnë edhe në të **Drejtën e KiE-së**.[553]

[BOX TYPE 2]

Shembull: Aksesi tek të dhënat e tij apo të saj, do ta ndihmonte subjektin e të dhënave të përcaktonte nëse të dhënat e tij apo të saj janë të sakta. Për rrjedhojë, ka rëndësi thelbësore që subjekti i të dhënave të informohet, në një formë të kuptueshme, jo vetëm për të dhënat personale që janë faktikisht objekt përpunimi, por gjithashtu edhe për kategoritë e këtyre të dhënave personale, sikurse emri, adresa e IP-së, koordinatat e gjeolokalizimit, numrat e kartës së kreditit, etj.

Informacioni që ka të bëjë me burimin e të dhënave – në rastin kur të dhënat nuk janë mbledhur drejtpërdrejtë nga subjekti i të dhënave – duhet të përfshihet në përgjigje të një kërkese për akses, për aq sa ky informacion është i disponueshëm. Kjo dispozitë duhet kuptuar në kontekstin e parimeve të drejtësisë, transparencës dhe përgjegjshmërisë. Kontrolluesi nuk mund të shkarërrojë informacionin në lidhje me burimin e të dhënave në mënyrë që të përjashtohet nga detyrimi për ta komunikuar atë, përvçse kur fshirja mund të ketë ndodhur pavarësisht se ka marrë një kërkesë për akses dhe sidoqoftë duhet të respektojë kriteret e përgjithshme të 'përgjegjshmërisë'.

Sikurse është përcaktuar nha jurisprudence e GJDBE-së, e drejta për akses tek të dhënat personale nuk duhet kufizuar në mënyrë të paarsyeshme për shkak të afateve. Subjekteve të të dhënave u duhet dhënë

[551] GJDBE, Çështje të bashkuara C-141/12 dhe C-372/12, *YS k. Minister voor Immigratie, Integratie en Asiel* dhe *Minister voor Immigratie, Integratie en Asiel k. M dhe S*, 17 korrik 2014.
[552] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 15, pika 1.
[553] Shih Konventën 108 të Modernizuar, nenin 8, pika 1, gërma (c).

gjithashtu mundësi të arsyeshme për t'u informuar në lidhje me aktivitetet e përpunimit të të dhënave që janë kryer në të kaluarën.

[BOX TYPE 1]

Shembull: Tek çështja *Rijkeboer*,[554] GJDBE-së iu kërkua të përcaktonte nëse e drejta e një personi për akses në informacionin në lidhje me marrësit, ose me kategoritë e marrësve të të dhënave personale dhe në përmbajtjen e të dhënave, mund të kufizohej deri në një vit përpara kërkesës për akses të tij apo të saj.

Për të përcaktuar nëse legjislacioni i BE-së autorizon këtë afat kohor, GJDBE-ja vendosi të interpretonte nenin 12, duke iu referuar qëllimeve të direktivës. Fillimisht GJDBE-ja theksoi se e drejta për akses ishte e nevojshme për t'i mundësuar subjektit të të dhënave të ushtrojë të drejtën për t'i kërkuar kontrolluesit të korrigjojë, fshijë apo bllokojë të dhënat e tij apo të saj, apo për të njoftuar palët e treat tek të cilat të dhënat mund të jenë komunikuar, në lidhje me atë korrigjim, fshirje apo bllokim. Një e drejtë aksesi e efektshme është po aq e rëndësishme për t'i mundësuar subjektit të të dhënave të ushtrojë të drejtën për të kundërshtuar përpunimin e të dhënave personale të tij apo të saj, apo për të paraqitur ankesë dhe për të kërkuar kompensim dëmi.[555]

Në mënyrë që të garantohet efekti i duhur i të drejtave që u jepen subjekteve të të dhënave, GJDBE-ja u shpreh se "ajo e drejtë duhet detyrimisht të lidhet me të kaluarën. Nëse nuk do të ishte kështu, subjekti i të dhënave nuk do të kishte mundësi të ushtronte në mënyrë efikase të drejtat e tij apo të saj për të kërkuar korrigjimin, fshirjen ose bllokimin e të dhënave të supozuara si të paligjshme, apo të pasakta dhe të përftonte kompensim për dëmin e pësuar".

6.1.2. E drejta për korrigjim

Në të drejtën e BE-së dhe **në të drejtën e KiE-së**, subjektet e të dhënave kanë të drejtën të korrigjojnë të dhënat e tyre personale. Saktësia e të dhënave personale është thelbësore për garantimin e një niveli të lartë të mbrojtjes së të dhënave për subjektet e të dhënave.[556]

[BOX TYPE 1]

Shembull: tek çështja *Ciubotaru k. Moldavisë*,[557] kërkuesi nuk mundej të ndryshonte regjistrimin e origjinës së tij etnike në regjistrat zyrtarë, nga moldav në rumun, me pretendimin se kërkesa e tij ishte e pambështetur. GJEDNJ-ja vlerësoi se është e pranueshme që Shtetet të kërkojnë prova objektive në momentin e regjistrimit të identitetit etnik të një personi. Kur një pretendim i tillë mbështetet në arsye thjesht subjektive e të pabazuara, autoritetet mund të refuzojnë. Megjithatë, pretendimi i kërkuesit nuk mbështetej vetëm në perceptimin subjektiv të etnisë së tij: ai kishte provuar në mënyrë objektive lidhje të verifikueshme me grupin etnik rumun, sikurse gjuhën, emrin, ndjeshmërinë dhe të tjera. Sidoqoftë, sipas së drejtës kombëtare, kërkuesi duhej të jepte prova që prindërit e tij i kishin përkitur grupit etink rumun. Duke pasur parasysh realitetet historike të Moldavisë, ky kriter kishte krijuar një barrierë të pakapërcyeshme për regjistrimin e një identiteti etnik të ndryshëm nga ai që autoritetet sovjetike kishin regjistruar për prindërit e tij. Duke penguar kërkuesin që pretendimi i tij të shqyrtohej, bazuar në prova

[554] GJDBE, C-553/07, *College van burgemeester en wethouders van Rotterdam k. M. E. E. Rijkeboer*, 7 maj 2009.
[555] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 15, pika 1, gërmat (c) dhe (f), 16, 17, pika 2 dhe 21, dhe Kreun VIII.
[556] *Ibid*., neni 16 dhe paragrafi 65 i Preambulës; Konventa 108 e Modernizuar, neni 9, pika 1, gërma (e).
[557] GJEDNJ, *Ciubotaru k. Moldavisë*, nr. 27138/04, 27 prill 2010, paragrafët 51 dhe 59.

objektivisht të verifikueshme, shteti nuk kishte zbatuar detyrimin pozitiv të tij për t'i siguruar kërkuesit respektim të efekshtëm të jetës së tij private. Gjykata vendosi se ishte shkelur neni 8 i KEDNJ-së.

Në disa raste, subjekti i të dhënave mjafton thjesht të kërkojë korrigjimin, për shembull, të shqiptimit të emrit, ndryshimin e adresës ose të numrit të telefonit. Sipas së **drejtës së BE-së** dhe **së drejtës së KiE-së**, të dhënat personale të pasakta duhen korrigjuar pa vonesë të panevojshme apo të tepruar.[558] Gjithësesi, nëse kërkesa të tilla lidhen me çështje juridike me rëndësi domethënëse, sikurse identiteti ligjor i subjektit të të dhënave, apo adresa e saktë e banimit për pajisjen me dokumente ligjore, vetëm kërkesa për korrigjim mund të mos mjaftojë dhe kontrolluesi mund të ketë të drejtën të kërkojë provë për pasaktësinë e pretenduar. Këto kërkesa nuk duhet t'i ngarkojnë subjektit të të dhënave një barrë prove të paarsyeshme, e cila t'i pengojë subjektet e të dhënave që të korrigjojnë të dhënat e tyre. GJEDNJ-ja ka gjetur shkelje të nenit 8 të KEDNJ-së në çështje të ndryshme ku kërkuesi nuk ka mundur të kundërshtojë saktësinë e informacionit që mbahej në regjistra sekretë.[559]

[BOX TYPE 1]

Shembull: tek *Cemalettin Canli k. Turqisë*,[560] GJEDNJ-ja gjeti një shkelje të nenit 8 të KEDNJ-së në raportimin jo korrekt nga ana e policisë në lidhje me procedimin penal.

Këkuesi ishte proceduar dy herë penalisht për me dyshimin për anëtarësim në organizata të paligjshme, por nuk ishte dënuar. Kur kërkuesi ishte arrestuar dhe akuzuar sërish për një vepër tjetër penale, policia kishte depozituar pranë gjykatës penale një raport të titulluar "*kartelë informacioni mbi vepra të tjera penale*", në të cilën thuhej se kërkuesi ishte anëtar i dy organizatave të paligjshme. Kërkesa e kërkuesit për ndryshimin e raportit dhe dosjes policore nuk ishte pranuar. GJEDNJ-ja mbajti qëndrimin se informacioni në raportin policor hynte në fushën e zbatimit të nenit 8 të KEDNJ-së, meqenëse mbledhja në mënyrë sistematike e informacionit publik, që përfshihet në dosje të cilat mbahen nga autoritetet, mundet gjithashtu të hynte në sferën e 'jetës private'. Për më tepër, raporti policor ishte i pasaktë në përmbajtje dhe depozitimi i tij pranë gjykatës penale nuk ishte në përputhje me të drejtën e brendshme. Gjykata vendosi se kishte pasur shkelje të nenit 8.

Gjatë një çështjeje civile, apo procedimi nga ana e një autoriteti publik, për të vendosur nëse të dhënat janë të sakta ose jo, subjekti i të dhënave mund të kërkojë që në dosjen e të dhënave të tij apo të saj të vendoset një shënim, i cili të theksojë se saktësia e të dhënave është kundërshtuar dhe se pritet një vendim zyrtar në lidhje me këtë.[561] Gjatë kësaj kohe, kontrolluesi i të dhënave nuk duhet t'i paraqesë të dhënat sikur janë të sakta, apo sikur nuk janë subjekt korrigjimi, sidomos kundrejt palëve të treta.

6.1.3. E drejta e fshirjes ('e drejta për t'u harruar')

E drejta që u jepet subjekteve të të dhënave që të dhënat e tyre të fshihen, është me rëndësi të posaçme për zbatimin efikas të parimeve të mbrojtjes së të dhënave dhe sidomos parimit të minimizimit të të dhënave (të dhënat personale duhet të kufizohen vetëm në atë që është e nevojshme për qëllimet për të cilat përpunohen të dhënat). Për rrjedhojë, e drejta e fshirjes gjendet si në instrumentet ligjore të KiE-së, ashtu edhe të BE-së.[562]

[BOX TYPE 1]

[558] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 16; Konventa 108 e Modernizuar, neni 9, pika 1.
[559] GJEDNJ, *Rotaru k. Rumanisë* [ÇB], nr. 28341/95, 4 maj 2000.
[560] GJEDNJ, *Cemalettin Canli k. Turqisë,* nr. 22427/04, 18 nëntor 2008, parag. 33 dhe 42–43; GJEDNJ, *Dalea k. Francës, nr.* 964/07, 2 shkurt 2010.
[561] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 18 dhe paragrafi 67 i Preambulës.
[562] *Ibid*., neni 17.

Shembull: tek *Segerstedt-Wiberg dhe të Tjerët k. Suedisë*,[563] kërkuesit ishin angazhuar në disa parti politike të caktuara liberale dhe komuniste. Ata dyshonin se disa informacione në lidhje me ta ishin regjistruar në dosjet e policisë sekrete dhe kërkuan fshirjen e tyre. GJEDNJ-ja pranoi se mbajtja e të dhënave kishte bazë ligjore dhe qëllim legjitim. Sidoqoftë, për sa i takon disa prej kërkuesve, GJEDNJ-ja vlerësoi se vazhdimi i mbajtjes së të dhënave përbënte ndërhyrje jo proporcionale në jetët e tyre private. Për shembull, në rastin e një kërkuesi, autoritetet mbanin informacion që në vitin 1969, ai dyshohej se bënte thirrje për rezistencë të dhunshme ndaj kontrolleve policore gjatë demonstratave. GJEDNJ-ja vlerësoi se ky informacion nuk mund të kishte interes për sigurinë publike, sidomos për shkak të karakterit historik të tij. Gjykata gjeti shkelje të nenit 8 të KEDNJ-së për katër nga pesë kërkuesit, meqenëse referuar periudhës së gjatë kohore që kishte kaluar nga kryerja e dyshuar e këtyre akteve nga ana e kërkuesve, mbajtja në vazhdim e të dhënave të tyre nuk kishte më vlerë.

Shembull: tek *Brunet k. Francës*,[564] kërkuesi kishte kundërshtuar mbajtjen e informacionit personal të tij në një bazë të dhënash të policisë, e cila mbante informacion në lidhje me persona të dënuar, të akuzuar dhe viktima. Megjithëse procedimi penal kundër kërkuesit ishte pushuar, informacionet në lidhje me të vijonin të shfaqeshin në bazën e të dhënave. GJEDNJ-ja vendosi se kishte pasur shkelje të nenit 8 të KEDNJ-së. Për të dalë në këtë vendim, Gjykata vlerësoi se në praktikë subjektit të të dhënave nuk i jepej asnjë mundësi që të fshinte të dhënat e tij personale nga baza e të dhënave. GJEDNJ-ja shqyrtoi gjithashtu natyrën e informacionit që mbahej tek kjo bazë të dhënash dhe vlerësoi se ishte ndërhyrëse në privatësinë e kërkuesit, pasi në të përfshiheshin të dhëna të hollësishme të identitetit dhe personalitetit të tij. Gjykata vendosi gjithashtu se afati prej 20 vitesh i mbajtjes së skedave personale në bazën e të dhënave, ishte i tepruar, sidomos duke pasur parasysh se kërkuesi nuk ishte dënuar kurrë me vendim gjyqësor.

Konventa 108 e Modernizuar njeh shprehimisht se çdo person ka të drejtën e fshirjes së të dhënave të pasakta, false apo të përpunuara në mënyrë të paligjshme.[565]

Në të drejtën e BE-së, neni 17 i GDPR-së u jep efekt kërkesave të subjekteve të të dhënave për fshirjen e të dhënave. E drejta për fshirjen e të dhënave pa vonesë të paarsyeshme zbatohet kur:

- Të dhënat personale nuk nevojiten më për sa i takon qëllimeve për të cilat ato janë mbledhur ose përpunuar;
- Subjekti it ë dhënave tërheq pëlqimin mbi të cilin bazohet përpunimi dhe nuk ka asnjë shkak tjetër ligjor për përpunimin;
- Subjekti i të dhënave kundërshton përpunimin dhe nuk ka shkaqe legjitime mbizotëruese për përpunimin;
- Të dhënat janë përpunuar në mënyrë të paligjshme;
- Të dhënat personale duhen fshirë për të përmbushur një detyrim ligjor në të drejtën e Bashkimit apo të Shtetit anëtar, së cilës i nënshtrohet kontrolluesi;
- Të dhënat personale janë mbledhur në lidhje me ofrimin e shërbimeve të shoqërisë së informacionit për një fëmijë, në përputhje me nenin 8 të GDPR-së.[566]

Barra e provës për të vërtetuar se përpunimi it ë dhënave është ligjitim, bie mbi kontrolluesit e të dhënave, meqenëse ata janë përgjegjës për ligjshmërinë e përpunimit.[567] Sipas parimit të

[563] GJEDNJ, *Segerstedt-Wiberg dhe të Tjerët k. Suedisë*, nr. 62332/00, 6 qershor 2006, parag. 89 dhe 90; shih gjithashtu, për shembull, GJEDNJ, *M.K. k. Francës*, nr. 19522/09, 18 prill 2013.
[564] GJEDNJ, *Brunet k. Francës*, nr. 21010/10, 18 shtator 2014.
[565] Konventa 108 e Modernizuar, neni 9, pika 1, gërma (e).
[566] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 17, pika 1.
[567] *Ibid*.

përgjegjshmërisë, kontrolluesi duhet të jetë në gjendje të demonstrojë në çdo moment se ka një bazë ligjore të fortë për përpunimin e tij të të dhënave, përndryshe përpunimi duhet të ndalet.[568] GDPR-ja përcakton përjashtimet nga e drejta për t'u harruar, përfshirë edhe kur përpunimi it ë dhënave personale është i nevojshëm për:

- Ushtrimin e së drejtës së lirisë së shprehjes dhe të informimit;
- Përmbushjen e një detyrimi ligjor, i cili kërkon përpunimin sipas së drejtës së Bashkimit apo të Shtetit Anëtar të cilës i nënshtrohet kontrolluesi, ose për përmbushjen e një detyre në interesin public, ose në ushtrim të autoritetit zyrtar të veshur kontrolluesit;
- Shkaqe të interest publik në sferën e shëndetit publik;
- Qëllime arkivore në interesin publik, ose qëllme të kërkimit shkencor apo historik, ose për qëllime statistikore;
- Ngritjen, ushtrimin ose mbrojtjen e pretendimeve ligjore.[569]

GJDBE-ja e ka pohuar rëndësinë e të drejtës së fshirjes për garantimin e një niveli të lartë të mbrojtjes së të dhënave.

[BOX TYPE 1]

Shembull: tek çështja *Google Spain,*[570] GJDBE-ja shqyrtoi nëse Google-i ishte i detyruar të fshinte informacione të vjetra në lidhje me vështirësitë financiare të kërkuesit nga lista e rezultateve të kërkimit. Ndër të tjera, Google-i kundështoi përgjegjësinë, me arsyetimin se ai thjesht vinte në dispozicion lidhjen me faqen në internet të publikuesit që mban informacionin, në rastin konkret një gazetë që raportone mbi problematikat e falimentit të kërkuesit.[571] Google-i theksonte se kërkesa për të fshirë një informacion të vjetëruar nga një faqe interneti i duhej bërë zotëruesit të faqes dhe jo Google-it, i cili thjesht ofronte një lidhje me faqen burimore. GJDBE-ja doli në përfundimin se kur Google-i kërkon në rrjet për informacion dhe faqe interneti dhe kur indekson përmbajtjen me qëllim që të ofrojë rezultatet e kërkimit, shndërrohet në kontrollues, ndaj të cilit zbatohen përgjegjësitë dhe detyrimet sipas së drejtës së BE-së.

GJDBE-ja qartësoi se motorët e kërkimit në internet dhe rezultatet e kërkimit që ofrojnë të dhëna personale, mund të përcaktojnë një profil të hollësishëm në lidhje me një person.[572] Motorët e kërkimit bëjnë që informacionet e këtyre listave të rezultateve të jenë të kudondodhura. Duke pasur parasysh se sa e rëndë mund të jetë kjo ndërhyrje, ajo nuk mund të justifikohet thjesht me interesin ekonomik që ka operatori i një motori për atë përpunim. Duhet gjetur një ekuilibër i drejtë, sidomos midis interesit legjitim të përdoruesve të internetit për akses në informacion, me të drejtat themelore të subjektit të të dhënave, sipas neneve 7 dhe 8 të Kartës së të Drejtave Themelore të BE-së. Në një shoqëri gjithnjë e më të digjitalizuar, kriteri që të dhënat personale të jenë të sakta dhe përdorimi i tyre të jetë i kufizuar vetëm tek ajo çka është e nevojshme (për shembull për informimin e publikut), është themelor për të garantuar nivel të lartë të mbrojtjes së të dhënave të subjekteve. "Brenda kuadrit të përgjegjësive, kompetencave dhe aftësive të tij, kontrolluesi duhet të garantojë se përpunimi plotëson të gjitha

[568] *Ibid*., neni 5, pika 2.
[569] *Ibid*., neni 17, pika 3.
[570] GJDBE, C-131/12, *Google Spain SL, Google Inc. k. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [ÇB] , 13 maj 2014, parag. 55–58.
[571] Google kundërshtoi gjithashtu zbatimin e rregullave të mbrojtjes së të dhënave të BE-së nisur nga fakti se Google Inc. e ka selinë në SHBA dhe përpunimi i të dhënave objekt i çështjes, kryhej gjithashtu në SHBA. Një argument i dytë për moszbatueshmërinë e legjislacionit të BE-së për mbrojtjen e të dhënave kishte të bënte me pretendimin se motorët e kërkimit nuk duhen konsideruar si 'kontrollues' në lidhje me të dhënat e shfaqura tek rezultatet, pasi ato nuk nuk njohuri për të dhënat e as nuk ushtrojnë kontroll mbi to. GJDBE-ja i hodhi poshtë të dy argumentet, me qëndrimin se Direktiva 95/46/EC gjente zbatim në këtë rast dhe vijoi me shqyrtimin e fushës së të drejtave që garanton Direktiva, veçanërisht të së drejtës për fshirje të të dhënave personale.
[572] *Ibid*., paragrafët 36, 38, 80–81 dhe 97.

kërkesat" e së drejtës së BE-së, në mënyrë që garancitë ligjore që përcakton ajo të kenë efekt të plotë.[573] Kjo nënkupton se e drejta e subjektit për fshirjen e të dhënave personale të tij apo të saj kur përpunimi është i vjetëruar, ose nuk është më i nevojshëm, përfshin gjithashtu edhe kontrolluesit e të dhënave që i riprodhojnë informacionet.[574]

Në lidhje me çështjen nëse Google-i ishte i detyruar të hiqte lidhjet që kishin të bënin me kërkuesin, GJDBE-ja u shpreh se personat kanë të drejtën të kërkojnë fshirjen e të dhënave personale sipas disa kushteve të caktuara. Kjo e drejtë mund të përdoret kur informacioni që ka të bëjë me një person është i pasaktë, i papërshtatshëm, i parëndësishëm ose i tepruar, në raport me qëllimet e përpunimit të të dhënave. GJDBE-ja pranoi se kjo e drejtë nuk është absolute, porse ajo duhet ekuilibruar me të drejta dhe interesa të tjera, sidomos me interesin e publikut të gjerë për të pasur akses në informacione të caktuara. Çdo kërkesë për fshirje duhet trajtuar rast pas rasti, me qëllim që të vendoset ekuilibri i duhur midis të drejtave themelore për mbrojtje të të dhënave personale dhe jetës private të subjektit të të dhënave nga njëra anë dhe interesave legjitime të përdoruesve të internetit, përfshirë ato të botuesve, nga ana tjetër. GJDBE-ja dha orientime në lidhje me faktorët që duhen marrë parasysh kur kërkohet të vendoset ky ekuilibër. Natyra e informacionit objekt çështjeje është një faktor me rëndësi të veçantë. Nëse informacioni ka të bëjë me jetën private të personit dhe nuk ekziston ndonjë interes i përgjithshëm që informacioni të jetë publik, mbrojtja e të dhënave dhe privatësisë do të prevalojnë mbi të drejtën e publikut të gjerë për të pasur akses tek ai informacion. Ndërsa nga ana tjetër, nëse duket se subjekti i të dhënave është figurë publike, ose nëse informacioni ka natyrë të tillë që justifikon disponueshëmrinë e tij për publikun e gjerë, atëherë interesi mbizotërues i publikut të gjerë për të pasur akses tek informacioni, mund të justifikojë ndërhyrjen tek të drejtat themelore të subjektit të të dhënave për mbrojtjen e të dhënave dhe privatësisë.

Në vijim të këtij vendimi, Grupi i Punës së Nenit 29 miratoi udhëzuesin për zbatimin e vendimit të GJDBE-së.[575] Udhëzuesi përfshin një listë kriteresh të përbashkëta që mund të përdoren nga autoritetet mbikëqyrëse kur trajtojnë ankesa në lidhje me kërkesat e personave për fshirje dhe shpjegojnë çfarë mbart e drejta për fshirje, si dhe i udhëzojnë ato në përpjekjet për të ekuilibruar të drejtat. Udhëzuesi rikujton se vlerësimi duhet bërë rast pas rasti. Meqenëse e drejta për t'u harruar nuk është absolute, rezultati i një kërkese mund të ndryshojë në varësi të rastit. Diçka e tillë ilustrohet nga jurisprudence e GJDBE-së pas çështjes Google.

[BOX TYPE 1]

Shembull: Tek çështja *Camera di Commercio di Lecce k. Manni*,[576] GJDBE-së iu kërkua të shqyrtonte nëse përsoni kishte të drejtën të përftonte fshirjen e të dhënave personale të tij, të cilat ishin publikuar në Regjistrin Publik të Shoqërive Tregtare pasi shoqëria e tij kishte pushuar së ekzistuari. Z. Manni i kishte kërkuar Dhomës së Tregtisë së Leçes të fshinte të dhënat e tij personale nga ai regjistër, pasi kishte zbuluar se klientët e mundshëm, mund të kontrollonin regjistrin dhe të shihnin se ai kishte qenë më parë adminstratori i një shoqërie që kishte shpallur falimentin më shumë se një dekadë më parë. Kërkuesi besonte se ky informacion mund të ndikonte negativisht tek klientët e mundshëm.

[573] *Ibid*., paragrafët 81–83.
[574] GJDBE, C-131/12, *Google Spain SL, Google Inc. k. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [ÇB], 13 maj 2014, parag. 88. Shih gjithashtu: Grupi i Punës së Nenit 29 (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, WP 225, Bruksel, 26 nëntor 2014 dhe Rekomandimin CM/Rec 2012(3) të Komitetit të Ministrave të shteteve anëtare për mbrojtjen e të drejtave të njeriut në lidhje me motorët e kërkimit, 4 prill 2012.
[575] Grupi i Punës së Nenit 29 (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, WP 225, Bruksel, 26 nëntor 2014.
[576] GJDBE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce k. Salvatore Manni*, 9 mars 2017.

Me qëllim që të peshonte të drejtën e z. Manni për mbrojtjen e të dhënave personale të tij kundrejt interesit të publikut të gjerë për akses në atë informacion, GJDBE-ja shqyrtoi fillimisht qëllimin e regjistrit publik. Gjykata nënvizoi faktin se publikimi ishte i parashikuar me ligj dhe në mënyrë të veçantë nga një direktivë e BE-së, e cila kishte si qëllim ta bënte informacionin në lidhje me shoqëritë tregtare më të lehtë për t'u aksesuar nga palët e treta. Kësisoj, këto të fundit duhet të kishin akses në të dhe të kishin mundësi të analizonin dokumentet bazë të një shoqërie dhe informacione të tjera mbi shoqërinë, "sidomos identitein e personave të cilët marrin vendime në lidhje me të". Qëllimi i publikimit ishte gjithashtu të garantonte siguri juridike, duke pasur parasysh intensifikimin e tregtisë ndërmjet Shteteve Anëtare, nëpërmjet garantimit të aksesit nga ana e palëve të treta tek të gjitha informacionet përkatëse në lidhje me shoqëritë në të gjithë BE-në.

GJDBE-ja vërejti më tej se edhe me kalimin e kohës, madje edhe pas shpërbërjes së një shoqërie, të drejtat dhe detyrimet ligjore në lidhje me atë shoqëri shpesh vijojnë të ekzistojnë. Mosmarrëveshjet për shpërbërjet e shoqërive zgjasin në kohë dhe çështje që kanë të bëjnë me shoqërinë, administratorët dhe likuidatorët e saj, mund të shfaqen edhe shumë vite pasi shoqëria ka pushuar së ekzistuari. GJDBE-ja theksoi se për shkak të shumëllojshmërisë së skenarëve të mundshëm dhe dallimeve që ekzistojnë në Shtetet Anëtare për sa i përket afateve të parashkrimit, "duket e pamundur në këtë moment to identifikohet një afat kohor unik, që nga shkrirja e shoqërisë, në përfundim të së cilës përfshirja e këtyre të dhënave në regjistër dhe publikimi i tyre nuk do të ishtë më i nevojshëm". Për shkak të qëllimit legjitim për publikimin e tyre dhe vështirësisë për të përcaktuar një periduëh kohore, në përfundim të së cilës të dhënat personale mund të fshihen nga regjistri, pa dëmtuar interesat e palëve të treta, GJDBE-ja vendosi se rregullat e mbrojtjes së të dhënave të BE-së nuk garantojnë të drejtën e fshirjes së të dhënave personale për personat në situatën e z. Manni.

Kur kontrolluesi i ka publikuar të dhënat personale dhe i kërkohet që t'i fshijë ato, kontrolluesi i të dhënave është i detyruar dhe duhet të ndërmarrë veprime të 'arsyeshme' për të informuar kontrolluesit e tjerë që përpunojnë të njëjtat të dhëna, në lidhje me kërkesën e subjektit të të dhënave për fshirjen e tyre. Në aktivitetin e tij, kontrolluesi duhet të marrë parasysh teknologjitë e disponueshme dhe kostot e zbatimit të tyre.[577]

6.1.4. E drejta për kufizimin e përpunimit

Neni 18 i GDPR-së u jep subjekteve të të dhënave të drejtën për të përftuar nga kontrolluesi kufizim të përkohshëm të përpunimit të të dhënave personale të tyre. Subjektet e të dhënave mund të kërkojnë nga kontrolluesi që të kufizojë përpunimin kur:

- Kundërshtohet saktësia e të dhënave personale;
- Përpunimi është i paligjshëm dhe subjekti i të dhënave kërkon kufizimin e përdorimit të të dhënave personale në vend të fshirjes së tyre;
- Të dhënat duhen mbajtur për të ushtruar ose mbrojtur pretendimet ligjore;
- Pritet verifikimi nëse interesat legjitime të kontrolluesit të të dhënave mbizotërojnë ato të subjektit të të dhënave.[578]

Metodat me të anë të së cilave kontrolluesi mund të kufizojë përpunimin e të dhënave personale mund të konsistojnë për shembull në zhvendosjen e përkohshme të të dhënave të përzgjedhura në një system

[577] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 17, pika 2 dhe paragrafi 66 i Preambulës.
[578] *Ibid*., neni 18, pika 1.

tjetër përpunimi, bërjen e të dhënave të padisponueshme për përdoruesit, ose heqjen përkohësisht të të dhënave personale.[579] Kontrolluesi duhet të njoftojë subjektin e të dhënave përpara se të hiqet kufizimi i përpunimit.[580]

Detyrimi për të njoftuar në lidhje me korrigjimin ose fshirjen e të dhënave personale ose kufizimin e përpunimit

Për çdo korrigjim, ose fshirje të të dhënave personale, apo kufizim të përpunimit, kontrolluesi duhet informojë çdo marrës të cilit ai i ka komunikuar të dhënat personale, në masën që diçka e tillë të mos jetë e pamundur, apo jo proporcionale.[581] Nëse subjekti i të dhënave kërkon informacion për marrësit, kontrolluesi duhet t'ia japë këtë informacion.[582]

6.1.5. E drejta për transferueshmërinë e të dhënave

Sipas GDPR-së, subjektet e të dhënave gëzojnë të drejtën e transferueshmërisë së të dhënave, në situatat kur të dhënat personale që ata i kanë dhënë një kontrolluesi, janë përpunuar me anë të mjeteve të automatizuara mbi bazën e pëlqimit, ose kur përpunimi i të dhënave është i nevojshëm për përmbushjen e një kontrate dhe kryhet me mjete të automatizuara. Kjo nënkupton se e drejta për transferueshmërinë e të dhënave nuk zbatohet në situatat kur përpunimi i të dhënave personale mbështetet tek një bazë ligjore e ndryshme nga pëlqimi ose kontrata.[583]

Nëse e drejta e transferueshmërisë gjen zbatim, subjektet e të dhënave kanë të drejtën që të dhënat e tyre personale të transmotohen drejtpërdrejtë nga njëri kontrollues tek tjetri, nëse diçka e tillë është e mundur teknikisht.[584] Për ta lehtësuar këtë, kontrolluesi duhet të krijojë formate ndërvepruese, që mundësojnë transferueshëmrinë e të dhënave për subjektet e të dhënave.[585] GDPR-ja përcakton se këto formate duhet të jenë të strukturuara, të përdorura gjerësisht dhe të lexueshme automatikisht, në mënyrë që të lehtësojë ndërveprueshmërinë.[586] Ndërveprueshmëria mund të përkufizohet në një kuptim të gjerë si mundësia që kanë sistemet e informacionit për të shkëmbyer të dhëna dhe për të ndarë informacione.[587] Ndërsa qëllimi i përdorimit të këtyre formateve është që të mundësojnë ndërveprueshmërinë, GDPR-ja nuk jep rekomandime të veçanta për formatet specifike që duhen përdorur: formatet ndryshojnë nga sektori në sektor.[588]

Sipas udhëzuesit të Grupit të Punës së Nenit 29, e drejta e transferueshmërisë së të dhënave "mbështet zgjedhjet e përdoruesit, kontrollin nga ana e tij dhe e fuqizon atë", duke synuar t'i japë subjektit të të dhënave kontroll mbi të dhënat e veta personale.[589] Udhëzuesi qartëson elementet kryesore të trasferueshmërisë së të dhënave, ku përfshihen:

- E drejta e subjektit të të dhënave për të marrë të dhënat e veta personale të përpunuara nga kontrolluesi në një format të strukturuar, të përdorur gjerësisht, të lexueshëm automatikisht dhe të ndërveprueshëm;
- E drejta për të transmetuar të dhëna personale nga një kontrollues të dhënash tek një tjetër, pa asnjë pengesë nga i pari, nëse diçka e tillë është teknikisht e mundur;

[579] *Ibid*., paragrafi 67 i Preambulës.
[580] *Ibid*., neni 18, pika 3.
[581] *Ibid.*, neni 19.
[582] *Ibid.*.
[583] *Ibid*., paragrafi 68 i Preambulës dhe neni 20, pika 1.
[584] *Ibid*., neni 20, pika 2.
[585] *Ibid*., paragrafi 68 i Preambulës dhe neni 20, pika 1.
[586] *Ibid*., paragrafi 68 i Preambulës.
[587] Komisioni Evropian, Communication on stronger and smarter information systems for borders and security, COM(2016) 205 final, 2 prill 2016.
[588] Grupi i Punës së Nenit 29 (2016), *Guidelines on the right to data portability*, WP 242, 13 dhjetor 2016 dhe ndryshuar më 5 prill 2017, fq. 13.
[589] *Ibid.*

- Regjimi i kontrollit të të dhënave – kur një kontrollues i përgjigjet një kërkese për transferueshmëri të dhënash, ai vepron sipas udhëzimeve të subjektit të të dhënave, që do të thotë se ai nuk është përgjegjës për përputhshmërinë e marrësit me legjislacionin e mbrojtjes së të dhënave, pasi është subjekti i të dhënave që vendos se tek kush do të transferohen të dhënat;
- Ushtrimi i të drejtës së transferueshmërisë së të dhënave nuk duhet të cënojë asnjë të dhënë tjetër, sikurse asnjë të drejtë të përcaktuar në GDPR.

6.1.6. E drejta për të kundërshtuar

Subjektet e të dhënave mund të përdorin të drejtën e kundërshtimit të përpunimit të të dhënave, për shkaqe që kanë të bëjnë me situatën e tyre të veçantë dhe me përpunimin e të dhënave për qëllime marketingu të drejtpërdrejtë. E drejta për të kundërshtuar mund të ushtrohet me anë të mjeteve të automatizuara.

E drejta për të kundërshtuar për shkaqe që kanë të bëjnë me situatën e veçantë të subjekteve të të dhënave

Subjektet e të dhënave nuk kanë një të drejtë të përgjithshme për të kundërshtuar përpunimin e të dhënave të tyre.[590] Neni 21, pika 1 e GDPR-së u jep subjekteve të të dhënave të drejtën të ngrenë kundërshtime për shkaqe që lidhen me situatën e tyre të veçantë, në masën që baza ligjore për përpunimin është përmbushja nga ana e kontrolluesit të një detyre që kryhet në interes publik, ose kur përpunimi bazohet mbi interesat legjitime të kontrolluesit.[591] E drejta për të kundërshtuar gjen zbatim për aktivitetet e profilizimit. Një e drejtë e ngjashme njihet edhe nga Konventa 108 e Modernizuar.[592]

E drejta për të kundërshtuar për shkaqe që lidhen me situatën e veçantë të subjektit të të dhënave synon të ekuilibrojë në mënyrën e duhur të drejtat e subjektit të të dhënave për mbrojtjen e të dhënave, me të drejtat legjitime të të tjerëve për të përpunuar ato të dhëna. Megjithatë GJDBE-ja ka qartësuar se të drejtat e e subjektit prevalojnë 'si rregull i përgjithshëm' mbi interesat ekonomike të kontrolluesit të të dhënave, në varësi të "natyrës së informacionit të përfshirë dhe sensitivitetit të tij për jetën private të subjektit të të dhënave dhe interesit të publikut për ta marrë atë informacion".[593] Sipas GDPR-së, barra e provës u takon kontrolluesve, të cilët duhet të demonstrojnë shkaqe të forta për të vijuar përpunimin.[594] Në mënyrë të ngjashme, Raporti Shpjegues i Konventës 108 të Modenrizuar qartëson se ekzistenca e shkaqeve legjitime për përpunimin e të dhënave (të cilat mund të prevalojnë mbi të drejtën e subjekteve të të dhënave për të kundërshtuar) duhet demonstruar rast pas rasti.[595]

[BOX TYPE 1]

[590] Shih gjithashtu GJEDNJ, *M.S. k. Suedisë*, nr. 20837/92, 27 gusht 1997 (ku të dhënat mjekësore ishin komunikuar pa pëlqim, apo mundësi për të kundërshtuar); GJEDNJ, *Leander k. Suedisë*, nr. 9248/81, 26 mars 1987; GJEDNJ, *Mosley k. Mbretërisë së Bashkuar*, nr. 48009/08, 10 maj 2011.
[591] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 69 i Preambulës; neni 6, pika 1, gërmat (e) dhe (f).
[592] Konventa 108 e Modernizuar, neni 9, pika 1, gërma (d); Rekomandimi mbi Profilizimin, neni 5, pika 3.
[593] GJDBE, C-131/12, *Google Spain SL, Google Inc. k. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [ÇB] , 13 maj 2014 parag. 81.
[594] Shih gjithashtu Konventën 108 të Modernizuar, nenin 98, pika 1, gërma (d) që përcakton se subjekti it ë dhënave mund të kundërshtojë përpunimin e të dhënave të tij apo të saj "përveçse kur kontrolluesi demonstron shkaqe legjitime për përpunimin, të cilat prevalojnë mbi interesat, apo të drejtat dhe liritë themelore të tij ose të saj."
[595] Raporti Shpjegues i Konventës 108 të Modernizuar, parag. 78.

Shembull: tek çështja *Manni*,[596] GJDBE-ja u shpreh se për shkak të qëllimit legjitim të përhapjes së të dhënave personale në regjistrin e shoqërive tregtare, sidomos nevojës për të mbrojtur interest e palëve të treta dhe për të garantuar siguri juridike, në parim, z. Manni nuk kishte të drejtë të kërkonte fshirjen e të dhënave personale të tij nga regjistri i shoqërive tregtare. Sidoqoftë, ajo pranoi ekzistencën e së drejtës për të kundërshtuar përpunimit, duke u shprehur se "nuk përjashtohet se […] mund të ketë situata të caktuara, në të cilat shkaqet mbizotëruese dhe legjitime që lidhen me rastin konkret të një personi, justifikojnë në mënyrë përjashtimore që aksesi në të dhënat personale të një regjistri, të kufizohet pasi të ketë kaluar një periudhë mjaftueshmërisht e gjatë […] për palët e treta që mund të demonstrojnë interes specifik për t'i parë ato të dhëna.".

GJDBE-ja vlerësoi se ishte përgjegjësi e gjykatave kombëtare të vlerësonin secilin rast, duke marrë parasysh të gjitha rrethanat përkatëse të personit dhe nëse ekzistojnë shkaqe legjitime dhe mbikzotëruese që mund të justifikojnë në mënyrë përjashtimore kufizimin e aksesit të palëve të treta tek të dhënat personale të një regjistri shoqërish tregtare. Megjithatë, ajo qartësoi se në rastin e z. Manni, vetëm fakti se përhapja e të dhënave personale të tij në një regjistër mund të kishte pasoja për klientelën e tij, nuk mund të konsiderohej se përbënte shkak të tillë legjitim dhe mbizotërues. Ishte në interesin legjitim të klientëve të mundshëm të z. Manni për të pasur akses në informacionin në lidhje me falimentimin e shoqërisë së tij të mëparshme.

Një kundërshtim i suksesshëm sjell si pasojë që kontrolluesi nuk mund të përpunojë më të dhënat e përfshira. Aktivitetet e përpunimit që janë kryer tek të dhënat e subjektit përpara se të kundërshtoheshin, mbeten gjithësesi legjitime.

E drejta për të kundërshtuar përpunimin e të dhënave për qëllime marketingu të drejtpërdrejtë

Neni 21, pika 2 e GDPR-së parashikon një të drejtë specifike për të kundërshtuar përdorimin e të dhënave personale për qëllime marketingu të drejtpërdrejtë, duke qartësuar më tej nenin 13 të Direktivës së e-Privatësisë. Kjo e drejtë përcaktohet gjithashtu edhe në Konventën 108 të Modernizuar, si dhe në Rekomandimin e KiE-së në lidhje me Marketingun e Drejtpërdrejtë.[597] Raporti Shpjegues i Konventës 108 të Modernizuar qartëson se kundërshtimet ndaj përpunimit të të dhënave për qëllime marketingu të drejtpërdrejtë duhet të sjellin si pasojë fshirjen ose heqjen e pakushtëzuar të të dhënave personale të përfshira.[598]

Subjekti i të dhënave ka të drejtën të kundërshtojë përdorimin e të dhënave personale të tij apo të saj, për qëllime marketingu të drejtpërdrejtë, në çdo moment dhe pa pagesë. Subjektet e të dhënave duhen informuar në lidhje me këtë të drejtë, në mënyrë të qartë dhe veçmas nga çdo informacion tjetër.

E drejta për të kundërshtuar me anë të mjeteve të automatizuara

Kur informacioni personal përdoret apo përpunohet për shërbimet e shoqërisë së informacionit, subjekti i të dhënave mund të ushtrojë të drejtën e tij apo të saj për të kundërshtuar përpunimin e të dhënave personale që i përkasin me anë të mjeteve të automatizuara.

[596] GJDBE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce k. Salvatore Manni*, 9 mars 2017, parag. 47 dhe 60.
[597] Këshilli i Evropës, Komiteti i Ministrave (1985), Recommendation Rec(85)20 to member states on the protection of personal data used for the purposes of direct marketing, 25 tetor 1985, neni 4, pika 1.
[598] Raporti Shpjegues i Konventës 108 të Modernizuar, parag. 79.

Shërbimet e shoqërisë së informacionit përkufizohen si çdo lloj shërbimi i zakonshëm që bëhet kundrejt pagesës, në distancë, me anë të mjeteve elektronike dhe me kërkesën individuale të një marrësi të shërbimit.[599]

Kontrolluesit e të dhënave që ofrojnë shërbime të shoqërisë së informacionit duhet të marrin masat e duhura teknike dhe procedurale, në mënyrë që të garantojnë që e drejta për të kundërshtuar me anë të mjeteve të automatizuara, të mund të ushtrohet në mënyrë të efektshme.[600] Për shembull, mund të përfshihet këtu bllokimi i identifikuesve (cookies) në faqet e internetit, ose ndalja e gjurmimit të lundrimit në internet.

E drejta për të kundërshtuar për qëllime të kërkimit shkencor, ose historik, apo për qëllime statistikore

Sipas së drejtës së BE-së, kërkimi shkencor duhet interpretuar në mënyrë të zgjeruar, ku përfshihet, për shembull, zhvillimi dhe demonstrimi i teknologjive, kërkimi themelor, kërkimi i aplikuar dhe kërkimi i financuar nga sektori privat.[601] Kërkimi historik përfshin gjithashtu kërkimin për qëllime gjenealogjike, duke pasur parasysh faktin se rregullorja nuk do të zbatohet për personat e vdekur.[602] Qëllimet statistikore nënkuptojnë çdo aktivitet mbledhjeje dhe përpunimi të dhënash personale, të nevojshme për pyetësorë statistikorë, ose për prodhimin e rezultateve statistikore.[603] Edhe në këtë rast, situate e veçantë e një subjekti të dhënash, përbën bazën ligjore të së drejtës për të kundërshtuar përpunimin e të dhënave personale për qëllime kërkimore.[604] Përjashtim bëhet vetëm për domosdoshmërinë e përpunimit për përmbushjen e një detyre që kryhet për qëllime në interesin publik. Megjithatë, e drejta për fshirje nuk do të gjejë zbatim kur përpunimi është i nevojshëm (për arsye të interesit publik ose jo) për qëllime të kërkimit shkencor, ose historik, apo për qëllime statistikore.[605]

GDPR-ja vendos ekuilibrin ndërmjet nevojave për kërkim shkencor, statistikor, ose historik dhe të drejtave të subjekteve të të dhënave, duke parashikuar garanci dhe përjashtime specifike në nenin 89. Kështu, e drejta e Bashkimit, ose e Shteteve Anëtare, mund të përcaktojë përjashtime nga e drejta për të kundërshtuar, për aq kohë sa kjo e drejtë ka gjasa ta pamundësojë, ose dëmtojë rëndë përmbushjen e qëllimeve kërkimore dhe që këto përjashtime janë të nevojshme për arritjen e këtyre qëllimeve.

Në të **drejtën e KiE-së**, neni 9, pika 2 e Konventës 108 të Modernizuar përcakton se kufizimet e të drejtave të subjekteve të të dhënave, përfshirë edhe të së drejtës për të kundërshtuar, mund të parashikohen me ligj, në lidhje me përpunimin e të dhënave për qëllime arkivore në interesin publik, për qëllime të kërkimit shkencor ose historik, apo për qëllime statistikore, në masën që nuk identifikohet asnjë risk për shkeljen e të drejtave dhe lirive themelore të subjekteve të të dhënave.

Megjithatë, Raporti Shpjegues (paragrafi 41) parashikon gjithashtu se subjekteve të të dhënave duhet t'u jepet mundësia për të dhënë pëlqimin e tyre vetëm për disa fusha të caktuara të kërkimit, ose në pjesë të caktuara të projekteve kërkimore, në masën që qëllimi i parashikuar ta lejojë diçka të tillë dhe

[599] Direktiva 98/34/EC ndryshuar me Direktivën 98/48/EC që përcakton procedurën për informimin në fushën e normave dhe rregullimeve teknike, neni 1, pika 2.
[600] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 21, pika 5.
[601] *Ibid*., paragrafi 159 i Preambulës.
[602] *Ibid*., paragrafi 160 i Preambulës.
[603] *Ibid.,* paragrafi 162 i Preambulës.
[604] *Ibid.,* neni 21, pika 6.
[605] *Ibid*., neni 17, pika 3, gërma (d).

të kundërshtojnë nëse gjykojnë që përpunimi cënon në mënyrë të tepruar të drejtat dhe liritë pa një bazë legjitime.

Me fjalë të tjera, një përpunim i tillë rrjedhimisht do të konsiderohej *a priori* si i përshtatshëm, me kusht që të ekzistojnë garanci dhe që parimisht aktivitetet të mos përfshijnë asnjë përdorim informacioni të përftuar për vendimmarrje, apo për masa në lidhje me një person të caktuar.

6.1.7. Vendimmarrja individuale e automatizuar, përfshirë profilizimin

Me vendime të automatizuara kuptohet përdorimi i të dhënave përsonale që përpunohen vetëm me anë të mjeteve të automatizuara, pa asnjë ndërhyrje njerëzore. **Sipas së drejtës së BE-së**, subjektet e të dhënave nuk duhet t'i nënshtrohen vendimeve të automatizuara, të cilat krijojnë pasoja ligjore, ose pasoja që i cënojnë njësoj në mënyrë të konsiderueshme. Nëse këto vendime kanë të ngjarë të kenë ndikim të rëndësishëm në jetët e personave, pasi ato kanë të bëjnë, për shembull, me përshtatshmërinë e tyre për të marrë kredi, e-punësimin, vlerësimin e punës, ose analizën e sjelljes apo besueshmërisë, atëherë nevojitet mbrojtje e veçantë për të shmangur pasojat negative. Vendimmarrjet e automatizuara, përfshirë profilizimin, konsistojnë në çdo formë vlerësimi të automatizuar të "aspekteve personale që lidhen me një person fizik, veçanërisht për të analizuar, ose parashikuar aspekte që kanë të bëjnë me vlerësimin e punës së subjektit të të dhënave, gjendjen ekonomike, shëndetësore, preferencat apo interesat personale, besueshmërinë ose sjelljen, vendnndodhjen ose zhvendosjet".[606]

[BOX TYPE 2]

Shembull: për të vlerësuar me shpejtësi përshtatshmërinë e një klienti të ardhshëm për të marrë kredi, agjencitë e vlerësimit të kredive (AVK-të) mbledhin disa të dhëna të caktuara, sikurse në lidhje me mënyrën se si klienti ka shlyer kreditë dhe si ka menaxhuar pagesat e shërbimeve/faturave, adresat e mëparshme të klientit, ashtu si dhe informacion nga burime publike, sikurse nga lista e zgjedhësve, regjistrat publikë (përfshirë vendimet gjyqësore), apo të dhëna për falimentin dhe likudimin. Më pas, këto të dhëna regjistrohen në një algoritëm pikëzimi, i cili përllogarit vlerën e përgjithshme që përfaqëson përshtatshmërinë e kreditimit të klientit të mundshëm.

Sipas Grupit të Punës së Nenit 29, e drejta për të mos iu nënshtruar vendimeve të bazuara krejtësisht në përpunimin e automatizuar, i cili mund të sjellë pasoja ligjore për subjektin e të dhënave, apo ta cënojë atë në mënyrë të konsiderueshme, përbën ndalim të përgjithshëm dhe nuk kërkon që subjekti i të dhënave të kundërshtojë në mënyrë aktive një vendim të tillë.[607]

Megjithatë, sipas GDPR-së, vendimmarrja e automatizuar me pasoja ligjore, apo që cënon personat në mënyrë të konsiderueshme, mund të jetë e pranueshme nëse është e nevojshme për të lidhur një kontratë, apo për përmbushjen e një kontrate midis kontrolluesit të të dhënave dhe subjektit të të dhënave, ose nëse subjekti i të dhënave ka dhënë pëlqimin e tij të qartë. Gjithashtu, vendimmarrja e automatizuar është e pranueshme nëse është e parashikuar me ligj dhe nëse të drejtat, liritë dhe interesat legjitime të subjektit të të dhënave garantohen në mënyrën e duhur.[608]

GDPR-ja përcakton gjithashtu se ndër detyrimet që ka kontrolluesi për të informuar subjektet e të dhënave kur mblidhen të dhënat personale, ai duhet gjithashtu t'u bëjë me dije ekzistencën e vendimmarrjes së automatizuar, përfshirë profilizimin.[609] E drejta e aksesit tek të dhënat personale që

[606] *Ibid*., paragrafi 71 i Preambulës, neni 4, pika 4 dhe neni 22.
[607] Grupi i Punës së Nenit 29, *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 3 tetor 2017, fq. 15.
[608] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 22, pika 2.
[609] *Ibid*., neni 12.

përpunohen nga kontrolluesi mbetet e pacënuar.[610] Informacioni nuk duhet thjesht të përmendë faktin se do të kryhet profilizimi, por duhet të japë informacion të plotë në lidhje me logjikën e përdorur për profilizimin dhe pasojat e parashikuara të përpunimit për personat.[611] Për shembull, një shoqëri sigurimi shëndetësore që përdor vendimmarrjen e automatizuar në lidhje me kërkesat, duhet t'u japë subjekteve të të dhënave informacion të përgjithshëm mbi mënyrës si punon algoritmi dhe cilët faktorë përdor ai për të përllogaritur policën siguruese. Në të njëjtën mënyrë, kur ushtrojnë 'të drejtën e tyre të aksesit', subjektet e të dhënave mund të kërkojnë informacion nga kontrolluesi për ekzistencën e vendimmarrjes së automatizuar, si dhe informacion të nevojshëm për logjikën e përdorur.[612]

Informacioni që u jepet subjekteve të të dhënave ka për qëllim të rrisë transparencën dhe t'u mundësojë subjekteve të të dhënave që, nëse është rasti, të japin pëlqimin në mënyrë të informuar, apo të kërkojnë ndërhyrje njerëzore. Kontrolluesi i të dhënave është i detyruar të marrë masat e duhura për mbrojtjen e të drejtave, lirive dhe interesave legjitime të subjektit të të dhënave. Në to përfshihet së paku e drejta për të kërkuar ndërhyrje njerëzore nga ana e kontrolluesit dhe mundësinë që subjekti i të dhënave të shprehë pikëpamjen e tij dhe të kundërshtojë një vendim të bazuar në përpunimin e automatizuar të të dhënave personale të tij apo të saj.[613]

Grupi i Punës së Nenit 29 ka dhënë orientime të tjera në lidhje me përdorimin e vendimmarrjes së automatizuar në kuadër të GDPR-së.[614]

Në të drejtën e KiE-së, personat kanë të drejtën të mos i nënshtrohen një vendimi që mund t'i cënojë ata në mënyrë të konsiderueshme dhe që mund të jetë tërësisht i bazuar në përpunimin e automatizuar pa marrë parasysh mendimin e tyre.[615] Kriteri që mendimi i subjektit të të dhënave duhet marrë parasysh kur vendimet bazohen tërësisht në përpunimin e automatizuar, nënkupton se ai apo ajo ka të drejtën ta kundërshtojë atë vendim, të ketë mundësi të kundërshtojë çdo pasaktësi të të dhënave personale që përdor kontrolluesi, si dhe rë kundërshtojë çdo profil që i atribuohet atij apo asaj.[616] Megjithatë, subjekti i të dhënave nuk mund ta ushtrojë këtë të drejtë nëse vendimi i automatizuar është i parashikuar në ligjin të cilit i nënshtrohet kontrolluesi dhe i cili përcakton gjithashtu masat e duhura për mbrojtjen e të drejtave, lirive dhe interesave legjitime të subjektit të të dhënave. Gjithashtu, subjektet e të dhënave kanë të drejtën të kërkojnë dhe t'u bëhet i ditur arsyetimi për përpunimin e të dhënave të kryer.[617] Raporti Shpjegues i Konventës 108 të Modernizuar jep shembullin e pikëzimit për vlerësimin e kredimarrësit. Personat nuk duhet të kenë të drejtën të njihen thjesht me vendimin pozitiv, apo negativ të vlerësimit të kredimarrësit, por edhe me *logjikën* që qëndron në themel të përpunimit të të dhënave të tyre personale, si rezultat i së cilës u mor një vendim i tillë. "Të kuptuarit e këtyre elementeve ndihmon në ushtrimin efikas të garancive të tjera thelbësore, sikurse të drejtës për të kundërshtuar dhe të drejtës për t'u ankuar pranë një autoriteti kompetent".[618]

Rekomandimi i profilizimit, paçka se nuk është ligjërisht i detyrueshëm, specifikon kushtet për mbledhjen dhe përpunimin e të dhënave personale në kuadër të profilizimit.[619] Ai përmban dispozita në lidhje me nevojën për të garantuar që përpunimi në kuadër të profilizimit të jetë i drejtë, i ligjshëm, proporcional dhe për qëllime legjitime e të përcaktuara. Ai përfshin gjithashtu dispozita mbi informacionin që kontrolluesit duhet t'u japin subjekteve të të dhënave. Parimi i cilësisë së të dhënave, i cili kërkon që kontrolluesit të marrin masa për të korrigjuar faktorët e pasaktësisë së të dhënave, të kufizojnë rreziqet ose gabimet që mund të gjenerojë profilizimi dhe të analizojnë në mënyrë periodike cilësinë e të të dhënave dhe algoritmeve të përdorura, parashikohet gjithashtu në këtë rekomandim.

---

[610] *Ibid*., neni 15.
[611] *Ibid*., neni 13, pika 2, gërma (f).
[612] *Ibid*., neni 15, pika 1, gërma (h).
[613] *Ibid*., neni 22, pika 3.
[614] Grupi i Punës së Nenit 29 (2017), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP 251, 3 tetor 2017.
[615] Konventa 108 e Modernizuar, neni 9, pika 1, gërma (a).
[616] Raporti Shpjegues i Konventës 108 të Modernizuar, parag. 75.
[617] Konventa 108 e Modernizuar, neni 9, pika 1, gërma (c).
[618] Raporti Shpjegues i Konventës 108 të Modernizuar, parag. 77.
[619] Këshilli i Evropës, Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, neni 5, pika 5.

6.2. Mjetet juridike, përgjegjësia, penalitetet dhe kompensimi

Pikat kryesore

- Sipas Konventës 108 të Modernizuar, e drejta kombëtare e Palëve Kontraktuese duhet të përcaktojë mjetet e ankimit dhe sanksionet e përshtatshme ndaj shkeljeve të së drejtës për mbrojtje të të dhënave.
- Në BE, GDPR-ja parashikon mjetet juridike për subjektet e të dhënave në raste shkeljesh të të drejtave të tyre, si dhe sanksionet ndaj kontrolluesve dhe përpunuesve që nuk respektojnë dispozitat e rregullores. Ajo parashikon gjithashtu të drejtën e kompensimit dhe përgjegjësinë.
    - Subjektet e të dhënave kanë të drejtën të ankohen tek autoriteti mbikëqyrës për shkeljet e pretenduara të rregullores, si dhe të drejtën për mjet gjyqësor dhe për të marrë kompensim.
    - Për ushtrimin e së drejtës për mbrojtje të efektshme, personat mund të përfaqësohen nga organizata jo-fitimprurëse që veprojnë në fushën e mbrojtjes së të dhënave.
    - Kontrolluesi ose përpunuesi është përgjegjës për çdo dëm material ose jo, të ardhur si rezultat i shkeljes.
    - Autoritetet mbikëqyrëse kanë kompetencën të vendosin masa administrative gjobe për shkeljen e rregullorës deri në 20,000,000 euro, ose në rastin e një ndërmarrjeje, 4 % të xhiros së përgjithshme vjetore botërore – cilado është më e lartë.
- Si mjet i fundit dhe me disa kushte të caktuara, subjektet e të dhënave mund t'i drejtohen GJEDNJ-së për shkelje të legjislacionin të mbrojtjes së të dhënave.
- Çdo person fizik ose juridik ka të drejtën të paraqesë ankesë pranë GJDBE-së kundër çdo vendimi të Bordit Evropian të Mbrojtjes së të Dhënave sipas disa kushteve të përcaktuara në Traktate.

Miratimi i instrumenteve ligjore nuk është i mjaftueshëm për të garantuar mbrojtje të të dhënave personale në Evropë. Për t'u dhënë efektshmëri rregullave evropiane të mbrojtjes së të dhënave, është e nevojshme të përcaktohen mekanizma që u mundësojnë personave të kundërshtojnë shkeljet e të drejtave të tyre dhe të kërkojnë kompensim për çdo dëm të pësuar. Është po aq e rëndësishme që autoritetet mbikëqyrëse të kenë kompetencën për të vendosur sanksione të efektshme, shtrënguese dhe proporcionale në raport me shkeljen.

Të drejtat që përcakton legjislacioni i mbrojtjes së të dhënave mund të ushtrohen nga personi të drejtat e të cilit janë kërcënuar; bëhet fjalë për subjektin e të dhënave. Megjithatë, edhe persona të tjerë, të cilët plotësojnë kushtet e nevojshme sipas së drejtës kombëtare, mund të përfaqësojnë subjektet e të dhënave në ushtrimin e të drejtave të tyre. Në një sërë legjislacionesh kombëtare, fëmijët dhe personat me paaftësi mendore, mund të përfaqësohen nga kujdestari.[620] Sipas legjislacionit të mbrojtjes së të dhënave të BE-së, shoqatat që kanë si objekt promovimin e të drejtave të mbrojtjes së të dhënave, mund të përfaqësojnë subjektet e të dhënave pranë një autoriteti mbikëqyrës ose në gjykatë.[621]

6.2.1. E drejta për të paraqitur ankesë tek autoriteti mbikëqyrës

Si në të drejtën e **KiE-së**, ashtu edhe në të të **BE-së**, personat kanë të drejtën të paraqesin kërkesa dhe ankesa pranë autoritetit mbikëqyrës kompetent, në rast se vlerësojnë se përpunimi i të dhënave personale të tyre nuk është duke u kryer në përputhje me ligjin.

Konventa 108 e Modernizuar njeh të drejtën e subjekteve të të dhënave për të kërkuar ndihmë nga autoriteti mbikëqyrës për të ushtruar të drejtat që u jep konventa, pavarësisht shtetësisë apo vendbanimit

[620] FRA (2015), Manual i së drejtës evropiane në lidhje me të drejtat e fëmijëve, Luksemburg, Zyra e Publikimeve; FRA (2013), Zotësia ligjore e personave me paaftësi mendore dhe personave me probleme të shëndetit mendor, Luksemburg, Zyra e Publikimeve.
[621] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 80.

të tyre.[622] Kërkesa për ndihmë mund të refuzohet vetëm në rrethana të jashtëzakonshme dhe subjektet e të dhënave nuk duhet të paguajnë shpenzime dhe tarifa në lidhje me ndihmën.[623]

Dispozita të ngjashme gjenden edhe në sistemin juridik të BE-së. GDPR-ja detyron autoritetet mbikëqyrëse të zbatojnë masa për të lehtësuar paraqitjen e ankesave, si për shembull krijimin e një formulari elektronik të depozitimit të ankesës.[624] Subjekti i të dhënave mund të depozitojë ankesë pranë autoritetit mbikëqyës në Shtetin Anëtar të vendbanimit e zakonshëm të tij apo të saj, vendit ku punon apo vendit ku ka ndodhur shkelja e pretenduar.[625] Ankesat duhen hetuar dhe autoriteti mbikëqyrës duhet të informojë subjektin për rezultatin e hetimit.[626]

Shkeljet e mundshme nga ana e institucioneve ose organeve të BE-së mund t'i bëhen me dije Mbikëqyrësit Evropian të Mbrojtjes së të Dhënave.[627] Në rast mungese përgjigjeje nga ana e EDPS-së Brenda gjashtë muajve, ankesa duhet konsideruar si e refuzuar. Ankimi ndaj vendimeve të EDPS-së mund të bëhet pranë GJDBE-së brenda kuadrit të Rregullores (EC) nr. 45/2001, e cila detyron institucionet dhe organet e BE-së të zbatojnë rregullat e mbrojtjes së të dhënave.

Vendimet e autoritetit mbikëqyrës kombëtar duhet të jetë e mundur të kundërshtohen në gjykatë. Kjo vlen si për subjektin e të dhënave, ashtu edhe për kontrolluesit e përpunuesit të cilët kanë qenë palë në hetimin e autoritetit mbikëqyrës.

[BOX TYPE 3]

Shembull: në shtator 2017, Autoriteti Spanjoll i Mbrojtjes së të Dhënave gjobit Facebook-un për disa shkelje të rregullave të mbrojtjes së të dhënave. Autoriteti mbikëqyrës ndëshkoi rrjetin social për mbledhjen, mbajtjen dhe përpunimin e të dhënave personale, përfshirë edhe të kategorive të veçanta të të dhënave personale, për qëllime publicitare dhe pa pëlqimin e subjekteve të të dhënave. Vendimi u mbështet në një hetim të zhvilluar kryesisht nga autoriteti mbikëqyrës.

6.2.2. E drejta për një mjet mbrojtës gjyqësor efikas

Përveç të drejtës për t'u ankuar tek autoriteti mbikëqyrës, personat duhet të kenë të drejtën e një mjeti mbrojtës gjyqësor efikas dhe për të paraqitur ankesë në gjykatë. E drejta për mjetin juridik të zgjidhjes është e rrënjosur më së miri në traditën juridike evropiane dhe njihet si e drejtë themelore si nga neni 47 i Kartës së të Drejtave Themelore të BE-së, ashtu edhe nga neni 13 i KEDNJ-së.[628]

Në të drejtën e BE-së, shfaqet qartë rëndësia që kanë mjetet juridike për subjektet e të dhënave në rasye shkeljes së të drejtave të tyre, si në GDPR – e cila përcakton të drejtën për një mjet mbrojtës gjyqësor efikas ndaj autoriteteve mbikëqyrëse, kontrolluesve dhe përpunuesve – ashtu edhe në jurisprudencën e GJDBE-së.

[BOX TYPE 1]

Shembull: tek çështja *Schrems*,[629] GJDBE-ja e shpalli të pavlefshëm Vendimin e Përshtatshmërisë së Portit të Sigurt. Ky vendim kishte mundësuar transferimet ndërkombëtare të të dhënave nga BE-ja drejt organizatave të vendosura në SHBA dhe të cilat ishin vetë-certifikuar me anë të skemës së Portit të

[622] Modernised Convention 108, Art. 18.
[623] *Ibid*., Art. 16–17.
[624] General Data Protection Regulation, Art. 57 (2).
[625] *Ibid*., Art. 77 (1).
[626] *Ibid*., Art. 77 (2).
[627] Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, OJ 2001 L 8.
[628] See for example ECtHR, *Karabeyoğlu v. Turkey*, No. 30083/10, 7 June 2016; ECtHR, *Mustafa Sezgin Tanrıkulu v. Turkey*, No. 27473/06, 18 July 2017.
[629] CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [ÇB] , 6 October 2015.

Sigurt. GJDBE-ja vlerësoi se skema e Portit të Sigurt kishte disa mangësi, të cilat kompromentonin të drejtat themelore të shtetasve të BE-së për mbrojtje të privatësisë, mbrojtjes së të dhënave personale dhe të drejtës për mjet mbrojtës gjyqësor efikas.

Për sa i takon shkeljes së të drejtave për privatësi dhe mbrojtje të të dhënave, GJDBE-ja theksoi se legjislacioni i SHBA-ve u lejonte disa autoriteteve publike të kishin akses tek të dhënave personale të transferuara nga Shtetet Anëtare drejt SHBA-ve dhe t'i përpunonin ato jo në përputhje me qëllimet fillestare të transferimit të tyre dhe përtej asaj çka ishte e domosdoshme dhe proporcionale për mbrojtjen e sigurisë kombëtare. Në lidhje me të drejtën për mjet juridik efikashëm, ajo vërejti se subjektet e të dhënave nuk dispononin mjete zgjidhjeje administrative apo gjyqësore, të cilat të bënin të mundur që, sipas rastit, të aksesonin, korrigjonin apo fshinin të dhënat e tyre. GJDBE-ja doli në përfundimin se një legjislacion, i cili nuk parashikon asnjë mundësi për akses, korrigjim, ose fshirje të të dhënave personale, "nuk respekton thelbin e së drejtës themelore për mbrojtje të efektshme gjyqësore, sikurse sanksionohet në nenin 47 të Kartës". Ajo theksoi se ekzistenca e mjetit gjyqësor mbrojtës, i cili garanton respektimin e normave ligjore, është pjesë e pandashme e shtetit të së drejtës.

Personat, kontrolluesit, ose përpunuesit, të cilët kundërshtojnë një vendim detyrues të një autoriteti mbikëqyrës, nëpërmjet ankimit në gjykatë.[630] Nocioni 'vendim' duhet interpretuar në mënyrë të zgjeruar, ku të përfshihet ushtrimi nga ana e autoriteteve mbikëqyrëse i kompetencave hetimore, sanksionuese dhe autorizuese, sikurse edhe vendimet për të mospranuar apo refuzuar një ankesë. Megjithatë, masat me forcë juridike jo detyruese që jepen nga një autoritet mbikëqyrës, sikurse opinionet apo këshillimet, nuk mund të jenë objekt ankimi gjyqësor.[631] Ankimi duhet bërë pranë gjykatave të Shtetit Anëtar në të cilin është i vendosur autoriteti mbikëqyrës përkatës.[632]

Në rastet kur një kontrollues apo përpunues shkel të drejtat e subjektit të të dhënave, ky i fundit ka të drejtën të ankohet në gjykatë.[633] Në rastet e ankimit kundër kontrolluesit apo përpunuesit, është veçanërisht e rëndësishme që personat të kenë mundësi të përzgjedhin se ku do të paraqesin padinë. Ata mund të zgjedhin ta bëjnë këto qoftë në Shtetin Anëtar në të cilin ka strukturën kontrolluesi ose përpunuesi, apo në Shtetin Anëtar në të cilin subjektet e të dhënave të përfshirë kanë vendbanimin e tyre të zakonshëm.[634] Mundësia e dytë lehtëson së tepërmi personat gjatë ushtrimit të të drejtave të tyre, pasi u mundëson të ankohen brenda shtetit në të cilin banojnë dhe pranë një juridiksioni të cilin e njohin. Nëse u kufizohet vendi në të cilin mund të bëhet ankimi kundër kontrolluesve dhe përpunuesve në Shtetin Anëtar në të cilin këta të fundit kanë një strukturë, mund t'i pengojë subjektet e të dhënave që banojnë në Shtete Anëtare të tjera që të paraqesin padinë, pasi diçka e tillë do të lypte udhëtime dhe kosto shtesë dhe procedura do të zhvillohej në gjuhë e juridiksion të huaj. I vetmi përjashtim ka të bëjë me rastet kur kontrolluesi, apo përpunuesi, janë autoritete publike dhe përpunimi kryhet në kuadër të ushtrimit të kompetencave të tyre publike. Në një rast të tillë, vetëm gjykatat e shtetit përkatës të autoritetit publik, kanë kompetencë për çështjen.[635]

Paçka se në shumicën e rasteve, çështjet që kanë të bëjnë me rregullat e mbrojtjes së të dhënave shqyrtohen nga gjykatat e Shteteve Anëtare, disa çështje mund të paraqiten drejtpërdrejtë në GJDBE. Mundësia e parë është kur subjekti i të dhënave, kontrolluesi, përpunuesi, apo autoriteti mbikëqyrës paraqesin ankesë për anulimin e një vendimi të EDPB-së. Ankesa gjithësesi i nënshtrohet kushteve të nenit 263 të TFBE-së, çka nënkupton se që të jetë e pranueshme, këta persona, apo njësi duhet të demonstrojnë që vendimi i Bordit i prek ata drejtpërdrejtë dhe individualisht.

Skenari i dytë lidhet me rastet kur institucionet apo organet e BE-së përpunojnë të dhëna personale në mënyrë të paligjshme. Në rastet kur institucionet e BE-së shkelin legjislacionin e mbrojtjes së të dhënave, subjektet e të dhënave mund të ankohen drejtpërdrejtë në Gjykatën e Përgjithshme të BE-së

[630] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 78.
[631] *Ibid*., paragrafi 143 i Preambulës.
[632] *Ibid*., neni 78, pika 3.
[633] *Ibid*., neni 79.
[634] *Ibid*., neni 79, pika 2.
[635] *Ibid*.

(Gjykata e Përgjithshme është pjesë e GJDBE-së). Gjykata e Përgjithshme, në shkallë të parë, është përgjegjëse për ankesat për shkelje të së drejtës së BE-së nga ana e institucioneve të BE-së. Kësisoj, ankesat ndaj EDPS-së, në cilësinë e institucionin të BE-së, mund të paraqiten gjithashtu pranë Gjykatës së Përgjithshme.[636]

[BOX TYPE 1]

Shembull: tek çështja *Bavarian Lager*,[637] shoqëria i kërkoi Komisionit Evropian t'i jepte akes tek process-verbali i plotë i mbledhjes së mbajtur nga Komisioni, e cila pretendohej se kishte pasur të bënte me çështje ligjore me rëndësi për shoqërinë. Komisioni e refuzoi kërkesën e shoqërisë për akses, mbi bazën e interesave prevaluese të mbrojtjes së të dhënave.[638] Bavarian Lager-i, mbështetur në nenin 32 të Rregullores së Mbrojtjes së të Dhënave të Institucioneve të BE-së, paraqiti ankesë pranë Gjykatës së Shkallës së Parë (pararendëses së Gjykatës së Përgjithshme) në lidhje me vendimin. Në vendimin e saj (çështja T-194/04, *The Bavarian Lager Co. Ltd k. Komisionit të Komuniteteve Evropiane*), Gjykata e Shkallës së Parë anuloi vendimin e Komisionit për refuzimin e kërkesës për akses. Komisioni Evropian e apeloi këtë vendim në GJDBE.

Gjykata e Drejtësisë (në Dhomën e Madhe) rrëzoi vendimin e Gjykatës së Shkallës së Parë dhe konfirmoi refuzimin nga ana e Komisionit Evropian të kërkesës për akses në process-verbalin e plotë të mbledhjes, me qëllim mbrojtjen e të dhënave personale të personave të pranishëm në mbledhje. GJDBE-ja vlerësoi se Komisioni kishte refuzuar me të drejtë përhapjen e informacionit, pasi pjesëmarrësit nuk kishin dhënë pëlqimin e tyre për përhapjen e të dhënave personale të tyre. Gjithashtu, Bavarian Lager-i nuk kishte provuar se aksesi në atë informacion ishte i domosdoshëm.

Së fundmi, subjektet e të dhënave, autoritetet mbikëqyrëse, kontrolluesit dhe përpunuesit, gjatë një procesi gjyqësor, mund t'i kërkojnë gjykatës kombëtare të kërkojë qartësime nga ana e GJDBE-së për interpretimin dhe vlefshmërinë e akteve të institucioneve, organeve, zyrave ose agjencive të BE-së. Këto lloj qartësimesh njihen si vendime paragjyqësore, të cilat nuk përbëjnë mjet juridik të drejtpërdrejtë për kërkuesin, por u mundësojnë gjykatave kombëtare të garantojnë zbatim të saktë të së drejtës së BE-së. Çështje themelore, sikurse *Digital Rights Ireland* dhe *Kärntner Landesregierung dhe të Tjerët*[639] dhe *Schrems*[640], të cilat patën ndikim të madh në zhvillimin e legjislacionit të mbrojtjes së të dhënave të BE-së, shkuan në GJDBE pikërisht nëpërmjet këtij mekanizmi vendimesh paragjyqësore.

[BOX TYPE 1]

Shembull: *Digital Rights Ireland* dhe *Kärntner Landesregierung dhe të Tjerët*[641] ishte një çështje e bashkuar e paraqitur nga Gjykata e Lartë e Irlandës dhe Gjykata Kushtetuese e Austrisë, e cila kishte të bënte me përputhshmërinë e Direktivës 2006/24/EC (Direktiva e Mbajtjes së të Dhënave) me legjislacionin e mbrojtjes së të dhënave të BE-së. Gjykata Kushtetuese e Austrisë depozitoi disa pyetje pranë GJDBE-së, që kishin të bënin me vlefshmërinë e neneve nga 3 deri në 9 të Direktivës 2006/24/EC, duke iu referuar neneve 7, 9 dhe 11 të Kartës së të Drejtave Themelore të BE-së. Në këto pyetje shtrohej çështja nëse disa dispozita të Ligjit Federal Austriak për Telekomunikacionet që transpozonin Direktivën e Mbajtjes së të Dhënave ishin në kundërshtim me disa aspekte të Direktivës së shfuqizuar të Mbrojtjes së të Dhënave dhe me Rregulloren e Mbrojtjes së të Dhënave të Institucioneve të BE-së.

---

[636] Rregullorja (EC) nr. 45/2001, neni 32, pika 3.
[637] GJDBE, C-28/08 P, *Komisioni Evropian k. The Bavarian Lager Co. Ltd* [ÇB] , 2010.
[638] Për një analizë të argumentit, shih EDPS (2011), *Public access to documents containing personal data after the Bavarian Lager ruling*, Bruksel, EDPS.
[639] GJDBE, Çështje të bashkuara C-293/12 dhe C-594/12, *Digital Rights Ireland Ltd k. Minister for Communications, Marine and Natural Resources dhe të Tjerët* dhe *Kärntner Landesregierung dhe të Tjerët* [ÇB], 8 prill 2014.
[640] GJDBE, C-362/14, *Maximilian Schrems k. Data Protection Commissioner* [ÇB], 6 tetor 2015.
[641] GJDBE, Çështje të Bashkuara C-293/12 dhe C-594/12, *Digital Rights Ireland Ltd k. Minister for Communications, Marine and Natural Resources dhe të Tjerët* dhe *Kärntner Landesregierung dhe të Tjerët* [ÇB], 8 prill 2014.

Në çështjen *Kärntner Landesregierung dhe të Tjerët,* z. Seitlinger, njëri prej kërkuesve në procesin në Gjykatën Kushtetuese, deklaroi se ai i përdorte telefonin, internetin dhe postën elektronike si për arsye pune, ashtu edhe private. Për rrjedhojë, informacioni që ai dërgonte e merrte kalonte nëpër rrjetet publike të telekomunikacionit. Sipas ligjit austriak të telekomunikacioneve të vitit 2003, operator i tij i telekomunikacionit ishte ligjërisht i detyruar të mblidhte dhe mbante të dhëna në lidhje me përdorimin që ai i bënte rrjetit. Z. Seitlinger besonte se mbledhja dhe mbajtja e të dhënave personale të tij ishte e panevojshme për qëllimet teknike të dërgimit dhe marrjes së informacionit nëpërmjet rrjetit. Gjithashtu, as mbledhja e mbajtja e këtyre të dhënave për qëllime faturimi nuk ishte e nevojshme. Z. Seitlinger theksoi se ai nuk kishte dhënë pëlqimin për këtë lloj përdorimi të të dhënave personale të tij, të cilat mblidheshin dhe mbaheshin thjesht në zbatim të ligjit austriak të telekomunikacioneve të vitit 2003.

Më pas, z. Seitlinger paraqiti ankim kushtetues në Gjykatën Kushtetuese të Austrisë, në të cilin pretendonte se detyrimet ligjore që kishte operator i tij i telekomunikacionit, shkelte të drejtat e tij themelore sipas nenit 8 të Kartës së të Drejtave Themelore të BE-së. Meqenëse legjislacioni austriak zbatonte legjislacionin e BE-së (Direktivën e Mbajtjes së të Dhënave të shfuqizuar), Gjykata Kushtetuese e Austrisë ia referoi çështjen GJDBE-së, për të vendosur mbi përputhshmërinë e direktivës me të drejtat për privatësi dhe mbrojtje të të dhënave, të sanksionuara nga Karta e të Drejtave Themelore të BE-së.

Dhoma e Madhe e GJDBE-së mori vendim në lidhje me çështjen, si rezultat i së cilit u anulua Direktiva e BE-së për Mbajtjen e të Dhënave). GJDBE-ja konstatoi se direktiva krijonte ndërhyrje të rënda tek të drejtat themelore për privatësi dhe mbrojtje të të dhënave, ndërhyrje të tilla që nuk kufizoheshin tek nevoja absolute. Direktiva kishte qëllim legjitim, meqenëse u jepte autoriteteve kombëtare më shumë mundësi për të hetuar dhe ndjekur penalisht krimet e rënda, çka e bënte një mjet të çmuar për hetimet penale. Gjithësesi, GJDBE-ja vërejti se kufizimet e të drejtave themelore zbatohen vetëm kur është absolutisht e nevojshme dhe duhen shoqëruar me rregulla të qarta e të sakta për sa i përket qëllimit të tyre, si dhe me masa mbrojtëse për personat.

Sipas GJDBE-së, direktiva nuk e kalonte testin e domosdoshmërisë. Së pari, ajo nuk përcaktonte rregulla të qarta e të sakta për kufizimin e shtrirjes së ndërhyrjes. Në vend që të përcaktonte një marrëdhënie midis të dhënave të mbajtura dhe krimeve të rënda, direktiva zbatohej për të gjitha të dhënat e trafikut, e të gjithë përdoruesve, të të gjitha mjeteve të komunikimit elektronik. Kësisoj, ajo krijonte një ndërhyrje tek të drejtat për privatësi dhe mbrojtje të të dhënave të pothuajse gjithë popullësisë së BE-së, çka mund të konsiderohej si jo proporcionale. Ajo nuk përmbante kushte për kufizimin e aksesit të personave të autorizuar tek të dhënat personale dhe as aksesi vetë nuk i nënshtrohej kritereve procedurale, sikurse kriterit për të marrë miratimin paraprak nga një autoritet administrativ, apo nga një gjykatë. Përfundimisht, direktiva nuk përcaktonte garanci të qarta për mbrojtjen e të dhënave të mbajtura. Rrjedhimisht, ajo nuk garantonte mbrojtje të efektshme të të dhënave nga rreziku i abuzimit me to dhe nga çdo lloj aksesi, apo përdorimi të paligjshëm të të dhënave.[642]

Si parim, GJDBE-ja duhet t'u përgjigjet pyetjeve që i referohen dhe nuk mund të refuzojë dhënien e një vendimi paragjyqësor, me arsyetimin se përgjigjja nuk do të ishtë as e rëndësishmë, e as në kohën e duhur, në raport me çështjen. Megjithatë, ajo mund të refuzojë pyetje, nëse ato janë jashtë fushës së kompetencës së saj.[643] GJDBE-ja merr vendim vetëm për elementet përbërëse të çshtjes që i është

[642] GJDBE, Çështje të bashkuara C-293/12 dhe C-594/12, *Digital Rights Ireland Ltd k. Minister for Communications, Marine and Natural Resources dhe të Tjerët* dhe *Kärntner Landesregierung dhe të Tjerët* [ÇB], 8 prill 2014, parag. 69.
[643] GJDBE, C-244/80, *Pasquale Foglia k. Mariella Novello (No. 2),* 16 dhjetor 1981; GJDBE, C-467/04, *Criminal Proceedings kundër Gasparini dhe të Tjerët,* 28 shtator 2006.

referuar për vendim paragjyqësor, ndërsa gjykata kombëtare mbetet kompetente për të vendosur për themelin e çështjes.[644]

Në të drejtën e KiE-së, Palët Kontraktuese duhet të miratojnë mjete mbrojtëse gjyqësore dhe jo gjyqësore të përshtatshme, për shkeljet e dispozitave të Konventës 108 të Modernizuar.[645] Pretendimet për shkelje të së drejtës për mbrojtjen e të dhënave të nenit 8 të KEDNJ-së, kundër një Pale Kontraktuese të KEDNJ-së, mund gjithashtu të paraqiten në GJEDNJ, pasi të gjitha mjetet mbrojtëse gjyqësore të brendshme të jenë shteruar. Kërkesat e paraqitura në GJEDNJ, për shkeljen e nenit 8 të KEDNJ-së duhet të plotësojnë edhe kritere të tjera pranueshmërie (nenet 34–35 të KEDNJ-së).[646]

Megjithëse kërkesat që i paraqiten GJEDNJ-së mund të drejtohen vetëm kundër Palëve Kontraktuese, ato mund të kenë të bëjnë tërthorazi me veprimet, ose mosveprimet e personave fizikë, në masën që një Palë Kontraktuese të mos ketë përmbushur detyrimet e saj pozitive që rrjedhin nga KEDNJ-ja dhe të mos ketë siguruar mbrojtje të mjaftueshme kundër shkeljeve të të drejtave për mbrojtje të të dhënave në legjislacionin e saj të brendshëm.

[BOX TYPE 1]

Shembull: tek çështja *K.U. k. Finlandës*,[647] kërkuesi ishte një i mitur që ankohej për një reklamë me karakter seksual, e cila ishte postuar në një faqe interneti për njohje. Operatori i shërbimit nuk e zbuloi identitetin e personit që kishte postuar informacionin, për shkak të detyrimeve të konfidencialitetit të përcaktuara nga ligji finlandez. Kërkuesi pretendonte se legjislacioni finlandez nuk ofronte mbrojtje të mjaftueshme ndaj veprimeve të një personi që publikonte në internet të dhëna kompromentuese në lidhje me kërkuesin. GJEDNJ-ja u shpreh se shtetet jo vetëm që ishin të detyruara të mos ndërhynin arbitrarisht në jetën private të personave, por mund edhe t'u nënshtrohen detyrimeve positive, që përfshijnë "miratimin e masave që synojnë të garantojnë respektimin e jetës private edhe në sferën e marrëdhënieve ndërmjet vetë personave". Në rastin e kërkuesit, mbrojtja e tij në mënyrë praktike dhe tëë efektshme bëhej duke ndërmarrë hapat e duhur për të identifikuar dhe proceduar autorin. Megjithatë, shteti nuk e kishte garantuar këtë mbrojtje dhe Gjykata vendosi se ishte shkelur neni 8 i KEDNJ-së.

Shembull: tek çshtja *Köpke k. Gjermanisë*,[648] kërkuesja kishte qenë e dyshuar për vjedhje në vendin e punës dhe ishte vendosur në përgjim të fshehtë me videokamera. GJEDNJ-ja doli në përfundimin se nuk kishte pasur "asgjë që tregonte se autoritetet vendase, me aq sa mund ta vlerësonin ato, nuk kishin ekuilibruar si duhet të drejtën e kërkueses për respektim të jetës private sipas nenit 8, me interesin e punëdhënësit për të mbrojtur të drejtat e tij pronësore dhe interesin publik në mirëadministrimin e drejtësisë". Për rrjedhojë, vendosi mospranimin e kërkesës.

Nëse GJEDNJ-ja vendos se një Palë Kontraktuese ka shkelur një nga të drejtat e mbrojtura nga KEDNJ-ja, Pala Kontraktuese është e detyruar të ekzekutojë vendimin e GJEDNJ-së (neni 46 i KEDNJ-së). Masat e ekzekutimit së pari duhet të pushojnë shkeljen dhe të dhe të korrigjojnë aq sa është e mundur, pasojat negative për kërkuesin. Për ekzekutimin e vendimeve mund të nevojiten gjithashtu masa të përgjithshme për të parandaluar shkelje të ngjashme me ato të konstatuara nga Gjykata, si me anë ndryshimeve në legjislacion, të jurisprudencës, apo të masave të tjera.

Kur GJEDNJ-ja gjen shkelje të KEDNJ-së, neni 41 i Konventës parashikon se ajo mund t'i akordojë kërkuesit "shpërblim të drejtë" me shpenzimet e Palës Kontraktuese.

E drejta për t'u përfaqësuar nga një organ, organizatë apo shoqatë jo fitimprurëse

[644] GJDBE, C-438/05, *International Transport Ëorkers' Federation, Finnish Seamen's Union k. Viking Line ABP, OÜ Viking Line Eesti* [ÇB], 11 dhjetor 2007, parag. 85.
[645] Konventa 108 e Modernizuar, neni 12.
[646] KEDNJ, nenet 34–37.
[647] GJEDNJ, *K.U. k. Finlandës*, nr. 2872/02, 2 dhjetor 2008.
[648] GJEDNJ, *Köpke k. Gjermanisë* (dec.), nr. 420/07, 5 tetor 2010.

GDPR-ja u mundëson personave që paraqesin ankesë pranë një autoriteti mbikëqyrës, ose në gjykatë, të përfaqësohen nga një organ, organizatë, apo shoqatë jo fitimprurëse.[649] Këto njësi jo fitimprurëse duhet të kenë objektiva statutore brenda sferës së interesit publik dhe të jenë aktive në fushën e mbrojtjes së të dhënave. Ato mund të depozitojnë ankesë, ose të ushtrojnë të drejtën për mjet mbrojtës gjyqësor për llogari të subjektit ose subjekteve të të dhënave. Rregullorja u jep Shteteve Anëtare mundësinë të vendosin, në përputhje me të drejtën e brendshme, nëse një organ mund të paraqesë pa prokurë ankesa për llogari të subjekteve të të dhënave.

Kjo e drejtë përfaqësimi u mundëson personave të përfitojnë nga ekspertiza dhe kapaciteti financiar e organizativ i njësive të tilla jo-fitimprurëse, duke lehtësuar kësisoj së tepërmi personat në ushtrimin e të drejtave të tyre. GDPR-ja u mundëson këtyre njësive të ndërmarrin veprime kolektivisht për llogari të shumë subjekteve të të dhënave. Diçka e tillë është në dobi të një sistemi gjyqësor funksional dhe efikas, pasi ankesat e ngjashme grupohen dhe shqyrtohen bashkërisht.

6.2.3. Përgjegjësia dhe e drejta e kompensimit

E drejta për mjet juridik efikas duhet t'u mundësojë personave të kërkojnë kompensim për çdo dëm të pësuar, si rezultat i përpunimit të të dhënave personale të tyre në shkelje të legjislacionit në fuqi. Përgjegjësia e kontrolluesve dhe përpunuesve për përpunimin e paligjshëm, përcaktohet qartë në GDPR.[650] Rregullorja u jep personave të drejtën të marrin kompensim nga kontrolluesi, ose përpunuesi, si për dëmet materiale, ashtu edhe për ato jo-materiale, ndërsa preambula e saj përcakton se "koncepti i dëmit duhet të interpretohet më gjerë nën dritën e praktikës gjyqësore të Gjykatë së Drejtësisë në një mënyrë që reflekton tërësisht objektivat e kësaj Rregulloreje.".[651] Kontrolluesit janë përgjegjës dhe mund të jenë subjekt kërkesash për kompensim nëse nuk përmbushin detyrimet e tyre sipas rregullores. Përpunuesit e të dhënave personale janë përgjegjës për dëmet e shkaktuara nga përpunimi vetëm nëse ai nuk ka respektuar detyrimet e rregullores që u drejtohen veçanërisht përpunuesve, ose kur ka vepruar përtej, apo në kundërshtim me udhëzimet e ligjshme të kontrolluesit. Nëse një kontrollues, apo përpunues ka paguar kompensim të plotë, GDPR-ja parashikon se kontrolluesi, apo përpunuesi mund të kërkojë t'i kthehet nga kontrolluesit, apo përpunuesit e përfshirë në të njëjtin përpunim, pjesa e kompensimit që përputhet me shkallën e përgjegjësisë për dëmin.[652] Njëkohësisht, përjashtimet nga përgjegjësia janë tepër të kufizuara dhe duhet të provohet se kontrolluesi, apo përpunuesi nuk është në asnjë mënyrë përgjegjës për situatën që shkaktoi dëmin.

Kompensimi duhet të jetë 'i plotë dhe efikas' në raport me dëmin e pësuar. Kur dëmi i shkaktuar nga përpunimi i disa kontrolluesve dhe përpunuesve, secili kontrollues, apo përpunues duhet të mbahet përgjegjës për të gjithë dëmin. Ky rregull synon të garantojë kompensim efikas për subjektet e të dhënave dhe një qasje të koordinuar për sa i përket përputhshmërisë së kontrolluesve dhe përpunuesve të përfshirë në aktivitetet e përpunimit.

[BOX TYPE 2]

Shembull: subjektet e të dhënave nuk janë të detyruar të ngrenë pretendime dhe të kërkojnë kompensim nga të gjitha njësitë përgjegjëse për dëmin, pasi diçka e tillë mund të kërkojë procedime të kushtueshme dhe të zgjatura. Mjafton të bëhet padi kundër njërit prej kontrolluesve të përbashkët, i cili më pas mund të mbahet përgjegjës për të gjithë dëmin. Në raste të tilla, një kontrollues, apo përpunues që paguan dëmet, ka të drejtën më pas t'i kthehet shuma e paguar prej njësive të tjera të përfshira në përpunim dhe përgjegjëse për shkeljen, për pjesën e tyre për përgjegjësisë për dëmin. Këto procedime midis bashkë-

[649] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 80.
[650] *Ibid*., neni 82.
[651] *Ibid*., paragrafi 146 i Preambulës.
[652] *Ibid*., neni 82, pikat 2 dhe 5.

kontrolluesve të përpunuesve mund të zhvillohet pasi subjekti i të dhënave ka marrë kompensimin dhe nuk është pjesë e tyre.

Në sistemin juridik të KiE-së, neni 12 i Konventës 108 të Modernizuar kërkon që Palët Kontraktuese të përcaktojnë mjete juridike të përshtatshme për shkeljet e së drejtës kombëtare që zbaton dispozitat e Konventës. Raporti Shpjegues i Konventës 108 të Modernizuar saktëson se mjetet juridike duhet të përmbajnë mundësinë për të kundërshtuar në rrugë gjyqësore një vendim, apo një praktikë, si dhe mjetet juridike jo-gjyqësore duhet të jenë po ashtu në dispozicion.[653] Modalitetet dhe rregullat e ndryshme që lidhen me aksesin në këto mjete juridike, së bashku me procedurën që duhet ndjekur, lihen në diskrecionin e secilës Pale Kontraktuese. Palët Kontraktuese dhe gjykatat kombëtare duhet gjithashtu të parashikojnë dispozita për kompensimin financiar për dëmet materiale dhe jo-materiale të shkaktuara nga përpunimi, si dhe veprimet kolektive.[654]

6.2.4. Sanksionet

Sipas së drejtës së KiE-së, neni 12 i Konventës 108 të Modernizuar parashikon se secila Palë Kontraktuese duhet të përcaktojë sanksionet dhe mjetet juridike të përshtatshme, për shkeljet e së drejtës së brendshme, që u jep efekt parimeve bazë të mbrojtjes së të dhënave të sanksionuara në Konventën 108. Konventa nuk përcakton, apo detyron ndonjë tërësi të caktuar sanksionesh. Përkundrazi, ajo thekson qartë se është në diskrecionin e secilës Pale Kontraktuese të përcaktojë natyrën e sanksioneve gjyqësore, ose jo-gjyqësore, të cilat mund të jenë penale, administrative ose civile. Raporti Shpjegues i Konventës 108 të Modernizuar parashikon se sanksionet duhet të jenë të efektshme, proporcionale dhe penguese.[655] Palët Kontraktuese duhet të respektojnë këtë parim kur përcaktojnë natyrën dhe ashpërsinë e sanksioneve në rendin e tyre të brendshëm juridik.

Sipas së drejtës së BE-së, neni 83 i GDPR-së u jep autoriteteve mbikëqyrëse të Shteteve Anëtare kompetencën të vendosin gjoba administrative ndaj shkeljeve të rregullores. Niveli i gjobave dhe rrethanat që autoritetet kombëtare marrin parasysh kur përcaktojnë nëse duhet të vendosin një gjobë, ashtu si edhe vlerën maksimale të saj, përcaktohen gjithashtu në nenin 83. Kësisoj regjimi sanksionues është i harmonizuar në të gjithë BE-në.

GDPR-ja parashikon një qasje progresive të gjobave. Autoritetet mbikëqyrëse kanë kompetencën të vendosin gjoba administrative për shkeljet e rregullores deri në 20,000,000 €, ose në rastin e një ndërmarrjeje, 4 % të xhiros së përgjithshme vjetore botërore, cilado është më e lartë. Shkeljet që mund të justifikojnë një nivel të tillë gjobe përfshijnë shkeljet e parimeve bazë të përpunimit dhe kushteve për pëlqimin, shkeljet e së drejtave të subjekteve të të dhënave dhe shkeljet e dispozitave të rregullores që përcaktojnë transferimin e të dhënave personale drejt marrësve në vendet e treta. Për shkeljet e tjera, autoritetet mbikëqyrëse mund të vendosin gjoba deri në 10,000,000 €, ose në rastin e një ndërmarrjeje, dy përqind të xhiros së saj të përgjithshme vjetore botërore, cilado është më e lartë.

Për të përcaktuar llojin dhe nivelin e gjobës që do të vendosin, autoritetet mbikëqyrëse duhet të marrin parasysh një sërë faktorësh.[656] Për shembull, ata duhet të vlerësojnë si duhet natyrën, rëndësinë dhe kohëzgjatjen e shkeljes, kategoritë e të dhënave personale të ndikuara dhe nëse ka pasur karakter të qëllimshëm, apo neglizhent. Kur një kontrollues, apo përpunues ka marrë masa për të lehtësuar dëmin e pësuar nga subjektet e të dhënave, kjo duhet marrë parasysh gjithashtu. Po ashtu, shkalla e bashkëpunimit me autoritetin mbikëqyrës pasi ka ndodhur shkelja dhe mënyrën në të cilën ka marrë dijeni për shkeljen autoriteti mbikëqyrës (për shembull, nëse i është njoftuar shkelja nga njësia

[653] Raporti Shpjegues i Konventës 108 të Modernizuar, paragrafi 100.
[654] *Ibid*.
[655] *Ibid*.
[656] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 83, pika 2.

përgjegjëse për përpunimin, apo nga subjekti i të dhënave, të drejtat e së cilit janë shkelur) janë faktorë të tjerë të rëndësishëm që orientojnë vendimmarrjen e autoriteteve mbikëqyrëse.[657]

Përveç kompetencës për të vendosur gjoba administrative, autoritetet mbikëqyrëse kanë në dispozicion një gamë të gjerë tagrash të tjera korrigjuese. Të ashtuquajturat tagra 'korrigjuese' të autoriteteve mbikëqyrëse përcaktohen në nenin 58 të GDPR-së. Ato variojnë nga nxjerrja e urdhërave, paralajmërimeve dhe vërejtje drejtuar kontrolluesve dhe përpunuesve, deri tek vendosja e ndalimit të përkohshëm, ose edhe të përhershëm të aktiviteteve të përpunimit.

Për sa i përket sanksioneve ndaj shkeljeve të legjislacionit të BE-së nga institucione, ose organet e BE-së, nisur nga qëllim specifik i Rregullores së Mbrojtjes së të Dhënave të Institucioneve të BE-së, sanksionet mund të parashikohen në formën e masave disiplinore. Sipas nenit 49 të kësaj rregulloreje "çdo shkelje e detyrimeve të kësaj Rregulloreje, qoftë e qëllimshme, apo për shkak të neglizhencës nga ana e tij apo e saj, bën me përgjegjësi për sanksion disiplinor një zyrtar, ose çdo nëpunës tjetër të Komuniteteve Evropiane [...]".

[657] Grupi i Punës së Nenit 29 (2017), *Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679*, WP 253, 3 tetor 2017.

7 Transferimet dhe qarkullimet ndërkombëtare të të dhënave personale

BE	Çështje të trajtura	KiE
Transferimet e të dhënave personale		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 44	Koncepti	Konventa 108 e Modernizuar, neni 14, pikat 1 dhe 2
Free floë of personal data		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 1, pika 3 dhe paragrafi 170 i Preambulës	Midis Shteteve Anëtare të BE-së	
	Midis Palëve Kontraktuese të Konventës 108	Konventa 108 e Modernizuar, neni 14, pika 1
Transferimet e të dhënave personale drejt vendeve të treta, ose organizatave ndërkombëtare		
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 45 C-362/14, *Maximillian Schrems k. Data Protection Commissioner* [GC], 2015	Vendim përshtatshmërie/vendet e treta, ose organizatat ndërkombëtare me nivel të përshtatshëm mbrojtjeje	Konventa 108 e Modernizuar, neni 14, pika 2
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 46, pika 1 dhe 46, pika 2	Garancitë e përshtatshme, përfshirë realizueshmërinë e të drejtave dhe mjetet juridike për subjektet e të dhënave, që sigurohen nëpërmjet modelit të klauzolave kontraktuese, rregullave të detyrueshme të korporatave, kodeve të sjelljes dhe mekanizmave të certifikimit	Konventa 108 e Modernizuar, neni 14, pikat 2, 3, 5 dhe 6
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 46, pika 3	Me kushtin që të autorizohen nga autoriteti mbikëqyrës kompetent: klauzolat kontraktuese dhe dispozitat e përfshira në marrëveshjet administrative midis autoriteteve publike	

Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 46, pika 5	Autorizimet vijuese në bazë të Direktivës 95/46	
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 47	Rregullat e detyrueshme të korporatave	
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 49	Përjashtimet në situata specifike	Konventa 108 e Modernizuar, neni 14, pika 4
Shembuj: Marrëveshja PNR, BE-SHBA Marrëveshja SWIFT, BE-SHBA	Marrëveshjet ndërkombëtare	Konventa 108 e Modernizuar, neni 14, pika 3, gërma (a)

Në të drejtën e BE-së, Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave parashikon qarkullim të lirë të dhënave brenda Bashkimit Evropian. Megjithatë, ajo përmban kërkesa specifike në lidhje me transferimet e të dhënave personale drejt shteteve të treta jashtë BE-së dhe drejt organizatave ndërkombëtare. Rregullorja e njeh rëndësinë e këtyre transferimeve, sidomos në kontekstin e tregtisë dhe bashkëpunimt ndërkombëtar, por njeh gjithashtu edhe rrezikun e shtuar për të dhënat personale. Për rrjedhojë, rregullorja synon të ofrojë të njëjtin nivel mbrojtjeje të të dhënave personale kur transferohen drejt vendeve të treta sikurse ajo që gëzojnë brenda BE-së.[658] E drejta e KiE-së njeh po ashtu rëndësinë e zbatimit të rregullave për qarkullimet ndërkufitare të të dhënave, bazuar në qarkullimin e lirë midis palëve dhe parashikon kritere specifike për transferimet drejt shteteve të treta.

7.1. Natyra e transferimeve të të dhënave personale

Pikat kryesore

- E drejta e BE-së dhe ajo e KiE-së përmbajnë rregulla në lidhje me transferimet e të dhënave personale drejt marrësve në vende të treta, ose në organizata ndërkombëtare.
- Mbrojtja e të drejtave të subjektit të të dhënave kur të dhënat transferohen jashtë BE-së bwn tw mundur qw mbrojtja e ofruar nga legjislacioni i BE-sw tw ndjekw tw dhwnat personale qw e kanw prejardhjen nga BE-ja.

Në të **drejtën e KiE-së**, qarkullimet ndërkufitare të të dhënave përshkruhen si transferime të të dhënave personale tek marrës të cilët i nënshtrohen një juridiksioni të huaj.[659] Qarkullimet ndërkufitare të të dhënave tek një marrë që nuk është subjekt i një Pale Kontraktuese lejohen vetëm nëse garantohet nivel i përshtatshëm mbrojtjeje.[660]

E drejta e BE-së rregullon transferimet "e të dhënave personale që janë objekt përpunimi, ose janë të destinuara të përpunohen pas transferimit tek një vend i tretë, ose tek një organizatë ndërkombëtare [...]".[661] Këto lloj qarkullimesh të dhënash lejohen vetëm nëse janë në përputhje me rregullat e përcaktuara në kreun V të GDPR-së.

Qarkullimet ndërkufitare të të dhënave personale lejohen tek një marrës i cili është subjekt i juridiksionit të një Pale Kontraktuese, ose një Shteti Anëtar, respektivisht sipas së drejtës së KiE-së dhe asaj të BE-

[658] Rregullorja e Përgjithshme e Mbrojtjes së të dhënave, paragrafët 101 dhe 116 të Preambulës.
[659] Raporti Shpjegues i Konventës 108 të Modernizuar, parag. 102.
[660] Konventa 108 e Modernizuar, neni 14, pika 2.
[661] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 44.

së. Të dy sistemet ligjore lejojnë gjithashtu transferimin e të dhënave tek një vend që nuk është Palë Kontraktuese, apo Shtet Anëtar, me kusht që të plotësohen disa kritere të caktuara.

7.2. Lëvizja/qarkullimi i lirë i të dhënave personale ndërmjet Shteteve Anëtare, ose Palëve Kontraktuese

Pikat kryesore

- Qarkullimi i të dhënave personale brenda BE-së, ashtu si edhe transferimet e të dhënave personale ndërmjet Palëve Kontraktuese të Konventës 108 të Modernizuar, duhet të bëhen pa pengesa. Megjithatë, duke qenë se jo të gjitha Palët Kontraktuese të Konventës 108 të Modernizuar janë Shtete Anëtare të BE-së, transferimet nga një Shtet Anëtar i BE-së tek një vend i tretë, që pavarësisht se është Palë Kontraktuese e Konventës 108, nuk janë të mundur, përveçse nëse plotësohet kushtet e përcaktuara në GDPR.

Sipas së drejtës së KiE-së, midis Palëve Kontraktuese të Konventës 108 të Modernizuar duhet të ketë qarkullim të lirë të të dhënave personale. Sidoqoftë, transferimi mund të jetë i ndaluar nëse ka "rrezik real dhe serioz që transferimi tek një Palë tjetër mund të mund të çojë në shmangie nga dispozitat e Konventës", ose nëse një Palë është e detyruar ta bëjë këtë për shkak të "rregullave të harmonizuara të mbrojtjes që janë të përbashkëta për Shtetet të cilat i përkasin një organizate rajonale ndërkombëtare".[662]

Sipas së drejtës së BE-së, kufizimet, apo ndalimet e qarkullimit të lirë të të dhënave personale midis Shteteve Anëtare të BE-së, për arsye të mbrojtjes së personave fizikë në lidhje me përpunimin e të dhënave personale, janë të ndaluara.[663] Hapësira e qarkullimit të lirë të të dhënave është zgjeruar nga Marrëveshja për Zonën Ekonomike Evropiane (EEA),[664] e cila përfshin Islandën, Lihtenshtejnin dhe Norvegjinë në tregun e brendshëm.

[BOX TYPE 2]

Shembull: nëse një filial in një grupi ndërkombëtar shoqërish, i vendosur në disa Shtete Anëtare, midis së cilave në Slloveni dhe në Francë, dërgon të dhëna personale nga Sllovenia në Francë, ky qarkullim të dhënash nuk duhet kufizuar, apo ndaluar nga e drejta kombëtare e Sllovenisë, për arsye që lidhen me mbrojtjen e të dhënave personale.

Nga ana tjetër, nëse i njëjti filian slloven dëshiron të dërgojë të njëjtat të dhëna personale tek shoqëria nënë në Malajzi, atëherë eksportuesi slloven duhet të marrë parasysh rregullat e kreut V të GDPR-së. Këto dispozita kanë për qëllim të mbrojnë të dhënat personale të subjekteve të të dhënave që i nënshtrohen juridiksionit të BE-së.

Në të drejtën e BE-së, qarkullimet e të dhënave personale tek Shtetet Anëtare të ZAA-së për qëllime të parandalimit, hetimit, zbulimit apo ndjekjes së veprave penale, apo për ekzekutimet e dënimeve personale, i nënshtrohen Direktivës 2016/680.[665] Kjo garanton që shkëmbimi i të dhënave personale nga autoritetet kompetente brenda Bashkimit të mos kufizohet, apo ndalohet për arsye të mbrojtjes së të dhënave. Në të drejtën e KiE-së, përpunimi i të gjitha të dhënave personale (përfshirë qarkullimin e tyre ndërkufitar me Palë të tjera të Konventës 108), pa përjashtime në bazë të qëllimeve, apo fushave të

[662] Konventa 108 e Modernizuar, neni 14, pika 1.
[663] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 1, pika 3.
[664] Vendim i Këshillit dhe i Komisionit i 13 dhjetorit 1993 mbi lidhjen e Marrëveshjes për Zonën Ekonomike Evropiane midis Komuniteteve Evropiane, Shteteve Anëtare të tyre dhe Republikës së Austrisë, Republikës së Finlandës, Republikës së Islandës, Principatës së Lihtenshtejnit, Mbretërisë së Norvegjisë, Mbretërisë së Suedisë dhe Konfederatës së Zvicrës, FZ 1994 L 1.
[665] Direktiva (BE) 2016/680 e Parlamentit Evropian dhe e Këshillit e 27 prillit 2016 për mbrojtjen e personave fizikë në lidhje me përpunimin e të dhënave personale nga autoritetet kompetente, për qëllime të parandalimit, hetimit, zbulimit, ose ndjekjes së veprave penale, ose për ekzekutimin e dënimeve penale dhe për lëvizjen e lirë të këtyre të dhënave dhe që shfuqizon Vendimin Kuadër të Këshillit 2008/977/JHA, FZ 2016 L119.

aktivitetit, përfshihen në fushën e zbatimit të Konventës 108, megjithëse Palët Kontraktuese mund të parashikojnë përjashtime. Të gjithë anëtarët e ZAA-së janë po ashtu Palë të Konventës 108.

7.3. Transferimet e të dhënave personale drejt vendeve të treta/vendeve jo palë, ose organizatave ndërkombëtare

Pikat kryesore

- Si e drejta e **KiE-së**, ashtu edhe ajo e **BE-së**, lejojnë transferimet e të dhënave personale drejt vendeve të treta, ose organizatave ndërkombëtare, me kusht që të plotësohen disa kushte për mbrojtjen e të dhënave personale.
    - **Në të drejtën e KiE-së**, niveli i përshtatshëm i mbrojtjes mund të arrihet me anë të legjislacionit të shtetit, apo organizatës ndërkombëtare, ose duke garantuar normat e përshtatshme.
    - **Në të drejtën e BE-së**, transferimet mund të kryhen nëse vendi i tretë garanton nivel të përshtatshëm mbrojtjeje, ose nëse kontrolluesi, apo përpunuesi i të dhënave ofron garanci të përshtatshme, përfshirë realizueshmërinë e të drejtave dhe mjetet juridike për subjektet e të dhënave, me anë të mjeteve të tilla sikurse janë modeli i klauzolave kontraktuese, apo rregullat e detyrueshme të korporatave.
- **Si e drejta e KiE-së, ashtu edhe ajo e BE-së** parashikojnë klauzola përjashtimore, të cilat autorizojnë transferimin e të dhënave personale në rrethana të caktuara, pavarësisht se nuk ekziston një nivel i përshtatshëm i mbrojtjes, e as garancitë e përshtatshme.

Megjithëse e drejta e KiE-së dhe ajo e BE-së lejojnë qarkullimin e të dhënave me vendet e treta, ose organizatat ndërkombëtare, ato parashikojnë kushte të ndryshme. Secili grup kushtesh merr parasush strukturën dhe qëllimet e ndryshme të organizatave përkatëse.

Në të **drejtën e BE-së**, ekzistojnë si parim dy mënyra sipas së cilave lejohet transferimi i të dhënave personale tek vende të treta, ose organizata ndërkombëtare. Transferimet e të dhënave personale mund të kryhen mbi bazën: e një vendimi përshtatshmërie nga ana e Komisionit Evropian;[666] ose, në mungesë të një vendimi të tillë përshtatshmërie, kur kontrolluesi apo përpunuesi ofron garanci të përshtatshme, përfshirë realizueshmërinë e të drejtave dhe mjetet juridike për subjektin e të dhënave.[667] Në mungesë të qoftë një vendimi përshtatshmërie, apo të garancive të përshtatshme, ka në dispozicion një numër përjashtimesh.

Ndërsa, në të drejtën e **KiE-së**, transferimi i lirë i të dhënave tek vende jo-palë të konventës, lejohet vetëm bazuar në:

- Legjislacionin e shtetit, apo organizatës ndërkombëtare, përfshirë traktatet ose marrëveshjet ndërkombëtare të zbatueshme, që ofrojnë garancitë e përshtatshme;
- Garancitë ad hoc ose të standardizuara të miratuara, të përcaktuara me instrumente ligjërisht detyruese dhe të zbatueshme, të miratuara dhe të zbatuara nga personat e përfshirë në transferim dhe në përpunimin e mëtejshëm.[668]

Ashtu sikurse dhe në të drejtën e BE-së, në mungesë të nivelit të përshtatshëm të mbrojtjes së të dhënave, ka në dispozicion një numër përjashtimesh.

7.3.1. Transferimet mbi bazën e një vendimi përshtatshmërie

[666] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 45.
[667] *Ibid*., neni 46.
[668] Konventa 108 e Modernizuar, neni 14, pika 3, gërmat (a) dhe (b).

Në të drejtën e BE-së, qarkullimi i lirë i të dhënave personale me vendet e treta që kanë nivel të përshtatshëm të mbrojtjes së të dhënave, parashikohet në nenin 45 të GDPR-së. GJDBE-ja ka qartësuar se nocioni "nivel i përshtatshëm i mbrojtjes" kërkon që vend i tretë të garantojë nivel mbrojtjeje të të drejtave dhe lirive themelore, i cili të jetë "thelbësisht i barasvlershëm"[669] me garancitë ligjore të së drejtës së BE-së. Në të njëjtën kohë, mjetet të cilat përdor një vend i tretë, për të garantuar një nivel të tillë mbrojtjeje mund të jenë të ndryshme nga ato të përdorura brenda BE-së, meqenëse kriteri i përshtatshmërisë nuk kërkon riprodhim identik të rregullave BE-së.[670]

Komisioni Evropian analizon nivelin e mbrojtjes së të dhënave në vendet e treta duke shqyrtuar legjislacionin kombëtar dhe detyrimet ndërkombëtare të zbatueshme. Pjesëmarrja e një vendi të tretë në organizata shumëpalëshe, ose rajonale, sidomos në fushën e mbrojtjes së të dhënave personale, duhet të merret parasysh gjithashtu. Nëse Komisioni Evropian del në përfundimin se vendi i tretë, apo organizata ndërkombëtare garanton nivel të përshtatshëm të mbrojtjes, ai merr vendim përshtatshmërie, i cili ka efekt detyrues.[671] Sidoqoftë, GJDBE-ja ka theksuar se autoritetet kombëtare mbikëqyrëse mbeten kompetente për të shqyrtuar kërkesat e personave, në lidhje me mbrojtjen e të dhënave personale që janë transferuar tek një vend i tretë, i cili është përcaktuar nga Komisioni si vendi i cili garanton nivel të përshtatshëm, kur personat pretendojnë se legjislacioni dhe praktikat në fuqi në vendin e tretë, nuk garantojnë nivel të përshtatshëm mbrojtjeje.[672]

Komisioni Evropian mund të shqyrtojë gjithashtu përshtatshmërinë e një territory brenda një vendi të tretë, ose të kufizohet vetëm në sektorë të caktuar, sikurse ishte për shembull rasti i Kanadasë, për të drejtën tregtare private.[673] Ka gjithashtu vendime përshtatshmërie për transferimet mbi bazën e marrëveshjeve midis BE-së dhe vendeve të treta. Këto vendime kanë të bëjnë ekskluzivisht me një lloj të vetëm transferimi të dhënash, si për shembull transmetimi i të dhënave të pasagjerëve (PNR) nga shoqëritë e transportit ajror tek autoritetet e huaja të kontrollit kufitar, kur shoqëritë e transportit ajror kryejnë udhëtime nga BE-ja drejt disa destinacioneve të caktuara (shih Seksionin 7.3.4).

Vendimet e përshtatshmërisë i nënshtrohen monitorimit të vazhdueshëm. Komisioni Evropian i rivlerëson rregullisht këto vendime, me qëllim që të kontrollojë nëse ka zhvillime që mund të cënojnë statusin e tyre. Kështu, nëse Komisioni Evropian del në përfundimin se vend i tretë, apo organizata ndërkombëtare nuk i përmbush më kriteret e vendimit të përshtatshmërisë, aim und të ndryshojë, pezullojë, apo shfuqizojë vendimin. Komisioni mund të hyjë gjithashtu në negociata me vendin e tretë, apo me organizatën ndërkombëtare të përfshirë, me qëllim që të adresojë problematikën në lidhje me vendimin e tij.

Vendimet e përshtatshmërisë së miratuara nga Komisioni Evropian në bazë të Direktivës 95/46/EC mbeten në fuqi deri sa të ndryshohen, zëvendësohen, apo shfuqizohen me Vendim Komisioni të miratuar në përputhje me rregullat e nenit 45 të GDPR-së.

Deri më sot, Komisioni Evropian ka njohur si vende me nivel të përshtatshëm mbrojtjeje Andorrës, Argjentinën, Kanadanë (shoqëritë tregtare që janë subjekt i Ligjit për Informacionin Personal dhe Dokumentet Elektronike – PIPEDA), Ishujt Faroe, Guernsin, Ishullin Man, Izraelin, Xhërzin, Zelandën e Re, Zvicrën dhe Uruguajin. Për sa i përket transferimeve me SHBA-të, Komisioni Evropian ka miratuar një vendim përshtatshmërie në vitin 2000, i cili lejon transferimet drejt shoqërive që janë vetë-certifikuar për mbrojtjen e të dhënave personale të transferuara nga BE-ja dhe që zbatojnë të ashtuquajturat 'parimet e Portit të Sigurt'.[674] GJDBE-ja e shpalli të pavlefshëm këtë vendim në vitin

---

[669] GJDBE, C-362/14, *Maximillian Schrems k. Komisionerit të Mbrojtjes së të Dhënave* [ÇB], 6 tetor 2015, parag. 96.

[670] *Ibid*., parag. 74. Shih gjithashtu, Komisioni Evropian (2017), Komunikatë e Komisionit për Parlamentin Evropian dhe Këshillit "Shkëmbimi dhe Mbrojtja e të Dhënave Personale në një Botë të Globalizuar", COM(2017)7 final, 10 janar 2017, fq. 6.

[671] Për listën e përditësuar vazhdimisht të vendeve që kanë marrë vendim përshtatshmërie, shiko faqen kryesore në internet të Drejtorisë së Përgjithshme të Drejtësisë të Komisionit Evropian.

[672] GJDBE, C-362/14, *Maximilian Schrems k. Komisionerit të Mbrojtjes së të Dhënave* [ÇB], 6 tetor 2015, paragrafët 63 dhe 65– 66.

[673] Komisioni Evropian (2002), Vendimi 2002/2/EC i 20 dhjetorit 2001 sipas Direktivës 95/46/EC të Parlamentit Evropian dhe Këshillit mbi mbrojtjen e përshtatshme të të dhënave personale që ofron Ligji Kanadez për Mbrojtjen e Informacionit Personale dhe Dokumenteve Elektronike, FZ 2002 L 2.

[674] Vendim i Komisionit 2000/520/EC i 26 korrikut 2000 sipas Direktivës 95/46/EC të Parlamentit Evropian dhe Këshillit mbi përshtatshmërinë e mbrojtjes që ofrojnë parimet e privatësisë së "portit të sigurt" dhe të pyetjeve më të shpeshta që kanë të bëjnë me to, të miratuara nga Departamenti i Tregtisë së SHBA-ve, FZ L 215. Vendimi u shpall i pavlefshëm nga GJDBE-ja në çështjen C-632/14, *Maximilian Schrems k. Komisionerit të Mbrojtjes së të Dhënave* [ÇB].

2015 dhe një vendim i ri përshtatshmërie u miratua në korrik të 2016-ës, i cili autorizon shoqëritë të aderojnë në të duke nisur nga data 1 gusht 2016.

[BOX TYPE 1]

Shembull: tek çështja *Schrems,*[675] Maximilian Schrems-i, një shtetas austriak, kishte qenë përdorues i Facebook-ut për disa vite. Një pjesë, ose të gjitha të dhënat që z. Schrems i kishte dhënë Facebook-ut, ishin transferuar nga filiali i Facebook-ut në Irlandë, tek serverët e tij në SHBA, ku ishin përpunuar. Z. Schrems paraqiti ankesë pranë autoritetit irlandez të mbrojtjes së të dhënave, ku vlerësonte se, referuar informacioneve të bëra publike nga sinjalizuesi amerikan Edward Snowden në lidhje me aktivitetet e survejimit që kryenin shërbimet informative të SHBA-ve, legjislacioni dhe praktikat amerikane nuk ofronin mbrojtje të mjaftueshme të të dhënave që transferohen në atë vend. Autoriteti irlandez e refuzoi ankesën me arsyetimin se vendimi i Komisionit i datës 26 korrik 2000 përcaktonte se sipas skemës së 'Portit të Sigurt', SHBA-të garantonin nivel të përshtatshëm të mbrojtjes së të dhënave personale të transferuara. Çështja u dërgua në Gjykatën e Lartë të Irlandës, e cila ia përcolli GJDBE-së për vendim paragjyqësor.

GJDBE-ja doli në përfundimin se vendimi i Komisionit për përshtatshmërinë e kuadrit të Portit të Sigurt ishte i pavlefshëm. GJDBE-ja vërejti fillimisht se vendimi lejonte kufizimin e parimeve të mbrojtjes së të dhënave të Portit të Sigurt, për arsye të sigurisë kombëtare, interesit publik, apo nevojave të zbatimit të ligjit, ose në bazë të së drejtës së brendshme të SHBA-ve. Për pasojë vendimi mundësonte ndërhyrjen tek të drejtat themelore të personave, të dhënat personale të të cilëve ishin transferuar, ose mund të transferoheshin në SHBA.[676] Ajo vërejti më tej se vendimi nuk përmbante asnjë konstatim mbi ekzistencën e rregullave të SHBA-ve, që të kishin për qëllim të kufizonin një ndërhyrje të tillë, apo mbi ekzistencën e mbrojtjes ligjore të efektshme ndaj kësaj ndërhyrjeje.[677] GJDBE-ja theksoi se niveli i mbrojtjes së të drejtave dhe lirive themelore të garantuara në BE, kërkonte që legjislacioni i cili ndërhynte tek nenet 7 dhe të 8, të përcaktonte rregulla të qarta dhe të sakta për rregullimin e objektit dhe zbatimit të një mase dhe të përcaktonte minimumin e garancive, përjashtimeve dhe kufizimeve në lidhje me mbrojtjen e të dhënave personale.[678] Duke qenë se vendimi i Komisionit nuk shprehej se SHBA-të në fakt e garantonin një nivel të tillë mbrojtjeje, për shkak të së drejtës së brendshme, apo angazhimeve ndërkombëtare, GJDBE-ja doli në përfundimin se ajo nuk i përmbushte kriteret e parashikuara nga dispozita përkatëse për transferimin e Direktivës së Mbrojtjes së të Dhënave dhe rrjedhimisht ishte i pavlefshëm.[679]

Kësisoj, niveli i mbrojtes së ofruar nga SHBA-të nuk ishte 'thelbësisht i barasvlershëm' me të drejtat dhe liritë themelore të garantuara nga BE-ja.[680] GJDBE-ja vendosi se ishin shkelur shumë nene të Kartës së të Drejtave Themelore të BE-së. Së pari, nuk ishte respektuar thelbi i nenit 7, pasi legjislacioni i SHBA-ve "lejonte autoritetet publike të kishin akses në mënyrë të përgjithshme në brendinë e komunikimeve elektronike". Së dyti, ishte shkelur gjithashtu thelbi i nenit 47, pasi legjislacioni nuk u jepte personave mjete juridike në lidhje me aksesin tek të dhënat personale, apo korrigjimin, ose fshirjen e të dhënave personale. Së fundmi, meqenëse marrëveshja e Portit të Sigurt shkelte nenet e sipërpërmendur, të dhënat personale nuk përpunoheshin më në mënyrë të ligjshme, çka përbënte shkelje të nenit 8.

Pasi GJDBE-ja e shpalli të pavlefshme marrëveshjen e Portit të Sigurt, Komisioni dhe SHBA-të ranë dakord për një kuadër të ri, Mburojën e Privatësisë BE-SHBA. Më 12 korrik 2016, Komisioni miratoi vendimin i cili shpallte se SHBA-të garantonin nivel të përshtatshëm të mbrojtjes së të dhënave personale, të transferuara nga Bashkimi tek organizatat në SHBA në kuadër të Mburojës së Privatësisë.[681]

---

[675] GJDBE, C-362/14, *Maximilian Schrems k. Komisionerit të Mbrojtjes së të Dhënave* [ÇB], 6 tetor 2015.
[676] *Ibid*., parag. 84.
[677] *Ibid*., parag. 88–89.
[678] *Ibid*., parag. 91–92.
[679] *Ibid*., parag. 96–97.
[680] *Ibid*., parag. 73–74 dhe 96.
[681] Vendim Ekzekutiv i Komisionit (BE) 2016/1250 i 12 korrikut 2016 sipas Direktivës 95/46/EC të Parlamentit Evropian dhe Këshillit mbi përshtatshmërinë e mbrojtjes së ofruar nga "Mburoja e Privatësisë" BE-SHBA, FZ L 207. Grupi i Punës së Nenit 29 mirëpriti përmirësimet që solli mekanizmi i Mburojës së Privatësisë, krahasuar me vendimin e "Portit të Sigurt" dhe përshëndeti Komisionin dhe autoritetet amerikane

Ashtu sikurse marrëveshja e Portit të Sigurt, Mburoja e Privatësisë BE-SHBA synon të mbrojë të dhënat personale që transferohen nga BE-ja drejt SHBA-vë për qëllime tregtare.[682] Shoqëritë amerikane nuk të vetë-certifikohen vullnetarisht duke aderuar në listën e Mburojës së Privatësisë, duke u angazhuar të respektojnë normat e mbrojtjes së të dhënave të këtij kuadri. Autoritetet kompetente të SHBA-ve monitorojnë dhe verifikojnë respektimin e këtyre normave nga shoqëritë e certifikuara.

Skema e Mburojës së Privatësisë parashikon sidomos:

Detyrimet në lidhje me mbrojtjen e të dhënave për shoqëritë të cilat përftojnë të dhëna personale nga BE-ja;

Mbrojtje dhe mjete juridike për personat, sidomos krjimin e mekanizmit të Avokatit të Popullit, të pavarur nga shërbimet informative të SHBA-ve dhe që trajton ankesat e personave që besojnë se të dhënat e tyre personale janë përdorur në mënyrë të paligjshme nga autoritetet amerikane në fushën e sigurisë kombëtare;

Rishikim të përbashkët të përvitshëm për të monitoruar zbatimin e këtij kuadri;[683] rishikimi i parë u zhvillua në shtator 2017.[684]

Qeveria e Shteteve të Bashkuara ka marrë angazhime dhe ka dhënë garanci me shkrim, të cilat shoqërojnë vendimin e Mburojës së Privatësisë. Ato parashikojnë kufizimet dhe garancitë në lidhje me aksesin nga ana e qeverisë tek të dhënat personale për qëllime ligjzbatuese dhe të sigurisë kombëtare.

7.3.2 Transferimet me garanci të mjaftueshme

Si **e drejta e BE-së**, ashtu edhe ajo e **KiE-së** i njohin garancitë e përshtatshme midis kontrolluesit që eksporton të dhëna dhe marrësit të një vendi të tretë, apo një organizate ndërkombëtare, si mundësi për të siguruar nivel të mjaftueshëm të mbrojtjes së të dhënave për marrësin.

Në të **drejtën e BE-së**, transferimet e të dhënave personale drejt një vendi të tretë, apo një organizate ndërkombëtare lejohen nëse kontrolluesi, apo përpunuesi ofron garancitë e përshtatshme dhe të drejta të realizueshme dhe me kusht që mjetet juridike të jenë të disponueshme për subjektet e të dhënave.[685] Lista e 'garancive të përshtatshme' përcaktohet ekskluzivisht në legjislacionin e mbrojtjes së të dhënave të BE-së. Garancitë e përshtatshme mund të përcaktohen nëpërmjet:

- Një instrumenti ligjor detyrues dhe të ekzekutueshëm midis autoriteteve, apo organeve publike;
- Rregullave të detyrueshme të korporatave;
- Modelit të klauzolave kontraktuese të mbrojtjes së të dhënave, të miratuara qoftë nga Komisioni Evropian, ashtu edhe nga një autoritet mbikëqyrës;

---

që morën parasysh në variantin përfundimtar të dokumenteve në lidhje me "Mburojën e Privatësisë", shqetësimet e ngritura në opinionin e grupit të punës WP238 mbi projekt-vendimin e përshtatshmërisë "Mburoja e Privatësisë" BE-SHBA. Megjithatë, grupi i punës nënvizoi një sërë shqetësimesh të patrajtuara. Për më tepër hollësi, shih: Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, miratuar më 13 prill 2016, 16/EN WP 238.

[682] Për më tepër informacion, shih: EU-U.S. Privacy Shield factsheet.

[683] Për më shumë informacion, shih faqen në internet të Komisionit Evropian në lidhje me EU-U.S. Privacy Shield.

[684] Komisioni Evropian, Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield, COM(2017) 611 final, 18 tetor 2017. Shih gjithashtu: Article 29 Working Party, *EU – U.S. Privacy Shield – First annual Joint Review*, miratuar më 28 nëntor 2017, 17/EN WP 255.

[685] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 46.

- Kodeve të sjelljes;
- Mekanizmave të certifikimmit.[686]

Klauzolat kontraktuese të përshtatura midis kontrolluesve ose përpunuesve në BE dhe marrësve të të dhënave në një vend të tretë, janë po ashtu mjete që ofrojnë garanci të përshtatshme. Megjithatë, këto klauzola kontraktuese duhet të autorizohen nga autoriteti mbikëqyrës kompetent përpara se të përdoren si mjet për transferimin e të dhënave personale. Po njësoj, edhe autoritetet publike mund të përdorin dispozitat e mbrojtjes të mbrojtjes së të dhënave që përfshihen në marrëveshjet e tyre administrative, me kusht që ato t'i ketë autorizuar autoriteti mbikëqyrës.[687]

Në të drejtën e KiE-së, qarkullimet e të dhënave me një shtet, apo një organizatë ndërkombëtare që nuk është palë e Konventës 108 të Modernizuar lejohen me kusht që të sigurohet nivel i përshtatshëm mbrojtjeje. Një nivel i tillë arrihet nëpërmjet:

- Të drejtës së shtetit, apo organizatës ndërkombëtare, ose
- Garancive *ad hoc* ose të standardizuara, të cilat të jenë të integruara në një dokument me ligjërisht të detyrueshëm.[688]

Transferimet me klauzola kontraktuese

Si **e drejta e KiE-së**, ashtu edhe ajo **e BE-së** njohin klauzolat kontraktuese midis kontrolluesit që eksporton të dhënat dhe marrësit në një vend të tretë si mjet të mundshëm për të garantuar nivel të mjaftueshëm të mbrojtjes së të dhënave për marrësin.[689]

Në **nivel BE-je**, Komisioni Evropian me mbështetjen e Grupit të Punës së Nenit 29, ka hartuar modelin e klauzolave kontraktuese të mbrojtjes së të dhënave, të cilat u certifikuan zyrtarisht nga Komisioni me anë të një vendimi, si provë që vërteton mbrojtje të përshtatshme të të dhënave.[690] Duke qenë se vendimet e Komisionit janë detyruese për të gjitha Shtetet Anëtare, autoritetet kombëtare që mbikëqyrin transferimet e të dhënave duhet ta njohin këtë model klauzolash kontraktuese në procedurat e tyre.[691] Kështu, nëse kontrolluesi që eksporton të dhëna dhe marrësi i një vendi të tretë, bien dakord dhe nënshkruajnë këto klauzola, kjo duhet të përbëjë provë të mjaftueshme për autoritetin mbikëqyrës se ekzistojnë garancitë e përshtatshme. Megjithatë, tek çështja *Schrems*, GJDBE-ja u shpreh se Komisioni Evropian nuk kishte kompetencë të kufizonte tagret e autoriteteve mbikëqyrëse kombëtare, për të monitoruar transferimin e të dhënave personale tek një vend i tretë, i cili ka përftuar vendim përshtatshmërie nga Komisioni.[692] Kësisoj, autoritetet mbikëqyrëse kombëtare nuk pengohen në ushtrimin e tagreve të tyre, përfshirë edhe atë për të pezulluar, apo ndaluar transferimin e të dhënave personale, kur ky transferim kryhet në shkelje të së drejtës së BE-së, apo të drejtës së brendshme në lidhje me mbrojtjen e të dhënave, sikurse, për shembull kur importuesi i të dhënave nuk respekton modelin e klauzolave kontraktuese.[693]

---

[686] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 46, pika 1, gërmat (c), (d), (2), gërmat (a), (b), (e), (f) dhe 47.
[687] *Ibid*., neni 46, pika 3.
[688] Konventa 108 e Modernizuar, neni 14, pika 3, gërma (b).
[689] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave,neni 46, pika 3; Konventa 108 e Modernizuar, neni 14, pika 3, gërma (b).
[690] *Ibid*., neni 46, pika 2, gërma (b) dhe neni 46, pika 5.
[691] *Ibid*., neni 46, pika 2, gërma (c); Traktati mbi Funksionimin e Bashkimit Evropian, neni 288
[692] GJDBE, C-362/14, *Maximilian Schrems k. Data Protection Commissioner* [ÇB], 6 tetor 2015, parag. 96–98 dhe 102–105.
[693] Me qëllim që të përputheshin me qëndrimin e GJDBE-së në lidhje me çështjen *Schrems*, Komisioni ndryshoni Vendimin e tij për Modelin e Klauzolave Kontraktuese. Vendim Ekzekutiv i Komisionit (BE) 2016/2297 i 16 dhjetorit 2016, që ndryshon Vendimet 2001/497/EC dhe 2010/87/EU në lidhje me modelin e klauzolave kontraktuese për transferimin e të dhënave personale tek vendet e treta dhe tek përpunuesit e këtyre vendeve, në përputhje me Direktivën 95/46/EC të Parlamentit Evropian dhe Këshillit, FZ 2016 L344.

Ekzistenca e modelit të klauzolave të mbrojtjes së të dhënave në kuadrin ligjor të BE-së nuk i pengon kontrolluesit që të hartojnë klauzola të tjera individuale ad hoc, me kusht që këto klauzola t'i ketë miratuar autoriteti mbikëqyrës.[694] Ato duhet gjithsesi të garantojnë të njëjtin nivel mbrojtjeje sikurse modeli i klauzolave kontraktuese të mbrojtjes së të dhënave. Për të miratuar këto klauzola *ad hoc*, autoritetet mbikëqyrëse duhet të zbatojnë mekanizmin e njëtrajtshmërisë, me qëllim që të garantojnë qasje rregullatore të njëtrajtshme në të gjithë BE-në.[695] Kjo nënkupton se autoriteti mbikëqyrës kompetent është i detyruar t'i komunikojë EDPB-së projekt-vendimin e tij në lidhje me klauzolat. EDPB-ja do të miratojë opinion në lidhje me këtë dhe autoriteti mbikëqyrës duhet ta marrë mirë parasysh këtë opinion gjatë finalizimit të vendimit. Nëse autoriteti mbikëqyrës nuk synon të ndjekë opinionin e EDPB-së, do të aktivizohet mekanizmi i zgjidhjes së mosmarrëveshjeve dhe Bordi do të miratojë vendim detyrues.[696]

Karakteristikat më të rëndësishme të modelit të klauzolave kontraktuese janë:

- Një klauzolë për palën e tretë përfituese, e cila u mundëson subjekteve të të dhënave të ushtrojnë të drejtat kontraktuese edhe duke mos qenë palë në kontratë;
- Marrësi i të dhënave ose importuesi pranon t'i nënshtrohet juridiksionit të autoritetit kombëtar mbikëqyrës dhe/ose gjykatave të eksportuesit të të dhënave në rast mosmarrëveshjeje.

Ekzistojnë aktualisht dy tërësi klauzolash kontraktuese për transferimet midis kontrolluesve, prej së cilave eksportuesi i të dhënave mund të zgjedhë.[697] Për transferimet midis kontrolluesit dhe përpunuesit ekziston vetëm një model klauzolash kontraktuese.[698] Megjithatë, ky model klauzolash kontraktuese është aktualisht në shqyrtim gjyqësor.

[BOX TYPE 3]

Shembull: pasi GJDBE-ja e shpalli të pavlefshëm Vendimin e Portit të Sigurt,[699] transferimet e të dhënave personale drejt SHBA-ve nuk mund të mbështeteshin më në atë vendim përshtatshmërie. Teksa vijonin negociatat me autoritetet amerikane dhe në pritje të miratimit të një vendimi të ri përshtatshmërie (i cili përfundimisht u miratua më 12 korrik 2016),[700] transferimet mund të kryheshin vetëm mbështetur në baza të tjera ligjore, sikurse në modelin e klauzolave kontraktuese, apo në rregullat e detyrueshme të korporatave. Shumë shoqëri, përfshirë degën e Facebook-ut në Irlandë (kundër të cilës u bë ankimi i cili solli shfuqizimin e Vendimit të Portit të Sigurt), kaluan në modelin e klauzolave kontraktuese për të vijuar transferimet e tyre midis BE-së dhe SHBA-ve.

---

[694] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 46, pika 3, gërma (a).

[695] *Ibid*., neni 63 dhe neni 64, pika 1, gërma (e).

[696] *Ibid*., neni 64 dhe neni 65.

[697] Seti I ndodhet në Shtojcën e Vendimit të Komisionit 2001/497/EC, Komisioni Evropian (2011), i 15 qershorit 2001 në lidhje me modelin e klauzolave kontraktuese për transferimin e të dhënave personale tek vendet e treta, sipas Direktivës 95/46/EC, FZ 2001 L 181; Seti II ndodhet në Shtojcën e Vendimit të Komisionit 2004/915/EC, Komisioni Evropian (2004), i 27 dhjetorit 2004 që ndryshon Vendimin 2001/497/EC për sa i përket miratimit të një seti alternative modeli klauzolash kontraktuese për transferimin e të dhënave personale tek vendet e treta, FZ 2004 L 385.

[698] Komisioni Evropian(2010), Vendim i Komisionit 2010/87 i 5 shkurtit 2010 në lidhje me modelin e klauzolave kontraktuese për transferimin e të dhënave personale tek përpunuesit e vendosur në vende të treat, sipas Direktivës 95/46/EC të Parlamentit Evropian dhe të Këshillit, FZ 2010 L 39. Në periudhën kur po hartohej ky manual, përdorimi i modelit të klauzolave kontraktuese si bazë për transferimin e të dhënave personale drejt SHBA-ve ishte në shqyrtim gjyqësor në Gjykatën e Lartë të Irlandës.

[699] GJDBE, C-362/14, *Maximillian Schrems k. Data Protection Commissioner* [ÇB] , 6 tetor 2015.

[700] Vendim Ekzekutiv i Komisionit (BE) 2016/1250 i 12 korrikut 2016 në pajtim me Direktivën 95/46/EC të Parlamentit Evropian dhe të Këshillit në lidhje me përshtatshmërinë e mbrojtjes së ofruar nga Mburoja e Privatësisë BE-SHBA, FZ L 207.

Z. Schrems depozitoi ankesë pranë autoritetit mbikëqyrës irlandez, me të cilën kërkonte që të pezulloheshin transferimet e të dhënave bazuar tek modeli i klauzolave kontraktuese drejt SHBA-ve. Në thelb, ai pretendonte se kur të dhënat e tij personale transferoheshin nga filiali Irlandez i Facebook-ut tek Facebook Inc.-u dhe tek serverët në SHBA, nuk ekzistonin garanci se ato do të mbroheshin. Facebook Inc.-u ishte subjekt i së drejtës amerikane, e cila mund ta detyronte të përhapte të dhëna personale për autoritetet ligjzbatuese të SHBA-ve dhe qytetarët evropianë nuk kishin asnjë mjet gjyqësor në dispozicion për ta kundërshtuar këtë praktikë.[701] Për këto arsye, GJDBE-ja doli në përfundimin se Vendimi i Portit të Sigurt ishte i pavlefshëm dhe megjithëse vendimi i gjykatës kufizohej vetëm në shqyrtimin e atij vendimi, kërkuesi i vlerësonte problematikat që ai ngrinte po aq të vlefshme edhe kur transferimi bazohet në klauzolat kontraktuese. Gjatë hartimit të këtij manuali, çështja po shqyrtohej nga Gjykata e Lartë e Irlandës. Me sa duket, kërkuesi ka ndërmend ta dërgojë çështjen në GJDBE, ku qëllimi i tij është të kundërshtojë vlefshmërinë e vendimit të Komisionit Evropian mbi modelin e klauzolave kontraktuese. Sikurse përshkruhet në Kapitullin 5, vetëm GJDBE-ja ka kompetencën ta shpallë të pavlefshëm një instrument të BE-së.

Transferimet me anë të rregullave të detyrueshme të korporatave

E drejta e BE-së lejon gjithashtu transferimet e të dhënave personale mbështetur tek rregullat e detyrueshme të korporatave, për transferimet ndërkombëtare që zhvillohen brenda të njëjtit grup ndërmarrjesh, apo ndërmarrjesh të cilat janë pjesë e një aktiviteti të përbashkët ekonomik.[702] Përpara se të përdoren rregullat e detyrueshme të korporatave si mjet për transferimin e të dhënave personale, autoriteti mbikëqyrës kompetent duhet t'i miratojë ato në përputhje me mekanizmin e njëtrajtshmërisë.

Në mënyrë që të miratohen, rregullat e detyrueshme të korporatave duhen të jenë ligjërisht detyruese, të mbulojnë të gjitha parimet thelbësore të mbrojtjes së të dhënave, të zbatohen për dhe nga të gjithë anëtarët e një grupi. Ato duhet të përcaktojnë qartësisht të drejta të realizueshme për subjektet e të dhënave, të përfshijnë të gjitha parimet thelbësore të mbrojtjes së të dhënave dhe të respektojnë disa kritere formale, si për shembull të përshkruajnë strukturën e ndërmarrjes, transferimet dhe mënyrën se si do të zbatohen parimet e mbrojtjes së të dhënave. Këtu përfshihet informimi i subjekteve të të dhënave në lidhje me këtë informacion. Rregullat e detyrueshme të korporatave duhet të parashikojnë gjithashtu ndër të tjera, të drejtat e subjekteve të të dhënave dhe dispozita në lidhje me përgjegjësinë në rast shkeljeje të rregullave.[703] Për miratimin e rregullave të detyrueshme të korporatave, aktivizohet mekanzimi i njëtrajtshmërisë për bashkëpunimin e autoriteteve mbikëqyrëse (sikurse përshkruhet në Kapitullin 5).

Në kuadrin e mekanizmit të njëtrajshmërisë, autoriteti mbikëqyrës kryesor shqyrton projekt-rregullat e deytueshme të korporatave, miraton një project-vendim dhe ia komunikon atë EDPB-së. Bordo jep mendim në lidhje me çështjen dhe autoriteti mbikëqyrës kryesor mund t'i miratojë zyrtarisht rregullat e detyrueshme të korporatave, duke 'marrë plotësisht parasysh' mendimin e Bordit. Mendimi i këtij të fundit nuk është ligjërisht detyrues, por nëse autoriteti mbikëqyrës synon të mos e marrë parasysh,

[701] Për më tepër informacion, shih ankesën e ndryshuar kundër Facebook Ireland Ltd, depozituar pranë Komisionerit Irlandez të Mbrojtjes së të Dhënave nga Maximilian Schrems-i më 1 dhjetor 2015.

[702] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 47.

[703] Për një përshkrim më të hollësishëm, shih Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave, nenin 47.

aktivizohet mekanizmi i zgjidhjes së mosmarrëveshjeve dhe Bordit do t'i duhet të miratojë një vendim ligjërisht detyrues, me një shumicë prej dy të tretave të anëtarëve të tij.[704]

Në **të drejtën e KiE-së**, garancitë ad hoc ose të standardizuara, të cilat janë të përcaktuara në një dokument ligjërisht detyrues,[705] përfshijnë gjithashtu rregullat e detyrueshme të korporatave.

7.3.3 Përjashtimet në situata të caktuara

Në të drejtën e BE-së, transferimet e të dhënave personale tek vendet e treta mund të justifikohen edhe në mungesë të një vendimi përshtatshmërie, apo të garancive, sikurse janë modeli i klauzolave kontraktuese, apo rregullat e detyrueshme të korporatave, në një nga rrethanat në vijim:

- Subjekti i të dhënave ka dhënë pëlqimin e qartë për transferimin e të dhënave;
- Subjekti i të dhënave është, ose po përgatitet të bëhet, palë në një marrëdhënie kontraktuese, për të cilën transferimi i të dhënave jashtë vendit është i nevojshëm;
- Për të lidhur një kontratë midis një kontrolluesi të dhënash dhe një pale të tretë, në interes të subjektit të të dhënave;
- Për shkaqe të rëndësishme të interesit publik;
- Për të ngritur, ushtruar, apo mbrojtur pretendime ligjore;
- Për të mbrojtur interesat jetike të subjektit të të dhënave;
- Për transferimin e të dhënave nga regjistrat publikë (ky është një shembull i interesave mbizotëruese të publikut të gjerë, për të pasur akses në informacionet që mbahen në regjistrat publikë).[706]

Nëse asnjë nga këto kushte nuk gjen zbatim dhe nëse transferimet nuk mund të mbështeten tek një vendim përshtatshmrie, apo në garancitë e përshtatshme, transferimi mund të kryhet vetëm nëse nuk është i përsëritur, nëse lidhet me një numër të kufizuar subjektesh të dhënash dhe nëse është i nevojshëm për qëllime të interesave legjitime detyruese të kontrolluesit të të dhënave, në masën që këto interesa të mos tejkalohen nga të drejtat e subjektit të të dhënave.[707] Në këto raste, kontrolluesi duhet të vlerësojë rrethanat që kanë të bëjnë me transferimin dhe të ofrojë garanci. Gjithashtu, ai duhet të informojë autoritetin mbikëqyrës dhe subjektet e të dhënave që preken, si për transferimin ashtu edhe për interesin legjitim që e justifikon atë.

Fakti që këto përjashtime janë mjeti i fundit për transferime të ligjshme[708] (që mund të përdoren vetëm në mungesë të një vendimi përshtatshmërie dhe të garancive të tjera) thekson natyrën e tyre përjashtimore dhe evidentohet më tej në paragrafët e prambulës së GDPR-së[709]. Në vetvete, përjashtimet pranohen si mundësi "për transferime në rrethana të caktuara" mbi bazën e pëlqimit dhe kur "transferimi është rastësor dhe i nevojshëm"[710] në lidhje me një kontratë ose një pretendim ligjor.

Gjithashtu, sipas orientimeve të Grupit të Punës së Nenit 29, përdorimi i përjashtimeve në situata të caktuara duhet të jetë përjashtimor, në raste të veçuara dhe nuk mund të përdoret për transferime masive ose të përsëritura.[711] Mbikëqyrësi Evropian i Mbrojtjes së të Dhënave ka nënvizuar gjithashtu karakterin e jashtëzakonshëm të përdorimit të përjashtimeve, si bazë ligjore për transferimet sipas

[704] *Ibid*., neni 57, pika 1, gërma (s), 58, pika 1, gërma (j), 64, pika 1, gërma (f), 65, pikat 1 dhe 2.
[705] Konventa 108 e Modernizuar, neni 14, pika 3, gërma (b).
[706] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 49.
[707] *Ibid*.
[708] *Ibid*., neni 49, pika 1.
[709] Shih Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave, nenin 49, pika 1, gërmat (a), (b) dhe (e) dhe paragrafin 113 të Preambulës.
[710] *Ibid*., neni 49, pika 1.
[711] Grupi i Punës së Nenit 29 (2005), *Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995*, WP 114, Bruksel, 25 nëntor 2005.

Rregullores 45/2001, duke theksuar se kjo zgjidhje duhet përdorur në 'raste të kufizuara' dhe 'për transferime rastësore'.[712]

[BOX TYPE 2]

Shembull: një shoqëri shërbimesh, Global Distribution System (GDS), me seli në SHBA, ofron sistemin rezervimit në internet për shoqëri fluturimi, hotele dhe anije turistike nga e gjithë bota dhe përpunon të dhëna për dhjetëra miliona qytetarë të BE-së. Për transferimin fillestar të të dhënave tek serverët e saj në SHBA, shoqëria GDS mbështetet tek një nga përjashtimet, si bazë ligjore për transferimet, konkretisht nevojën për të lidhur një kontratë. Kështu, ajo nuk ofron asnjë garanci tjetër për të dhënat personale që e kanë origjinën nga Evropa, të cilat transferohen në SHBA dhe më pas shpërndahen sërish në hotelet anembanë botës (çka do të thotë se nuk ekzistojnë garanci as për transferimin e mëtejshëm). Shoqëria GDS nuk respekton kriteret e GDPR-së për transferimet ndërkombëtare të ligjshme të të dhënave, pasi ajo mbështetet tek përjashtimet si arsye të ligjshme për transferime masive.

BE-ja ose Shtetet Anëtare të saj, përveçse kur ekziston një vendim përshtatshmërie, mund të kufizojnë transferimin e kategorive të caktuara të të dhënave personale tek një vend i tretë, pavarësisht nëse ai përmbush kushtet e tjera për këto lloj transferimesh, për shembull për arsye të rëndësishme të interesit publik. Këto kufizime duhen konsideruar si përjashtimore dhe Shtetet Anëtare janë të detyruara t'ia bëjnë me dije Komisionit këto dispozita.[713]

E drejta e KiE-së lejon qarkullimet e të dhënave tek territore të cilat nuk kanë nivel të përshtatshëm mbrojtjeje të të dhënave në rastet kur:

- Subjekti i të dhënave ka dhënë pëlqimin;
- Interesat e subjektit të të dhënave e bëjnë të domosdoshëm një transferim të tillë;
- Ekzistojnë interesa legjitime prevaluese, sidomos interesa publike të rëndësishme të parashikuara me ligj;
- Transferimi përbën një masë të nevojshme dhe proporcionale në një shoqëri demokratike.[714]

7.3.4 Transferimet bazuar në marrëveshjet ndërkombëtare

BE-ja mund të lidhë marrëveshje ndërkombëtare me vende të treta, të cilat rregullojnë transferimin e të dhënave personale për qëllime specifike. Këto marrëveshje duhet të përmbajnë garancitë e përshtatshme për të siguruar mbrojtjen e të dhënave personale të personave të përfshirë. GDPR-ja nuk cënon këto marrëveshje ndërkombëtare.[715]

Shtetet Anëtare mund të lidhin gjithashtu marrëveshje ndërkombëtare me vende të treta, ose me organizata ndërkombëtare që parashikojnë nivel të përshtatshëm të mbrojtjes së të drejtave dhe lirive themelore të personave, në masën që këto marrëveshje nuk cënojnë zbatimin e GDPR-së.

Një rregull i ngjashëm përcaktohet në nenin 12, pika 3, gërma (a) të Konventës 108 të Modernizuar.

Shembuj të marrëveshjeve ndërkombëtare që përfshijnë transferimin e të dhënave personale janë marrëveshjet për regjistrin e emrave të pasagjerëve (PNR).

---

[712] Mbikëqyrësi Evropian i Mbrojtjes së të Dhënave, *The transfer of personal data to third countries and international organisations by EU institutions and bodies*, dokument qëndrimi, Bruksel, 14 korrik 2014, fq. 15.
[713] Shih Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave, nenin 49, pika 5.
[714] Konventa 108 e Modernizuar, neni 14, pika 4.
[715] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 102 i Preambulës.

Regjistri i Emrave të Pasagjerëve

Të dhënat e PNR-së mblidhen nga shoqëritë e udhëtimit ajror gjatë procesit të rezervimit të udhëtimit, ku përfshihen ndër të tjera, emrat, adresat, të dhënat e kartës së kreditit dhe numrat e ulëseve të pasagjerëve të udhëtimit ajror. Shoqëritë e udhëtimit ajror i mbledhin gjithashtu këto informacione për qëllimet e veta tregtare. BE-ja ka lidhur marrëveshje me disa vende të treta (Australinë, Kanadanë dhe SHBA-të) për transferimin e të dhënave të PNR-së për qëllime të parandalimit, zbulimit, hetimit dhe ndjekjes së veprave terroroste, apo krimeve të rënda transnacionale. Gjithashtu, Bashkimi ka miratuar Direktivën (BE) 2016/861 – të njohur si Direktiva BE-PNR[716] – në 2016-ën. Kjo direktivë përcakton një kuadër ligjor për Shtetet Anëtare të BE-së për të transferuar të dhënat e PNR-së tek autoritetet kompetente të vendeve të treta, njësoj për të parandaluar, zbuluar, hetuar apo ndjekur veprat terroriste dhe krimet e rënda. Transferimet e PNR-së tek autoritetet e vendeve të treta bëhen rast pas rasti dhe i nënshtrohen një vlerësimi individual për sa i përket domosdoshmërisë së transferimit kundrejt qëllimeve të specifikuara në direktivë dhe me kusht që të respektohen të drejtat themelore.

Për sa i përket marrëveshjeve për PNR-në që lidhen nga BE-ja me vendet e treta, përputhshmëria e tyre me të drejtat themelore për mbrojtjen e privatësisë dhe të dhënave, të garantuara nga Karta e të Drejtave Themelore të BE-së, është kundërshtuar. Kur, pasi zhvilloi negociatat me Kanadanë, BE-ja nënshkroi marrëveshjen për transferimin dhe përpunimin e të dhënave të PNR-së në 2014-ën, Parlamenti Evropian vendosi t'ia referonte çështjen GJDBE-së për të vlerësuar përputhshmërinë e marrëveshjes me të drejtën e BE-së dhe veçanërisht me nenet 7 dhe 8 të Kartës.

[BOX TYPE 1][SHËNIM PËR DIZAJNERIN: gjatë faqosjes, mos i ndaj kutitë, por formatoi si të gjitha kutitë e tjera me shembuj]

Shembull: tek Opinion i saj në lidhje me ligjshmërinë e marrëveshjes së PNR-së BE-Kanada,[717] GJDBE-ja u shpreh se në formën e saj aktuale, marrëveshja e parashikuar nuk ishte në përputhje me të drejtat themelore të njohura nga Karta dhe rrjedhimisht nuk mund të nënshkrohej. Duke qenë se ajo përfshinte përpunim të të dhënave personale, ajo ndërhynte në të drejtën për mbrojtje të të dhënave personale, të garantuar nga neni 8 i Kartës. Njëkohësisht, marrëveshja paraqiste po ashtu kufizim të së drejtës për respektim të jetës private, të sanksionuar në nenin 7, meqenëse të marra në tërësinë e tyre, të dhënat e PNR-së mund të kombinohen dhe analizohen në mënyrë të tillë që të zbulojnë zakonet në lidhje me udhëtimit, marrëdhëniet midis personave të ndryshëm, informacion në lidhje me gjendjen e tyre financiare, zakonet në lidhje me ushqyerjen dhe gjendjen shëndetësore, duke cënuar kësisoj jetët private të tyre.

Ndërhyrja tek të drejtat themelore që marrëveshja e parashikuar shkaktonte tek të drejtat themelore, ndiqte një objektiv në interesin publik, konkretisht sigurinë publike dhe luftën kundër terrorizmit dhe krimeve të rënda transnacionale. Gjithësesi, GJDBE-ja u shpreh se në mënyrë që ndërhyrja të jetë e justifikuar, duhet të jetë e kufizuar në atë çka është absolutisht e nevojshme për të arritur qëllimin e synuar. Pasi analizoi dispozitat e saj, GJDBE-ja doli në përfundimin se marrëveshja e parashikuar nuk e përmbushte kriterin 'nevojë absolute'. Ndër faktorët që GJDBE-ja mori parasysh për të arritur në atë përfundim ishin si vijon:

- Faktin që marrëveshja e parashikuar përfshinte transferimin e të dhënave sensitive. Të dhënat e PNR-së të mbledhura sipas marrëveshjes së parashikuar, mund të përfshinte të dhëna sensitive, sikurse informacion që zbulon origjinën racore ose etnike, besimet fetare, apo

[716] Direktiva (BE) 2016/681 e Parlamentit Evropian dhe e Këshillit e 27 prillit 2016 në lidhje me përdorimin e të dhënave të regjistrit të emrave të pasagjerëve (PNR) për parandalimin, zbulimin, hetimin dhe ndjekjen e veprave terroriste dhe krimeve të rënda, FZ 2016 L 119.
[717] GJDBE, *Opinioni 1/15 i Gjykatës (Dhoma e Madhe)*, 26 korrik 2017.

gjendjen shëndetësore të pasagjerit. Transferimi dhe përpunimi i të dhënave sensitive nga autoritetet kanadeze mund të paraqiste rrezik për parimin e mos-diskriminimit dhe kësisoj kërkonte përligjje të saktë dhe të fortë, bazuar në shkaqe të ndryshme nga ato të sigurisë publike dhe luftës kundër krimeve të rënda. Marrëveshja e parashikuar nuk përmbante një përligjje të tillë.[718]

- Mbajtja e pandërprerë e të dhënave të PNR-së të të gjithë pasagjerëve, për një periudhë pesëvjeçare, edhe pasi pasagjerët largoheshin nga Kanadaja, u konsiderua po ashtu si përtej kufirit të nevojës absolute. GJDBE-ja vlerësoi se do të ishte e lejueshme që autoritetet kanadeze të mbanin të dhënat e pasagjerëve, të cilët, në bazë të provave objektive, paraqisnin kërcënim për sigurinë publike, edhe pasi ato persona largoheshin nga Kanadaja. Përndryshe, mbajtja e të dhënave personale të të *gjithë* pasagjerëve, për të cilët nuk ka as prova të tërthorta se mund të paraqesin rrezik për sigurinë publike, ishte e pajustifikueshme.[719]

Komiteti Konsultativ i Konventës 108 ka nxjerrë një opinion në lidhje me ndërlikimet për mbrojtjen e të dhënave të marrëveshjeve për PNR-në në kuadër të së drejtës së KiE-së.[720]

Të dhënat e mesazheve

Shoqata Botërore e Telekomunikimit Ndër-bankar (SWIFT) me seli në Belgjikë, e cila përpunon pjesën më të madhe të transfertave botërore të parave nga bankat evropiane, operonte me një qendër 'binjake' në SHBA. Asaj iu paraqit një kërkesë për komunikim të dhënash nga Departamenti i Thesarit të SHBA-ve për qëllime të hetimit të terrorizmit, mbështetur në Programin e tij të Gjurmimit të Financimit të Terrorizmit.[721]

Në këndvështrimin e BE-së, nuk ekzistonte një bazë ligjore e mjaftueshme për t'ua komunikuar SHBA-ve këto të dhëna, të cilat lidheshin kryesisht me qytetarë të BE-së, thjesht për arsyen se një nga qendrat e përpunimit të të dhënave të SWIFT-it ndodhej në SHBA.

Një marrëveshje speciale u lidh në vitin 2010 midis BE-së dhe SHBA-së, e njohur si marrëveshja për SËIFT-in, me qëllim që të sigurohej baza e nevojshme ligjore dhe të garantoheshin standardet e përshtatshme të mbrojtjes së të dhënave.[722]

Sipas kësaj marrëveshjeje, të dhënat financiare që mban SËIFT-i vijojnë t'i komunikohen Departamentit të Thesarit të SHBA-ve për qëllime të parandalimit, hetimit, zbulimit ose ndjekjes së terrorizmit, apo financimit të terrorizmit. Departamenti i Thesarit të SHBA-ve mund të kërkojë të dhëna financiare nga SWIFT-i, në masën që kërkesa:

- Të identifikojë sa më qartë që të jetë e mundur të dhënat financiare të kërkuara;
- Të justifikojë qartë nevojën për këto të dhëna;

---

[718] *Ibid*., parag. 165.
[719] *Ibid*., parag. 204–207.
[720] Këshilli i Evropës, *Opinion në lidhje me ndërlikimet për mbrojtjen e të dhënave nga përpunimi i Regjistrit të Emrave të Pasagjerëve*, T-PD(2016)18rev, 19 gusht 2016.
[721] Shih në këtë kontekst: Grupi i Punës së Nenit 29 (2011), *Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing*, WP 186, Bruksel, 13 qershor 2011; Grupi i Punës së Nenit 29 (2006), *Opinion 10/2006 on the processing of personal data by the Society for worldwide Interbank Financial Telecommunications (SWIFT)*, WP 128, Bruksel, 22 nëntor 2006; Komisioni i Belgjikës për Mbrojtjen e Privatësisë (*Commission de la protection de la vie privée*) (2008), *'Control and recommendation procedure initiated with respect to the company SWIFT scrl'*, Vendim, 9 dhjetor 2008.
[722] Vendimi i Këshillit 2010/412/EU i 13 korrikut 2010 mbi lidhjen e Marrëveshjes midis Bashkimit Evropian dhe Shteteve të Bashkuara të Amerikës në lidhje me përpunimin dhe transferimin e të Dhënave të Mesazheve Financiare nga Bashkimi Evropian tek Shtetet e Bashkuara për qëllime të Programit të Gjurmimit Financiar të Terrorizmit, FZ 2010 L 195, fq. 3 dhe 4. Teksti i Marrëveshjes i bashkëlidhet këtij Vendimi, FZ 2010 L 195, fq. 5–14.

- Të jetë e përshtatur sa më shumë të jetë e mundur, me qëllim që të minimizohet sasia e të dhënave të kërkuara;
- Të mos kërkojë asnjë të dhënë që lidhet me Zonën Unike të Pagesave në Euro (SEPA).[723]

Europolit duhet t'i dërgohet një kopje të secilës kërkese të Departamentit të Thesarit të SHBA-ve dhe të verifikohet nëse janë respektuar parimet e Marrëveshjes për SWIFT-in.[724] Nëse konfirmohet që ato janë zbatuar, SWIFT-i duhet t'ia japë të dhënat financiare drejtpërdrejtë Departamentit të Thesarit të SHBA-ve. Departamenti duhet t'i ruajë të dhënat financiare në një mjedis fizik të sigurt, ku ato të mund të aksesohen vetëm nga analistët që hetojnë terrorizmin, ose financimin e tij dhe të dhënat financiare nuk duhet të ndërlidhen me asnjë bazë tjetër të dhënash. Përgjithësisht, të dhënat financiare të përftuara nga SWIFT-i duhen fshirë jo më vonë se pesë vite nga momenti i marrjes së tyre. Të dhënat financiare që janë me rëndësi për hetime, apo ndjekje penale të caktuara, mund të mbahen vetëm për aq kohë sa ato të dhëna janë me rëndësi për hetimet apo ndjekjet penale.

Departamenti i Thesarit të SHBA-ve mund të transferojë informacion nga të dhënat e marra prej SWIFT-it tek autoritete të caktuara të zbatimit të ligjit, sigurisë publike, apo kundër-terrorizmit, brenda ose jashtë SHBA-ve, ekskluzivisht për qëllime të hetimit, zbulimit, parandalimit apo ndjekjes së terrorizmit dhe financimit të tij. Kur transferimi i mëtejshëm i të dhënave financiare përfshin qytetarë, apo me persona me banim në një Shtet Anëtar, çdo shkëmbim të dhënash me autoritetet e një vendi të treta, i nënshtrohet miratimit paraprak nga autoritetet kompetente të Shtetit Anëtar të përfshirë. Mund të bëhen përjashtime kur shkëmbimi i të dhënave është thelbësor për parandalimin e një kërcënimi të menjëhershëm dhe të rëndë të sigurisë publike.

Mbikëqyrës të pavarur, ku përfshihet dhe një person i caktuar nga Komisioni Evropian, monitorojnë respektimin e parimeve të Marrëveshjes për SWIFT-in. Ata mund të shqyrtojnë në kohë reale dhe në mënyrë prapavepruese të gjitha kërkimet që u bëhen të dhënave të përftuara, të kërkojnë informacion shtesë për të justifikuar lidhjen e këtyre kërkimeve me terrorizmin dhe autoritetin për të bllokuar një pjesë, ose të gjitha kërkimet që duket se janë në shkelje të garancive të parashikuara në marrëveshje.

Subjektet e të dhënave kanë të drejtë të kërkojnë që autoritetet mbikëqyrëse të BE-së t'u konfirmojnë nëse janë respektuar të drejtat e tyre për mbrojtje të të dhënave personale. Subjektet e të dhënave kanë po ashtu të drejtën e korrigjimit, fshirjes, ose bllokimit të të dhënave të tyre, që janë mbledhur dhe mbahen nga Departamenti i Thesarit të SHBA-ve në kuadër të Marrëveshjes për SWIFT-in. Megjithatë, të drejtat e aksesit të subjekteve të të dhënave mund t'u nënshtrohen disa kufizimeve ligjore. Kur aksesi refuzohet, subjekti i të dhënave duhet informuar me shkrim për refuzimin dhe për të drejtën që të drejtën e ankimit administrative dhe gjyqësor në SHBA.

Marrëveshja për SWIFT-in është e vlefshme për pesë vite dhe peiudha e saj e parë e vlefshmërisë zgjati deri në gusht të 2015-ës. Ajo zgjatet automatikisht për periudha të mëtejshme njëvjeçare, përveçse nëse njëra nga palët njofton palën tjetër, të paktën gjashtë muaj përpara, se nuk dëshiron ta zgjasë marrëveshjen. Zgjatja automatike ka ndodhur në gusht të viteve 2015, 2016 dhe 2017 dhe siguron vlefshmërinë e Marrëveshjes për SWIFT-in deri të paktën në gusht të 2018-ës.[725]

[723] *Ibid*.; neni 4, pika 2.
[724] Organ i Përbashkët Mbikëqyrës i Europolit ka kryer auditime të aktiviteteve të Europolit në këtë fushë.
[725] *Ibid*.; neni 23, pika 2.

8 Mbrojtja e të dhënave në kontekstin e policise dhe drejtësisë penale

BE	Çështje të trajtuara	KiE
Direktiva e Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale	Në përgjithësi	Konventa 108 e Modernizuar
	Policia	Rekomandimi për Policinë Udhëzues praktik për përdorimin e të dhënave personale në sektorin e policisë GJEDNJ, *B.B. k. Francës*, nr. 5335/06, 2009 GJEDNJ, *S. dhe Marper k. Mbretërisë së Bashkuar* [ÇB], nr. 30562/04 dhe 30566/04, 2008 GJEDNJ, *Allan k. Mbretërisë së Bashkuar,* nr. 48539/99, 2002 GJEDNJ, *Malone k. Mbretërisë së Bashkuar*, nr. 8691/79, 1984 GJEDNJ, *Klass dhe të Tjerët k. Gjermanisë*, nr. 5029/71, 1978 GJEDNJ, *Szabó dhe Vissy k. Hungarisë*, nr. 37138/14, 2016 GJEDNJ, *Vetter k. Francës*, nr. 59842/00, 2005
	Mbikëqyrja	
	Krimi kibernetik	Konventa për Krimin Kibernetik
Intstrumente të tjera ligjore specifike		

Vendimi Prüm	Për të dhëna të veçanta: gjurmë gishtash, ADN, huliganizëm, informacion i pasagjerëve të transportit ajror, të dhëna të telekomunikacioneve, etj.	Konventa 108 e Modernizuar, neni 6 Rekomandimi për Policinë, Udhëzues praktik për përdorimin e të dhënave personale në sektorin e policisë
Iniciativa Suedeze (Vendimi Kuadër i Këshillit 2006/960/JHA)	Thjeshtimi i shkëmbimit të informacionit dhe të dhënave hetimore midis autoriteteve ligjzbatuese	GJEDNJ, *S. dhe Marper k.Mbretërisë së Bashkuar* [ÇB], nr. 30562/04 dhe 30566/04, 2008
Direktiva (BE) 2016/681 mbi përdorimin e të dhënave të regjistrit të emrave të pasagjerëve (PNR) për parandalimin, zbulimin, hetimin dhe ndjekjen e veprave terroriste dhe krimeve të rënda GJDBE, Çështje të bashkuara C-293/12 dhe C-594/12, *Digital Rights Ireland* dhe *Kärntner Landesregierung dhe të Tjerët* [ÇB], 2014 GJDBE, Çështje të bashkuara C-203/15 dhe C-698/15, *Tele2 Sverige* dhe *Home Department k. Tom Ëatson dhe të Tjerët* [ÇB], 2016	Mbajtja e të dhënave personale	GJEDNJ, *B.B. k. Francës*, nr. 5335/06, 2009
Europol Regulation Vendimi për Eurojust-in	Nga agjencitë speciale	Rekomandimi për Policinë
Vendimi Schengen II Rregullorja VIS Rregullorja Eurodac Vendimi CIS	Nga sistemet speciale të përbashkëta të informacionit	Rekomandimi për Policinë GJEDNJ, *Dalea k. Francës,* nr. 964/07, 2010

Për të ekuilibruar interesat e personale për mbrojtjen e të dhënave dhe interesat e shoqërisë për të mbledhur të dhëna, për qëllime të luftës kundër krimit dhe garantimit të sigurisë kombëtare dhe publike, KiE-ja dhe BE-ja kanë miratuar instrumente specifike ligjore. Ky kapitull ofron një vështrim të përgjithshëm të së drejtës së KiE-së (seksioni 8.1) dhe BE-së (seksioni 8.2) në lidhje me mbrojtjen e të dhënave në fushën e policisë dhe drejtësisë penale.

8.1. E drejta e KiE-së në fushën e mbrojtjes së të dhënave në lidhje me çështje të sigurisë kombëtare, policisë dhe drejtësisë penale

Pikat kryesire

- Konventa 108 e Modernizuar dhe Rekomandimi i KiE-së për Policinë zbatohen për mbrojtjen e të dhënave në të gjitha fushat e aktivitetit policor.
- Konventa e Krimit Kibernetik (Konventa e Budapestit) është një instrument ligjor detyrues ndërkombëtar që ka për objekt krimet e kryera ndaj dhe me anë të rrjeteve elektronike. Ajo ka rëndësi po ashtu edhe për hetimin e krimeve jo kibernetike, që përfshijnë prova elektronike.

Një ndryshim i rëndësishëm midis së drejtës së KiE-së me atë të BE-së është se **e drejta e KiE-së**, ndryshe nga e drejta e BE-së, zbatohet edhe në fushën e sigurisë kombëgtare. Kjo nënkupton se Palët Kontraktuese duhet të respektojnë kufijtë e nenit 8 të KENJ-së edhe për aktivitetet që lidhen me sigurinë kombëtare. Shumë vendime të GJEDNJ-së kanë të bëjnë me akvitietet shtetërore në fushat sensitive të së drejtës dhe praktikave të sigurisë kombëtare.[726]

Për sa i përket policisë dhe drejtësisë penale, në nivel evropian, Konventa 108 e Modernizuar mbulon të gjitha fushat e përpunimit të të dhënave personale dhe dispozitat e saj kanë si qëllim të rregullojnë përpunimin e të dhënave në përgjithësi. Për rrjedhojë, Konventa 108 e Modernizuar zbatohet për mbrojtjen e të dhënave në fushën e policisë dhe drejtësisë penale. Përpunimi i të dhënave gjenetike, të dhënave personale në lidhje me veprat penale, procedimet penale, dënimet dhe çdo masë tjetër sigurie që lidhet me to, të dhënat biometrike që identifikojnë një person në mënyrë unike, si dhe çdo e dhënë personale sensitive, lejohet vetëm me kusht që të ekzistojnë garancitë e përshtatshme kundës risqeve që ky përpunim të dhënash mund të shkaktojë për interesat, të drejtat dhe liritë themelore të subjektit të të dhënave, veçanërisht rrezikut të diskriminimit.[727]

Misioni ligjor i autoriteteve policore dhe të drejtësisë penale nevojit shpesh përpunimin e të dhënave personale, i cili mund të sjellë pasoja të rënda për personat e përfshirë. Rekomandimi për Policinë, i miratuar nga KiE-ja në vitin 1987 përmban udhëzime për shtetet anëtare në lidhje me mënyrën se si të zbatojnë parimet e Konventës 108 në kontekstin e përpunimit të të dhënave personale nga ana e autoriteteve policore.[728] Rekomandimi u plotësua edhe me një udhëzues praktik për përdorimin e të dhënave personale në sektorin e policisë, miratuar nga Komiteti Konsultativ i Konventës 108.[729]

[BOX TYPE 1]

Shembull: tek çështja *D.L. k. Bullgarisë*,[730] shërbimet sociale e vendosën kërkuesen në një institucion edukimi sipas një urdhri gjykate. E gjithë korrespondenca e shkruar dhe bisedat telefonike i ishin nënshtruar një përgjimi të përgjithshëm dhe sistematik nga ana e institucionit. GJEDNJ-ja doli në

[726] Shih për shembull, GJEDNJ, *Klass dhe të Tjerët k. Gjermanisë*, nr. 5029/71, 6 shtator 1978; GJEDNJ, *Rotaru k. Rumanisë* [ÇB], nr. 28341/95, 4 maj 2000 dhe GJEDNJ, *Szabó dhe Vissy k. Hungarisë*, nr. 37138/14, 12 janar 2016.
[727] Konventa 108 e Modernizuar, neni 6.
[728] Këshilli i Evropës, Komitetit i Ministrave (1987), Rekomandimi Rec(87)15 për shtetet anëtare që rregullon përdorimin e të dhënave personale në sektorin e policisë, 17 shtator 1987.
[729] Këshilli i Evropës (2018), Komiteti Konsultativ i Konventës 108, Udhëzues praktik për përdorimin e të dhënave personale në sektorin e policisë, T-PD(2018)1.
[730] GJEDNJ, *D.L. k. Bullgarisë*, nr. 7472/14, 19 maj 2016.

përfundimin se neni 8 ishte shkelur, duke qenë se masa në fjalë nuk ishte e nevojshme në një shoqëri demokratike. Gjykata u shpreh se duhej bërë gjithçka e mundur që të miturit e vendosur në një institucion, të kishin kontakte të mjaftueshme me botën e jashtme, pasi diçka e tillë ishte pjesë përbërëse e së drejtës së tyre për t'u trajtuar me dinjitet dhe absolutisht thelbësore për t'i përgatitur për t'u integruar sërish në shoqëri. Kjo vlente sa për vizitat, po aq edhe për korrespondencën e shkruar, apo bisedat telefonike. Gjithashtu, përgjimi bëhej njësoj si për komunikimet me anëtarët e familjes, ashtu edhe për OJQ-të që përfaqësojnë të drejtat e fëmijëve, apo avokatëve. Për më tepër, vendimi për të përgjuar komunikimet nuk bazohej në një analizë individuale të risqeve në secilin rast konkret.

Shembull: tek çështja *Dragojević k. Kroacisë*,[731] kërkuesi ishte i dyshuar si i përfshirë në trafik droge. Ai ishte shpallur fajtor pasi një gjyqtar-hetues kishte autorizuar përdorimin e masave të përgjimit të fshehtë, për të interceptuar telefonatat e kërkuesit. GJEDNJ-ja doli në përfundimin se kjo masë, ndaj së cilës ishte bërë ankesë, përbënte ndërhyrje në të drejtën për respektim të jetës private dhe korrespondencës. Autorizimi i dhënë nga gjyqtari-hetues bazohej thjesht në pohimin e autoritetit të ndjekjes penale se "hetimi nuk mund të kryhej me mjete të tjera". GJEDNJ-ja theksoi gjithashtu se gjykatat penale kishin kufizuar vlerësimin e tyre në lidhje me përdorimin e masave të përgjimit dhe se qeveria nuk kishte bërë me dije se cilat ishin mjetet ligjore të disponueshme. Për pasojë, ishte shkelur neni 8.

8.1.1. Rekomandimi për policinë

GJEDNJ-ja është shprehur në mënyrë sistematike se regjistrimi dhe mbajtja e të dhënave nga ana e policisë, apo e autoriteteve të sigurisë kombëtare, përbën ndërhyrje në nenin 8, pika 1 të KEDNJ-së. Shumë vendime të GJEDNJ-së trajtojnë justifikimin e një ndërhyrjeje të tillë.[732]

[BOX TYPE 1]

Shembull: tek çështja *B.B. k. Francës*,[733] kërkuesi ishte dënuar dënuar për krime seksuale duke shpërdoruar detyrën ndaj të miturve në moshë pesëmbëdhjetë vjeç. Ai e kreu dënimin me burgim në vitin 2000. Një vit më vonë, ai kërkoi fshirjen e këtij dënimi nga dosja e gjendjes gjyqësore, por kërkesa ishte refuzuar. Në vitin 2004, një ligj francez përcaktonte krijimin e bazës kombëtare të të dhënave gjyqësore të të dënuarve për krime seksuale dhe kërkuesi ishte informuar për përfshirjen e tij në të. GJEDNJ-ja u shpreh se përfshirja e një të dënuari për krime seksuale në një bazë kombëtare të të dhënave gjyqësore, hynte në fushën e zbatimit të nenit 8 të KEDNJ-së. Megjithatë, duke qenë se ishin zbatuar masat e duhura për mbrojtjen e të dhënave, sikurse e drejta e subjektit të të dhënave për të kërkuar fshirjen e të dhënave, kohëzgjatja e kufizuar e mbajtjes së të dhënave dhe kufizimi i aksesit tek këto të dhëna, ishin ekuilibruar drejt interesat e kundërta private me ato publike. Gjykata doli në përfundimin se nuk kishte pasur shkelje të nenit 8 të KEDNJ-së.

Shembull: tek çështja *S. dhe Marper k. Mbretërisë së Bashkuar*,[734] dy kërkuesit ishin akuzuar, por nuk ishin dënuar, për vepra penale. Pavarësisht kësaj, gjurmët e tyre të gishtave, kampionët qelizorë dhe profilet e tyre të ADN-së ishin regjistruar dhe vijon të mbaheshin nga policia. Mbajtja e pakufizuar në kohë e të dhënave biometrike të sipërpërmendura parashikohej me ligj, për rastet kur një person dyshohej për kryerjen e një vepre penale, pavarësisht nëse i dyshuari ishte shpallur i pafajshëm, apo

[731] GJEDNJ, *Dragojević k. Kroacisë*, nr. 68955/11, 15 janar 2015.
[732] Shih, për shembull, GJEDNJ, *Leander k. Suedisë*, nr. 9248/81, 26 mars 1987; GJEDNJ, *M.M. k. Mbretërisë së Bashkuar*, nr. 24029/07, 13 nëntor 2012; GJEDNJ, *M.K. k. Francës*, nr. 19522/09, 18 prill 2013, ose GJEDNJ, *Aycaguer k. Francës*, nr. 8806/12, 22 qershor 2017.
[733] GJEDNJ, *B.B. k. Francës*, nr. 5335/06, 17 dhjetor 2009.
[734] GJEDNJ, *S. dhe Marper k. Mbretërisë së Bashkuar* [ÇB], nr. 30562/04 dhe 30566/04, 4 dhjetor 2008, paragrafët 119 dhe 125.

kishte pushuar hetimi. GJEDNJA-ja u shpreh se mbajtja pa dallim dhe sistematike e të dhënave personale, pa afate kohore dhe kur personat që nuk ishin shpallur fajtorë kishin mundësi minimale për të kërkuar fshirjen e tyre, përbënte ndërhyrje të shpërpjesëtuar tek e drejta e kërkuesve për respektim të jetës private. Gjykata doli në përfundimin se kishte pasur shkelje të nenit 8 të KEDNJ-së.

Në kontekstin e komunikimeve elektronike, një çështje me rëndësi thelbësore është ndërhyrja nga autoritetet publike tek të drejtat për privatësi dhe mbrojtje të të dhënave. Përdorimi i mjeteve të përgjimit, ose të interceptimit të komunikimeve, sikurse pajisjet e përgjimeve telefonike, lejohet vetëm nëse parashikohet me ligj dhe nëse përbën një masë të nevojshme në një shoqëri demokratike, për interesa të tilla si:

- Mbrojtja e sigurisë shtetërore;
- Siguria publike;
- Interesat financiare të shtetit;
- Lufta kundër krimit; ose
- Mbrojtja e subjektit të të dhënave, ose e të drejtave dhe lirive të të tjerëve.

Shumë vendime të tjera të GJEDNJ-së kanë si objekt justifikimin e ndërhyrjes tek e drejta për privatësi të kryer nëpërmjet përgjimit.

[BOX TYPE 1]

Shembull: tek çështja *Allan k. Mbretërisë së Bashkuar*,[735] autoritetet regjistruan në mënyrë të fshehtë bisedat private të një të dënuari me mikun e tij, në zonën e vizitave të burgut dhe me një të bashkëakuzuar në një qeli të burgut. GJEDNJ-ja vlerësoi se përdorimi i pajisjeve të regjistrimit audio dhe video në qelinë e kërkuesit, në zonën e vizitave të burgut dhe për një bashkëvuajtës, përbënte ndërhyrje në jetën private të kërkuesit. Meqenëse në atë kohë, nuk ekzistonte asnjë system normativ për përdorimin e pajisjeve të fshehta të regjistrimit, një ndërhyrje e tillë nuk ishte e parashikuar me ligj. Gjykata doli në përfundimin se kishte pasur shkelje të nenit 8 të KEDNJ-së.

Shembull: tek çështja *Roman Zakharov k. Rusisë*,[736] kërkuesi bëri ankim gjyqësor kundër tre operatorëve të telefonisë celulare. Ai pretendonte se ishte shkelur e drejta e tij për privatësi të komunikimeve telefonike, meqenëse operatorët kishin instaluar pajisje që i mundësonin Shërbimit Federal të Sigurisë të interceptonte komunikimet e tij telefonike, pa miratimin paraprak të autoriteteve gjyqësore. GJEDNJ-ja vlerësoi se dispozitat e brendshme ligjore që rregullonin interceptimin e komunikimeve, nuk ofronin garanci të përshtatshme dhe të efektshme mbrojtjeje ndaj arbitraritetit dhe rrezikut të abuzimit. Në mënyrë të veçantë, e drejta kombëtare nuk përcaktonte detyrimin për fshirjen e të dhënave të regjistruara pasi përmbushej qëllimi për mbajtjen e tyre. Gjithashtu, pavarësisht se kërkohej autorizim gjyqësor, kontrolli gjyqësor ishte i kufizuar.

Shembull: tek çështja *Szabó dhe Vissy k. Hungarisë*,[737] kërkuesit pretendonin se legjislacioni hungarez shkelte nenin 8 të KEDNJ-së, pasi nuk përmbante hollësitë dhe saktësinë e duhur. Gjithashtu, pretendohej se legjislacioni nuk ofronte garancitë e mjaftueshme të mbrojtjes ndaj abuzimit dhe arbitraritetit. GJEDNJ-ja vlerësoi se legjislacioni hungarez nuk përcaktonte kriterin që mbikëqyrja t'i nënshtrohej autorizimit nga gjykata. Gjykata vërejti se pavarësisht se mbikëqyrja ishte subjekt miratimi nga Ministria e Drejtësisë, ajo kishte karakter qartësisht politik, si dhe nuk garantonte që të kryhej vlerësimi i duhur i 'nevojës absolute'. Për më tepër, e drejta kombëtare nuk parashikonte kontroll

[735] GJEDNJ, *Allan k. Mbretërisë së Bashkuar,* nr. 48539/99, 5 nëntor 2002.
[736] GJEDNJ, *Roman Zakharov k. Rusisë*, nr. 47143/06, 4 dhjetor 2015.
[737] GJEDNJ, *Szabó dhe Vissy k. Hungarisë*, nr. 37138/14, 12 janar 2016.

gjyqësor, meqenëse subjekteve nuk u ishte dërguar asnjë njoftim. Gjykata vendosi se kishte pasur shkelje të nenit 8 të KEDNJ-së.

Për shkak se përpunimi i të dhënave nga autoritetet policore mund të ketë ndikim domethënës tek personat e përfshirë, rregullat e hollësishme të mbrojtjes së të dhënave për përpunimin e të dhënave personale në këtë fushë, marrin rëndësi të veçantë. Rekomandimi i KiE-së për Policinë synon të zgjidhë këtë problematikë, nëpërmjet udhëzimeve për mënyrën se si duhen mbledhur të dhënat personale për qëllime të aktivitetit policor, si duhen mbajtur dosjet e të dhënave në këtë fushë, kush duhet lejuar të ketë akses në këto dosje, si dhe kushtet për transferimin e të dhënave personale në autoritetet policore të huaja, mënyrën se si subjektet e të dhënave mund të ushtrojnë të drejtat e tyre për mbrojtje të të dhënave dhe si duhet kryer kontrolli nga ana e autoriteteve të pavarura. Ai trajton gjithashtu kriterin për të garantuar siguri të përshtatshme të të dhënave.

Rekomandimi nuk parashikon mbledhje të hapur dhe të përgjithshme të të dhënave personale nga ana e autoriteteve policore. Ai kufizon mbledhjen e të dhënave personale nga autoritetet policore vetëm për nevoja të parandalimit të një rreziku real, apo për ndjekjen e një vepre penale specifike. Çdo mbledhje tjetër të dhënash duhet të mbështetet në legjislacionin specifik kombëtar. Përpunimi i të dhënave sensitive duhet të kufizohet vetëm tek ajo çka është absolutisht e nevojshme në kontekstin e një hetimi të caktuar.

Kur të dhënat personale mblidhen pa dijeninë e subjektit të të dhënave, ky i fundit duhet informuar për këtë mbledhje të dhënash menjëherë sapo kjo përhapje të dhënash nuk cënon më hetimin. Mbledhje e të dhënave nëpërmjet mbikëqyrjes teknike, apo mjeteve të tjera automatike, duhet të mbështetet tek një bazë ligjore konkrete.

[BOX TYPE 1]

Shembull: tek çështja *Versini-Campinchi dhe Crasnianski k. Francës,*[738] kërkuesja, e cila ishte avokate, kishte kryer një bisedë telefonike me një klient, linja e telefonit të të cilit përgjohej me kërkesë të gjyqtarit-hetues. Nga transkriptimi i bisedës u pa se ajo kishte përhapur informacion që mbrohej nga sekreti profesional ligjor. Prokurori ia dërgoi këtë informacion Këshillit të Dhomës së Avokatisë, i cili i vendosi kërkueses një sanksion. GJEDNJ-ja pranoi se kishte pasur një ndërhyrje tek e drejta për respektim të jetës private dhe korrespondencës, jo vetëm të personit, telefoni i së cilit ishte përgjuar, por edhe të kërkueses, komunikimet e së cilës ishin interceptuar dhe transkriptuar. Ndërhyrja ishte bërë në përputhje me ligjin dhe synonte objektivin legjitim të mbrojtjes së rendit. Për kërkuesen ishte bërë e mundur kryerja e një verifikimi të ligjshmërisë së depozimit të transkriptit të regjistrimeve telefonike, në konteksin e procedimit disiplinor të zhvilluar kundër saj. Paçka se asaj nuk i ishte pranuar kërkesa për anulimin e transkriptimit të bisedës telefonike, GJEDNJ-ja vlerësoi se kishte pasur kontroll efikas, që mund të kufizonte ndërhyrjen e pretenduar në atë çka është e nevojshme në një shoqëri demokratike. GJEDNJ-ja doli në përfundimin se mundësia që një hetim penal kundër një avokati, bazuar në atë transkriptim, mund të kishte pasojë negative në lirinë e komunikimit midis një avokati dhe klientit të tij, apo të saj dhe rrjedhimisht tek mbrojtja e këtij të fundit, nuk ishte e besueshme, në masën që përhapja e të dhënave nga vetë avokatja përbënte sjellje të paligjshme nga ana e saj. Për rrjedhojë, Gjykata nuk gjeti shkelje të nenit 8.

Rekomandimi i KiE-së për Policinë parashikon se, kur regjistrohen të dhëna personale, duhet bërë dallim i qartë midis: të dhënave administrative dhe të dhënave policore, të dhënave personale të llojeve të ndryshme të subjekteve të të dhënave, sikurse të dyshuarve, të dënuarve, viktimave dhe dëshmitarëve, si dhe të dhënave të konsideruara si fakte të provuara, me ato të mbështetura në dyshime, ose spekullime.

[738] GJEDNJ, *Versini-Campinchi dhe Crasnianski k. Francës*, nr. 49176/11, 16 qershor 2016.

Qëllimi i përdorimit të të dhënave policore duhet të jetë rreptësisht i kufizuar. Përhapja e të dhënave policore tek palë të treta ka pasoja: transferimi, apo komunikimi i këtyre të dhënave në sektorin e policisë duhet të varet nga çështja nëse ekziston interes legjitim për shkëmbimin e informacionit. Transferimi, apo komunikimi i këtyre të dhënave jashtë sektorit të policisë, duhet të lejohet vetëm kur ekziston një detyrim, apo autorizim ligjor i qartë.

[BOX TYPE 1]

Shembull: tek çështja *Karabeyoğlu k. Turqisë*,[739] kërkuesit, i cili ishte gjyqtar, i ishin përgjuar linjat telefonike në kontekstin e hetimit penal të një organizate të paligjshme, së cilës ai dyshohej se i përkiste, apo që mendohej se i jepte ndihmë dhe mbështetje. Pasi mori vendimin për pushimin e çështjes, prokurori publik i ngarkuar për këtë hetim penal, shkatërroi regjistrimet në fjalë. Megjithatë, një kopje e tyre mbeti tek hetuesit gjyqësorë, të cilët e përdorën më pas materialin në kuadër të një hetimi disiplinor kundër kërkuesit. GJEDNJ-ja vlerësoi se legjislacioni përkatës ishte shkelur, pasi informacioni ishte përdorur për qëllime të ndryshme nga ato për të cilat ishte mbledhur dhe nuk ishte shkatërruar brenda afatit kohor të përcaktuar me ligj. Ndërhyrja tek e drejta e kërkuesit për respektim të jetës së tij private, nuk ishte në përputhje me ligjin, për sa i përkiste procedimit disiplinor të zhvilluar kundër tij.

Transferimi, apo komunikimi në nivel ndërkombëtar duhet të kufizohet vetëm tek autoritetet policore të huaja dhe të bazohet në dispozita ligjore specifike, përveçse kur është e nevojshme për parandalimin e një rreziku të rëndë dhe të menjëhershëm.

Përpunimi i të dhënave nga ana e policisë duht t'i nënshtrohet mbikëqyrjes së pavarur, për të garantuar që është në përputhje me të drejtën e brendshme të mbrojtjes së të dhënave. Subjektet e të dhënave duhet të gëzojnë të gjitha të drejtat e aksesit, të parashikuara nga Konventa 108 e Modernizuar. Kur të drejtat e aksesit të subjekteve të të dhënave janë kufizuar sipas nenit 9 të Konventës 108, në interes të efikasitetit të hetimeve policore dhe ekzekutimit të dënimeve penale, subjektit të të dhënave duhet t'i njihet nga legjislacioni i brendshëm, e drejta për t'u ankuar tek autoriteti kombëtar mbikëqyrës i mbrojtjes së të dhënave, ose tek një organ tjetër i pavarur.

8.1.2. Konventa e Budapestit mbi Krimin Kibernetik

Duke ditur se aktivitetet kriminale përdorin e shtrihen gjithnjë e më shumë tek sistemet elektronike të përpunimit të të dhënave, nevojiten dispozita të reja penale për t'u përballur me këtë sfidë. Për këtë, KiE-ja ka miratuar një instrument ligjor ndërkombëtar, Konventën mbi Krimin Kibernetik, e cila njihet po ashtu si Konventa e Budapestit, për t'iu përgjigjur problematikës së krimeve të kryera kundër dhe me anë të rrjeteve elektronike.[740] Kjo konventë është e hapur për anëtarësim gjithashtu edhe për shtetet jo-anëtare të KiE-së. Në fillim të vitit 2018, 14 shtete jo-anëtare të KiE-së[741] kishin aderuar në konventë dhe shtatë shtete të tjera jo-anëtare ishin ftuar të aderonin.

Konventa mbi Krimin Kibernetik mbetet traktati ndërkombëtar me ndikimin më të madh, i cili trajton shkeljet ligjore që bëhen në internet, apo në rrjetet e tjera të informacionit. Ajo detyron palët të përditësojnë dhe të harmonizojnë të drejtën e tyre penale kundër piratimit dhe shkeljeve të tjera të sigurisë, përfshirë shkeljet e së drejtës së autorit, mashtrimit kompjuterik, pornografisë me të mitur dhe aktiviteteve të tjera kibernetike të paligjshme. Konventa parashikon gjithashtu kompetenca të tjera procedurale, që përfshijnë kontrollin e rrjeteve kompjuterike dhe interceptimin e komunikimeve, në kuadër të luftës kundës krimit kibernetik. Së fundi, ajo mundëson bashkëpunim ndërkombëtar efikas.

[739] GJEDNJ, *Karabeyoğlu k. Turqisë*, nr. 30083/10, 7 qershor 2016.
[740] Këshilli i Evropës, Komitetit i Ministrave (2001), Konventa mbi Krimin Kibernetik, CETS nr. 185, Budapest, 23 nëntor 2001, hyrë në fuqi më 1 korrik 2004.
[741] Australia, Kanadaja, Kili, Kolumbia, Republika Domenikane, Izraeli, Japonia, Morisi, Panamaja, Senegale, Sri Lanka, Tonga, Tunizia dhe Shtetet e Bashkuara. Shih Tabelën e nënshkrimeve dhe ratifikimeve të Traktatit 185, statusin e tyre që nga korriku 2017.

Një protokoll shtesë i konventës trajton kriminalizimin e propagandës raciste dhe ksenofobike në rrjetet kompjuterike.

Paçka që konventa nuk është një instrument që synon promovimin e mbrojtjes së të dhënave, ajo kriminalizon aktivitete që mund të shkelin të drejtën e subjektit të të dhënave për mbrojtjen e të dhënave të tij apo të saj. Gjithashtu, ajo kërkon nga Palët Kontraktuese që të miratojnë masa legjislative, për t'u mundësuar autoriteteve të tyre kombëtare të interceptojnë të dhëna të trafikut dhe përmbajtësore.[742] Ajo detyron gjithashtu Palët Kontraktuese që, kur zbatojnë konventën, të parashikojnë mbrojtje të përshtatshme të të drejtave dhe lirive të njeriut, përfshirë ato të garantuara nga KEDNJ-ja, sikurse të drejtën për mbrojtje të të dhënave.[743] Palët kontraktuese nuk janë të detyruara të aderojnë edhe në Konventën 108 për t'u anëtarësuar në Konventën e budapestit për Krimin Kibernetik.

8.2. E drejta e BE-së në fushën e mbrojtjes së të dhënave në lidhje me policinë dhe drejtësinë penale

Pikat kryesore

- Në BE, mbrojtja e të dhënave në sektorin e policisë dhe të drejtësisë penale, rregullohet si në kontekstin e përpunimit kombëtar, ashtu edhe atë ndërkufitar që kryejnë autoritetet policore dhe të drejtësisë penale të Shteteve Anëtare dhe të aktorëve të BE-së.
- Në nivel Shteti Anëtar, Direktiva e Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale duhet integruar në të drejtën kombëtare.
- Mbrojtja e të dhënave në fushën e bashkëpunimit ndërkombëtar nga ana e policisë dhe agjencive ligjzbatuese, sidomos për luftën kundër terrorizmit dhe krimit ndërkufitar, rregullohet me intrumente specifike ligjore.
- Ekzistojnë rregulla speciale për mbrojtjen e të dhënave në lidhje me Zyrën Policore Evropiane (Europol-i), Njësinë e Bashkëpunimit Gjyqësore të BE-së (Eurojust-i), dhe Zyrës së krijuar së fundmi të Prokurorit Publik Evropian, që janë organe të BE-së, të cilat mbështesin dhe promovojnë aktivitetin ligjzbatues ndërkufitar.
- Ekzistojnë po ashtu rregulla speciale për mbrojtjen e të dhënave për sistemet e përbashkëta të informacionit, të cilat janë krijuar në nivel BE-je, me qëllim shkëmbimin e informacionit ndërkufitar midis autoriteteve kompetente policore dhe gjyqësore. Shembuj me rëndësi janë Sistemi i Informacionit Schengen II (SIS II), Sistemi i Informacionit të Vizave (VIS) dhe Eurodac-u, i cili është një system i përqendruar për mbajtjen e të dhënave të gjurmëve të gishtave të shtetasve të vendeve të treta dhe personave pa shtetësi, të cilët aplikojnë për azil në një nga Shtetet Anëtare të BE-së.
- BE-ja është duke përditësuar dispozitat e mbrojtjes së të dhënave të përmendura më lart, me qëllim harmonizimin me dispozitat e Direktivës së Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale.

8.2.1. Direktiva e Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale

Direktiva (BE) 2016/680 për mbrojtjen e personave fizikë në lidhje me përpunimit e të dhënave personale nga autoritetet kompetente, për qëllime të parandalimit, hetimit, zbulimit, ose ndjekjes së veprave penale, apo ekzekutimit të dënimeve penale dhe për lëvizjen e lirë të këtyre të dhënave

[742] Këshilli i Evropës, Komiteti i Ministrave (2001), Konventa mbi Krimin Kibernetik, CETS nr. 185, Budapest, 23 nëntor 2001, nenet 20 dhe 21.
[743] *Ibid.,* neni 15, pika 1.

(Direktiva e Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale)[744] ka për objektiv të mbrojë të dhënat personale, të mbledhura dhe të përpunuara për qëllime të drejtësisë penale, sikurse:

- Për parandalimin, hetimin, zbulimin, ose ndjekjen e veprave penale, apo për ekzekutimin e dënimeve penale, përfshirë edhe masat kundër dhe për parandalimin e kërcënimeve ndaj sigurisë publike;
- Për ekzekutimin e një dënimi penal; dhe
- Në rastet kur policia, apo autoritetet e tjera ligjzbatuese veprojnë për të zbatuar ligjin dhe për të mbrojtur dhe parandaluar kërcënimet ndaj sigurisë publike dhe të drejtave themelore të shoqërisë, të cilat mund të përbëjnë vepër penale.

Direktiva e Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale mbron të drejtat personale të kategorive të ndryshme të personave të përfshirë në procedime penale, sikurse janë dëshmitarët, informatorët, viktimat, të dyshuarit dhe bashkëpunëtorët. Autoritetet policore dhe ato të drejtësisë penale janë të detyruara të respektojnë dispozitat e direktivës sa herë që përpunojnë të dhëna personale për qëllime të zbatimit të ligjit, që përfshihen në fushën e zbatimit personal dhe lëndor të direktivës.[745]

Gjithsesi, përdorimi i të dhënave për një qëllim të ndryshëm, lejohet gjithashtu me disa kushte të caktuara. Përpunimi i të dhënave për një qëllim ligjzbatimi të ndryshëm nga ai për të cilat ato janë mbledhur më parë, lejohet vetëm në masën që të jetë i ligjshëm, i nevojshëm dhe proporcional sipas së drejtës kombëtare, apo asaj të BE-së.[746] Për qëllime të tjera, zbatohen normat e Rregullores së Përgjithshme të Mbrojtjes së të Dhënave. Regjistrimi dhe dokumentimi i shkëmbimit të të dhënave është një nga detyrat specifike të autoriteteve kompetente, për të ndihmuar me qartësimin e përgjegjësive që burojnë nga ankesat.

Autoritetet kompetente që punojnë në fushën e policisë dhe drejtësisë penale janë autoritete publike, ose autoritete të cilave e drejta kombëtare dhe autoriteti publik u ka besuar kryerjen e disa funksioneve publike,[747] p.sh. burgjet private.[748] Zbatueshmëria e direktivës shtrihet si tek përpunimi i të dhënave në nivel kombëtar, ashtu edhe tek përpunimi ndërkufitar midis autoriteteve policore dhe gjyqësore të Shteteve Anëtare, si dhe tek transferimet ndërkombëtare nga ana ana e autoriteteve kompetente drejt vendeve të treta dhe organizatave ndërkombëtare.[749] Ajo nuk mbulon sigurinë kombëtare, ose përpunimin e të dhënave personale nga institucionet, organet, zyrat dhe agjencitë e BE-së.[750]

Në një masë të madhe, direktiva mbështetet tek parimet dhe përkufizimet e Rregullores së Përgjithshme të Mbrojtjes së të Dhënave, nga këndvështrimi i natyrës së veçantë të fushave të policisë dhe të drejtësisë penale. Mbikëqyrja mund të bëhet nga autoritetet e të njëjtit Shtet Anëtar që e ushtron atë edhe sipas Rregullores së Përgjithshme të Mbrojtjes së të Dhënave. Caktimi i Nëpunësve të Mbrojtjes së të Dhënave dhe kryerja e Vlerësimeve të Ndikimit tek Mbrojtja e të Dhënave janë integruar në direktivë si detyrime të reja për autoritetet policore dhe të drejtësisë penale.[751] Megjithëse këto koncepte janë frymëzuar nga Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, direktiva i trajton nga këndvështrimi i veçantë i autoriteteve policore dhe të drejtësisë penale. Krahasuar me përpunimin e të

[744] Direktiva 2016/680/BE e Parlamentit Evropian dhe e Këshillit e 27 prillit 2016, për mbrojtjen e personave fizikë në lidhje me përpunimin e të dhënave personale nga autoritetet kompetente, për qëllime të parandalimit, hetimit, zbulimit, ose ndjekjes së veprave penale, apo për ekzekutimin e dënimeve penale dhe për lëvizjen e lirë të këtyre të dhënave dhe që shfuqizon Vendimin Kuadër të Këshillit 2008/977/JHA, FZ 2016 L 119, fq. 89 (Direktiva e Mbrojtjes së të Dhënave për Autoritetet e Policisë dhe të Drejtësisë Penale).
[745] Direktiva e Mbrojtjes së të Dhënave për Autoritetet e Policisë dhe të Drejtësisë Penale, neni 2, pika 1.
[746] *Ibid*., neni 4, pika 2.
[747] *Ibid.*, neni 3, pika 7.
[748] Komisioni Evropian (2016), Komunikatë e Komisionit për Parlamentin Evropian, sipas nenit 294, pika 6 të Traktatit për Funksionimin e Bashkimit Evropian që ka të bëjë me pozicionin e Këshillit për miratimin e Direktivës së Parlamentit Evropian dhe të Këshillit për mbrojtjen e personave në lidhje me përpunimin e të dhënave personale nga autoritetet kompetente, për qëllime të parandalimit, hetimit, zbulimit, ose ndjekjes së veprave penale, apo për ekzekutimin e dënimeve penale dhe për lëvizjen e lirë të këtyre të dhënave dhe që shfuqizon Vendimin Kuadër të Këshillit 2008/977/JHA, COM(2016) 213 final, Bruksel, 11 prill 2016.
[749] Direktiva e Mbrojtjes së të Dhënave për Autoritetet e Policisë dhe të Drejtësisë Penale, Kreu V.
[750] *Ibid.*, neni 2, pika 3.
[751] *Ibid*., në nenin 32 dhe nenin 27, përkatësisht.

dhënave për qëllime tregtare, i cili rregullohet nga rregullorja, përpunimi i të dhënave që lidhen me sigurinë mund të kërkojë një farë niveli fleksibiliteti. Për shembull, nëse edhe në kontekstin ligjzbatues, subjekteve të të dhënave do t'u jepej i njëjti nivel mbrojtje në lidhje me të drejtat për t'u informuar, për akses, apo për fshirje të të dhënave të tyre personale, sikurse parashikon Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, atëherë do të zhvlerësohej çdo aktivitet survejimi që zhvillohet për qëllime të zbatimit të ligjit. Për këtë arsye direktiva nuk parashikon parimin e transparencës. Po ashtu, edhe parimet e minimizimit të të dhënave dhe kufizimit të qëllimit, që përcaktojnë se të dhënat personale duhet të jenë të kufizuara vetëm tek ajo çka është e nevojshme për qëllimet e përpunimit të tyre dhe të përpunohen për qëllime të përcaktuara dhe të qarta, duhen zbatuar me fleksibilitet në kuadrin e përpunimit të të dhënave që lidhet me sigurinë. Informacioni që mblidhet dhe mbahet nga autoritetet kompetente për një çështje të caktuar, mund të jetë jashtëzakonisht i rëndësishëm për zbardhjen e çështjeve të mëvonshme.

Parime në lidhje me përpunimin

Direktiva e Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale përcakton disa garanci thelbësore për sa i takon përdorimit të të dhënave personale. Ajo saktëson gjithashtu parimet që drejtojnë përpunimin e këtyre të dhënave. Shtetet Anëtare duhet të garantojnë që të dhënat personale:

- Të përpunohen në mënyrë të ligjshme dhe të drejtë;
- Të mblidhen për qëllime të përcaktuara, të qarta dhe legjitime dhe të mos përpunohën në mënyrë të papajtueshme me ato qëllime;
- Të jenë të përshtatshme, të rëndësishme dhe jo të tepruara në lidhje me qëllimet për të cilat ato përpunohen;
- Të sakta dhe, kur është e nevojshme, të përditësuara; duhet marrë çdo masë e arsyeshme për të garantuar që të dhënat personale të pasakta, në raport me qëllimet për të cilat ato janë përpunuar, të fshihen ose të korrigjohen pa vonesë;
- Të mbahen në formë të tillë që mundëson identifikimin e subjekteve të të dhënave për një kohë jo më të gjatë se sa është e nevojshme për qëllimet për të cilat ato janë përpunuar;
- Të përpunohen në mënyrë të tillë që të garantohet siguria e duhur e të dhënave personale, përfshirë mbrojtjen nga përpunimi i paautorizuar, ose i paligjshëm dhe nga humbja, shkatërrimi, ose dëmtimi aksidental, duke marrë masat e përshtatshme teknike ose organizative.[752]

Sipas direktivës, përpunimi është i ligjshëm vetëm kur ai kryhet në masën që është e nevojshme për përmbushjen e misionit përkatës. Gjithashtu, ai duhet kryer nga një autoritet kompetent, për qëllimet e përcaktuara në direktivë dhe në bazë të së drejtës së BE-së, ose asaj kombëtare.[753] Të dhënat nuk duhen mbajtur për kohë më të gjatë se sa është e nevojshme dhe duhen fshirë, ose verifikuar në mënyrë periodike në periudha të caktuara. Ato duhen përdorur vetëm nga një autoritet kompetent dhe për qëllimin për të cilin të dhënat janë mbledhur, transmetuar, ose vënë në dispozicion.

Të drejtat e subjektit të të dhënave

Direktiva përcakton gjithashtu të drejtat e subjektit të të dhënave, ku përfshihen:

- E drejta për t'u informuar. Shtetet Anëtare duhet të detyrojnë kontrolluesin e të dhënave t'i bëjë me dije subjektit të të dhënave: 1) identitetin dhe adresën e kontaktit të kontrolluesit, 2) adresën e kontaktit të nëpunësit të mbrojtjes së të dhënave, 3) qëllimet e përpunimit të parashikuar, 4) të drejtën për të paraqitur ankesë pranë autoritetit mbikëqyrës kompetent dhe adresën e kontraktit të tij, apo të saj, si dhe 5) të drejtën për akses, korrigjim, apo fshirje të të dhënave personale dhe për kufizimin e përpunimit të të dhënave.[754] Përveç këtyre kritereve të informimit të përgjithshëm, direktiva duhet të përcaktojë se, në raste të caktuara dhe për mundësuar

[752] *Ibid*., neni 4, pika 1.
[753] *Ibid.*, neni 8.
[754] *Ibid.*, neni 13, pika 1.

ushtrimin e këtyre të drejtave, kontrolluesit duhet t'u japin subjekteve të të dhënave informacion në lidhje me bazën ligjore për përpunimin dhe afatet kohore të mbajtjes së të dhënave. Nëse të dhënat personale do të transmetohen në marrës të tjerë, përfshirë edhe vendet e treta, ose organizatat ndërkombëtare, subjektet e të dhënave duhet të informohen për kategoritë e këtyre marrësve. Së fundmi, kontrolluesit duhet të japin çdo informacion tjetër, duke marrë parasysh rrethanat e caktuara në të cilat janë përpunuar të dhënat, për shembull kur të dhënat personale janë mbledhur gjatë përfshimit të fshehtë, dmth pa dijeninë e subjektit të të dhënave. Diçka e tillë garanton përpunim të drejtë kundrejt subjektit të të dhënave.[755]

- E drejta për akses tek të dhënat personale. Shtetet Anëtare duhet të garantojnë që subjekti i të dhënave të gëzojë të drejtën për të ditur nëse po përpunohen, apo jo, të dhënat personale të tij, apo të saj. Nëse po përpunohen, subjekti i të dhënave duhet të ketë akses në një sasi informacioni, sikurse për kategoritë e të dhënave që po përpunohen.[756] Megjithatë, kjo e drejtë mund të kufizohet, për shembull për të parandaluar pengimin e hetimit, apo dëmtimit të ndjekjes së një krimi, apo për të mbrojtur sigurinë publike dhe të drejtat e liritë e të tjerëve.[757]

- Të drejtën për të korrigjuar të dhënat personale. Shtetet Anëtare janë të detyruara të garantojnë që subjekti i të dhënave mund të përftojë, pa vonesë të panevojshme, korrigjimin e të dhënave personale të pasakta. Gjithashtu, subjekti i të dhënave ka edhe të drejtën të përftojë plotësimin e të dhënave personale të paplota.[758]

- Të drejtën për të fshirë të dhënat personale dhe për të kufizuar përpunimin. Në disa raste, kontrolluesi duhet të fshijë të dhënat personale. Gjithashtu, subjekti i të dhënave mund të përftojë fshirjen e të dhënave personale të tij apo të saj, por vetëm kur ato janë përpunuar në mënyrë të paligjshme.[759] Në disa situata, përpunimi i të dhënave personale mund të kufizohet, në vend që ato të fshihen. Kjo mund të ndodhë në rastet kur: 1) është kundërshtuar saktësia e të dhënave personale, por diçka e tillë nuk mund të vërtetohet, ose 2) kur të dhënat personale nevojiten për qëllim prove.[760]

Kurdo që kontrolluesi refuzon të korrigjojë, ose të fshijë të dhënat personale, apo të kufizojë përpunimin e të dhënave, subjekti i të dhënave duhet informuar me shkrim. Shtetet Anëtare mund të kufizojnë këtë të drejtë informimi, ndër të tjera, për të mbrojtur sigurinë publike, apo të drejtat dhe liritë e të tjerëve, për të njëjtat arsye sikurse për kufizimin e së drejtës për akses.[761]

Normalisht, subjekti i të dhënave ka të drejtën të informohet për përpunimin e të dhënave personale të tij, apo të saj dhe ka të drejtën e aksesit, korrigjimit, ose fshirjes së të dhënnave, ashtu si dhe të drejtën e kufizimit të përpunimit, të cilat mund t'i ushtrojë drejtpërdrejtë me kontrolluesin. Si alternativë, ushtrimi në mënyrë të tërthortë i të drejtave të subjektit të të dhënave, nëpërmjet autoritetit të tij mbikëqyrës së mbrojtjes së të dhënave, është i mundshëm edhe sipas Direktivës së Mbrojtjes së të Dhënave për Policinë dhe Drejtësinë Penale dhe hyn në veprim kur kontrolluesi kufizon të drejtën e subjektit të të dhënave.[762] Neni 17 i direktivës kërkon që Shtetet Anëtare të miratojnë masa, të cilat garantojnë se të drejtat e subjekteve të të dhënave mund të ushtrohen gjithashtu nëpërmjet autoritetit mbikëqyrës. Kjo është arsyeja për të cilën kontrolluesi duhet të informojë subjektin e të dhënave për mundësinë e aksesit të tërthortë.

Detyrimet e kontrolluesit dhe të përpunuesit

Në kontekstin e Direktivës së Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale, kontrolluesit e të dhënave janë autoritete publike kompetente, ose organe të tjera me kompetenca publike dhe autoritet publik përkatës, të cilët përcaktojnë qëllimet dhe mënyrat e përpunimit të të

[755] *Ibid.*, neni 13, pika 2.
[756] *Ibid.*, neni 14.
[757] *Ibid.*, neni 15.
[758] *Ibid.*, neni 16, pika 1.
[759] *Ibid.*, neni 16, pika 2.
[760] *Ibid.*, neni 16, pika 3.
[761] *Ibid*., neni 16, pika 4.
[762] *Ibid*., neni 17.

dhënave personale. Direktiva përcakton disa detyrime për kontrolluesit e të dhënave, në mënyrë që të garantojnë nivel të lartë mbrojtjeje të të dhënave personale të përpunuara për qëllime të zbatimit të ligjit.

Autoritetet kompetente duhet të mbajnë një regjistër të operacioneve të përpunimit që ata kryejnë me anë të sistemeve të automatizuara të përpunimit. Regjistrat duhen mbajtur të paktën për mbledhjen, modifikimin, konsultimin, komunikimin përfshirë edhe transferimet, kombinimin dhe fshirjen e të dhënave personale.[763] Direktiva parashikon se regjistrat e konsultimit dhe të komunikimit, duhet të bëjnë të mundur që të përcaktohen arsyet, data dhe ora e kryerjes së këtyre operacioneve dhe për aq sa është e mundur, të identifikojnë person ii cili ka konsultuar sistemin, apo ka komunikuar të dhënat personale dhe marrësit e këtyre të dhënave personale. Regjistrat duhen përdorur vetëm për qëllim të verifikimit të ligjshmërisë së përpunimit, për auto-kontroll, për të garantuar integritetin dhe sigurinë e të dhënave personale për qëllime procedimesh penale.[764] Kontrolluesi dhe përpunuesi duhet t'ia vendosin në dispozicion regjistrat autoritetit mbikëqyrës, me kërkesën e këtij të fundit.

Ekziston veçanërisht një detyrim i përgjithshëm për kontrolluesit, i cili është marrja e masave të duhura teknike dhe organizative, për të garantuar që përpunimi të kryhet në përputhje me direktivën dhe për të vërtetuar ligjshmërinë e përpunimit.[765] Kur planifikojnë masat, ata duhen të marrin parasysh natyrën, objektin, kontekstin e përpunimit dhe sidomos çdo risk të mundshëm për të drejtat dhe liritë e personave. Kontrolluesit duhet të miratojnë politika të brendshme dhe të zbatojnë masa për lehtësimin e respektimit të parimeve të mbrojtjes së të dhënave, sidomos të parimit të mbrojtjes së të dhënave që në fazën e konceptimit dhe asaj me parapërzgjedhje.[766] Kur përpunimi ka të ngjarë të krijojë risk të lartë për të drejtat e personave, për shembull për shkak të përdorimit të teknologjive të reja, kontrolluesit duhet të kryejnë vlerësimin e ndikimit tek mbrojtja e të dhënave përpara nisjes së përpunimit.[767] Direktiva rendit gjithashtu masat që duhen zbatuar nga kontrolluesit, me qëllim që të garantojnë sigurinë e përpunimit. Këto përfshijnë masat për parandalimin e aksesit tek të dhënat personale të përpunuara nga ana e tyre, për të garantuar që personat e autorizuar të kenë akses vetëm tek të dhënat personale që mbulon autorizimi i tyre i aksesit, që funksionet e sistemit të përpunimit të punojnë në mënyrën e duhur dhe të dhënat personale që mbahen të mos kompromentohen nga një keqfunksionim i sistemit.[768] Nëse ndodh një shkelje tek të dhënat personale, kontrolluesit duhet të njoftojnë autoritetin mbikëqyrës brenda tre ditësh, duke përshkruar natyrën e shkeljes, pasojat e mundshme të saj, kategoritë e subjekteve të të dhënave të përfshirë dhe numrin e përafërt të subjekteve të të dhënave të prekur. Shkelja tek të dhënat personale duhet t'i komunikohet gjithashtu subjektit të të dhënave, "pa vonesë të panevojshme", kur shkelja ka të ngjarë të shkaktojë një risk të lartë për të drejtat dhe liritë e tij, apo të saj.[769]

Direktiva përfshin parimin e përgjegjshmërisë, i cili vendos detyrimin që kontrolluesit të zbatojnë masa për të garantuar respektimin nga ana e tyre të këtij parimi. Kontrolluesit duhet të mbajnë regjistra për të gjitha kategorië të aktiviteteve të përpunimit nën përgjegjësinë e tyre: përmbajtja e hollësishme e këtyre regjistrave përcaktohet në nenin 24 të direktivës. Regjistrat duhet t'i vihen në dispozicion autoritetit mbikëqyrës me kërkesën e tij, në mënyrë që ai të monitorojë operacionet e përpunimit që kryen kontrolluesi. Një masë tjetër e rëndësishme për rritjen e përgjegjshmërisë është caktimi i Nëpunësit të Mbrojtjes së të Dhënave (DPO). Kontrolluesit duhet të caktojnë një DPO, megjithëse direktiva i lejon Shtetet Anëtare të përjashtojnë nga ky detyrim gjykatat dhe autoritetet e pavarura gjyqësore.[770] Detyrat e Nëpunësit të Mbrojtjes së të Dhënave ngjasojnë me ato që përcakton Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave. Ai ose ajo kontrollon respektimin e direktivës, informon dhe këshillon punonjësit që kryejnë përpunim të dhënash, për detyrimet e tyre sipas legjislacionit të mbrojtjes së të dhënave. DPO-ja këshillon gjithashtu për nevojën e kryerjes së vlerësimit të ndikimit tek mbrojtja e të dhënave dhe vepron si pikë kontakti me autoritetin mbikëqyrës.

Transferimet tek vendet e treta dhe organizatat ndërkombëtare

[763] *Ibid*., neni 25, pika 1.
[764] *Ibid*., neni 25, pika 2.
[765] *Ibid*., neni 19.
[766] *Ibid*., neni 20.
[767] *Ibid*., neni 27.
[768] *Ibid*., neni 29.
[769] *Ibid*., nenet 30 dhe 31.
[770] *Ibid*., neni 32.

Ashtu sikurse Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, edhe direktiva përcakton kushtet për transferimin e të dhënave personale tek vendet e treta, ose organizatat ndërkombëtare. Nëse të dhënat personale do të transferoheshin lirshëm jashtë juridiksionit të BE-së, garancitë dhe mbrojtja e fortë që ofron legjislacioni i BE-së mund të kompromentoheshin. Gjithsesi, kushtet për transferimit janë mjaft të ndryshme nga ato të Rregullores së Përgjithshme të Mbrojtjes së të Dhënave. Transferimi i të dhënave personale drejt vendeve të treta, ose organizatave ndërkombëtare lejohet nëse:[771]

- Tranferimi është i nevojshëm për qëllimet e direktivës.
- Të dhënat personale transferohen tek një autoritet kompetent, sipas kuptimit të direktivës, të vendit të tretë, apo organizatës ndërkombëtare, megjithëse bëhet një përjashtim nga ky rregull në raste të veçanta dhe të caktuara.[772]
- Transferimi tek vendet e treta, ose organizatat ndërkombëtare i të dhënave personale të përftuara në kuadër të bashkëpunimit ndërkufitar kërkon autorizimin e Shtetit Anëtar nga i cili burojnë të dhënat, megjithëse bëhen përjashtime në rastet urgjente.
- Është miratuar një vendim përshtatshmërie nga Komisioni Evropian, ekzistojnë garancitë e duhura, ose gjen zbatim përjashtimi për transferimet në situata të caktuara.
- Transferimi i mëtejshëm i të dhënave personale drejt një vendi të tretë, ose një organizate ndërkombëtare, kërkon autorizim paraprak nga autoriteti kompetent i origjinës, i cili do të marrë parasysh ndër të tjera, seriozitetin e veprës penale dhe nivelin e mbrojtjes së të dhënave në vendin përftues të transferimit të dytë ndërkombëtar.[773]

Sipas direktivës, transferimet e të dhënave personale mund të kryhen nëse përmbushet një nga të tre kushte. I pari është kur Komisioni Evropian ka miratuar një vendim përshtatshmërie sipas direktivës. Vendimi mund të zbatohet për të gjithë territorin e vendit të tretë, ose për sektorë të caktuar të një vendi të tretë, ose për një organizatë ndërkombëtare. Megjithatë, diçka e tillë është e mundur vetëm nëse garantohet nivel i përshtatshëm mbrojtjeje dhe nëse përmbushen kriteret e përcaktuara në direktivë.[774] Në këto raste, transferimi i të dhënave personale nuk i nënshtrohet autorizimit të Shtetit Anëtar.[775] Komisioni Evropian duhet të monitorojë zhvillimet që mund të cënojnë funksionimin e vendimeve të përshtatshmërisë. Gjithashtu, vendimi duhet të përfshijë një mekanizëm për rishikimin periodik. Komisioni mundet gjithashtu të shfuqizojë, ndryshojë, ose pezullojë një vendim, kur ka informacione që tregojnë se kushtet në vendin e tretë, apo organizatën ndërkombëtare, nuk garantojnë më nivel të përshtatshëm mbrojtjeje. Në një rast të tillë, Komisioni duhet të nisë konsultimet me vendin e tretë, apo organizatën ndërkombëtare, me qëllim që të ndreqë situatën.

Në mungesë të një vendimi përshtatshmërie, transferimet mund të bazohen në garancitë e përshtatshme. Këto garanci mund të përcaktohen në një instrument ligjërisht të detyrueshëm, ose kontrolluesi mund të bëjë një vetëvlerësim të rrethanave në lidhje me transferimin e të dhënave personale dhe të dalë në përfundimin se ekzistojnë garancitë e përshtatshme. Vetëvlerësimi duhet të marrë në konsideratë marrëveshjet e mundshme të lidhura midis Europol-it dhe Eurojust-it me vendin e tretë, ose organizatën ndërkombëtare, ekzistencën e detyrimeve në lidhje me konfidencialitetin dhe kufizimin e qëllimit, ashtu si dhe me garancitë që jepen se të dhënat nuk do të përdoren për asnjë lloj forme trajtimi mizor dhe çnjerëzor, përfshirë dënimin me vdekje.[776] Në lidhje me këtë të fundit, kontrolluesi duhet të informojë autoritetin mbikëqyrës kompetent për kategoritë e transferimeve sipas kësaj kategorie.[777]

Nëse nuk është miratuar një vendim përshtatshmërie, ose nuk ekzistojnë garancitë e përshtatshme, transferimet mund të lejohen gjithsesi në disa situate të caktuara, të parashikuara në direktivë. Ndër të tjera, përfshihen mbrojtja e interesave jetike të subjektit të të dhënave, ose të një personi tjetër dhe

[771] *Ibid*., neni 35.
[772] *Ibid*, neni 39.
[773] *Ibid.*, neni 35, pika 1.
[774] *Ibid.*, neni 36.
[775] *Ibid.*, neni 36, pika 1.
[776] *Ibid.*, paragrafi 71 i preambulws.
[777] *Ibid.*, neni 37, pika 1.

parandalimi i një kërcënimi të menjëhershëm dhe të rëndë për sigurinë publike të Shtetit Anëtar, ose të një vendi të tretë.[778]

Në raste të veçanta dhe të caktuara, transferimet nga ana e autoriteteve kompetente drejt marrësve të vendosur në vendet e treta, të cilët nuk janë autoritete kompetente, përveç njërit prej kushteve të përshkruara më lart, duhet të plotësojnë edhe kushte të tjera shtesë, të përcaktuara nga neni 39 i direktivës. Në mënyrë të veçantë, transferimi duhet të jetë absolutisht i nevojshëm për përmbushjen e një detyre nga ana e autoritetit kompetent që kryen transferimin, i cili është gjithashtu përgjegjës për të verifikuar se të drejtat, apo liritë themelore të personave nuk prevalojnë mbi interesin public që justifikon transferimin. Ky lloj transferimi duhet dokumentuar dhe autoriteti kompetent që kryen transferimin duhet të informojë autoritetin mbikëqyrës kompetent.[779]

Së fundmi, për sa i përket vendeve të treta dhe organizatave ndërkombëtare, direktiva kërkon gjithashtu që të zhvillohen mekanzima bashkëpunimi ndërkombëtar, për të lehtësuar zbatimin efikas të legjislacionit, duke ndihmuar kësisoj autoritetet mbikëqyrëse të mbrojtjes së të dhënave që të bashkëpunojnë me homologët e tyre të huaj.[780]

Mbikëqyrja e pavarur dhe mjetet juridike për subjektet e të dhënave

Secili Shtet Anëtar duhet të garantojë që një, ose disa autoritete mbikëqyrëse kompetente të pavarura, janë përgjegjëse për të dhënë konsulencë dhe për të monitoruar zbatimin e dispozitave të miratuara në zbatim të direktivës.[781] Autoriteti mbikëqyrës i përcaktuar për qëllime të direktivës, mund të jetë i njëjti autoritet mbikëqyrës i ngritur sipas Rregullores së Përgjithshme të Mbrojtjes së të Dhënave, por Shtetet Anëtare janë të lira të përcaktojnë një autoritet të ndryshëm, me kusht që ai të përmbushë kriterin e pavarësisë. Autoritetet mbikëqyrëse duhet gjithashtu të trajtojnë ankesat e paraqitura nga çdo person në lidhje me mbrojtjen e të drejtave dhe lirive e tij, apo të saj, për sa i takon përpunimit të të dhënave personale nga autoritetet kompetente.

Kur ushtrimi i të drejtave të subjektit të të dhënave refuzohet për arsye bindëse, subjekti i të dhënave duhet të ketë të drejtën të kundërshtojë vendimin pranë autoritetit mbikëqyrës kompetent kombëat dhe/ose në gjykatë. Nëse një person pëson dëme për shkak të shkeljes së ligjit kombëtar që zbaton direktivës, ai ose ajo ka të drejtën e kompensimit nga kontrolluesi, ose nga çdo autoritet tjetër kompetent sipas së drejtës së Shtetit Anëtar.[782] Përgjithësisht, subjektet e të dhënave duhet të kenë akses në një mjet juridik gjyqësor, për çdo shkelje të të drejtave të tyre, të garantuara nga legjislacioni kombëtar që zbaton direktivën.[783]

8.3. Instrumente të tjera ligjore specifike të mbrojtjes së të dhënave për çështje të zbatimit të ligjit

Përveç Direktivës së Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale, shkëmbimi i informacionit që mbahet nga Shtetet Anëtare në fusha të caktuara, rregullohet nga një numër instrumentesh ligjore, sikurse është Vendimi Kuadër i Këshillit 2009/315/JHA mbi organizimin dhe përmbajtjen e shkëmbimit të informacionit që nxirret nga të dhënat penale midis Shteteve Anëtare, Vendimi i Këshillit 2000/642/JHA që ka të bëjë me rregullimet në lidhje me bashkëpunimin midis njësive të inteligjencës financiare të Shteteve Anëtare, për sa i takon shkëmbimit të informacionit dhe Vendimi Kuadër i Këshillit 2006/960/JHA i 18 dhjetorit 2006 mbi shjeshtimin e shkëmbimit të informacionit dhe të dhënave operative midis autoritetevve ligjzbatuese të Shteteve Anëtare të Bashkimit Evropian.[784]

---

[778] *Ibid*., neni 38, pika 1.
[779] *Ibid.*, neni 37, pika 3.
[780] *Ibid.*, neni 40.
[781] *Ibid.*, neni 41.
[782] *Ibid.*, neni 56.
[783] *Ibid.*, neni 54.
[784] Këshilli i Bashkimit Evropian (2009), Vendimi Kuadër i Këshillit 2009/315/JHA i 26 shkurtit 2009 mbi organizimin dhe përmbajtjen e shkëmbimit të informacionit të nxjerrë nga të dhënat penale midis Shteteve Anëtare, FZ 2009 L 93; Këshilli i Bashkimit Evropian (2000), Vendimi i Këshillit 2000/642/JHA i 17 tetorit 2000 që ka të bëjë me rregullimet për bashkëpunimin midis njësive të inteligjencës financiare

Është me rëndësi të saktësohet se bashkëpunimi ndërkufitar[785] midis autoriteteve kompetente, përfshin gjithnjë e më shumë shkëmbimin e të dhënave të emigracionit. Kjo fushë e së drejtës nuk konsiderohet si pjesë e çështjeve të policisë dhe drejtësisë penale, por është e rëndësishme në shumë aspekte për punën e autorieteve policore dhe të drejtësisë. Njësoj vlen edhe për të dhënat në lidhje me mallrat që importohen, apo eksportohen nga BE-ja. Heqja e kufijve të brendshëm në zonën Schengen, ka rritur rrezikun e mashtrimit dhe njëkohësisht të nevojës për forcimin e bashkëpunimit midis Shteteve Anëtare, kryesisht nëpërmjet rritjes së shkëmbimit ndërkufitar të informacionit, për të zbuluar dhe ndjekur penalisht në mënyrë më të efektshme shkeljet e së drejtës doganore kombëtare dhe asaj të BE-së. Gjithashtu, vitet e fundit bot aka dëshmuar rritje të krimeve të rënda, krimit të organizuar dhe terrorizmit, që mund të përfshijnë udhëtimin ndërkombëtar dhe ka treguar se nevojitet shtimi i bashkëpunimit ndërkufitar policor dhe ligjzbatues në shumë raste.[786]

Vendimi Prüm

Një shembull i rëndësishëm i bashkëpunimit ndërkufitar të institucionalizuar nëpërmjet shkëmbimit të të dhënave që mbahen në nivel kombëtar, është Vendimi i Këshillit 2008/615/JHA, së bashku me dispozitat zbatuese të tij në Vendimin 2008/615/JHA, mbi thellimin e bashkëpunimit ndërkufitar, sidomos për të luftuar terrorizmin dhe krimin ndërkufitar (Vendimi Prüm), i cili transpozoi Traktatin e Prüm-it në të drejtën e BE-së në 2008-ën.[787] Traktati i Prüm-it ishte një marrëveshje ndërkombëtare bashkëpunimi policor, e nënshkruar në 2005-ën nga Austria, Belgjika, Franca, Gjermani, Luksemburgy, Vendet e Ulëta dhe Spanja.[788]

Vendimi Prüm ka për qëllim të ndihmojë Shtetet Anëtare nënshkruese të përmirësojnë shkëmbimin e informacionit për qëllime të parandalimit dhe luftës kundër krimit në tre fusha: terrorizmi, krimi ndërkufitar dhe emigrimi i paligjshëm. Për këtë qëllim, vendimi përcakton dispozita që kanë të bëjnë me:

- Aksesin e automatizuar në profilet e AND-së, të dhënat e gjurmëve të gishtave dhe në disa të dhëna të regjistrit kombëtar të automjeteve;
- Transmetimin e të dhënave në lidhje me ngjarje madhore, që kanë dimension ndërkufitar;
- Transmetimin e informacionit për parandalimin e veprave terroriste;
- Masa të tjera për thellimin e bashkëpunimit policor ndërkufitar.

Bazat e të dhënave që janë vënë në dispozicion sipas Vendimit Prüm, rregullohen plotësisht nga e drejta kombëtare, por shkëmbimi i të dhënave rregullohet gjithashtu edhe nga vendimi, përputhshmëria e së cilit me Direktivën e Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale duhet vlerësuar. Organet kompetente për mbikëqyrjen e këtyre qarkullimeve të të dhënave, janë autoritetet kombëtare mbikëqyrëse të mbrojtjes së të dhënave.

të Shteteve Anëtare, për sa i takon shkëmbimit të informacionit, FZ 2000 L 271; Vendimi Kuadër i Këshillit 2006/960/JHA i 18 dhjetorit 2006 mbi thjeshtimin e shkëmbimit të informacionit dhe të dhënave operative midis autoriteteve ligjzbatuese të Shteteve Anëtare të Bashkimit Evropian, FZ L 386.

[785] Komisioni Evropian (2012), *Komunikatë e Komisionit për Parlamentin Evropian dhe Këshillin – Forcimi i bashkëpunimit ligjzbatues në BE: Modeli Evropian i Shkëmbimit të Informacionit (EIXM)*, COM(2012) 735 final, Bruksel, 7 dhjetor 2012.

[786] Shih, Komisioni Evropian (2011), Propozim për një Direktivë të Parlamentit Evropian dhe Këshillit në lidhje me përdorimin e Regjistrimit të Emrave të Pasagjerëve për qëllime të parandalimit, zbulimit, hetimit dhe ndjekjes së veprave terroriste dhe krimeve të rënda, COM(2011) 32 final, Bruksel, 2 shkurt 2011, fq. 1.

[787] Këshilli i Bashkimit Evropian (2008), Vendimi i Këshillit 2008/615/JHA i 23 qershorit 2008 mbi thellimin e bashkëpunimit ndërkufitar, sidomos për të luftuar terrorizmin dhe krimin ndërkufitar, FZ 2008 L 210.

[788] Konventa ndërmjet Mbretërisë së Belgjikës, Republikës Federale të Gjermanisë, Mbretërisë së Spanjës, Republikës Franceze, Dukatit të Madh të Luksemburgut, Mbretërisë së Vendeve të Ulëta dhe Republikës së Austrisë mbi thellimin e bashkëpunimit ndërkufitar, sidomos për të luftuar terrorizmin, krimin ndërkufitar dhe emigrimin e paligjshëm.

Vendimi Kuadër 2006/960/JHA – Iniciativa suedeze

Vendimi Kuadër 2006/960/JHA (Iniciativa suedeze)[789] përfaqëson një tjetër shembull bashkëpunimi ndërkufitar, për sa i përket shkëmbimit të të dhënave që mbahen në nivel kombëtar, nga ana e autoriteteve ligjzbatuese. Iniciativa suedeze përqendrohet veçanërisht në shkëmbimin e informacionit dhe të dhënave operative dhe përcakton rregulla specifike për mbrojtjen e të dhënave në nenin 8.

Sipas këtij instrumenti, përdorimi i informacionit dhe të dhënave operative që shkëmbehen, duhet t'i nënshtrohet dispozitave kombëtare të mbrojtjes së të dhënave të Shtetit Anëtar që merr informacionin, në përputhje me të njëjtat rregulla sikur të ishin mbledhur në po atë Shtet Anëtar. Neni 8 shkon më tej, duke përcaktuar se kur jepet informacion dhe të dhëna operative, autoriteti kompetent ligjzbatues mund të vendosë kushte që janë në përputhje me të drejtën kombëtare të tij, për sa i takon përdorimit të tyre nga ana e autoritetit kompetent ligjzbatues që i përfton ato. Kushtet mund të gjejnë zbatim edhe për raportimin e rezultatit të hetimit penal, apo të operacioneve informative penale, për të cilat është kërkuar shkëmbim informacioni dhe të dhënash operative. Megjithatë, kur e drejta kombëtare parashikon përjashtime për kufizimet e përdorimit (p.sh. për autoritetet gjyqësore, organet legjislative, etj.), informacioni dhe të dhënat operative mund të përdoren vetëm pas konsultimit paraprak me Shtetin Anëtar dërgues.

Informacioni dhe të dhënat operative të dërguara, mund të përdoren:

- Për qëllimet për të cilat janë transmetuar; ose
- Për të parandaluar një kërcënim të menjëhershëm dhe të rëndë për sigurinë publike.

Përpunimi për qëllime të tjera mund të jetë i lejuar, por vetëm me autorizimin paraprak të Shtetit Anëtar dërgues.

Iniciativa suedeze thekson se të dhënat personale të përpunuara, duhet të mbrohen në përputhje me instrumentet ndërkombëtare, sikurse janë:

- Konventa e Këshillit të Evropës për Mbrojtjen e Personave në lidhje me Përpunimin e Automatizuar të të Dhënave Personale;[790]
- Protokolli Shtesë i kësaj Konvente i 8 nëntorit 2001, në lidhje me Autoritetet Mbikëqyrëse dhe Qarkullimet Ndërkufitare të të Dhënave;[791]
- Rekomandimi nr. R(87) 15 i Këshillit të Evropës që Rregullon Përdorimin e të Dhënave Personale në Sektorin e Policisë.[792]

Direktiva PNR e BE-së

Të dhënat e Regjistrit të Emrave të Pasagjerëve (PNR) kanë të bëjnë me informacionin që lidhet me pasagjerët e transportit ajror, që mblidhet dhe mbahet nga sistemet e rezervimit dhe të kontrollit të udhëtimeve të shoqërive të transportit ajror për qëllimet e tyre tregtare. Këto të dhëna përmbajnë disa lloje të ndryshme informacioni, sikurse datat e udhëtimit, itinerarin e udhëtimit, informacionin e biletës,

[789] Këshilli i Bashkimit Evropian (2006), Vendimi Kuadër i Këshillit 2006/960/JHA i 18 dhjetorit 2006 mbi thjeshtimin e shkëmbimit të informacionit dhe të dhënave operative midis autoriteteve ligjzbatuese të Shteteve Anëtare të Bashkimit Evropian FZ L 386/89 i 29 dhjetorit 2006.
[790] Këshilli i Evropës (1981), Konventa për Mbrojtjen e Personave në lidhje me Përpunimin e Automatizuar të të Dhënave Personale, ETS nr. 108.
[791] Këshilli i Evropës (2001), Protokolli Shtesë i Konventës për Mbrojtjen e Personave në lidhje me Përpunimin e Automatizuar të të Dhënave Personale, në lidhje me autoritetet mbikëqyrëse dhe qarkullimet ndërkufitare të të dhënave, ETS nr. 108.
[792] Këshilli i Evropës (1987), Rekomandimi nr. R (87) 15 i Komitetit të Ministrave të shteteve anëtare që rregullon përdorimin e të dhënave personale në sektorin e policisë (miratuar nga Komiteti i Ministrave më 17 shtator 1987 në mbledhjen e 410-të të Zëvendësministrave).

adresën e kontaktit, agjentin e udhëtimit ku është rezervuar udhëtimi, mënyra e pagesës, numri i ulëses dhe informacioni i bagazheve.[793] Përpunimi i të dhënave të PNR-së mund të ndihmojë autoritetet ligjzbatuese të identifikojnë të dyshuar të njohur, ose të mundshëm dhe të analizojnë skemat e lëvizjeve të tyre dhe tregues të tjerë, të cilët lidhen përgjithësisht me aktivitetet kriminale. Analiza e të dhënave të PNR-së mundëson gjithashtu gjurmimin restrospektiv të itinerareve dhe kontaktet e personave të dyshuar si të përfshirë në aktivitete kriminale, duke ndihmuar autoritetet ligjzbatuese të identifikojnë rrjetet kriminale.[794] BE-ja ka lidhur disa marrëveshje me vende të treta, për shkëmbimin e të dhënave të PNR-së, sikurse shpjegohet në Kapitullin 7. Gjithashtu, ajo ka përfshirë përpunimin e të dhënave të PNR-së në BE, me anë të Direktivës 2016/681/BE mbi përdorimin e të dhënave të PNR-së për parandalimin, zbulimin, hetimin dhe ndjekjen e veprave terroriste dhe krimeve të rënda (Direktiva PNR e BE-së).[795] kjo direktivë parashikon detyrimet për shoqëritë e transportit ajror, që t'u transmetojnë autoriteteve kompetente të dhënat e PNR-së dhe përcakton garanci strikte për mbrojtjen e të dhënave, në lidhje me përpunimin dhe mbledhjen e këtyre të dhënave. Direktiva PNR e BE-së zbatohet si për fluturimet ndërkombëtare drejt dhe nga BE-ja, por gjithashtu edhe për fluturimet brenda BE-së, nëse një Shtet Anëtar vendos kësisoj.[796]

Të dhënat e PNR-së të mbledhura, duhet të përmbajnë vetëm informacionet që lejon Direktiva PNR e BE-së. Këto informacione duhen mbajtur në një njësi unike informacioni, në një vendndodhje të sigurtë në secilin Shtet Anëtar. Të dhënat e PNR-së duhen depersonalizuar gjashtë muaj pasi janë transmetuar nga shoqëria e transportit ajror dhe të mbahen për një periudhë maksimale prej pesë vitesh.[797] Të dhënat e PNR-së shkëmbehen midis Shteteve Anëtare, midis Shteteve Anëtare dhe Europol-it dhe me vende të treta, por vetëm rast pas rasti.

Transmetimi dhe përpunimi i të dhënave të PNR-së dhe të drejtat e garantuara për subjektet e të dhënave, duhet të jenë në përputhje me Direktivën e Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale dhe duhet të ofrojnë nivel të lartë mbrojtjeje të privatësisë dhe të të dhënave personale, sikurse kërkohet nga Karta, Konventa 108 e Modernizuar dhe nga KEDNJ-ja.

Autoritetet e pavarura mbikëqyrëse kombëtare dhe që janë kompetente sipas Direktivës së Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale, janë gjithashtu përgjegjëse për të monitoruar dhe për të këshilluar në lidhje me zbatimin e dispozitave të miratuara nga Shtetet Anëtare sipas Direktivës PNR të BE-së.

Mbajtja e të dhënave të telekomunikimeve

Direktiva e Mbajtjes së të Dhënave[798], e cila u shpall e pavlefshme më 8 prill 2014, në çështjen *Digital Rights Ireland*, detyronte operatorët e shërbimeve të komunikimit të mbanin të disponueshme të dhënat e trafikut, për qëllimin konkret të luftës kundër krimeve të rënda, për të paktën gjashtë dhe maksimumi 24 muaj, pavarësisht nëse operatorit i nevojiteshin të dhënat edhe më gjatë, për qëllime faturimi shërbimi, apo për të ofruar teknikisht shërbimin.

---

[793] Komisioni Evropian (2011), Propozim për një Direktivë të Parlamentit Evropian dhe Këshillit mbi përdorimin e të dhënave të Regjistrit të Emrave të Pasagjerëve, për parandalimin, zbulimin, hetimin dhe ndjekjen e veprave terroriste dhe krimeve të rënda, COM(2011) 32 final, Bruksel, 2 shkurt 2011, fq. 1.

[794] Komisioni Evropian (2015), Dokument Teknik për Luftën kundër Terrorizmit në nivel BE-je, një vështrim i përgjithshëm mbi veprimet, masat dhe iniciativat e Komisionit, Bruksel, 11 janar 2015.

[795] Direktiva (BE) 2016/681 e Parlamentit Evropian dhe Këshillit e 27 prillit 2016, mbi përdorimin e të dhënave të regjistrit të emrave të pasagjerëve (PNR), për parandalimin, zbulimin, hetimin dhe ndjekjen e veprave terroriste dhe krimeve të rënda, FZ 2016 L 119, fq. 132.

[796] Direktiva PNR, L 119, fq. 132, neni 1, pika 1 dhe neni 2, pika 1.

[797] *Ibid.*, neni 12, pika 1 dhe neni 12, pika 2.

[798] Direktiva 2006/24/KE e Parlamentit Evropian dhe Këshillit e 15 marsit 2006, në lidhje me mbajtjen e të dhënave të gjeneruara, ose të përpunuara, që kanë të bëjnë me ofrimin e shërbimeve të komunikimeve elektronike të aksesueshme nga publiku, ose të rrjeteve publike të komunikimeve dhe që ndryshon Direktivën 2002/58/KE, FZ 2006 L 105.

Mbajtja e të dhënave të telekomunikimeve ndërhyn qartësisht tek e drejta për mbrojtje të të dhënave.[799] Legjitimiteti i kësaj ndërhyrjeje është kundërshtuar në disa çështje gjyqësore të zhvilluara Shtetet Anëtare të BE-së.[800]

[BOX TYPE 1]

Shembull: tek çështja *Digital Rights Ireland* dhe *Kärntner Landesregierung dhe të Tjerët,*[801] grupi Digital Rights dhe z. Seitlinger u ankuan respektivisht në Gjykatën e Lartë të Irlandës dhe në Gjykatën Kushtetuese të Austrisë, për ligjshmërinë e masave kombëtare që autorizonin mbajtjen e të dhënave të komunikimeve elektronike. Grupi Digital Rights i kërkoi gjykatës irlandeze të shpallte të pavfleshme Direktivën 2006/24 dhe pjesën e së drejtës penale kombëtare që lidhej me veprat terroriste. Po ashtu, z. Seitlinger dhe mbi 11,000 kërkues të tjerë kundërshtuan dhe kërkuan anulimin e një dispozite të legjislacionit austriak në lidhje me telekomunikimet, që transpozonte Direktivën 2006/24.

Në përgjigje të këtyre kërkesave për vendim paragjyqësor, GJDBE-ja e shpalli të pavlefshme Direktivën e Mbajtjes së të Dhënave. Sipas GJDBE-së, të dhënat që mund të mbaheshin sipas direktivës, ofronin informacion të saktë në lidhje me personat, nëse ato trajtoheshin në tërësinë e tyre. Nga ana tjetër, GJDBE-ja shqyrtoi shkallën e ndërhyrjes tek të drejtat themelore për respektim të jetës private dhe për mbrojtje të të dhënave personale. Ajo doli në përfundimin se mbajtja e të dhënave përmbushtte një objektiv me interes publik, konkretisht luftën kundër krimeve të rënda dhe për rrjedhojë sigurinë publike. Pavarësisht kësaj, GJDBE-ja theksoi se ligjvënësi i BE-së, duke miratuar direktivën, kishte shkelur parimin e proporcionalitetit. Paçka se direktiva mund të ishte e përshtatshme për përmbushjen e objektivit të synuar, "ndërhyrja në shkallë të gjerë dhe tepër e rëndë e Direktivës tek të drejtat themelore për respektim të privatësisë dhe mbrojtje të të dhënave personale, nuk ishte e rregulluar si duhet, në mënyrë që të kufizohej tek nevoja absolute."

Mbajtja e të dhënave është e lejuar, nëse mungon legjislacioni specifik për mbajtjen e të dhënave, si një përjashtim nga konfidencialiteti i të dhënave të telekomunikimeve, sipas Direktivës 2002/58/KE (Direktiva mbi privatësinë dhe komunikimet elektronike),[802] si masë parandaluese, por duhet të bëhet vetëm për qëllime të luftës kundër krimeve të rënda. Mbajtja e këtyre të dhënave duhet të kufizohet tek nevoja absolute, për sa i përket kategorive të të dhënave të mbajtura, mjeteve të komunikimit të përfshira, personave të përfshirë dhe afateve të parashikuara të mbajtjes. Autoritetet kombëtare mund të kenë akses me kushte të rrepta tek të dhënat e mbajtura, ku përfshihet edhe kontrolli paraprak nga një autoritet i pavarur. Të dhënat duhen mbajtur brenda territorit të BEsë-.

[BOX TYPE 1]

Shembull: pas çështjes *Digital Rights Ireland* dhe *Kärntner Landesregierung dhe të Tjerët*[803], dy çështje të tjera iu paraqitën GJDBE-së, që kishin të bënin me detyrimin e përgjithshëm që ekzistonte në Suedi dhe Mbretërinë e Bashkuar, për operatorët e shërbimeve të komunikimeve elektronike, për të mbajtur të dhënat e telekomunikimeve, sikurse kërkohej nga Direktiva e shfuqizuar e Mbajtjes së të Dhënave.

[799] EDPS (2011), *Opinion i 31 majit 2011 mbi Raportin e Vlerësimit të Komisionit për Këshillin dhe Parlamentin Evropian, në lidhje me Direktivën e Mbajtjes së të Dhënave (Direktiva 2006/24/KE)*, 31 maj 2011.
[800] Gjermani, Gjykatat Kushtetuese Federale (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 mars 2010; Rumani, Gjykata Kushtetuese Federale (*Curtea Constituþională a României*), nr. 1258, 8 tetor 2009; Republika Çeke, Gjykata Kushtetuese (*Ústavní soud České republiky*), 94/2011 Coll., 22 mars 2011.
[801] GJDBE, Çështje të bashkuara C-293/12 dhe C-594/12, *Digital Rights Ireland Ltd k. Minister for Communications, Marine and Natural Resources dhe të Tjerët* dhe *Kärntner Landesregierung dhe të Tjerët* [ÇB], 8 prill 2014, parag. 65.
[802] Direktiva 2002/58/KE e Parlamentit Evropian dhe Këshillit e 12 korrikut 2002 që ka të bëjë me përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike (Direktiva mbi privatësinë dhe komunikimet elektronike), FZ 2002 L 201.
[803] GJDBE, Çështje të bashkuara C-293/12 dhe C-594/12, *Digital Rights Ireland Ltd k. Minister for Communications, Marine and Natural Resources dhe të Tjerët* dhe *Kärntner Landesregierung dhe të Tjerët* [ÇB], 8 prill 2014.

Tek çështja *Tele2 Sverige* dhe *Home Department k. Tom Watson dhe të Tjerët*,[804] GJDBE-ja vendosi se legjislacioni kombëtar që përcakton mbajtje të përgjithshme dhe pa dallim të të dhënave, pa kërkuar asnjë lidhje midis të dhënave që duhen mbajtur me një kërcënim ndaj sigurisë publike dhe pa përcaktuar asnjë kusht, p.sh. afate mbajtjeje, zonë gjeografike, grup personash që dyshohen sit ë përfshirë në krime të rënda, shkon përtej kufijve të nevojës absolute dhe nuk mund të konsiderohet e justifikuar në një shoqëri demokratike, sikurse kërkon Direktiva 2002/58/KE, e lexuar duke u mbështetur në Kartën e të Drejtave Themelore të BE-së.

Perspektiva

Në janar 2017, Komisioni Evropian publikoi një propozim për një Rregullore që ka të bëjë me respektimin e jetës private dhe mbrojtjen e të dhënave personale në komunikimet elektronike, e cila ka si qëllim të shfuqizojë dhe zëvendësojë Direktivën 2002/58/KE.[805] Propozimi nuk përmban ndonjë dispozitë të caktuar në lidhje me mbajtjen e të dhënave. Sidoqoftë, ai përcakton se Shtetet Anëtare mund të kufizojnë me ligj disa detyrime dhe të drejta të parashikuara nga rregullorja, kur një kufizim i tillë përbën masë të nevojshme dhe proporcionale për mbrojtjen e disa interesave publike, duke përfshirë sigurinë kombëtare, mbrojtjen, sigurinë publike dhe parandalimin, hetimin, zbulimin dhe ndjekjen e veprave penale, ose ekzekutimin e dënimeve penale.[806] Për rrjedhojë, Shtetet Anëtare do të kenë mundësi të mbajnë, ose të krijojnë një kuadër kombëtar për mbajtjen e të dhënave, i cili të përcaktojë masa mbajtjeje të shënjestruar, në masën që kuadri të jetë në përputhje me të drejtën e Bashkimit, duke marrë parasysh jurisprudencën e GJDBE-së mbi interpretimin e Direktivës e-Privatësia dhe Kartën e të Drejtave Themelore të BE-së.[807] Në momentin e hartimit të këtij manuali, vijojnë diskutimet për miratimin e rregullores.

Marrëveshja-kuadër BE-SHBA për mbrojtjen e të dhënave personale që shkëmbehen për qëllime ligjzbatuese

Më 1 shkurt 2017, hyri në fuqi marrëveshja-kuadër BE-SHBA (*Umbrella agreement*) për përpunimin e të dhënave personale për qëllime parandalimi, hetimi, zbulimi dhe ndjekjeje të veprave penale.[808] Marrëveshja-kuadër BE-SHBA synon të garantojë nivel të lartë mbrojtjeje të të dhënave të qytetarëve të BE-së, duke rritur njëkohësisht bashkëpunimin midis autoriteteve ligjzbatuese të BE-së dhe SHBA-ve. Ajo plotëson marrëveshjet ekzistuese BE-SHBA dhe Shtet Anëtar-SHBA midis autoriteteve ligjzbatuese, duke ndihmuar gjithashtu në përcaktimin në mënyrë të qartë dhe të harmonizuar të rregullave të mbrojtjes së të dhënave për marrëveshje të ardhshme në këtë fushë. Në këtë aspekt, marrëveshja synon të ndërtojë një kuadër ligjor të qëndrueshëm, për të lehtësuar shkëmbimin e informacionit.

Marrëveshja, në vetvete, nuk përbën bazë ligjore të përshtatshme për shkëmbimin e të dhënave personale, por nga ana tjetër ofron garancitë e përshtatshme në fushën e mbrojtjes së të dhënave për personat e përfshirë. Ajo mbulon përpunimin e të dhënave personale të nevojshëm për qëllime parandalimi, hetimi, zbulimi dhe ndjekjeje të veprave penale, duke përfshirë terrorizmin.[809]

---

[804] GJDBE, Çështje të bashkuara C-203/15 dhe C-698/15, *Tele2 Sverige AB k. Post- och telestyrelsen* dhe *Secretary of State for the Home Department k. Tom atson dhe të Tjerët* [ÇB], 21 dhjetor 2016.

[805] Komisioni Evropian (2017), *Propozim për një Rregullore të Parlamentit Evropian dhe Këshillit që ka të bëjë me respektimin e jetës private dhe mbrojtjen e të dhënave personale në komunikimet elektronike dhe që shfuqizon Direktivën 2002/58/EC (Rregullorja mbi Privatësinë dhe Komunikimet Elektronike)*, COM(2017) 10 final, Bruksel, 10 janar 2017.

[806] *Ibid.*, paragrafi 26.

[807] Shih memorandumin shpjegues të Propozimit për një Rregullore mbi Privatësinë dhe Komunikimet Elektronike COM(2017) 10 final, pika 1.3.

[808] Shih, Këshilli i BE-së (2016), "*Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign 'Umbrella agreement*'", komunikimi për shtyp 305/16, 2 qershor 2016.

[809] Marrëveshja midis Shteteve të Bashkuara të Amerikës dhe Bashkimit Evropian për mbrojtjen e informacionit personal në lidhje me parandalimin, hetimit, zbulimin dhe ndjekjen e veprave penale e 18 majit 2016, (OR.en) 8557/16, neni 3, pika 1. Shih gjithashtu njoftimin e Komisionit për negociatat për marrëveshjen e mbrojtjes së të dhënave BE-SHBA të 26 majit 2010, MEMO/10/216 dhe Njoftimin për shtyp të Komisionit të BE-së (2010) mbi standardet e larta të respektimit të privatësisë në marrëveshjen e mbrojtjes së të dhënave BE-SHBA, të 26 majit 2010, IP/10/609.

Marrëveshja përcakton shumë garanci për përdorimin e të dhënave personale vetëm për qëllimet e parashikuara në marrëveshje. Në mënyrë të veçantë, ajo përcakton mbrojtjen e mëposhtme për qytetarët e BE-së:

- Kufizime të përdorimit të të dhënave: të dhënat personale mund të përdoren për qëllime të parandalimit, hetimit, zbulimit, ose ndjekjes së veprave penale;
- Mbrojtje nga diskriminimi arbitrar dhe i pajustifikueshëm;
- Transferimet e mëtejshme: çdo transferim i mëtejshëm tek një vend i tretë përtej SHBA-ve dhe BE-së, apo një organizatë ndërkombëtare, duhet t'i nënshtrohet autorizimit paraprak të autoritetit kompetent të vendit nga ku burojnë të dhënat e transferuara;
- Cilësia e të dhënave: mbajtja e të dhënave personale duhet bërë me vëmendje ndaj saktësisë, rëndësisë, vlerës kohore dhe sa të plota janë;
- Siguria e përpunimit, duke përfshirë njoftimin e shkeljeve ndaj të dhënave personale;
- Përpunimi i të dhënave sensitive lejohet vetëm në masën që ekzistojnë garancitë e përshtatshme të parashikuara me ligj;
- Afatet e mbajtjes së të dhënave: të dhënat personale nuk mund të mbahen për një kohë më të gjatë se sa është e nevojshme dhe e përshtatshme;
- Të drejtat për akses dhe korrigjim: çdo person ka të drejtën e aksesit tek të dhënat personale të tij apo të saj, me disa kushte të caktuara dhe të kërkojë që të dhënat të korrigjohen nëse janë të pasakta;
- Vendimet e automatizuara kërkojnë garanci të përshtashme, ku përfshihet edhe mundësia për të siguruar ndërhyrje njerëzore në to;
- Kontroll efikas, duke përfshirë edhe bashkëpunimin midis autoriteteve mbikëqyrëse të BE-së dhe SHBA-ve; dhe
- Mjete mbrojtjeje gjyqësore dhe realizueshmëri: qytetarët e BE-së kanë të drejtën[810] e mjetit mbrojtës gjyqësor në gjykatat e SHBA-ve, në rastet kur autoritetet amerikane refuzojnë aksesin, apo korrigjimin, ose i përhapin të dhënat personale në mënyrë të paligjshme.

Marrëveshja kuadër përcakton gjithashtu një sistem për njoftimin e autoritetit mbikëqyrës kompetent në Shtetin Anëtar të personave të cënuar nga një shkelje ndaj të dhënave personale, nëse është e nevojshme. Garancitë ligjore të parashikuar nga marrëveshja sigurojnë trajtimin në mënyrë të barabartë të qytetarëve të BE-së në SHBA në rast shkeljeje ndaj privatësisë.[811]

8.3.1. Mbrojtja e të dhënave në agjencitë gjyqësore dhe ligjzbatuese të BE-së

Europol-i

Europol-i, agjencia e BE-së për bashkëpunim ligjzbatues, e ka selinë në Hagë, dhe Njësitë Kombëtare të Europol-it (ENU-të) në secilin Shtet Anëtar. Europol-i është krijuar në vitin 1998; statusi aktual i tij si institucion i BE-së bazohet në Rregulloren mbi Agjencinë e Bashkimit Evropian për Bashkëpunim

[810] US Judicial Redress Act [Ligji amerikan për mjetet mbrojtëse gjyqësore] u nënshkrua nga Presidenti Obama më 24 shkurt 2016.

[811] Mbikëqyrësi Evropian i Mbrojtjes së të Dhënave miratoi një Opinion mbi Marrëveshjen BE-SHBA ku rekomandonte, ndër të tjera, përshtatjet në vijim: 1) të shtohet 'për qëllimet specifike për të cilat ato janë transferuar' tek neni që përcakton mbajtjen e të dhënave për një kohë jo më të gjatë se sa është e nevojshme dhe proporcionale dhe 2) përjashtimin e transferimeve masive të të dhënave sensitive, të cilat janë të mundshme. Shih Opinionin 1/2016 të Mbikëqyrësit Evropian të Mbrojtjes së të Dhënave, *Preliminary Opinion on the agreement between the United State of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences*, § 35.

Ligjzbatues (Rregullorja e Europol-it.[812] Mandati i Europol-it konsiston në mbështetjen për parandalimin dhe hetimin e krimit të organizuar, terrorizmit dhe çdo forme tjetër krimi të rëndë, sikurse renditen në Shtojcën I të Rregullores së Europol-it, që prekin dy ose më shumë Shtete Anëtare. Këtë e bën nëpërmjet shkëmbimit të informacionit dhe duke vepruar si qendër informacioni e BE-së, si dhe duke kryer analiza të të dhënave operative dhe vlerësime të kërcënimeve.

Për përmbushjen e objektivave të tij, Europol-i ka ngritur Sistemin e Informacionit të Europol-it, i cili u ofron Shteteve Anëtare një bazë të dhënash për shkëmbimin e të dhënave operative penale dhe informacion nëpërmjet ENU-ve përkatëse. Sistemi i Informacionit të Europol-it mund të përdoret për të vënë në dispozicion të dhëna që kanë të bëjnë me: personat e dyshuar, apo të dënuar për vepra penale që përfshihen në kompetencën e Europol-it, apo personat për të cilët ka elemente prove se mund të kryejnë vepra penale të tilla. Europol-i dhe ENU-të mund të regjistrojnë, ose të marrin të dhëna drejtpërdrejtë nga Sistemi i Informacionit të Europol-it. Vetëm pala e cila ka regjistruar të dhënat në sistem, mund t'i ndryshojë, korrigjojë, apo fshijë ato. Edhe organet e BE-së, vendet e treta dhe organizatat ndërkombëtare mund t'i japin gjithashtu Europol-it informacion.

Informacioni, përfshirë edhe të dhënat personale, mund të merret nga Europol-i edhe nga burimet publike, sikurse interneti. Transferimet e të dhënave personale tek organet e BE-së lejohen vetëm nëse është e nevojshme për kryerjen e një detyre nga ana e Europolit, apo organit të BE-së që e përfton. Transferimet e të dhënave personale tek vendet e treta, ose organizatat ndërkombëtare lejohet vetëm nëse Komisioni Evropian vendos që ai vend, apo ajo organizatë ndërkomëtare garanton nivel të përshtatshëm të mbrojtjes së të dhënave ('vendim përshtatshmërie'), ose nëse ekziston një marrëveshje ndërkombëtare, apo bashkëpunimi. Europol-i mund të përftojë dhe të përpunojë të dhëna personale nga palë private dhe persona fizikë me kushtin e rreptë që ato të dhëna të jenë transferuar nga një ENU në përputhje me të drejtën kombëtare përkatësë, nëpërmjet një pike kontakti në vendin e tretë, apo një organizate ndërkombëtare me të cilën ka lidhur një marrëveshje bashkëpunimi, ose një autoritet të një vendi të tretë, ose një organizate ndërkombëtare, që është subjekt i një vendimi përshtatshmërie, ose me të cilën BE-ja ka lidhur një marrëveshje ndërkombëtare. Të gjitha shkëmbimet e informacionit bëhen nëpërmjet një Aplikacioni Rrjeti për Shkëmbim të Sigurt të Informacionit (SIENA).

Në përgjigje të zhvillimeve të reja, janë ngritur brenda Europol-it qendra të specializuara. Qendra Evropiane për Luftën kundër Krimit Kibernetik është ngritur brenda kësaj agjencie në vitin 2013.[813] Qendra shërben si një platformë informacioni e BE-së për krimin kibernetik dhe jep ndihmesë për reagime më të shpejta në raste krimesh në internet, zhvillon dhe zbaton kapacitete kriminalistike digjitale dhe harton praktika të mira në fushën e hetimit të krimeve kibernetike. Aktiviteti i saj përqendrohet në krimet kibernetike të cilat:

- Kryhen nga grupe të organizuara, për të gjeneruar fitime të mëdha kriminale, sikurse është mashtrimi në internet;
- Shkaktojnë dëme të mëdha për viktimat, sikuse shfytëzimi seksual i fëmijëve në internet;
- Cënojnë infrastrukturën kritike, apo sistemet e informacionit në BE.

Qendra Evropiane e Luftës kundër Terrorizmit (ECTC) është krijuar në janar të 2016-ës, me qëllim mbështetjen operative të Shteteve Anëtare për hetimet në lidhje me veprat terroriste. Ajo krahason në kohë reale të dhënat operative me të dhënat që disponon Europol-i, zbulon me shpejtësi lidhjet financiare dhe analizon të gjitha hollësitë hetimore, me qëllim ndërtimin e një panorame të strukturuar të një rrjeti terrorist.[814]

Qendra Evropiane e Luftës kundër Trafikut të Emigrantëve (EMSC) është ngritur në shkurt 2016, pas një mbledhjeje të Këshillit të mbajtur në nëntor 2015, për të mbështetur Shtetet Anëtare që të

[812] Regullorja (BE) 2016/794 e Parlamentit Evropian dhe e Këshillit e 11 majit 2016 mbi Agjencinë e Bashkimit Evropian për Bashkëpunim Ligjzbatues (Europol) dhe që zëvendëson e shfuqizon Vendimet e Këshillit 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA dhe 2009/968/JHA, FZ 2016 L 135, fq. 53.

[813] Shih gjithashtu, EDPS (2012), *Opinion of the Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre*, (Opinion i Mbikëqyrësit Evropian të Mbrojtjes së të Dhënave në lidhje me Komunikatën e Komisionit Evropian për Këshillin dhe Parlamentin Evropian në lidhje me ngritjen e Qendrës Evropiane të Luftës kundër Krimit Kibernetik), Bruksel, 29 qershor 2012.

[814] Shih faqen e internetit të Europol-it në lidhje me ECTC-në.

evidentojnë dhe shkatërrojnë rrjetet kriminale që merren me trafikim emigrantësh. Ajo shërben si një platformë informacioni në mbështetje të zyrave të Njësive Speciale Rajonale të BE-së në Katania (Itali) dhe në Pire' (Greqi), të cilat ndihmojë autoritetet kombëtare në fusha të ndryshme, përfshirë shkëmbimin e të dhënave operative, hetimet dhe ndjekjen penale të rrjeteve kriminale të trafikimit të personave.[815]

Regjimi i mbrojtjes së të dhënave që rregullon aktivitetet e Europol-it është përforcuar dhe mbështetet mbi parimet e Rregullores së Mbrojtjes së të Dhënave të Institucioneve të BE-së[816] dhe është në pajtim me Direktivën e Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale, Konventën 108 të Modernizuar dhe Rekomandimin për Policinë.

Përpunimi i të dhënave personale që kanë të bëjnë me viktimat e veprave penale, dëshmitarët, ose personat e tjerë që mund të japin informacion në lidhje me vepra penale, ose personat nën moshën 18 vjeç, lejohet në masën që është absolutisht i nevojshëm dhe proporcional me qëllimet e parandalimit, ose luftës kundër krimeve që përfshihen në objektivat e Europol-it.[817] Përpunimi i të dhënave personale sensitive është i ndaluar, përveçse kur është absolutisht i nevojshëm dhe proporcional me qëllimet e parandalimit, apo luftës kundër krimeve që përfshihen në objektivat e Europol-it dhe në masën që ato të dhëna plotësojnë të dhëna të tjera personale të përpunuara nga Europol-i.[818] Në të këto raste, vetëm Europol-i mund të ketë akses tek të dhënat përkatëse.[819]

Mbajtja e të dhënave lejohet vetëm për një kohëzgjatje të nevojshme dhe proporcionale dhe vazhdimësia e mbajtjes së tyre i nënshtrohet shqyrtimit çdo tre vite, pa kryerjen e së cilit ato të dhëna fshihen automatikisht.[820]

Europol-i mund të transferojë drejtpërdrejtë, me disa kushte të caktuara, të dhëna personale tek një organ i BE-së, apo një autoritet i një vendi të tretë, ose një organizatë ndërkombëtare.[821] Shkeljet ndaj të dhënave, nëse kanë gjasa të cënojnë rëndë të drejtat dhe liritë e subjekteve të të dhënave të përfshirë, duhet t'u bëhen me dije atyre pa vonesë të panevojshme.[822] Në nivel Shteti Anëtar, caktohet një autoritet mbikëqyrës kombëtar për të mbikëqyrur përpunimin e të dhënave personale nga ana e Europol-it.[823]

Mbikëqyrësi Evropian i Mbrojtjes së të Dhënave është përgjegjës për monitorimin dhe garantimin e mbrojtjes së të drejtave dhe lirive të personave fizikë në lidhje me përpunimin e të dhënave personale nga Europol- dhe për ta këshilluar Europol-in dhe subjektet e të dhënave për çdo çështje që ka të bëjë me përpunimin e të dhënave personale. Për këtë qëllim, EDPS-ja vepron luan rolin e një organi hetimi dhe ankimi dhe vepron në bashkëpunim të ngushtë me autoritetet mbikëqyrëse kombëtare.[824] EDPS-ja dhe autoritetet mbikëqyrëse kombëtare takohen të paktën dy herë në vit në kuadër të Bordit të Bashkëpunimit, i cili ka funksion këshillimor.[825] Shtetet Anëtare janë të detyruara të ngrenë me ligj një autoritet mbikëqyrës, kompetent për të monitoruar pranueshmërinë e transferimit të të dhënave personale nga një Shtet Anëtar tek Europol-i, ashtu si edhe si çdo ekstraktim dhe komunik të dhënash personale me Europol-in nga ana e Shtetit Anëtar[826] Shtetet Anëtare janë gjithashtu të detyruara të garantojnë që autoriteti mbikëqyrës kombëtar të veprojë në mënyrë plotësisht të pavarur gjatë ushtrimit të detyrave dhe përgjegjësive të tij sipas Rregullorës së Europol-it.[827] Me qëllim verifikimin e ligjshmërisë së përpunimit të të dhënave, për të vetëvlerësuar aktivitetet e tij dhe për të garantuar integritetin e sigurinë e përpunimit të të dhënave, Europol-i mban regjistra, ose dokumenton aktivitetet e tij të përpunimit të të dhënave. Këto regjistra përmbajnë informacion në lidhje me operacionet e

[815] Shih Europol's faqen e internetit të Europol-it në lidhje me EMSC-së.
[816] Rregullorja (KE) nr. 45/2001 e Parlamentit Evropian dhe e Këshillit e 18 dhjetorit 2000 për mbrojtjen e personave në lidhje me përpunimin e të dhënave personale nga institucionet dhe organet e Komunitetit dhe mbi lëvizjen e lirë të këtyre të dhënave, FZ 2001 L 8.
[817] Rregullorja e Europol-it, neni 30, pika 1.
[818] *Ibid*., neni 30, pika 2.
[819] *Ibid.,* neni 30, pika 3.
[820] *Ibid.,* neni 31.
[821] *Ibid*., nenet 24 dhe 25, përkatësisht.
[822] *Ibid*., neni 35.
[823] Rregullorja e Europol-it, neni 42.
[824] *Ibid*., nenet 43 dhe 44.
[825] *Ibid*., neni 45.
[826] *Ibid*., neni 42, pika 1.
[827] *Ibid*., neni 42, pika 1.

përpunimit në sistemet e automatizuara të përpunimit, që lidhen me mbledhjen, modifikimin, konsultimin, përhapjen, kombinimin dhe fshirjen e të dhënave.[828]

Kundër vendimeve të EDPS-së mund të bëhen ankim pranë GJDBE-së.[829] Çdo person i cili ka pësuar dëm si rezultat i një operacioni të paligjshëm përpunimi të dhënash, ka të drejtën të marrë kompensim për dëmin e pësuar, qoftë nga Europol-i, ose nga Shteti Anëtar përgjegjës, duke u ankuar në GJDBE në rastin e parë, ose në gjykatën kompetente kombëtare në rastin e dytë.[830] Gjithashtu, një Grup i Përbashkët Kontrolli Parlamentar (GPKP) i specializuar i parlamenteve komvëtare dhe i Parlamentit Evropian mund të kontrollojë aktivitetet e Europol-it.[831] Çdo person ka të drejtën e aksesit tek çdo e dhënë personale që Europol-i mund të mbajë në lidhje me të, ashtu sikurse të drejtën për të kërkuar që këto të dhëna personale të verifikohen, korrigjohen, ose fshihen. Këto të drejta mund t'u nënshtrohen përjashtimeve dhe kufizimeve.

Eurojust-i

Eurojust-i është ngritur në vitin 2002 dhe është një organ i BE-së me seli në Hagë. Ai nxit bashkëpunimin gjyqësor për hetime dhe ndjekje penale të krimeve të rënda që prekin të paktën dy Shtete Anëtare.[832] Eurojust-i ka tagret të:

- Nxisë dhe përmirësojë koordinimin e hetimeve dhe ndjekjeve penale midis autoriteteve kompetente të Shteteve Anëtare të ndryshme;
- Lehtësojë ekzekutimin e kërkesave dhe vendimeve që kanë të bëjnë me bashkëpunimin gjyqësor.

Funksionet e Eurojust-it ushtrohen nga anëtarët kombëtarë. Secili Shtet Anëtar delegon një gjyqtar, ose prokuror pranë Eurojust-it, statusi i të cilit i nënshtrohet të drejtës kombëtare dhe të cilit i jepen kompetencat e nevojshme për përmbushjen e detyrave të nevojshme për të nxitur dhe përmirësuar bashkëpunimin gjyqësor. Gjithashtu, anëtarët kombëtarë veprojnë në mënyrë kolegjiale për kryerjen e detyrave speciale të Eurojust-it.

Eurojust-i mund të përpunojë të dhëna personale për aq sa është e nevojshme për arritjen e objektivave të tij. Megjithatë, ky përpunim kufizohet tek informacioni i caktuar që ka të bëjë me personat e dyshuar për kryerjen, ose pjesëmarrjen, apo që janë dënuar për një vepër penale që është kompetencë e Eurojust-it. Eurojust-i mund të përpunojë gjithashtu disa informacione që lidhen me dëshmitarët, apo viktimat e veprave penale që përfshihen në kompetencat e Eurojust-it.[833] Në rrethana jo të zakonshme, Eurojust-i mund të përpunojë, për një periudhë të kufizuar kohore, të dhëna personale më të zgjeruara, që lidhen me rrethanat e një vepre penale, kur ato të dhëna janë menjëherë të rëndësishme për një hetim që po zhvillohet. Brenda sferës së kompetencës së tij, Eurojust-i mund të bashkëpunojë me institucione, organe dhe agjenci të tjera të BE-së dhe të shkëmbejë të dhëna personale me to. Eurojust-i mund të bashkëpunojë dhe të shkëmbejë të dhëna personale edhe me vende të treta e organizata ndërkombëtare.

Për sa i përket mbrojtjes së të dhënave, Eurojust-i duhet të garantojë nivel mbrojtjeje, të paktën të barasvlershëm me parimet e Konventës 108 të Modernizuar dhe me ndryshimet e mëvonshme të saj. Në rast shkëmbimi të dhënash, duhen respektuar rregullat dhe kufizimet specifike, të cilat janë

[828] *Ibid*., neni 40.
[829] *Ibid*., neni 48.
[830] *Ibid.,* neni 50.
[831] *Ibid*., neni 51.
[832] Këshilli i Bashkimit Evropian (2002), Vendim i Këshillit 2002/187/JHA i 28 shkurtit 2002 për ngritjen e Eurojust-it me qëllim përforcimin e luftës kundër krimeve të rënda, FZ 2002 L 63; Këshilli i Bashkimit Evropian (2003), Vendim i Këshillit 2003/659/JHA i 18 qershorit 2003 që ndryshon Vendimin 2002/187/JHA për ngritjen e Eurojust-it me qëllim përforcimin e luftës kundër krimeve të rënda, FZ 2003 L 44; Këshilli i Bashkimit Evropian (2009), Vendim i Këshillit 2009/426/JHA i 16 dhjetorit 2008 mbi forcimin e Eurojust-it dhe që ndryshon Vendimin 2002/187/JHA për ngritjen e Eurojust-it me qëllim përforcimin e luftës kundër krimeve të rënda, FZ 2009 L 138 (Vendimet për Eurojust-in).
[833] Varianti i konsoliduar i Vendimit të Këshillit 2002/187/JHA, ndryshuar me Vendimin e Këshillit 2003/659/JHA dhe me Vendimin e Këshillit 2009/426/JHA, neni 15, pika 2.

përcaktuar qoftë në marrëveshjen e bashkëpunimit, ashtu edhe në rregulloren e punës, në përputhje me Vendimin e Këshillit për Eurojust-in dhe Rregullat e Mbrojtjes së të Dhënave të Eurojust-it.[834]

Pranë Eurojust-it është ngritur një Organ i Përbashkët Mbikëqyrës (OPM), i cili ka për detyrë të kontrollojë përpunimin e të dhënave personale që zhvillon Eurojust-i. Çdo person mund të ankohet tek OPM-ja nëse nuk është i kënaqur me vendimin e Eurojust-it në lidhje me kërkesën për akses, korrigjim, bllokim, apo fshirje të të dhënave personale. Nëse Eurojust-i përpunon të dhëna personale në mënyrë të paligjshme, ai është përgjegjës për çdo dëm të shkaktuar ndaj subjektit të të dhënave, në përputhje me të drejtën kombëtare të Shtetit Anëtar në të cilin ndodhet selia e tij, konkretisht atë të Vendeve të Ulëta.

Perspektiva

Komisioni Evropian ka paraqitur në korrik 2013 një projekt-rregullore për reformimin e Eurojust-it. Ky projekt shoqërohej me një propozim për ngritjen e Zyrës së Prokurorit Publik Evropian (shih më poshtë). Kjo rregullore synon të ravijëzojë funksionet dhe strukturën e tij, me qëllim që të jenë në përputhje me Traktatin e Lisbonës. Gjithashtu, reforma ka për qëllim të përcaktojë një ndarje të qartë midis detyrave operative të Eurojust-it, që kryhen nga Kolegji i Eurojust-it, nga detyrat administrative të tij. Diçka e tillë do t'u mundësojë gjithashtu Shteteve Anëtare që të përqendrohen më shumë në detyrat operative. Një Bord i ri Ekzekutiv do të ngrihet, me qëllim që të ndihmojë kolegjin në përmbushjen e detyrave administrative.[835]

Zyra e Prokurorit Publik Evropian

Shtetet Anëtare kanë kompetencën ekskluzive për të ndjekur penalisht veprat penale të mashtrimit dhe keqpërdorimit të bugjetit të BE-së, që mund të kenë shtrirje ndërkufitare. Është rritur rëndësia e hetimit, ndjekjes penale dhe dërgimit përpara drejtësisë së autorëve të këtyre veprave penale, sidomos për shkak të krizës aktuale ekonomike.[836] Komisioni Evropian ka propozuar një Rregullore për ngritjen e Zyrës së Prokurorit Publik Evropian (EPPO)[837], që ka si objektiv të luftojë veprat penale që cënojnë interesat financiare të BE-së. EPPO-ja do të ngrihet me anë të procedurës së bashkëpunimit të përforcuar, e cila lejon një minimum prej nëntë Shtetesh Anëtare të ndërmarrin bashkëpunim të përforcuar në një fushë brenda strukturave të BE-së, pa përfshirë vendet e tjera të BE-së.[838] Belgjika, Bullgaria, Kroacia, Qiproja, Republika Çeke, Estonia, Finlanda, Franca, Gjermania, Greqia, Letonia, Lituania, Luksemburgu, Portugalia, Rumania, Sllovenia, Sllovakia dhe Spanja janë përfshirë në bashkëpunimin e përforcuar, ndërsa Austria dhe Italia kanë shprehur synimin e tyre për t'u përfshirë.[839]

EPPO-ja do të ketë kompetencën të hetojë dhe ndjekë penalisht mashtrimin dhe vepra të tjera penale që cënojnë interesat financiare të BE-së, me qëllimin për të koordinuar në mënyrë të efektshme hetimet dhe ndjekjet penale në rendet e ndryshme juridike kombëtare dhe për të përmirësuar përdorimin e burimeve dhe shkëmbimin e informacionit në nivel Evropian.[840]

EPPO-ja do të drejtohet nga një Prokuror Publik Evropian dhe do të ndihmohet nga të paktën një Prokuror Evropian i deleguar nga secili Shtet Anëtar, që do të jetë i ngarkuar me kryerjen e hetimeve dhe ndjekjeve penale në atë Shtet Anëtar.

Propozimi përcakton garanci të forta për respektimin e të drejtave të personave që përfshihen në hetimet e EPPO-së, në përputhje me të drejtën kombëtare, të drejtën e BE-së dhe Kartën e të Drejtave Themelore të BE-së. masat hetimore që prekin kryesisht të drejtat themelore, do të duhet të autorizohen nga një

---

[834] Rregullat e Procedurës mbi Përpunimin dhe Mbrojtjen e të Dhënave Personale nga Eurojust-i, FZ 2005 C 68/01, 19 mars 2005, fq. 1.
[835] Shih faqen e internetit për Eurojust-in të Komisionit Evropian.
[836] Shih: Komisioni Evropian (2013), Propozim për një Rregullore të Këshillit për ngritjen e Zyrës së Prokurorit Publik Evropian, COM(2013) 534 final, Bruksel, 17 korrik 2013, fq. 1 dhe faqen e internetit për EPPO-në të Komisionit Evropian.
[837] Komisioni Evropian (2013), Propozim për një Rregullore të Këshillit për ngritjen e Zyrës së Prokurorit Publik Evropian, COM(2013) 534 final, Bruksel, 17 korrik 2013.
[838] Traktati mbi Funksionimin e BE-së, neni 86, pika 1 dhe neni 329, pika 1.
[839] Shih njoftimin për shtyp të Këshillit të Bashkimit Evropian (2017), "*20 member states agree on the details of creating the European Public Prosecutor's Office (EPPO)*", 8 qershor 2017.
[840] Komisioni Evropian, (2013), Propozim për një Rregullore të Këshillit për ngritjen e Zyrës së Prokurorit Publik Evropian, COM(2013) 534 final, Bruksel, 17 korrik 2013, fq 1 dhe 51. Shih gjithashtu faqen e internetit për EPPO-në të Komisionit Evropian.

gjykatë kombëtare.[841] Hetimet e EPPO-së do t'i nënshtrohen kontrollit juridiksional nga gjykatat kombëtare.[842]

Rregullorja e Mbrojtjes së të Dhënave të Institucioneve të BE-së[843] do të zbatohet për përpunimin e të dhënave personale administrative që do të kryejë EPPO-ja. Për përpunimin e të dhënave personale që lidhen me çështje operative, ashtu sikurse për Europol-in, edhe EPPO-ja do të ketë një regjim mbrojtjeje të dhënash më vete, të ngjashëm me atë që rregullon aktivitetet e Europol-it dhe Eurojust-it, kjo pasi ushtrimi i funksioneve nga EPPO-ja do të përfshijë përpunim të dhënash personale me autoritetet ligjzbatuese dhe të ndjekjes penale në nivel Shteti Anëtar. Rregullat e mbrojtjes së të dhënave të EPPO-së janë rrjedhimisht pothuajse identike me rregullat e Direktivës së Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale. Sipas Propozimit për ngritjen e EPPO-së, përpunimi i të dhënave personale duhet të respektojë parimet e ligjshmërisë dhe drejtësisë, kufizimit të qëllimit, minimizimit të të dhënave, saktësisë, integritetit dhe konfidencialitetit. EPPO-ja duhet të bëjë dallim të qartë, për aq sa është e mundur, midis të dhënave personale të llojeve të ndryshme të subjekteve të të dhënave, sikurse për personat e dënuar për vepra penale, personat që janë thjesht të dyshuar, viktimat dhe dëshmitarët. Gjithashtu, ajo duhet të përpiqet të verifikojë cilësinë e të dhënave personale të përpunuara dhe të dallojë, për aq sa është e mundur, të dhënat personale të mbështetura mbi fakte, nga të dhënat personale që bazohen në gjykime personale.

Propozimi përfshin dispozita në lidhje me të drejtat e subjekteve të të dhënave, veçanërisht të drejtës për t'u informuar, për akses tek të dhënat personale, për korrigjim, fshirje dhe kufizim të përpunimit dhe parashikon se këto të drejta mund të ushtrohen edhe në mënyrë të tërthortë, me ndërmjetësimin e EDPS-së. Në të parashikohen gjithashtu parimet e sigurisë së përpunimit dhe përgjegjshmërië, të cilat detyrojnë EPPO-në të marrë masat e duhura teknike dhe organizative për të garantuar nivel të përshtatshëm sigurie kundër risqeve që paraqet përpunimi, të mbajë regjistra të të gjitha aktiviteteve të përpunimit dhe kryejë vlerësime ndikimi tek mbrojtja e të dhënave përpara nisjes së përpunimit, nëse një përpunim i caktuar (për shembull, përpunimi që përfshin përdorim teknologjish të reja) ka të ngjarë të shkaktojë rrezik të lartë për të drejtat e personave fizikë. Së fundmi, propozimi parashikon caktimin nga ana e kolegjit të një Nëpunësi të Mbrojtjes së të Dhënave, i cili, apo e cila, duhet përfshirë në të gjitha çështjet që lidhen me mbrojtjen e të dhënave personale dhe të kujdeset që EPPO-ja respekton legjislacionin përkatës të mbrojtjes së të dhënave.

8.3.2. Mbrojtja e të dhënave në sistemet e përbashkëta të informacionit në nivel BE-je

Përveç shkëmbimit të të dhënave midis Shteteve Anëtare dhe krijimit të autoriteteve speciale të BE-së për të luftuar krimin ndërkufitar, sikurse Europol-i, Eurojust-i dhe EPPO-ja, janë ngritur disa sistemeve informacioni në nivel BE-je, për të mundësuar dhe lehtësuar bashkëpunimin dhe shkëmbimin e të dhënave midis autoriteteve kompetente kombëtare dhe të BE-së, për qëllime të caktuara në fushat e mbrojtjes së kufijve, emigracionit dhe azilit dhe doganave. Meqenëse zona Schengen u krijua fillimisht me anë të një marrëveshjeje ndërkombëtare, të pavarur nga e drejta e BE-së, Sistemi i Informacionit të Schengen-it (SIS) u zhvillua nëpërmjet marrëveshjeve shumëpalëshe dhe u integrua më pas në të drejtën e Bashkimit. Sistemi i Informacionit të Vizave (VIS), Eurodac-u, Eurosur-i dhe Sistemi i Informacionit të Doganave (CIS) u krijuan si instrumente të rregulluara nga e drejta e BE-së.

Mbikëqyrja e këtyre sistemeve ndahet midis autoriteteve mbikëqyrëse kombëtare dhe EDPS-së. Për të garantuar nivel të lartë mbrojtjeje, këto autoritete bashkëpunojnë brenda Grupeve të Koordinimit të Mbikëqyrjes (SCG-të), që u referohen sistemeve TI në shkallë të gjerë si vijon: 1) Eurodac-u; 2) Sistemi i Informacionit të Vizave; 3) Sistemi i Informacionit të Schengen-it; 4) Sistemi i Informacionit të

[841] Komisioni Evropian (2013), Propozim për një Rregullore të Këshillit për ngritjen e Zyrës së Prokurorit Publik Evropian, COM(2013) 534 final, Bruksel, 17 korrik 2013, neni 26, pika 4.
[842] *Ibid.*, neni 36.
[843] Rregullorja (KE) nr. 45/2001 e Parlamentit Evropian dhe e Këshillit e 18 dhjetorit 2000 për mbrojtjen e personave në lidhje me përpunimin e të dhënave personale nga institucionet dhe organet e Komunitetit dhe për lëvizjen e lirë të këtyre të dhënave, FZ 2001 L 8.

Doganave dhe 5) Sistemi i Informacionit të Tregut të Brendshëm.[844] SCG-të mblidhen zakonisht dy herë në vit, nën drejtimin e një kryetari të zgjedhur dhe miratojnë udhëzues, diskutojnë çështje ndërkufitare, ose miratojnë kuadro të përbashkët inspektimesh.

Agjencia Evropiane për Sistemet e Teknologjisë së Informacionit në Shkallë të Gjerë (eu-LISA),[845] e ngritur në vitin 2012, është përgjegjëse për menaxhimin operativ të Sistemit të Informacionit të Schengen-it të gjeneratës së dytë (SIS II), Sistemit të Informacionit të Vizave (VIS) dhe Eurodac-ut. Detyra kryesore e eu-LISA-s është të garantojë shfrytëzimin në mënyrë të efektshme, të sigurt dhe të pandërprerë të sistemeve të teknologjisë së informacionit. Ajo është po ashtu përgjegjëse për marrjen e masave të nevojshme për të garantuar sigurinë e sistemeve dhe sigurinë e të dhënave.

Sistemi i Informacionit të Schengen-it

Në vitin 1985, disa Shtete Anëtare të të dikurshmit Komunitet Evropian, lidhën një Marrëveshje ndërmjet shteteve të Bashkimit Ekonomik të Beneluksit, Gjermanisë dhe Francës, në lidhje me heqjen të shkallëzuar të kontrolleve në kufijtë e tyre të përbashkët (Marrëveshja e Schengen-it), me synimin për të krijuar një zonë të lëvizjes së lirë të njerëzve, të papenguar nga kontrollet kufitare, brenda territorit të Schengen-it.[846] Për të kundërpeshuar kërcënimin ndaj sigurisë publike, që mund të krijohej nga kufijtë e hapur, u përforcuan kontrollet kufitare në kufijtë e jashtëm të zonës së Schengen-it dhe bashkëpunimi midis policive dhe autoriteteve gjyqësore kombëtare.

Si pasojë e anëtarësimit të mëtejshëm të shteteve të tjera në Marrëveshjen e Schengen-it, sistemi i Schengen-it u integrua përfundimisht në kuadrin ligjor të BE-së nëpërmjet Traktatit të Amsterdamit.[847] Ky vendim u zbatua në vitin 1999. Varianti më i ri i Sistemit të Informacionit të Schengen-it, i ashtuquajturi SIS II, hyri në veprim më 9 prill 2013. Ai i shërben tashmë pjesës më të madhe të Shteteve Anëtare të BE-së,[848] si dhe Islandës, Lihtenshtejnit, Norvegjisë dhe Zvicrës.[849] Europol-i dhe Eurojust-i kanë gjithashtu akses tek SIS II.

SIS II konsiston në një sistem qendror (C-SIS), një sistem kombëtar (N-SIS) në secilin Shtet Anëtar dhe në një infrastrukturë komunikimi midis sistemit qendror dhe sistemeve kombëtare. C-SIS-i përmban disa të dhëna të regjistruara nga Shtetet Anëtare, që lidhen me njerëz dhe objekte. SIS-i përdoret nga autoritet kombëtare të kontrollit kufitar, policia, doganat, vizat dhe autoritetet gjyqësore në të gjithë Zonën Schengen. Secili Shtet Anëtar përdor një kopje kombëtare të C-SIS-it, që njihet si Sistemi Kombëtar i Informacionit të Schengen-it (N-SIS), i cili përditësohet vazhdimisht, duke përditësuar rrjedhimisht C-SIS-in. SIS-i bën sinjalizime të llojeve të ndryshme:

- Personi nuk ka të drejtë të hyjë, apo të qëndrojë në territorin e Schengen-it; ose
- Personi, apo objekti është në kërkim nga autoritetet gjyqësore, apo ligjzbatuese (p.sh. urdhër arresti evropian, kërkesë për kontroll të kujdesshëm); ose
- Personi është shpallur i humbur; ose
- Mallrat, sikurse kartëmonedhat, veturat, kamionët, armët e zjarrit dhe dokumentet e identifikimit, janë sinjalizuar si të vjedhura, apo të humbura.

---

[844] Shih faqen në internet për Koordinimin e Mbikëqyrjes të Mbikëqyrësit Evropian të Mbrojtjes së të Dhënave.
[845] Rregullorja (BE) nr. 1077/2011 e Parlamentit Evropian dhe e Këshillit e 25 tetorit 2011 për ngritjen e Agjencisë Evropiane për menaxhimin operativ të sistemet të TI-së në shkallë të gjerë, në fushën e lirisë, sigurisë dhe drejtësisë, FZ 2011 L 286.
[846] Marrëveshje mids qeverive të shteteve të Bashkimit Ekonomik të Beneluksit, Republikës Federale të Gjermanisë dhe Republikës Franceze për heqjen e shkallëzuar të kontrolleve në kufijtë e tyre të përbashkët, FZ 2000 L 239.
[847] Komunitetet Evropiane (1997), Traktati i Amsterdamit që ndryshon Traktatin e Bashkimit Evropian, Traktatet që themelojnë Komunitetet Evropiane dhe disa akte të tjera të ndërlidhura, FZ 1997 C 340.
[848] Kroacia, Qiproja dhe Irlanda janë duke zhvilluar aktivitete përgatitore për të hyrë në SIS II, por nuk janë ende pjesë e tij. Shih informacionin në lidhje me Sistemin e Informacionit të Schengen-it në faqen në internet të Drejtorisë së Përgjithshme për Migracionin dhe Punët e Brendshme të Komisionit Evropian.
[849] Rregullorja (KE) nr. 1987/2006 e Parlamentit Evropian dhe e Këshillit e 20 dhjetorit 2006 për ngritjen, veprimin dhe përdorimin e Sistemit të Informacionit të Schengen-it të gjeneratës së dytë, FZ 2006 L 381 (SIS II) dhe Këshillit i Bashkimit Evropian (2007), Vendimin e Këshillit 2007/533/JHA të 12 qershorit 2007 për ngritjen, veprimin dhe përdorimin e Sistemit të Informacionit të Schengen-it të gjeneratës së dytë, (SIS II), FZ 2007 L 205.

Kur ka një sinjalizim, veprimet në vijim ndërmerren nga zyrat SIRENE. SIS II ka funksione të reja, sikurse mundësinë e regjistrimit të të dhënave biometrike, si gjurmët e gishtave dhe fotografitë, apo kategori sinjalizimesh të reja, si për shembull për anije, avionë, konteinerë, apo mjete pagese të vjedhura, sinjalizime të përmirësuara për persona dhe objekte dhe kopje urdhër-arrestesh evropiane (EAW-të) për persona të kërkuar për qëllime arrestimi, gjetjeje, apo ekstradimi.

SIS II mbështetet në dy akte që plotësojnë njëra-tjetrën: Vendimi SIS II[850] dhe Rregullorja SIS II.[851] Ligjvënësi i BE-së ka përdorur dy baza të ndryshme ligjore për miratimin e vendimit dhe të rregullores. Vendimi rregullon përdorimin e SIS II për qëllime të bashkëpunimit policor dhe gjyqësor për çështje penale (ish-shtylla e tretë e BE-së). Rregullorja zbatohet për procedurat e sinjalizimit që kanë të bëjnë me vizat, azilin, emigracionin dhe politika të tjera në lidhje me lëvizjen e lirë të personave (ish-shtylla e parë). Procedurat e sinjalizimit për secilën shtyllë duhet të rregulloheshin me akte më vete, meqenëse të dy aktet juridike u miratuan përpara Traktatit të Lisbonës dhe shfuqizimit të strukturës së shtyllave.

Të dy aktet ligjore përmbajnë rregulla për mbrojtjen e të dhënave. Vendimi SIS II ndalon përpunimin e të dhënave sensitive.[852] Përpunimi i të dhënave personale duhet të mbulohet nga fusha e zbatimit të Konventës 108 të Modernizuar.[853] Gjithashtu, personat kanë të drejtën e aksesit tek të dhënat personale në lidhje me ta, të cilat janë regjistruar në SIS II.[854]

Rregullorja SIS II përcakton kriteret dhe procedurat për regjistrimin dhe përpunimin e sinjalizimeve që kanë të bëjnë me hyrjen, apo qëndrimin e shtetasve të vendeve të treta. Ajo përcakton gjithashtu rregullat për shkëmbimin e informacionit plotësues dhe shtesë, për qëllime të hyrjes, apo qëndrimit në një Shtet Anëtar.[855] Kjo rregullore përmban gjithashtu rregulla në lidhje me mbrojtjen e të dhënave. Përpunimi i kategorive të të dhënave sensitive të referuara në nenin 9, pika 1 të Rregullores së Përgjithshme të Mbrojtjes së të Dhënave, është i ndaluar.[856] Rregullorja SIS II përmban gjithashtu disa të drejta për subjektin e të dhënave, të cilat janë:

- E drejta e aksesit tek të dhënat personale që lidhen me subjektin e të dhënave;[857]
- E drejta për të korrigjuar të dhëna të pasakta;[858]
- E drejta për të fshirë të dhëna që mbahen në mënyrë të paligjshme;[859] dhe
- E drejta për t'u informuar në rast sinjalizimi të subjektit të të dhënave. Informacioni duhet dhënë me shkrim dhe të shoqërohet me një kopje, apo referencë të vendimit të vendit që ka bërë sinjalizimin.[860]

E drejta për t'u informuar nuk do të zbatohet nëse: 1) të dhënat personale nuk janë marrë nga subjekti i të dhënave dhe dhënia e informacionit është e pamundur, apo kërkon përpjekje të shpërpjesëtuara, 2) subjekti i të dhënave është në dijeni të informacionit, ose 3) nëse e drejta kombëtare lejon kufizime, ndër të tjera për mbrojtjen e sigurisë kombëtare, apo parandalimin e veprave penale.[861]

Si për Vendimin SIS II, ashtu edhe për Rregulloren SIS II, e drejta e aksesit për personat në lidhje me SIS II mund të ushtrohet në çdo Shtet Anëtar dhe do të trajtohet në përputhje me të drejtën kombëtare të atij Shteti Anëtar.[862]

[BOX TYPE 1]

---

[850] Vendimi i Këshillit 2007/533/JHA i 12 qershorit 2007 për ngritjen, veprimin dhe përdorimin e Sistemit të Informacionit të Schengen-it të gjeneratës së dytë (SIS II), FZ L 205, 7 gusht 2007.
[851] Rregullorja (KE) nr. 1987/2006 e Parlamentit Evropian dhe e Këshillit e 20 dhjetorit 2006 për ngritjen, veprimin dhe përdorimin e Sistemit të Informacionit të Schengen-it të gjeneratës së dytë (SIS II), FZ L 381, 28 dhjetor 2006.
[852] Vendimi SIS II, neni 56; Rregullorja SIS II, neni 40.
[853] Vendimi SIS II, neni 57.
[854] Vendimi SIS II, neni 58; Rregullorja SIS II, neni 41.
[855] Rregullorja SIS II, neni 2.
[856] *Ibid.*, neni 40.
[857] *Ibid*., neni 41, pika 1.
[858] *Ibid*., neni 41, pika 5.
[859] *Ibid*., neni 41, pika 5.
[860] *Ibid*., neni 42, pika 1.
[861] *Ibid*., neni 42, pika 2.
[862] Rregullorja SIS II, neni 41, pika 1 dhe Vendimi SIS II, neni 58.

Shembull: tek çështja *Dalea k. Francës*,[863] kërkuesit i ishte refuzuar viza për të vizituar Francën, pasi autoritetet francize kishin raportuar në Sistemin e Informacionit të Schengen-it se atij duhej t'i refuzohej hyrja. Kërkuesi kishte kërkuar më kot nga Komisioni i Mbrojtjes së të Dhënave të Francës dhe më pas edhe nga Këshilli i Shtetit që t'i jepej akses dhe të korrigjonte, apo të fshinte të dhënat. GJEDNJ-ja vlerësoi se sinjalizimi i kërkuesit në Sistemin e Informacionit të Schengen-it, ishte në përputhje me ligjin dhe ndiqte qëllimin legjitim të mbrojtjes së sigurisë kombëtare. Meqenëse kërkuesi nuk kishte demonstruar se çfarë dëmi kishte pësuar ai, si rezultat i refuzimit të hyrjes në zonën Schengen dhe meqenëse ishin marrë masa të mjaftueshme për ta mbrojtur atë nga vendimet arbitrare, ndërhyrja tek e drejta e tij për respektim të jetës private kishte qenë proporcionale. Kësisoj, ankimi i paraqitur nga kërkuesi në bazë të nenit 8, u shpall i papranueshëm.

Autoriteti kombëtar mbikëqyrës kompetent në secilin Shtet Anëtar, monitoron N-SIS-in kombëtar. Autoriteti kombëtar mbikëqyrës duhet të garantojë që të kryhet auditimi i operacioneve të përpunimit të të dhënave brenda N-SIS-it kombëtar, të paktën një herë në çdo katër vjet.[864] Autoritetet kombëtare mbikëqyrëse dhe EDPS-ja bashkëpunojnë dhe sigurojnë monitorim të koordinuar të N-SIS-it, ndërsa EDPS-ja është përgjegjëse për monitorimin e C-SIS-it. Për qëllime transparence, do t'i paraqitet Parlamentit Evropian, Këshillit dhe eu-LISA-s, një raport i përbashkët aktivitetesh çdo dy vite. Grupi i Mbikëqyrjes së SIS II (SCG) është ngritur me qëllim garantimin e monitorimit të koordinuar të SIS-it dhe mblidhet deri në dy herë në vit. Ky grup përbëhet nga EDPS-ja dhe përfaqësuesit e autoriteteve mbikëqyrëse të atyre Shteteve Anëtare që zbatojnë SIS II, si dhe Islanda, Lihtenshtejni, Norvegjia dhe Zvicra, pasi SIS-i zbatohet edhe për këto vende, meqenëse janë anëtare të Schengen-it.[865] Qiproja, Kroacia dhe Irlanda nuk bëjnë ende pjesë në SIS II dhe për rrjedhojë vetëm ndjekin SCG-në si vëzhguese. EDPS-ja dhe autoritetet kombëtare mbikëqyrëse bashkëpunojnë në mënyrë active brenda kuadrit të SCG-së, duke shkëmbyer informacion, duke ndihmuar njëra-tjetrën për kryerjen e auditeve dhe inspektimeve, duke hartuar propozime të harmonizuara për zgjidhje të përbashkëta të problemeve të mundshme dhe për nxitjen e ndërgjegjësimit në lidhje me të drejtat për mbrojtje të të dhënave.[866] SCG-ja e SIS II miraton gjithashtu udhëzues, për të ndihmuar subjektet e të dhënave. Një shembull i tillë është udhëzuesi për të ndihmuar subjektin e të dhënave në ushtrimin e të drejtës së tyre për akses.[867]

Perspektiva

Në vitin 2016, Komisioni Evropian zhvilloi një vlerësim të SIS-it[868], në të cilin rezultonte se ekzistonin mekanzima në nivel kombëtar, për t'u mundësuar subjekteve të të dhënave të përftonin akses, korrigjim dhe fshirje të të dhënave të tyre personale në SIS II, apo kompensim në lidhje me të dhënat e pasakta. Për të përmirësuar efektshmërinë e SIS II, Komisioni Evropian ka paraqitur tre projekt-rregullore:

- Një rregullore për ngritjen, veprimin dhe përdorimin e SIS-it në fushën e kontrollit kufitar, e cila do të shfuqizojë Rregulloren SIS II;
- Një rregullore për ngritjen, veprimin dhe përdorimin e SIS-it në fushën e bashkëpunimit policor dhe bashkëpunimit gjyqësor për çështje penale, e cila do të shfuqizojë, ndër të tjera, Vendimin SIS II; dhe
- Një rregullore për përdorimin e SIS-it për kthimin e personave nga vendet e treta që qëndrojnë në mënyrë të paligjshme.

[863] GJEDNJ, *Dalea k. Francës,* nr. 964/07, 2 shkurt 2010.
[864] Rregullorja SIS II, neni 60, pika 2.
[865] Shih faqen e internetit për Sistemin e Informacionit të Schengen-it të Mbikëqyrësit Evropian të Mbrojtjes së të Dhënave.
[866] Rregullorja SIS II, neni 46 dhe Vendimi SIS II, neni 62.
[867] Shih SCG-në e SIS II, *The Schengen Information System. A guide for exercising the right of access*, i disponueshëm në faqen e internetit të EDPS-së.
[868] Komisioni Evropian (2016), Raport i Komisionit për Parlamentin Evropian dhe Këshillin mbi vlerësimin e Sistemit të Informacionit të Schengen-it të gjeneratës së dytë (SIS II) në bazë të nenit 24, pika 5, 43, pika 3 dhe 50, pika 5, të Rregullores (KE) nr. 1987/2006 dhe nenit 59, pika 3 dhe 66, pika 5 të Vendimit 2007/533/JHA, COM(2016) 880 final, Bruksel, 21 dhjetor 2016.

Ka rëndësi të theksohet se projekt-rregulloret autorizojnë përpunimin e kategorive të tjera të të dhënave biometrike dhe jo vetëm të fotografive dhe gjurmëve të gishtave, që janë aktualisht pjesë e regjimit SIS II. Gjurmët faciale, gjurmët e pëllëmbëve dhe profilet e ADN-së do të regjistrohen gjithashtu në bazën e të dhënave të SIS-it. Po ashtu, ndërsa Rregullorja SIS II dhe Vendimi SIS II parashikonin mundësinë e kërkimit të gjurmëve të gishtave, me qëllim identifikimin e një personi, projekt-rregulloret e bëjnë të detyrueshëm këtë kërkim, nëse identiteti i personit nuk mund të vërtetohet në një mënyrë tjetër. Imazhet e fytyrës, fotografitë dhe gjurmët e pëllëmbëve do të përdoren për të kërkuar në sistem dhe për të identifikuar njerëzit, kur kjo të jetë e mundur teknikisht. Rregullat e reja në lidhje me cilësitë biometrike, paraqesin risqe të veçanta për personat. Në opinionin e tij në lidhje me projekt-rregulloret e Komisionit,[869] Mbikëqyrësi Evropian i Mbrojtjes së të Dhënave theksonte se të dhënat biometrike kanë sensitivitet të lartë dhe përfshirja e tyre në baza të dhënash të një shkalle kaq të gjerë, duhet të mbështetet në një vlerësim të elementeve të provës që justifikojnë përfshirjen e tyre në SIS. Thënë ndryshe, duhet vërtetuar domosdoshmëria e përpunimit të këtyre cilësive të reja. EDPS-ja vlerësonte gjithashtu se është e nevojshme të qartësohet më mirë se çfarë lloj informacioni do të përfshihet në profiling e ADN-së. Duke pasur parasysh se profili i ADN-së mund të përmbajë informacion sensitiv, (shembulli më i njohur është informacioni që zbulon probleme shëndetësore), profilet e ADN-së në SIS duhet të përmbajnë: "vetëm minimumin e informacionit që është absolutisht i nevojshëm për identifikimin e personave të humbur dhe të përjashtojë qartësisht informacionin në lidhje me shërndetin, origjinën racore dhe çdo informacion tjetër sensitiv." [870] Megjithatë, projekt-rregulloret parashikojnë garanci shtesë për kufizimin e mbledhjes dhe përpunimit të mëtejshëm të të dhënave vetëm kur është domosdoshmëri dhe e detyrueshme në planin operativ, si dhe për kufizimin e aksesit vetëm për personat të cilët kanë domosdoshmëri operative për të përpunuar të dhënat personale.[871] Projekt-rregulloret i mundësojnë gjithashtu eu-LISA-s, të hartojë me intervale të rregullta, raporte për Shtetet Anëtare, në lidhje me cilësinë e të dhënave, me qëllim vlerësimin periodik të sinjalizimeve dhe garantimin e cilësisë së të dhënave.[872]

Sistemi i Informacionit të Vizave

Sistemi i Informacionit të Vizave (VIS), i cili shfrytëzohet edhe nga eu-LISA, u zhvillua me qëllim për të ndihmuar në zbatimin e politikës evropiane të përbashkët për vizat.[873] VIS-i u mundëson shteteve të Schengen-it të shkëmbejnë të dhëna në lidhje me kërkuesit e vizave, me anë të një sistemi plotësisht të pëqendruar, i cili ndërlidh konsullatat dhe amabasadat e shteteve të Schengen-it, që janë të vendosura në vendet jashtë BE-së, me pikat e jashtme të kalimit kufitar të të gjitha shteteve të Schengen-it. VIS-i përpunon të dhëna në lidhje me aplikimet për viza qëndrimi afatshkurtër, për të vizituar, apo kaluar tranzit nëpër zonën Schengen. VIS-i u mundëson autoriteteve kufitare të verifikojnë, me anë të cilësive biometrike, kryesisht gjurmëve të gishtave, nëse personi që paraqet një vizë, është mbajtësi i vërtetë i saj dhe për të identifikuar personat pa dokumente, apo me dokumente të falsifikuara.

Rregullorja (KE) nr. 767/2008 e Parlamentit Evropian dhe e Këshillit, në lidhje me Sistemin e Informacionit të Vizave (VIS) dhe shkëmbimin e të dhënave midis Shteteve Anëtare për vizat afatshkurtra (Rregullorja VIS) përcakton kushtet dhe procedurat për transferimin e të dhënave personale që kanë të bëjnë me aplikimet për viza afatshkurtra. Ajo gjithashtu kontrollon vendimet e marra në lidhje me aplikimet, duke përfshirë vendimet për anulimin, revokimin, ose zgjatjen e vizave.[874]

---

[869] EDPS (2017), Opinion i EDPS-së në lidhje me bazën e re ligjore të Sistemit të Informacionit të Schengen-it, Opinioni 7/2017, 2 maj 2017.
[870] *Ibid*., paragrafi 22.
[871] Komisioni Evropian (2016), Propozim për një Rregullore të Parlamentit Evropian dhe Këshillit për ngritjen, veprimin dhe përdorimin e Sistemit të Informacionit të Schengen-it (SIS) në fushën e bashkëpunimit policor dhe bashkëpunimit gjyqësor për çështje penale, që ndryshon Rregulloren (BE) nr. 515/2014 dhe shfuqizon Rregulloren (KE) nr. 1986/2006, Vendimin e Këshillit 2007/533/JHA dhe Vendimin e Komisionit 2010/261/EE, COM(2016) 883 final, Bruksel, 21 dhjetor 2016.
[872] *Ibid*., fq. 15.
[873] Këshilli i Bashkimit Evropian (2004), Vendim i Këshillit 2004/512/EC i 8 qershorit 2004 për ngritjen e Sistemit të Informacionit të Vizave (VIS), FZ 2004 L 213; Rregullorja (KE) nr. 767/2008 e Parlamentit Evropian dhe e Këshillit e 9 korrikut 2008 që ka të bëjë me Sistemin e Informacionit të Vizave (VIS) dhe shkëmbimin e të dhënave midis Shteteve Anëtare për vizat afatshkurtra, FZ 2008 L 218 (Rregullorja VIS); Këshilli i Bashkimit Evropian (2008), Vendim i Këshillit 2008/633/JHA i 23 qershorit 2008 që ka të bëjë me aksesin për konsultimin e Sistemit të Informacionit të Vizave (VIS) nga autoritetet e përcaktuara të Shteteve Anëtare dhe nga Europol-i për qëllime të parandalimit, zbulimit dhe hetimit të veprave terroriste dhe krimeve të tjera të rënda, FZ 2008 L 218.
[874] Rregullorja VIS, neni 1.

Rregullorja VIS mbulon kryesisht të dhënat për kërkuesin, vizat e tij, ose të saj, fotografitë, gjurmët e gishtave, lidhjet me aplikime të mëparshme dhe dosjet e aplikimit të personave që e shoqërojnë, apo të dhëna në lidhje me personat që bëjnë ftesë.[875] Aksesi në VIS, për qëllime regjistrimi, ndryshimi, apo fshirje të të dhënave, është i kufizuar vetëm për autoritetet e vizave, ndërsa aksesi për të konsultuar të dhënat u jepet autoriteteve kompetente për kontrolle në pikat e jashtme të kalimit kufitar, kontrollet e emigracionit dhe kërkesat për azil.

Autoritetet policore kombëtare kompetente dhe Europol-i mund të kërkojnë akses tek të dhënat e regjistruara në VIS, për qëllime të parandalimit, zbulimit, ose hetimit të veprave terroriste dhe penale, sipas disa kushteve të caktuara.[876] Meqenëse VIS-i është projektuar si një instrument për të mbështetur zbatimin e politikës së përbashkët të vizave, parimi i kufizimit të qëllimit, i cili, sikurse është shpjeguar në Kapitullin 3.2, përcakton se të dhënat personale duhet të përpunohen vetëm për qëllime specifike, të qarta dhe legjitime dhe duhet të jenë të përshtatshme, të rëndësishme dhe jo të tepruara për sa i takon qëllimeve për të cilat janë përpunuar të dhënat, do të shkelej nëse VIS-i do të shndërrohej në instrument ligjzbatues. Për këtë arsye, autoriteteve ligjzbatuese kombëtare dhe Europol-it nuk u është dhënë akses sistematik në bazën e të dhënave të VIS-it. Aksesi jepet vetëm rast pas rasti dhe shoqëruar me garanci rigoroze. Kushtet dhe garancitë për aksesin dhe konsultimin e VIS-it nga këto autoritete, rregullohen me Vendimin 2008/633/JHA të Këshillit.[877]

Po ashtu, Rregullorja VIS parashikon të drejtat e subjekteve të të dhënave, të cilat janë:

- E drejta për t'u informuar nga Shteti Anëtar përgjegjës për identitetin dhe adresën e kontaktit të kontrolluesit të të dhënave të ngarkuar për përpunimin e të dhënave personale në atë Shtet Anëtar, qëllimet për të cilat të dhënat e tyre personale do të përpunohen në VIS, kategoritë e personave tek të cilët do të transmetohen të dhënat (marrësit) dhe afatet e mbajtjes së të dhënave. Gjithashtu, kërkuesit e vizave duhet të informohen për faktin që mbledhja e të dhënave personale të tyre në kuadër të VIS-it, është i detyrueshëm në mënyrë që të shqyrtohet kërkesa e tyre, ndërsa Shtetet Anëtare duhet gjithashtu t'i informojnë ata se kanë të drejtën për akses në të dhënat e tyre, për të kërkuar korrigjimin, apo fshirjen e tyre dhe për procedurat që duhen ndjekur për ushtrimin e këtyre të drejtave.[878]
- E drejta për akses tek të dhënat personale të tyre, të cilat janë regjistruar në VIS.[879]
- E drejta për korrigjimin e të dhënave të pasakta.[880]
- E drejta për të fshirë të dhënat e mbajtura në mënyrë të jashtëligjshme.[881]

Grupi i Koordinimit të Mbikëqyrjes së VIS-it (VIS SCG) u ngrit me qëllime që të monitoronte VIS-in. Ai përbëhet nga përfaqësues të EDPS-së dhe të autoriteteve mbikëqyrëse kombëtare dhe mblidhet dy herë në vit. Në të marrin pjesë përfaqësuesit e 28 Shteteve Anëtare të BE-së dhe Islandës, Lihtenshtejnit, Norvegjisë dhe Zvicrës.

[875] Neni 5 i Rregullores (KE) nr. 767/2008 të Parlamentit Evropian dhe Këshillit të 9 korrikut 2008 që ka të bëjë me Sistemin e Informacionit të Vizave (VIS) dhe shkëmbimin e të dhënave midis Shteteve Anëtare për vizat afatshkurtra (Rregullorja VIS), FZ 2008 L 218.
[876] Këshilli i Bashkimit Evropian (2008), Vendim i Këshillit 2008/633/JHA i 23 qershorit 2008 që ka të bëjë me aksesin për konsultimin e Sistemit të Informacionit të Vizave (VIS) nga autoritetet e përcaktuara të Shteteve Anëtare dhe nga Europol-i për qëllime të parandalimit, zbulimit dhe hetimit të veprave terroriste dhe krimeve të tjera të rënda, FZ 2008 L 218.
[877] *Ibid.*
[878] Rregullorja VIS, neni 37.
[879] *Ibid*., neni 38, pika 1.
[880] *Ibid*., neni 38, pika 2.
[881] *Ibid*., neni 38, pika 2.

Eurodac-u

Eurodac-u është akronimi i "European Dactyloscopy", ose "daktiloskopisë evropiane"[882]. Bëhet fjalë për një sistem të përqendruar, në të cilin mbahen të dhënat e gjurmëve të gishtave të shtetasve të vendeve të treta dhe personave pa shtetësi, të cilët kanë aplikuar për azil në një nga Shtetet Anëtare të BE-së.[883] Sistemi është në funksionim që në janar 2003, pas miratimit të Rregullores së Këshillit nr. 2725/2000, ndërsa një rimodelim i tij është kryer në vitin 2015. Qëllimi i tij kryesor është të ndihmojë në përcaktimin se cili Shtet Anëtar, në bazë të Rregullores (KE) nr. 604/2013, duhet të jetë përgjegjës për shqyrtimin e një kërkese për azil. Kjo rregullore përcakton kriteret dhe mekanizmat për përcaktimin e Shtetit Anëtar përgjegjës për shqyrtimin e një aplikimi për mbrojtje ndërkombëtare, e cila është depozituar në një nga Shtetet Anëtare, nga një shtetas i një vendi të tretë, apo një person pa shtetësi (Rregullorja Dublin III).[884] Të dhënat personale të mbajtura në Eurodac, shërbejnë kryesisht për qëllime të lehtësimit të zbatimit të Rregullores Dublin III.[885]

Autoritetet ligjzbatuese kombëtare dhe Europol-i janë të autorizuara të bëjnë kraharimin e gjurmëve të gishtave që lidhen me hetime penale, me gjurmët e gishtave që mbahen në Eurodac, por vetëm për qëllime të parandalimit, zbulimit, apo hetimit të veprave terroriste, ose krimeve të tjera të rënda. Meqenëse Eurodac-u është konceptuar si një instrument për mbështetjen e zbatimit të politikave të BE-së për azilin dhe jo si instrument ligjzbatues, autoritetet ligjzbatuese kanë akses në bazën e të dhënave vetëm në raste të caktuara, në rrethana të caktuara dhe me kushte rigoroze.[886] Për përdorimin e mëtejshëm të të dhënave për qëllime ligjzbatuese, zbatohet Direktiva e Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale, ndërsa të dhënat e përdorura për qëllimin kryesor të lehtësimit të Rregullores Dublin III, mbrohen nga Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave. Transferimi i mëtejshëm i të dhënave personale të përftuara nga një Shtet Anëtar, apo Europol-i në bazë të Rregullores për Rimodelimin e Eurodac-ut tek çdo vend i tretë, organizatë ndërkombëtare, apo njësi private, të vendosur brenda apo jashtë BE-së, është i ndaluar.[887]

Eurodac-u konsiston në një njësi qendrore, që shfrytëzohet nga eu-LISA, për regjistrimin dhe krahasimin e gjurmëve të gishtave dhe një sistem elektonik transmetimi të dhënash midis Shteteve Anëtare dhe bazën qendrore të të dhënave. Shtetet Anëtare marrin dhe transmetojnë gjurmët e gishtave të çdo personi mbi 14 vjeç, që ka kërkuar azil në territorin e tyre dhe të çdo shtetasi të një vendi të tretë, apo personi pa shtetësi mbi 14 vjeç, që ndalohet për kalim të paligjshëm të kufijve të jashtëm. Shtetet Anëtare mund të marrin dhe të transmetojnë gjithashtu gjurmët e gishtave të shtetasve të vendeve të treta, apo personave pa shtetësi, të cilit konstatohen në territorin e tyre pa lejen përkatëse.

Paçka se çdo Shtet Anëtar mund të konsultojë Eurodac-un dhe të kërkojë krahasim të të dhënave të gjurmëve të gishtave, vetëm Shteti Anëtar që i ka mbledhur gjurmët e gishtave dhe i ka transmetuar ato në njësinë qendrore, ka të drejtën të ndryshojë të dhënat, nëpërmjet korrigjimit, plotësimit, apo fshirjes së tyre.[888] Eu-LISA regjistron të gjitha përpunimet e të dhënave, me qëllim që të monitorojë mbrojtjen e të dhënave dhe të garantojë sigurinë e të dhënave.[889] Autoritetet mbikëqyrëse kombëtare ndihmojnë

---

[882] Shih faqen e internetit për Eurodac-un të Kontrolluesit Evropian të Mbrojtjes së të Dhënave.
[883] Rregullorja (KE) nr. 2725/2000 e Këshillit e 11 dhjetorit 2000 që ka të bëjë me ngritjen e Eurodac-ut për krahasimin e gjurmëve të gishtave, për zbatimin efikas të Konventës së Dublinit, FZ 2000 L 316; Rregullorja (KE) nr. 407/2002 e Këshillit e 28 shkurtit 2002 që përcakton rregullat për zbatimin e Rregullores (KE) nr. 2725/2000 që ka të bëjë me ngritjen e Eurodac-ut për krahasimin e gjurmëve të gishtave, për zbatimin efikas të Konventës së Dublinit, FZ 2002 L 62 (Rregulloret Eurodac), Rregullorja (BE) nr. 603/2013 e Parlamentit Evropian dhe e Këshillit e 26 qershorit 2013 mbi ngritjen e 'Eurodac-ut' për krahasimin e gjurmëve të gishtave, për zbatimin efikas të Rregullores (BE) nr. 604/2013 që përcakton kriteret dhe mekanizmat për përcaktimin e Shtetit Anëtar përgjegjës për shqyrtimin e një aplikimi për mbrojtje ndërkombëtare, të depozituar në një nga Shtetet Anëtare, nga një shtetas i një vendi të tretë, apo nga një person pa shtetësi dhe në lidhje me kërkesat për krahasim me të dhënat e Eurodac-ut nga autoritetet ligjzbatuese të Shteteve Anëtare dhe nga Europol-i, për qëllime të zbatimit të ligjit dhe që ndryshon Rregulloren (BE) nr. 1077/2011 për ngritjen e Agjencisë Evropiane për menaxhimin operativ të sistemeve të TI-së në shkallë të gjerë, në fushën e lirisë, sigurisë dhe drejtësisë, FZ 2013 L 180, fq. 1 (Rregullorja për Rimodelimin e Eurodac-ut).
[884] Rregullorja (BE) nr. 604/2013 e Parlamentit Evropian dhe e Këshillit e 26 qershorit 2013 për përcaktimin e kritereve dhe mekanizmave për përcaktimin e Shtetit Anëtar përgjegjës për shqyrtimin e një aplikimi për mbrojtje ndërkombëtare, të depozituar në një Shtet Anëtar, nga një shtetas i një vendi të tretë, apo nga një person pa shtetësi, FZ 2013 L 180 (Rregullorja Dublin III).
[885] Rregullorja për Rimodelimin e Eurodac-ut, FZ 2013 L 180, fq. 1, neni 1 (1).
[886] *Ibid.*, neni 1, pika 2.
[887] *Ibid.*, neni 35.
[888] *Ibid.,* neni 27.
[889] *Ibid.*, neni 28.

dhe këshillojnë subjektet e të dhënave rreth ushtrimit të të drejtave të tyre.[890] Mbledhja dhe transmetimi i të dhënave të gjurmëve të gishtave i nënshtrohet kontrollit gjyqësor nga gjykatat kombëtare.[891] Rregullorja e Mbrojtjes së të Dhënave të Institucioneve të BE-së[892] dhe mbikëqyrja që ushtron EDPS-ja, përfshin aktivitetet e përpunimit të Sistemit Qendror, i cili menaxhohet nga eu-LISA për sa i përket Eurodac-ut.[893] Nëse një person pëson dëm si rezultat i një operacioni të paligjshëm përpunimi, ose nga çdo veprim që është në shkelje të rregullores së Eurodac-ut, ai person ka të drejtën e kompensimit nga Shteti Anëtar përgjegjës për dëmin e shkaktuar.[894] Gjithsesi, duhet theksuar se azilkërkuesit janë kategori njerëzish veçanërisht vulnerabël, të cilët shpesh kanë ndërmarrë një rrugë të gjatë dhe të rrezikshme. Për shkak të vulnerabilitetit dhe situatës së rrezikshme në të cilën ndodhen shpesh gjatë kohës së shqyrtimit të aplikimit për azil, ushtrimi i të drejtave të tyre në praktikë, përfshirë edhe të drejtën për kompensim, mund të paraqitet i vështirë.

Në mënyrë që të përdorin Eurodac-un për qëllime ligjzbatimi, Shtetet Anëtare duhet të caktojnë autoritetet që do të kenë të drejtën të kërkojnë akses, si dhe autoritetet që do të verifikojnë nëse janë të ligjshme kërkesat për krahasim.[895] Aksesi nga ana e autoriteteve kombëtare dhe Europol-i në të dhënat e gjurmëve të gishtave të Eurodac-ut, i nënshtrohet kushteve tepër rigoroze. Autoriteti kërkues mund të paraqesë një kërkesë elektronike të arsyetuar, vetëm pasi të ketë krahasuar të dhënat me ato që ekzistojnë në sistemevet e informacionit, sikurse në bazat e të dhënave të gjurmëve të gishtave në nivel kombëtar dhe në VIS. Duhet të ekzistojë një interes prevalues sigurie publike, në mënyrë që krahasimi të jetë proporcional. Krahasimi duhet të jetë vërtet i nevojshëm, të lidhet me një rast specific dhe duhet të ketë motive të arsyeshme për të menduar se krahasimi do të ndihmojë në mënyrë domethënëse në parandalimin, zbulimin, apo hetimin e një vepre penale të caktuar, sidomos nëse ka dyshime të arsyeshme se i dyshuari, autori, apo viktima e një vepre terroriste, apo çdo krimi tjetër të rëndë, hyn në kategorinë që i nënshtrohet mbledhjes së gjurmëve të gishtave në sistemin Eurodac. Krahasimi duhet bërë vetëm me të dhënat e gjurmëve të gishtave. Europol-i duhet të marrë gjithashtu autorizim nga Shteti Anëtar që ka mbledhur të dhënat daktiloskopike.

Të dhënat personale që mbahen në Eurodac, të cilat kanë të bëjnë me azilkërkuesit, ruhen për 10 vite, duke nisur nga data e marrjes së gjurmëve të gishtave, përveçse kur subjekti i të dhënave merr shtetësinë e një Shteti Anëtar të BE-së. Në një rast të tillë, të dhënat duhen fshirë menjëherë. Të dhënat në lidhje me shtetasit e huaj, të ndaluar për kalim të paligjshëm të kufijve të jashtëm, mbahen për 18 muaj. Këto të dhëna duhen fshirë menjëherë nëse subjekti i të dhënave pajiset me leje qëndrimi, largohet nga territori i BE-së, apo përfiton shtetësinë e një Shteti Anëtar. Të dhënat e personave të cilëve u është dhënë azil, mbeten të disponueshme për krahasim, në kuadër të parandalimit, zbulimit dhe hetimit të veprave terroriste dhe krimeve të tjera të rënda, për një periudhë tre vjeçare.

Përveç të gjitha Shteteve Anëtare të BE-së edhe Islanda, Norvegjia, Lihtenshtejni dhe Zvicra përdorin Eurodac-un në bazë të marrëveshjeve ndërkombëtare.

SCG-ja e Eurodac-ut është ngritur me qëllim që të sigurohet mbikëqyrja e Eurodac-ut. Ai përbëhet nga përfaqësuesit e EDPS-së dhe të autoriteteve mbikëqyrëse kombëtare dhe mblidhet dy herë në vit. Grupi mbledh përfaqësuesit e 28 Shteteve Anëtare të BE-së dhe të Islandës, Lihtenshtejnit, Norvegjisë dhe Zvicrës.[896]

Perspektiva

[890] *Ibid.,* neni 29.
[891] *Ibid.,* neni 29.
[892] Rregullorja (KE) nr. 45/2001 e Parlamentit Evropian dhe e Këshillit e 18 dhjetorit 2000 mbi mbrojtjen e personave në lidhje me përpunimin e të dhënave personale nga institucionet dhe organet e Komunitetit dhe mbi lëvizjen e lirë të këtyre të dhënave, FZ 2001 L 8.
[893] Rregullorja e Rimodelimit të Eurodac-ut, FZ 2013 L 180, fq. 1, neni 31.
[894] *Ibid.*, neni 37.
[895] Roots, L. (2015), 'The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination', *Baltic Journal of European Studies Tallinn University of Technology*, Vëllimi 5, nr 2, fq. 108–129.
[896] Shih faqen e internetit për Eurodac-un të Kontrolluesit Evropian të Mbrojtjes së të Dhënave.

Në maj 2016, Komisioni paraqiti një propozim për rimodelimin e Rregullores Eurodac, si pjesë e një reforme që synon përmirësimin e funksionimit të Sistemit të Përbashkët Evropian për Azilin (CEAS).[897] Rimodelimi i propozuar është i rëndësishëm, pasi do të zgjerojë në mënyrë të konsiderueshme fushën e zbatimit të bazës së të dhënave fillestare të Eurodac-ut. Eurodac-u u krijua fillimisht për të mbështetur zbatimin e regjimit të përbashkët evropian për azilin (CEAS), nëpërmjet ofrimit të provave daktiloskopike, për të mundësuar të përcaktohej se cili Shtet Anëtar ishte përgjegjës për shqyrtimin e një kërkesë për azil, të paraqitur në BE. Rimodelimi i propozuar do të zgjerojë fushën e zbatimit të bazës së të dhënave, për të lehtësuar kthimin e emigrantëve të paligjshëm.[898] Autoritetet kombëtare do të kenë mundësi të konsultojnë bazën e të dhënave, për qëllime të identifikimit të shtetasve të vendeve të treta, të cilët qëndrojnë në BE në mënyrë të parregullt, apo kanë hyrë në BE në mënyrë të parregullt, për ta pasur si provë për të ndihmuar Shtetet Anëtare që t'i kthejnë ato persona. Gjithashtu, ndërsa regjimi juridik aktual kërkon vetëm mbledhjen dhe mbajtjen e gjurmëve të gishtave, propozimi përfshin edhe mbledhjen e imazheve të fytyrës së personave,[899] të cilat janë një lloj tjetër të dhënash biometrike. Propozimi do të ulë gjithashtu edhe moshën minimale të fëmijëve, prej të cilëve mund të merren gjurmët e gishtave, deri në gjashtë vjeç,[900] në vend të 14 vjeç që është mosha minimale sipas rregullores së 2013-ës. Fusha e zgjeruar e zbatimit të propozimit nënkupton se ajo do të krijojë ndërhyrje në të drejtat për privatësi dhe mbrojtje të të dhënave të më shumë personave, të cilët do të përfshihen në bazën e të dhënave. Për të kundërpeshuar këtë ndërhyrje, propozimi dhe ndryshimet e sugjeruara nga Komiteti LIBE i Parlamentit Evropian,[901] synojnë të përforcojnë kriteret e mbrojtjes së të dhënave. Në periudhën gjatë së cilës po hartohej ky manual, vijonte të diskutohej ky propozim në Parlament dhe në Këshill.

Eurosur-i

Sistemi Evropian i Kontrollit Kufitar (Eurosur-i)[902] është krijuar për të rritur kontrollin e kufijve të jashtë të Schengen-it, nëpërmjet zbulimit, parandalimit dhe luftës kundër emigracionit të paligjshëm dhe krimeve ndërkufitare. Ai shërben për të shtuar shkëmbimin e informacionit dhe bashkëpunimin operativ midis qendrave kombëtare të koordinimit dhe Frontex-it, agjencisë së BE-së të ngarkuar [për zhvillimin dhe zbatimin e konceptit të ri të menaxhimit të integruar të kufirit.[903] Objektivat e përgjithshëm të tij janë:

- Të ulë numrin e emigrantëve të parregullt që hyjnë në BE pa u konstatuar;

---

[897] Komisioni Evropian, Propozim për një Rregullore të Parlamentit Evropian dhe të Këshillit mbi ngritjen e 'Eurodac-ut' për krahasimin e gjurmëve të gishtave, për zbatim efikas të [Rregullores (BE) nr. 604/2013 për përcaktimin e kritereve dhe mekanizmave për përcaktimin e Shtetit Anëtar përgjegjës, për shqyrtimin e një aplikimi për mbrojtje ndërkombëtare, të depozituar në një Shtet Anëtar, nga një shtetas i një vendi të tretë, apo nga një person pa shtetësi], për identifikimin e një shtetasi të një vendi të tretë, apo personi pa shtetësi, që qëndron në mënyrë të paligjshme dhe mbi kërkesat për krahasim me të dhënat e Eurodac-ut nga autoritetet ligjzbatuese të Shteteve Anëtare dhe nga Europol-i për qëllime ligjzbatuese (rimodelim), COM(2016) 272 final, 4 maj 2016.

[898] Shih relacionin shpjegues të propozimit, fq. 3.

[899] Komisioni Evropian, Propozim për një Rregullore të Parlamentit Evropian dhe të Këshillit mbi ngritjen e 'Eurodac-ut' për krahasimin e gjurmëve të gishtave, për zbatim efikas të [Rregullores (BE) nr. 604/2013 për përcaktimin e kritereve dhe mekanizmave për përcaktimin e Shtetit Anëtar përgjegjës, për shqyrtimin e një aplikimi për mbrojtje ndërkombëtare, të depozituar në një Shtet Anëtar, nga një shtetas i një vendi të tretë, apo nga një person pa shtetësi], për identifikimin e një shtetasi të një vendi të tretë, apo personi pa shtetësi, që qëndron në mënyrë të paligjshme dhe mbi kërkesat për krahasim me të dhënat e Eurodac-ut nga autoritetet ligjzbatuese të Shteteve Anëtare dhe nga Europol-i për qëllime ligjzbatuese (rimodelim), COM(2016) 272 final, 4 maj 2016, neni 2, pika 1.

[900] *Ibid.*, neni 2, pika 2.

[901] Parlamenti Evropian, *Raport në lidhje me propozimin për një rregullore të Parlamentit Evropian dhe të Këshillit mbi ngritjen e 'Eurodac-ut' për krahasimin e gjurmëve të gishtave, për zbatim efikas të [Rregullores (BE) nr. 604/2013 për përcaktimin e kritereve dhe mekanizmave për përcaktimin e Shtetit Anëtar përgjegjës, për shqyrtimin e një aplikimi për mbrojtje ndërkombëtare, të depozituar në një Shtet Anëtar, nga një shtetas i një vendi të tretë, apo një person pa shtetësi], për identifikimin e një shtetasi të një vendi të tretë, apo personi pa shtetësi dhe mbi kërkesat për krahasim me të dhënat e Eurodac-ut nga autoritetet ligjzbatuese të Shteteve Anëtare dhe nga Europol-i për qëllime ligjzbatuese (rimodelim),* PE 597.620v03-00, 9 qershor 2017.

[902] Rregullorja (BE) nr. 1052/2013 e Parlamentit Evropina dhe e Këshillit e 22 tetorit 2013 për ngritjen e Sistemit Evropian të Kontrollit Kufitar (Eurosur), FZ 2013 L 295.

[903] Rregullorja (BE) nr. 2916/1624 e Parlamentit Evropian dhe e Këshillit e 14 shtatorit 2016 mbi Rojet Kufitare dhe Detare Evropiane dhe që ndryshon Rregullores (BE) 2016/399 të Parlamentit Evropian dhe të Këshillit dhe që shfuqizon Rregulloren (KE) nr. 863.2007 të Parlamentit Evropian dhe të Këshillit, Rregullorja (KE) nr. 2007/2004 e Këshillit dhe Vendimi i Këshillit 2005/267/EC, FZ L 251.

- Të ulë numrin e vdekjeve të emigrantëve të parregullt, duke shpëtuar më shumë jetë në det;
- Të rrisë sigurinë e brendshme të BE-së në tërësinë e saj, duke dhënë ndihmesë në parandalimin e krimit ndërkufitar.[904]

Eurosur-i hyri në veprim më 2 dhjetor 2013 në të gjitha Shtetet Anëtare me kufij të jashtëm dhe më 1 dhjetor 2014 në të gjitha të tjerat. Rregullorja zbatohet për monitorimin e kufijve të jashtëm tokësorë, detarë dhe ajrorë të Shteteve Anëtare. Eurosur-i shëmben dhe përpunon të dhëna personale me shtrirje tepër të kufizuar, meqenëse Shtetet Anëtare dhe Frontex-i kanë të drejtën të shkëmbejnë vetëm numrat e identifikimit të anijeve. Eurosur-i shkëmben të dhëna operative, sikurse vendndodhjen e patrullave dhe incidenteve dhe si rregull i përgjithshëm, informacioni i shkëmbyer nuk mund të përfshijë të dhëna personale.[905] Në rastet e veçanta kur shkëmbehen të dhëna personale në kuadër të Eurosur-it, rregullorja parashikon se zbatohet plotësisht kuadri juridik i përgjithshëm i BE-së në lidhje me mbrojtjen e të dhënave.[906]

Kësisoj, Eurosur-i garanton të drejtën për mbrojtje të të dhënave, konkretisht duke përcaktuar se shkëmbimet e të dhënave personale duhet të respektojnë kriteret dhe garancitë e sanksionuara nga Direktiva e Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale dhe nga Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave.[907]

Sistemi i Informacionit të Doganave

Një sistem tjetër i rëndësishëm informacioni i ngritur në nivel BE-je, është Sistemi i Informacionit të Doganave (CIS).[908] Gjatë periudhës së krijimit të tregut të brendshëm, u hoqën të gjitha kontrollet dhe formalitetet për sa i përket lëvizjes së mallrave brenda territorit të BE-së, duke rritur kësisoj rrezikun e mashtrimit. Ky rrezik u kundërpeshua me bashkëpunim të thelluar midis administrative doganore të Shteteve Anëtare. Qëllimi i CIS-it është të ndihmojë Shtetet Anëtare në parandalimin, hetimin dhe ndjekjen penale të shkeljeve të rënda të legjislacionit doganor dhe atij bujqësor të BE-së. CIS-i u ngrit me anë të dy akteve ligjore, të miratuara mbështetur në baza të ndryshme ligjore: Rregulloren (KE) nr. 515/97 të Këshillit mbi bashkëpunimin midis autoriteteve administrative kombëtare të ndryshme për luftën kundër mashtrimit, në kuadrin e bashkimit doganor dhe politikës së përbashkët bujqësore, ndërsa Vendimi 2009/917/JHA i Këshillit synon të ndihmojë në parandalimin, hetimin dhe ndjekjen e shkeljeve të rënda të legjislacionit doganor. Kjo do të thotë se CIS-i nuk ka të bëjë vetëm me kuadrin ligjzbatues.

Informacioni që mbahet në CIS përfshin të dhëna personale në lidhje me artikuj, mjete transporti, njësi tregtare, persona, mallra dhe para të bllokuara, të sekuestruara, apo të konfiskuara. Kategoritë e të dhënave që mund të përpunohen janë përcaktuar qartësisht dhe përfshijnë emrat, kombësinë, gjininë, vendlindjen dhe datëlindjen e personave të përfshirë, arsyet për regjistrimin e të dhënave të tyre në sistem dhe numrin e regjistrimit të mjetit të transportit.[909] Ky informacion mund të përdoret vetëm për qëllime të konstatimit, raportimit, apo kryerjes së inpektimeve të veçanta, ose për analiza strategjike, apo operative në lidhje me personat e dyshuar për shkelje të dispozitave doganore.

---

[904] Shih gjithashtu: Komisioni Evropian (2008), *Komunikatë e Komisionit për Parlamentin Evropian, Këshillin, Komitetin Ekonomik dhe Shoqëror Evropian dhe Komitetin e Rajoneve: Analizë në lidhje me ngritjen e Sistemit Evropian të Kontrollit Kufitar (Eurosur),* COM(2008) 68 final, Bruksel, 13 shkurt 2008; Komisioni Evropian (2011), *Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (Eurosur),* Dokument pune, SEC(2011) 1536 final, Bruksel,12 dhjetor 2011, fq. 18.

[905] Komisioni Evropian, *EUROSUR: Protecting the Schengen external borders – protecting migrants' lives. EUROSUR in a nutshell*, 29 nëntor 2013.

[906] Rregullorja 1052/2013, paragrafi 13 dhe neni 13.

[907] *Ibid*., paragrafi 13 dhe neni 13.

[908] Këshilli i Bashkimit Evropian (1995), Akt i Këshillit i 26 korrikut 1995 për hartimin e Konventës për përdorimin e teknologjisë së informacionit për qëllime doganore, FZ 1995 C 316, ndryshuar me Rregulloren nr. 515/97 të 13 marsit 1997 të Këshillit të Bashkimit Evropian (2009) mbi ndihmën e ndërsjellë midis autoriteteve administrative të Shteteve Anëtare dhe bashkëpunimin midis tyre dhe Komisionit, për të garantuar zbatimin e duhur të legjislacionit doganor dhe bujqësor, Vendimi 2009/917/JHA i Këshillit i 30 nëntorit 2009 mbi përdorimin e teknologjisë së informacionit për qëllime doganore, FZ 2009 L 323 (Vendimi CIS).

[909] Shih Vendimin CIS, nenet 24, 25 dhe 28.

Aksesi në CIS u jepet autoriteteve doganore, fiskale, bujqësore, të shëndetit public dhe atyre policore në nivel kombëtar, si dhe Europol-it dhe Eurojust-it.

Përpunimi i të dhënave personale duhet të bëhet në përputhje me rregullat specifike të përcaktuara në Rregulloren nr. 515/97 dhe Vendimin 2009/917/JHA të Këshillit, si dhe me dispozitat e Rregullores së Përgjithshme të Mbrojtjes së të Dhënave, Rregulloren e Mbrojtjes së të Dhënave të Institucioneve të BE-së, Konventën 108 të Modernizuar dhe me Rekomandimin për Policinë. EDPS-ja është e ngarkuar për mbikëqyrjen e përputhshmërisë së CIS-it me Rregulloren (KE) nr. 45/2001. Ajo mbledh të paktën një herë në vit të gjitha autoritetet kombëtare mbikëqyrëse të mbrojtjes së të dhënave, të cilat janë kompetente për mbikëqyrjen e CIS-it.

Ndërveprueshmëria e sistemeve të informacionit të BE-së

Menaxhimi i migracionit, menaxhimi i integruar i kufijve të jashtëm të BE-së dhe lufta kundër terrorizmit, si dhe krimi ndërkufitar, përbëjnë sfida të rëndësishme, gjithnjë e më të ndërlikuara në një botë të globalizuar. Gjatë viteve të fundit, BE-ja ka punuar për një qasje gjithëpërfshirëse për mbrojtjen dhe ruajtjen e sigurisë, pa cënuar vlerat dhe liritë themelore të BE-së. Në kuadër të këtyre përpjekjeve, është thelbësor shkëmbimi efikas i informacionit ndërmjet autoriteteve ligjzbatuese kombëtare dhe midis Shteteve Anëtare me agjencitë përkatëse të BE-së.[910] Sistemet aktuale të informacionit të BE-së për menaxhimin e kufijve dhe sigurinë e brendshme, kanë objektivat, strukturat institucionale, subjektet e të dhënave dhe përdoruesit përkatës. BE-ja ka punuar për kapërcimin e mangësive në funksionet e menaxhimit të fragmentuar të të dhënave në BE midis sistemeve të ndryshme të informacionit, sikurse SIS II, VIS-i dhe Eurodac-u, duke studiuar aftësinë e tyre për ndërveprueshmëri.[911] Synimi kryesor është të bëhet e mundur që autoritetet kompetente policore, doganore dhe gjyqësore, të disponojnë informacionin e nevojshëm për kryerjen e detyrave të tyre, duke e mbajtur në ekuilibër me të drejtat për privatësi, mbrojtje të të dhënave dhe të drejtat e tjera themelore.

Ndërveprimi nënkupton 'aftësinë e sistemeve të informacionit për të shkëmbyer të dhëna dhe për të mundësuar ndarjen e informacionit'.[912] Ky shkëmbim nuk duhet të cënojë rregullat domosdoshmërisht rigoroze në lidhje me aksesin dhe përdorimin, që garantohen nga Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, Direktiva e Mbrojtjes së të Dhënave për Autoritetet Policore dhe të Drejtësisë Penale, Karta e të Drejtave Themelore të BE-së dhe nga norma të tjera përkatëse. Çdo zgjidhje tjetër e integruar për menaxhimin e të dhënave, nuk duhet të cënojë parimet e kufizimit të qëllimit, mbrojtjes së të dhënave që në fazën e konceptimit dhe mbrojtjen e të dhënave me parapërzgjedhje.[913]

Përveç përmirësimit të funksioneve të tre sistemeve kryesore të informacionit – SIS II, VIS dhe Eurodac – Komisioni ka propozuar ngritjen e një sistemit të katërt të përqendruar për menaxhimin e kufijve, për

---

[910] Komisioni Evropian (2016), Komunikatë e Komisionit për Parlamentin Evropian dhe Këshillin: *Stronger and Smarter Information Systems for Borders and Security*, COM(2016) 205 final, Bruksel, 6 prill 2016, Komisioni Evropian (2016), Komunikatë e Komisionit për Parlamentin Evropian, Këshillin Evropian dhe Këshillin: *Enhancing Security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders*, COM(2016) 602 final, Bruksel, 14 shtator 2016, Komisioni Evropian (2016), Propozim për një Rregullore të Parlamentit Evropian dhe të Këshillit mbi përdorimin e Sistemit të Informacionit të Schengen-it për kthimin e shtetasve të vendeve të treta që qëndrojnë në mënyrë të paligjshme. Shih gjithashtu, Komunikatën e Komisionit për Parlamentin Evropian, Këshillin Evropian dhe Këshillit: *Seventh progress report towards an effective and genuine Security Union*, COM(2017) 261 final, Bruksel, 16 maj 2017.

[911] Këshilli i Bashkimit Evropian (2005), Program i Hagës: Përforcimi i Lirisë, Sigurisë dhe Drejtësisë në Bashkimin Evropian, FZ 2005 C 53, Komisioni Evropian (2010), Komunikatë e Komisionit për Parlamentin Evropian dhe Këshillin: *Overview of information management in the area of freedom, security and justice*, COM(2010) 385 final, Komisioni Evropian (2016), Komunikatë e Komisionit për Parlamentin Evropian dhe Këshillin: *Stronger and Smarter Information Systems for Borders and Security*, COM(2016) 205 final, Bruksel, 6 prill 2016, Komisioni Evropian (2016), Vendim i Komisionit i 17 qershorit 2016 për ngritjen e Grupit të Ekspertëve të Nivelit të Lartë për Sistemet e Informacionit dhe Ndërveprueshmërinë e tyre, FZ 2016 C 257.

[912] Komisioni Evropian (2016), Komunikatë e Komisionit për Parlamentin Evropian dhe Këshillin: *Stronger and Smarter Information Systems for Borders and Security*, COM(2016) 205 final, Bruksel, 6 prill 2016, fq. 14.

[913] *Ibid*., fq. 4–5.

trajtimin e shtetasve të vendeve të treta: Sistemin e Hyrje-Daljeve (EES),[914] i cili pritet të kompletohet në vitin 2020.[915] Komisioni ka publikuar gjithashtu një propozim për ngritjen e Sistemit Evropian të Informacionit dhe Autorizimit të Udhëtimit (ETIAS),[916] sistem i cili do të mbledhë informacion për personat që udhëtojnë pa viza në BE, për të mundësuar kontrolle të përparuara sigurie dhe emigrimi të parregullt.

[914] Komisioni Evropian (2016), Propozim për një Rregullore të Parlamentit Evropian dhe të Këshillit për ngritjen e një Sistemi të Hyrje/Daljeve (EES) për të regjistruar të dhënat e hyrjeve dhe daljeve dhe të dhënave të ndalimit të hyrjes të shtetasve të vendeve të treta, të cilët kalojnë kufijtë e jashtëm të Shteteve Anëtare të Bashkimit Evropian dhe për përcaktimin e kushteve për akses në EES për qëllime ligjzbatuese dhe që ndryshon Rregulloren (KE) nr. 767/2008 dhe Rregulloren (BE) nr. 1077/2011, COM(2016) 194 final, Bruksel, 6 prill 2016.

[915] Komisioni Evropian (2016), Komunikatë e Komunisionit për Parlamentin Evropian dhe për Këshillin: *Stronger and Smarter Information Systems for Borders and Security*, COM(2016) 205 final, Bruksel, 6 prill 2016, fq. 5.

[916] Komisioni Evropian (2016), Propozim për një Rregullore të Parlamentit Evropian dhe Këshillit për ngritjen e Sistemit Evropian të Informacionit dhe Autorizimit të Udhëtimit (ETIAS) dhe që ndryshon Rregulloret (BE) nr. 515/2014, (BE) 2016/399, (BE) 2016/794 dhe (BE) 2016/1624, COM(2016) 731 final, 16 nëntor 2016.

9 Lloje të veçanta të dhënash dhe rregullat përkatëse të mbrojtjes së të dhënave

BE	Çështje të trajtuara	KiE
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave Direktiva për privatësinë dhe komunikimet elektronike	Komunikimet elektronike	Konventa 108 e Modernizuar Rekomandimi për Shërbimet e Telekomunikimeve
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 88	Marrëdhëniet e punësimit	Konventa 108 e Modernizuar Rekomandimi në fushën e punësimit GJEDNJ, *Copland k. Mbretërisë së Bashkuar*, nr. 62617/00, 2007
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 9, pika 2, gërmat (h) dhe (i)	Të dhënat mjekësore	Konventa 108 e Modernizuar Rekomandimi për të Dhënat Mjekësore GJEDNJ, *Z .k Finlandës*, nr. 22009/93, 1997
Rregullorja për Provat Klinike	Provat klinike	
Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 6, pika 4, neni 89	Statistikat	Konventa 108 e Modernizuar Rekomandimi për të Dhënat Statistikore
Rregullorja (KE) nr. 223/2009 për Statistikat Evropiane GJDBE, C-524/06, *Huber k. Bundesrepublik Deutschland* [ÇB], 2008	Statistikat zyrtare	Konventa 108 e Modernizuar Rekomandimi për të Dhënat Statistikore
Direktiva 2014/65/BE mbi tregjet e instrumenteve financiare Rregullorja (BE) nr. 648/2012 për derivativët mbi banak (OTC), kundërpalët qendrore dhe regjistrat e tregtimit Rregullorja (KE) nr. 1060/2009 mbi agjencitë e vlerësimit të kredive Direktiva 2007/64/KE mbi shërbimet e pagesave në tregun e brendshëm	Të dhënat financiare	Konventa 108 e Modernizuar Rekomandimi 90 (19) mbi të dhënat personale të përdorura për qëllime pagesash dhe veprimesh të tjera në lidhje me to GJEDNJ, *Michaud k. Francës*, nr. 12323/11, 2012

Në shumë raste, janë miratuar në nivel evropian instrumente ligjore speciale, për të bërë të zbatueshme në mënyrë më të hollësishme rregullat e përgjithshme të Konventës 108 të Modernizuar, apo Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave në situata të caktuara.

9.1 Komunikimet elektronike

Pikat kryesore

- Rregullat specifike të mbrojtjes së të dhënave në fushën e telekomunikacionit, me vëmendje të veçantë tek shërbimet telefonike, përcaktohen në Rekomandimin e KiE-së të 1995-ës.
- Përpunimi i të dhënave personale që kanë të bëjnë me ofromin e shërbimeve të komunikimit në nivel të BE-së, rregullohet nga Direktiva për privatësinë edhe komunikimet elektronike.
- Konfidencialiteti i komunikimeve elektronike nuk ka të bëjë vetëm me përmbajtjen e komunikimeve, por edhe me të dhënat e trafikut (për shembull kush komunikoi me kë, kur dhe sa kohë zgjati), si dhe të dhënat e vendndodhjes (për shembull, vendi nga i cili janë komunikuar të dhënat).

Rrjetet e komunikimit kanë aftësi të lartë ndërhyrjeje të pajustifikuar në sferën personale të përdoruesve, pasi ofrojnë mundësi të mëdha teknike për të dëgjuar dhe survejuar komunikimet e kryera nëpërmjet këtyre rrjeteve. Për rrjedhojë, janë nevojitur norma speciale për mbrojtjen e të dhënave, për t'iu përgjigjur rreziqeve të veçanta për përdoruesit e shërbimeve të komunikimit.

Në vitin 1995, **KiE-ja** publikoi një Rekomandim për mbrojtjen e të dhënave në fushën e telekomunikacioneve, më vëmendje të veçantë tek shërbimet telefonike.[917] Sipas këtij rekomandimi, qëllimet për mbledhjen dhe përpunimin e të dhënave personale në kontekstin e telekomunikimeve, duhet të kufizohen për: lidhjen e një përdoruesi me rrjetin, vënien në dispozicion të shërbimit të caktuar të telekomunikimit, faturimin, verifikimin, sigurimin e funksionimit teknik optimal dhe zhvillimin e rrjetit dhe të shërbimit.

Vëmendje e veçantë iu kushtua gjithashtu përdorimit të rrjeteve të telekomunikacionit për dërgimin e mesazheve të marketing të drejtpërdrejtë. Si rregull i përgjithshëm, mesazhet e marketingut të drejtpërdrejtë nuk mund t'i dërgohen asnjë abonenti, që ka kërkuar shprehimisht të mos marrë të tilla. Pajisjet telefonike të automatizuara, për transmetim mesazhesh publicitare të regjistruara paraprakisht, mund të përdoren vetëm në masën që abonenti ka shprehur pëlqimin. Legjislacioni kombëtar duhet të parashikojë norma të hollësishme për këtë fushë.

Për sa i përket **kuadrit ligjor të BE-së**, një përpjekje e parë u bë në vitin 1997, me miratimin në 2002-shin të Direktivës për privatësinë dhe komunikimet elektronike dhe ndryshimin e saj në 2009-ën, me qëllim **plotësimin dhe përshtatjen** e dispozitave të Direktivës së mëparshme të Mbrojtjes së të Dhënave në sektorin e telekomunikacioneve**.**[918]

Zbatimi i Direktivës për privatësinë dhe komunikimet elektronike kufizohet tek shërbimet e komunikimit në rrjetet elektronike publike.

Direktiva për privatësinë dhe komunikimet elektronike bën dallim midis tre kategorive kryesore të të dhënave që gjenerohen gjatë një komunikimi:

- Të dhënat që përbëjnë përmbajtjen e mesazheve të dërguara gjatë komunikimit: këto të dhëna janë rreptësisht konfidenciale;
- Të dhënat e nevojshme për lidhjen dhe vijimin e komunikimit: të ashtuquajturat 'të dhëna të trafikut', të tilla si informacioni në lidhje me palët që komunikojnë, momenti dhe kohëzgjatja e komunikimit;

[917] Këshilli i Evropës, Komiteti i Ministrave (1995), Rekomandimi Rec(95)4 për shtetet anëtare në lidhje me mbrojtjen e të dhënave personale në fushën e shërbimeve të telekomunikimit, me vëmendje të veçantë tek shërbimet telefonike, 7 shkurt 1995.
[918] Direktiva 2002/58/EC e Parlamentit Evropian dhe e Këshillit e 12 korrikut 2002 që ka të bëjë me përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike, FZ 2002 L 201 (Direktiva për privatësinë dhe komunikimet elektronike), ndryshuar me Direktivën 2009/136/KE të Parlamentit Evropian dhe Këshillit të 25 nëntorit 2009 që ndryshon Direktivën 2002/22/KE mbi shërbimin universal dhe të drejtat e përdoruesve lidhur me rrjetet dhe shërbimet e komunikimeve elektronike, Direktivën 2002/58/EC për përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike dhe Rregulloren (KE) nr. 2006/2004 mbi bashkëpunimin midis autoriteteve kombëtare përgjegjëse për zbatimin e ligjeve të mbrojtjes së konsumatorit, FZ 2009 L 337.

- Të dhënat e trafikut përmbajnë të dhëna që lidhen specifikisht me vendndodhjen e pajisjes së përdorur për komunikim, të ashtuquajturat 'të dhëna të vendndodhjes': këto të dhëna janë njëkohësisht të dhëna për vendndodhjen e përdoruesve të pajisjeve të përdorura për komunikim, veçanërisht të rëndësishme për përdoruesit e pajisjeve të komunikimit.

Të dhënat e trafikut mund të përdoren nga operator i shërbimit për qëllime faturimi dhe për të bërë të mundur teknikisht shërbimin. Megjithatë, me pëlqimin e subjektit të të dhënave, këto të dhëna mund të përhapen në kontrollues të tjerë, që ofrojnë shërbime me vlerë të shtuar, si për shembull dhënie informacioni për vendndodhjen e përdoruesit në raport me stacionin e metrosë, ose farmacinë, apo parashikimin e motit për vendin ku ai ndodhet.

Sipas nenit 15 të Direktivës së e-Privatësisë, çdo lloj aksesi tjetër tek të dhënat e komunikimeve në rrjetet elektronike, duhet të përmbushë kushtet për ndërhyrje të justifikuar tek e drejta për mbrojtje të të dhënave, sikurse përcaktohet nga neni 8, pika 2 e KEDNJ-së dhe konfirmuar nga Karta e të Drejtave Themelore të BE-së në nenet 8 dhe 52. Në këtë akses, mund të përfshihet aksesi për qëllime të hetimit të veprave penale.

Ndryshimet që iu bënë Direktivës për privatësinë dhe komunikimet elektronike[919] në 2009-ën, integruan elementet e mëposhtme:

- Kufizimet në lidhje me dërgimin e mesazheve të postës elektronike për qëllime marketingu të drejtpërdrejtë, u shtrinë edhe tek shërbimet e mesazheve SMS, shërbimet e mesazheve multimediale dhe në lloje të tjera aplikacionesh të tjera të ngjashme: mesazhet e postës elektronike për qëllime marketingu, janë të ndaluara, përveçse nëse është marrë pëlqimi paraprak. Pa këtë pëlqim, mesazhet e postës elektronike mund t'u dërgohen vetëm klientëve të mëparshëm, nëse ata kanë dhënë adresën e postës elektronike dhe nëse nuk kundërshtëojnë.
- U vendos një detyrim për Shtetete Anëtare që të vënë në dispozicion mjet mbrojtjeje gjyqësor kundër shkeljeve të ndalimit të dërgimit të komunikimeve të pakërkuara.[920]
- Vendosja e identifikuesve (cookies), që janë softuerë që monitorojnë dhe regjistrojnë veprimet e një përdoruesi kompjuteri, nuk lejohet më pa pëlqimin e përdoruesit të kompjuterit. Legjislacioni kombëtar duhet të rregullojë më në hollësi mënyrën se si duhet shprehur dhe marrë pëlqimi, për të garantuar mbrojtjen e duhur.[921]

Kur një shkelje ndaj të dhënave ndodh si pasojë e aksesit, humbjes, apo shkatërrimit të paautorizuar të të dhënave, autoriteti mbikëqyrës kompetent duhet informuar menjëherë. Abonentët duhen informuar kur shkelja ndaj të dhënave mund të shkaktojë dëme për ta.[922]

Direktiva e Mbajtjes së të Dhënave[923] detyronte operatorët e shërbimeve të komunikimit që të mbanin të dhënat e trafikut, Megjithatë, kjo direktivë u anulua nga GJDBE-ja (shih Seksionin 8.3 për më shumë hollësi).

Perspektiva

Në janar 2017, Komisioni Evropian miratoi një propozim të ri për një Rregullore të e-Privatësisë, për zëvendësimin e Rregullores së mëparshme me të njëjtin emër. Synimi do të mbetet ai i mbrojtjes "së të drejtave dhe lirive themelore të personave fizikë dhe juridikë lidhur me ofrimin dhe përdorimin e shërbimeve të komunikimeve elektronike, veçanërisht të drejtave për mbrojtje të jetës private dhe komunikimeve dhe mbrojtjen e personave fizikë në kontekstin e përpunimit të të dhënave personale".

---

[919] Direktiva 2009/136/KE e Parlamentit Evropian dhe e Këshillit e 25 nëntorit 2009 që ndryshon Direktivën 2002/22/KE mbi shërbimin universal dhe të drejtat e përdoruesve lidhur me rrjetet dhe shërbimet e komunikimeve elektronike, Direktivën 2002/58/EC për përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike dhe Rregulloren (KE) nr. 2006/2004 mbi bashkëpunimin midis autoriteteve kombëtare përgjegjëse për zbatimin e ligjeve të mbrojtjes së konsumatorit, FZ 2009 L 337.

[920] Shih direktivën e ndryshuar, neni 13.

[921] Shih *Ibid.,* nenin 5; shih gjithashtu: Grupi i Punës së Nenit 29 (2012), *Opinioni 04/2012 mbi përjashtimin nga detyrimi për marrjen e pëlqimit për disa identifikues (cookies) të caktuar*, WP 194, Bruksel, 7 qershor 2012.

[922] Shih gjithashtu: Grupi i Punës së Nenit 29 (2011), *Dokument pune 01/2011 mbi kuadrin ekzistues të BE-së lidhur me shkeljet ndaj të dhënave personale dhe rekomandimet për zhvillimet e ardhshme të politikave*, WP 184, Bruksel, 5 prill 2011.

[923] Direktiva 2006/24/KE e Parlamentit Evropian dhe e Këshillit e 15 marsit 2006 për mbajtjen e të dhënave të gjeneruara, apo të përpunuara në lidhje me ofrimin e shërbimeve të komunikimeve elektronike të disponueshme për publikun, ose të rrjeteve të komunikimeve publike dhe që ndryshon Direktivën 2002/58/KE, FZ 2006 L 105.

Njëkohësisht, ky propozim i ri synon të garantojnë lëvizjen e lirë të të dhënave të komunikimeve elektronike dhe shërbimeve të komunikimeve elektronike brenda Bashkimit[924] Ndërsa Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave trajton para së gjithash nenin 8 të Kartës së të Drejtave Themelore të BE-së, rregullorja e propozuar synon të integrojë nenin 7 të Kartës në legjislacionin dytësore të BE-së.

Rregullorja do të përshtasë dispozitat e direktivës së mëparshme, me teknologjitë dhe realitetin e ri të tregut, si dhe do të krijojë një kuadër gjithëpërfshirës dhe koherent me Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave. Në këtë kuptim, Rregullorja për e-Privatësinë do të jetë një *lex specialis* për Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave, duke e përshtatur atë për komunikimet elektronike që përbëjnë të dhëna personale. Rregullorja e re mbulon përpunimin "të dhënave të komunikimeve elektronike", përfshirë përmbajtjen e komunikimeve elektronike dhe të dhënat e trafikut, që nuk janë domosdoshmërisht të dhëna personale. Fusha e zbatimit territorial kufizohet brenda BE-së, përfshirë edhe kur të dhënat e përftuara në BE përpunohen jashtë saj dhe shtrihet tek operatorët e shërbimeve të komunikimit të aksesit të drejtpërdrejtë (over-the-top). Këta operatorë shërbimi ofrojnë shpërndarje përmbajtjeje, shërbimesh, apo aplikacionesh nëpërmjet internetit, pa përfshirjen e drejtpërdrejtë të një operatori rrjeti, ose operatori shërbimi interneti (ISP). Shembuj të këtyre operatorëve janë Skype-i (thirrje vokale dhe video), WhatsApp-i (shërbimi i mesazheve), Google-i (kërkime), Spotify (muzikë), apo Netflix-i (përmbajtje video). Për rregullore e rë do të aplikohen mekanizmat e zbatimit të Rregullores së Përgjithshme të Mbrojtjes së të Dhënave.

Rregullorja për e-Privatësinë synohet të miratohet përpara 25 majit 2018, kohë në të cilën Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave do të bëhet e zbatueshme në të gjithë 28 Shtetet Anëtare. Megjithatë, për miratimin e saj duhet të bien dakord Parlamenti Evropian me Këshillin.[925]

9.2 Të dhënat e punësimit

Pikat kryesore

- Rregullat specifike për mbrojtjen e të dhënave në kuadrin e marrëdhënieve të punësimit, përshkruhen në Rekomandimin e KiE-së për të Dhënat në fushën e Punësimit.
- Në Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave, marrëdhëniet e punësimit përmenden konkretisht vetëm në kontekstin e përpunimit të të dhënave sensitive.
- Vlefshmëria e pëlqimit, i cili duhet të jepet në mënyrë të lirë, si bazë ligjore për përpunimin e të dhënave në lidhje me të punësuarit, është e diskutueshme, duke pasur parasysh çekuilibrin ekonomik midis punëdhënësit dhe punëmarrësve. Rrethanat që lidhen me pëlqimin duhen vlerësuar me kujdes.

Përpunimi i të dhënave në kontekstin e punësimit i nënshtrohet legjislacionit të përgjithshëm të BE-së për mbrojtjen e të dhënave personale. Megjithatë, një rregullore[926] trajton specifikisht mbrojtjen e të dhënave personale nga ana e institucioneve evropiane në kuadrin e punësimit (ndër të tjera). Në Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave, marrëdhëniet e punësimit përmenden specifikisht në nenin 9, pika 2, i cili thekson se të dhënat personale mund të përpunohen për përmbushjen e detyrimeve, ose ushtrimin e të drejtave specifike të kontrolluesit, apo subjektit të të dhënave në fushën e punësimit.

Sipas Rregullores së Përgjithshme të Mbrojtjes së të Dhënave, punëmarrësit duhet t'i mundësohet të dallojë qartë se cilat të dhëna ai, apo ajo jep pëlqimin që të përpunohen/mbahen dhe qëllimet për të cilat

[924] Propozim për një Rregullore të Parlamentit Evropian dhe Këshillit që ka të bëjë me respektimin e jetës private dhe mbrojtjen e të dhënave personale në komunikimet elektronike dhe që shfuqizon Direktivën 2002/58/KE (Rregullorja për Privatësinë dhe Komunikimet Elektronike) (COM(2017) 10 final), neni 1.

[925] Për më shumë informacion, shih: Komisioni Evropian (2017), "Komisioni propozon përforcim të rregullave të privatësisë për të gjitha komunikimet elektronike dhe pëditëson rregullat e mbrojtjes së të dhënave për institucionet e BE-së", njoftim për shtyp, 10 janar 2017.

[926] Rregullorja (KE) nr. 45/2001 e Parlamentit Evropian dhe e Këshillit e 18 dhjetorit 2000 për mbrojtjen e personave në lidhje me përpunimin e të dhënave personale nga institucionet dhe organet e Komunitetit dhe për lëvizjen e lirë të këtyre të dhënave, FZ 2001 L 8.

mbahen të dhënat e tij apo të saj. Punonjësit duhen informuar gjithashtu për të drejtat e tyre dhe për afatet e mbajtjes së të dhënave të tyre, përpara se të japin pëlqimin. Nëse ndodh një shkelje ndaj të dhënave personale, që ka gjasa të shkaktojë risk të lartë për të drejtat e liritë e personave fizikë, punëdhënësi duhet t'ia komunikojë shkeljen punëmarrësit. Neni 88 i rregullores lejon Shtetet Anëtare që të përcaktojnë norma më specifike për garantimin e të drejtave dhe lirive të punonjësve, për sa i përket përpunimit të të dhënave personale të tyre në fushën e punësimit.

Shembull: tek çështja *Worten*,[927] të dhënat përfshinin një regjistër të kohës së punës, që përmbante oraret e përditshme të punës dhe të pushimit, të cilat përbënin të dhëna personale. Legjislacioni kombëtar mund të detyrojë një punëdhënës t'u vërë në dispozicion, autoriteteve kombëtare përgjegjëse për kontrollin e kushteve të punës, një regjistër të orareve të punës. Diçka e tillë mundëson akses të menjëhershëm tek të dhënat personale përkatëse. Megjithatë, aksesi tek të dhënat personale është i nevojshëm, për t'u mundësuar autoriteteve kombëtare të mbikëqyrin zbatimin e legjislacionit për kushtet e punës.[928]

Për sa i takon **KiE-së**, Rekomandimi për të Dhënat në fushën e Punësimit u publikua më 1989 dhe u rishikua më 2015.[929] Rekomandimi mbulon përpunimin e të dhënave personale për qëllime punësimi, si në sektorin privat, ashtu edhe në atë publik. Përpunimi duhet të respektojë disa parime dhe kufizime të caktuara, sikurse parimin e transparencës dhe të konsultimit me përfaqësuesit e punonjësve, përpara se të vendosen sisteme kontrolli në ambientet e punës. Rekomandimi thekson gjithashtu se punëdhënësit duhet të zbatojnë masa parandaluese, sikurse përdorimin e filtrave, në vend që të monitorojnë përdorimin e internetit nga ana e punonjësve.

Një studim i problematikave më të zakonshme për mbrojtjen e të dhënave në kuadër të punësimit, mund të gjenden në një dokument pune të Grupit të Punës së Nenit 29.[930] Grupi i punës analizoi rëndësinë e pëlqimit, si bazë ligjore për përpunimin e të dhënave të punësimit.[931] Ai doli në përfundimin se mungesa e ekuilibrit ekonomik midis pundhënësit që kërkon pëlqimin dhe punëmarrësit që jep pëlqimin, mund të vendosë në pikëpyetje nëse pëlqimi është dhënë lirisht ose jo. Për rrjedhojë, rrethanat në të cilat pëlqimi përdoret si bazë ligjore për përpunimin e të dhënave duhen analizuar me kujdes, kur vlerësohet vlefshmëria e pëlqimit në kontekstin e punësimit.

Një problem i zakonshëm për mbrojtjen e të dhënave në mjedisit tipik aktual të punës, është legjitimiteti i monitorimit të komunikimeve elektronike të punonjësve në vendin e punës. Shpesh pretendohet se ky problem mund të zgjidhet lehtësisht duke ndaluar përdorimin në mënyrë private të sistemeve të komunikimit të punës. Megjithatë, një ndalim i tillë i përgjithshëm mund të jetë jo proporcional dhe jo realist. Vendimet e GJEDNJ-së për çështjet *Copland k. Mbretërisë së Bashkuar* dhe *Bărbulescu k. Rumanisë* kanë rëndësi të veçantë në këtë kontekst.

[BOX TYPE 1]

Shembull: tek çështja *Copland k. Mbretërisë së Bashkuar*,[932] telefoni, posta elektronike dhe përdorimi i internetit nga një punonjëse e një kolegji, ishte monitoruar në mënyrë të fshehtë, për të verifikuar nëse ajo përdorte në mënyrë abuzive pajisjet e kolegjit për qëllime personale. GJEDNJ-ja vlerësoi se telefonatat e kryera nga mjedise profesionale, mbuloheshin nga nocioni i jetës private dhe korrespondencës. Për këtë shkak, telefonatat dhe posta elektronike të dërguara nga vendi i punës, ashtu si edhe informacioni që buronte nga monitorimi i përdorimit të internetit, mbroheshin nga neni 8 i KEDNJ-së. Në rastin e kërkueses, nuk ekzistonin norma për rregullimin e rrethanave në të cilat punëdhënësit mund të monitoronin përdorimin nga ana e punonjësve të telefonit, postës elektronike dhe

[927] GJDBE, C-342/12, *Worten – Equipamentos para o Lar SA k. Autoridade para as Condições de Trabalho (ACT)*, 30 maj 2013, parag. 19.
[928] *Ibid*., parag. 43.
[929] Këshilli i Evropës, Komiteti i Ministrave (2015), Rekomandimi Rec(2015)5 për shtetet anëtare mbi përpunimin e të dhënave personale në fushën e punësimit, prill 2015.
[930] Grupi i Punës së Nenit 29 (2017), *Opinion 2/2017 mbi përpunimin e të dhënave në vendin e punës*, WP 249, Bruksel, 8 qershor 2017.
[931] Grupi i Punës së nenit (2005), *Dokument pune mbi interpretimin e përbashkët të nenit 26, pika 1 të Direktivës 95/46/KE e 24 tetorit 1995*, WP 114, Bruksel, 25 nëntor 2005.
[932] GJEDNJ, *Copland k. Mbretërisë së Bashkuar*, nr. 62617/00, 3 prill 2007.

internetit. Për pasojë, ndërhyrja nuk ishte në përputhje me ligjin. Gjykata doli në përfundimin se kishte pasur shkelje të nenit 8 të KEDNJ-së.

Shembull: tek çështja *Bărbulescu k. Rumanisë,*[933] kërkuesi ishte pushuar nga puna për shkak se gjatë orarit të punës, kishte përdorur internetin në vendin e tij të punës, në shkelje të rregullores së brendshme. Punëdhënësi i tij kishte monitoruar komunikimet e tij. Disa regjistrime që tregonin se ai kishte shkëmbyer mesazhe me karakter privat, ishin paraqitur në gjykatën kombëtare. Megjithëse pohoi se gjente zbatim neni, GJEDNJ-ja e la të hapur çështjen nëse rregullorja kufizuese e punëdhënësit i kishte lënë kërkuesit ndonjë pritshmëri të arsyeshme për privatësi, por gjithsesi doli në përfundimin se rregullat që vendos një punëdhënës nuk mund ta reduktojnë në zero jetën shoqërore private.

Për sa i përket themelit, Palëve Kontraktuese duhej t'u lihej një fushë e gjerë veprimi për të vlerësuar nevojën për përcaktimin e një kuadri juridik, për rregullimin e kushteve në të cilat punëdhënësi mund të rregullojë komunikimet elektronike, apo çdo lloj komunikimi tjetër të karakterit jo professional, në vendin e punës, nga ana e punonjësve të tij. Pavarësisht kësaj, autoritetet vendase duhet të garantojnë se përdorimi nga punëdhënësi i masave për monitorimin e korrespondencës dhe komunikimeve të tjera, pavarësisht shtrirjes dhe kohëzgjatjes së këtyre masave, duhet të shoqërohet me garanci të përshtatshme dhe mjaftueshme kundër abuzimit. Proporcionaliteti dhe garancitë procedurale kundër arbitraritetit, ishin thelbësore dhe GJEDNJ-ja identifikoi një sërë faktorësh me rëndësi për rrethanat e çështjes. Ndër të tjera, aty përfshihen shtrirja e monitorimit nga punëdhënësi dhe shkalla e ndërhyrjes tek privatësia e punonjësit, pasojat për punonjësin dhe nëse ishin ofruar garancitë e përshtatshme. Gjithashtu, autoritetet vendase duhet të garantonin që një punonjës, komunikimet e të cilit ishin monitoruar, të kishte mundësi ankimi përpara një organi gjyqësor me kompetencën për të vendosur, të paktën në thelb, nëse ishin respektuar kriteret e përmendura dhe nëse nëse masat e kundërshtuara ishin të ligjshme.

Për këtë çështje, GJEDNJ-ja vendosi se ishte shkelur neni 8, pasi autoritetet vendase nuk kishin mbrojtur në mënyrën e duhur të drejtën e kërkuesit për respektim të jetës private dhe korrespondencës dhe si rrjedhojë nuk kishin ekuilibruar drejt interesat e kundërta.

Sipas Rekomandimit të KiE-së për mbrojtjen e të dhënave të punësimit, të dhënat personale të mbledhura për qëllime punësimi, duhen marrë drejtpërdrejtë nga secili punonjës.

Të dhënat personale të mbledhura për qëllime të marrjes në punë, duhet të kufizohen në informacionin e nevojshëm për të vlerësuar përshtatshmërinë e kandidatëve dhe aftësinë e tyre profesionale.

Rekomandimi përmend gjithashtu në mënyrë specifike të dhënat që lidhen me vlerësimin e punës, apo potencialin e secilit punonjës. Të dhënat e vlerësimit të punës duhet të bazohen në vlerësime të drejta dhe të ndershme dhe nuk duhet të formulohen në mënyrë fyese. Kjo përcaktohet nga parimet e përpunimit të drejtë të të dhënave dhe të saktësisë së të dhënave.

Një aspekt i veçantë i legjislacionin të mbrojtjes së të dhënave në marrëdhënien punëdhënës-punëmarrës, është roli i përfaqësuesve të punonjësve. Këta të fundit mund të përftojnë të dhëna personale të punonjësve vetëm në masën që është e nevojshme për përfaqësimin e interesave të punonjësve, ose nëse të dhënat janë të nevojshme për të përmbushur, apo mbikëqyrur detyrimet që rrjedhin nga marrëveshjet kolektive.

Të dhënat personale sensitive që mblidhen për qëllime të punësimit, mund të përpunohen vetëm në raste të veçanta dhe me garancitë e përcaktuara në legjislacionin e brendshëm. Punëdhënësit mund të pyesin punëmarrësit, apo punëkërkuesit për gjendjen shëndetësore, apo t'u kërkojnë kryerjen e analizave mjekësore vetëm kur diçka e tillë është e nevojshme, për shembull për të përcaktuar aftësinë për punë, për përmbushjen e kritereve të mjekësisë parandaluese, për të mbrojtur interesat jetike të subjektit të të dhënave, apo të punonjësve dhe personave të tjerë, për pagesën e sigurimeve shoqërore, apo për t'iu

[933] GJEDNJ, *Bărbulescu k. Rumanisë* [ÇB], nr. 61496/08, 5 shtator 2017, parag. 121.

përgjigjur kërkesave gjyqësore. Të dhënat e shëndetit duhen marrë nga vetë punonjësi dhe jo nga burime të tjera, përveç rastit kur është marrë pëlqimi i qartë dhe i informuar, ose kur e parashikon legjislacioni kombëtar.

Sipas Rekomandimit të mbrojtjes së të dhënave të punësimit, punonjësit duhen informuar për qëllimin e përpunimit të të dhënave të tyre personale, llojin e të dhënave personale të mbledhura, njësitë tek të cilat do të komunikohen rregullisht të dhënat dhe qëllimin dhe bazën ligjore për këto përhapje të dhënash. Në vendin e punës, komunikimet elektronike mund të aksesohet vetëm për arsye sigurie, apo arsye të tjera legjitime dhe vetëm pasi të jenë informuar punonjësit se punëdhënësi mund të ketë akses në këto lloj komunikimesh.

Punonjësit duhet të kenë të drejtën e aksesit në të dhënat e tyre në lidhje me punësimin, si dhe të drejtën për korrigjimin, apo fshirjen e tyre. Nëse përpunohen të dhëna të vlerësimit të punës, punonjësit duhet gjithashtu të kenë të drejtën të kundërshtojnë vlerësimit. Sidoqoftë, këto të drejta mund të kufizohen përkohësisht për qëllime hetimi të brendshëm. Nëse punonjësit i refuzohet aksesi, korrigjimi, apo fshirja e të dhënave personale në lidhje me punësimin, legjislacioni kombëtar duhet të parashikojë procedura të përshtatshme për t'u ankuar në lidhje me këtë refuzim.

9.3 Të dhënat e shëndetit

Pikat kryesore

- Të dhënat mjekësore janë të dhëna sensitive dhe therefore enjoy specific protection.

Të dhënat personale që kanë të bëjnë me shëndetin e subjektit të të dhënave, cilësohen si të dhëna sensitive nga neni 9, pika 1 e Rregullores së Përgjithshme të Mbrojtjes së të Dhënave dhe nga neni 6 i Konventës 108 të Modernizuar. Në këtë kuptim, të dhënat në lidhje me shëndetin i nënshtrohen një regjimi më rigoroz të përpunimit të të dhënave, krahasuar me të dhënat jo sensitive. Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave e ndalon përpunimin "e të dhënave personale që lidhen me shëndetin" (që duhen kuptuar si "të gjitha të dhënat që kanë të bëjnë me gjendjen shëndetësore, fizike dhe mendore, të shkuar, të tashme, apo të ardhme të subjektit të të dhënave")[934], ashtu si dhe të dhënave gjenetike e biometrike, përveçse kur kjo lejohet sipas nenit 9, pika 2. Këto dy lloje të dhënash i janë shtuar listës së "kategorive të veçanta të të dhënave".[935]

[BOX TYPE 1]

Shembull: tek çështja *Z k. Finlandës*,[936] ish-bashkëshorti i kërkueses, i cili ishte infektuar me HIV, kishte kryer disa krime seksuale. Më pasi, ai ishte dënuar për vrasje, në bazë të faktit se ai kishte ekspozuar me paramendim viktimat ndaj riskut të infektimit me HIV. Gjykata kombëtare urdhëroi që vendimi i plotë dhe dokumentacioni i çështjes të mbeteshin konfidencialë për 10 vite, pavarësisht kërkesave të kërkueses për një afat më të gjatë konfidencialiteti. Gjykata e Apelit i rrëzoi këto kërkesa dhe vendimi i saj përmbante emrat e plotë të ankueses dhe të ish-bashkëshortit të saj. GJEDNJ-ja u shpreh se ndërhyrja nuk çmohej e nevojshme në një shoqëri demokratike, pasi mbrojtja e të dhënave mjekësore ishte me rëndësi thelbësore për gëzimin e së drejtës për respektim të jetës private dhe familjare, sidomos kur bëhej fjalë për informacion në lidhje me infektimin me HIV, për shkak të stigmatizimit që i bëhet kësaj sëmundjeje në shumë shoqëri. Për rrjedhojë, Gjykata vendosi se duke

[934] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafi 35 i preambulës.
[935] *Ibid*., neni 2.
[936] GJEDNJ, *Z k. Finlandës*, nr. 22009/93, 25 shkurt 1997, parag. 94 dhe 112; shih gjithashtu: GJEDNJ, *M.S. k. Suedisë*, nr. 20837/92, 27 gusht 1997; GJEDNJ, *L.L. k. Francës*, nr. 7508/02, 10 tetor 2006; GJEDNJ, *I k. Finlandës*, nr. 20511/03, 17 korrik 2008; GJEDNJ, *K.H. dhe të Tjerët k. Sllovakisë*, nr. 32881/04, 28 prill 2009; GJEDNJ, *Szuluk k. Mbretërisë së Bashkuar*, nr. 36936/05, 2 qershor 2009.

lejuar aksesin në vendimin e Gjykatës së Apelit, në të cilin përshkruhej identiteti dhe gjendja shëndetësore e kërkueses, 10 vite pas shpalljes së vendimit, shkelej neni 8 i KEDNJ-së.

Në të **drejtën e BE-së**, neni 9, pika 2, gërma (h) e Rregullores së Përgjithshme të Mbrojtjes së të Dhënave lejon përpunimin e të dhënave mjekësore kur diçka e tillë është e nevojshme për qëllime të mjekësisë parandaluese, diagnostikimit mjekësor, ofrimin e kujdesit shëndetësor, apo për menaxhimin e shërbimeve të kujdesit shëndetësor. Megjithatë, përpunimi lejohet vetëm kur kryhet nga një profesionist shëndeti, që i nënshtrohet detyrimit për fshehtësi profesionale, apo çdo person tjetër që i nënshtrohet një detyrimi të barasvlershëm.

Në të **drejtën e KiE-së**, Rekomandimi i KiE-së për të Dhënat Mjekësore i 1997-ës zbaton më në hollësi parimet e Konventës 108, për përpunimin e të dhënave në fushën mjekësore.[937] Rregullat që propozon ai, janë në pajtim me ato të Rregullores së Përgjithshme të Mbrojtjes së të Dhënave për sa i takon qëllimeve legjitime të përpunimit të të dhënave mjekësore, detyrimeve të nevojshme për fshehtësi profesionale të personave që përdorin të dhëna shëndetësore dhe të drejtave të subjekteve të të dhënave për transparencë, akses, korrigjim dhe fshirje. Gjithashtu, të dhënat mjekësore që janë përpunuar në mënyrë të ligjshme nga profesionistët e shëndetit, nuk mund të transferohen tek autoritetet ligjzbatuese, përveçse kur ekzistojnë "garancitë e mjaftueshme për të penguar çdo përhapje, që është në kundërshtim me respektimin e jetës private, që garantohet nga neni 8 i KEDNJ-së".[938] E drejta kombëtare duhet gjithashtu "të hartohet me saktësinë e duhur dhe të parashikojë mbrojtje juridike të përshtatshme kundër arbitraritetit".[939]

Gjithashtu, Rekomandimi për të Dhënat Mjekësore përmban dispozita speciale në lidhje me të dhënat mjekësore të fetusit dhe personave me aftësi të kufizuar si dhe për përpunimin e të dhënave gjenetike. Kërkimi shkencor njihet shprehimisht si arsyeja për ruajtjen e të dhënave për një kohë më të gjatë se sa nevojiten ato të dhëna, edhe pse për këtë, zakonisht kërkohet anonimizimi i tyre. Neni 12 i Rekomandimit të të Dhënave Mjekësore propozon rregulla të hollësishme për rastet kur kërkuesit shkencorë kanë nevojë për të dhëna personale dhe nuk u mjaftojnë të dhënat e anonimizuara.

Pseudonimizimi mund të jetë një instrument i përshtatshëm për të përmbushur nevojat shkencore dhe në të njëjtën kohë, për të mbrojtur interesat e pacientëve të përfshirë. Koncepti i pseudonimizimit në kontekstin e mbrojtjes së të dhënave, shpjegohet më në hollësi në seksionin 2.1.1.

Rekomandimi i KiE-së i vitit 2016 për të dhënat që prodhohen nga testet gjenetike, gjen zbatim edhe për përpunimin e të dhënave në fushën mjekësore.[940] Ky rekomandim ka rëndësi të madhe për e-Shëndetin, që mbështetet tek TIK-u për të lehtësuar ofrimin e kujdesit shëndetësor. Një shembull i tillë është dërgimi i testit të atësisë së një pacienti nga një operator i kujdesit shëndetësor tek një tjetër. Ky rekomandim synon të mbrojë të drejtat e personave, të dhënat personale të së cilëve përpunohen për qëllime sigurimesh ndaj risqeve në lidhje me shëndetin, integritetin fizik, moshën, apo vdekjen e personit. Shoqëritë e sigurimit duhet të justifikojnë përpunimin e të dhënave në lidhje me shëndetin, i cili duhet të jetë proporcional me natyrën dhe rëndësinë e riskut të vlerësuar. Përpunimi i këtij lloji të dhënash varet nga pëlqimi i subjektit. Shoqëritë e sigurimit duhet të ofrojnë garanci për mbajtjen e të dhënave që lidhen me shëndetin.

Testet klinike, të cilat përfshijnë vlerësimin e pasojave të ilaçeve të reja tek pacientët në një mjedis kërkimor të dokumentuar, paraqesin ndërlikime të konsiderueshme për mbrojtjen e të dhënave. Testet klinike të produkteve mjekësore për përdorim njerëzor, rregullohen me Rregulloren (BE) nr. 536/2014 të Parlamentit Evropian dhe Këshillit e 16 prillit 2014 mbi testet klinike të medikamenteve për përdorim

[937] Këshilli i Evropës, Komiteti i Ministrave (1997), Rekomandimi Rec(97)5 për shtetet anëtare mbi mbrojtjen e të dhënave mjekësore, 13 shkurt 1997. Shënim: ky Rekomandim është në proces rishikimi.
[938] GJEDNJ, *Avilkina dhe të Tjerët k. Rusisë*, nr. 1585/09, 6 qershor 2013, parag. 53. Shih gjithashtu: GJEDNJ, *Biriuk k. Lituanisë*, nr. 23373/03, 25 nëntor 2008.
[939] GJEDNJ, *L.H. k. Letonisë*, nr. 52019/07, 29 prill 2014, parag. 59.
[940] Këshilli i Evropës, Komiteti i Ministrave (2016), Rekomandimi Rec(2016)8 për shtetet anëtare mbi përpunimin e të dhënave personale në lidhje me shëndetin për qëllime sigurimi, përfshirë të dhënat që prodhohen nga testet gjenetike, 26 tetor 2016.

njerëzor dhe që shfuqizon Direktivën 2001/20/KE (Rregullorja e Testeve Klinike).[941] Elementet kryesore të Rregullores së Testeve Klinike janë:

- Procedurë e thjeshtuar për depozitimin e kërkesave nëpërmjet portalit të BE-së;[942]
- Afate për shqyrtimin e kërkesave për teste klinike;[943]
- Një komitet etike merr pjesë në shqyrtim, në përputhje me të drejtën e Shteteve Anëtare (dhe me të drejtën e BE-së që përcakton afatet përkatëse);[944] dhe
- Përmirësohet transparenca e testeve klinike dhe rezultateve të tyre.[945]

Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave saktëson se për qëllime të dhënies së pëlqimit për të marrë pjesë në aktivitetet kërkimore shkencore në kuadër të testeve klinike, zbatohet Rregullorja (BE) nr. 536/2014.[946]

Shumë iniciativa legjislative dhe të tjera, që lidhen me të dhënat personale në sektorin e shëndetësisë, janë duke u shqyrtuar në nivel BE-je.[947]

Kartelat elektronike shëndetësore

Kartelat elektronike shëndetësore përkufizohen si "një dosje mjekësore e plotë, apo dokument i ngjashëm, mbi gjendjen shëndetësore fizike dhe mendore, të shkuar dhe të tashme, të një personi, në formë elektronike dhe që mundëson akses të lehtë tek këto të dhëna, për qëllime trajtimi mjekësor dhe qëllime të tjera që lidhen ngushtë me të".[948] Kartelat elektronike shëndetësore nënkuptojnë variantin elektronik të historikut mjekësor të pacientëve dhe mund të përmbajne të dhëna klinike në lidhje me ata persona, sikurse historikun mjekësor, problemet dhe sëmundjet, medikamentet dhe trajtimet, si dhe rezultate e raporte analizash dhe laboratory. Këto dosje elektronike, që mund të jenë kartela të plota, ose thjesht ekstrakte apo përmbledhje, mund të konsultohen nga mjekët, farmacistët dhe profesionistë të tjerë të shëndetit. Koncepti i 'e-Shëndetit' ka ta bëjë gjithashtu edhe me këto kartela klinike.

[BOX TYPE 2]

Shembull: z. A ka blerë një policë sigurimi tek shoqëria e sigurimit B. Kjo e fundit do të mbledhë disa të dhëna në lidhje me shëndetin nga A-ja, sikurse problemet shëndetësore, apo sëmundjet. Shoqëria e sigurimit duhet t'i mbajë të dhënat personale shëndetësore të A-së veçmas nga të dhënat e tjera. Shoqëria e sigurimit duhet po ashtu t'i mbajë të dhënat personale shëndetësore veçmas nga çdo e dhënë tjetër personale. Kjo nënkupton se vetëm operatori i dosjes së A-së do të ketë akses tek të dhënat shëndetësore të A-së.

Kartelat elektronike shëndetësore paraqesin gjithsesi disa problematika në lidhje me mbrojtjen e të dhënave, sikurse aksesueshmëria, mbajtja e përshtatshme dhe aksesi i tyre nga ana e subjektit të të dhënave.

Përveç kartelave elektronike shëndetësore, Komisioni Evropian ka publikuar më 10 prill 2014 një Libër të Gjebër mbi shëndetin në pajisjet e lëvizshme (m-Shëndeti), në të cilin vlerëson se m-Shëndeti është një fushë e re në zhvillim të shpejtë, që ka mundësi të transformojë kujdesin shëndetësor dhe të rrisë efekstshmërinë dhe cilësinë e tij. Ky nocion përfshin praktikat mjekësore dhe të shëndetit publik, me mbështetjen e pajisjeve të lëvizshme, sikurse janë telefonat celularë, pajisjet e monitorimit të pacientit,

---

[941] Rregullorja (BE) nr. 536/2014 e Parlamentit Evropian dhe e Këshillit e 16 prillit 2014 mbi testet klinike të medikamenteve për përdorim njerëzor dhe që shfuqizon Direktivën 2001/20/KE (Rregullorja e Testeve Klinike), FZ 2014 L 158.
[942] Rregullorja e Testeve Klinike, neni 5, pika 1.
[943] *Ibid*., neni 5, pikat 2–5.
[944] *Ibid*., neni 2, parag. 2, pika 11.
[945] *Ibid*., neni 9, pika 1 dhe paragrafi 67 i preambulës.
[946] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, paragrafët 156 dhe 161 të preambulës.
[947] EDPS (2013), *Opinion i Mbikëqyrësit Evropian të Mbrojtjes së të Dhënave në lidhje me Komunikatën e Komisionit mbi 'Planin e Veprimit për eShëndetin 2012–2020 – Kujdes shëndetësor novator për shekullin e 21-të*, Bruksel, 27 mars 2013.
[948] Rekomandim i Komisionit i 2 korrikut 2008 mbi ndërveprueshmërinë ndërkufitare të sistemeve të kartelave elektronike shëndetësore, pika 3, gërma (c).

asistentët digjitalë vetjakë dhe pajisje të tjera me valë, ashtu si edhe aplikacionet (për shembull, aplikacionet e mirëqenies), të cilat mund të lidhen me pajisjet mjekësore, ose me sensorët.[949] Dokumenti përvijon risqet për mbrojtjen e të dhënave personale që mund të mbartë zhvillimi i m-Shëndetit dhe përcakton se, duke pasur parasysh karakterin sensitiv të të dhënave shëndetësore, zhvillimi i tij duhet bërë duke integruar garanci specifike dhe të përshtatshme sigurie për të dhënat e pacientëve, sikurse kriptimin dhe mekanizmat e përshtatshme të autentifikimit të pacientit, me qëllim zvogëlimin e risqeve të sigurisë. Respektimi i rregullave të mbrojtjes së të dhënave personale, duke përfshirë detyrimin për informimin e subjektit të të dhënave, sigurinë e të dhënave dhe parimin e përpunimit të ligjshëm të të dhënave personale, është jetik për të krijuar besim tek m-Shëndeti.[950] Për këtë, ky sektor ka hartuar një Kod Sjelljeje, mbështetur në kontributet e një game të gjerë aktorësh, kryesisht përfaqësues të specializuar në mbrojtjen e të dhënave, në vetërregullim dhe në bashkërregullim, TIK dhe kujdes shëndetësor.[951] Gjatë kohës së hartimit të këtij manuali, një projekt-kod sjelljeje u depozitua pranë Grupit të Punës së Nenit 29 për miratim zyrtar.

9.4 Përpunimi i të dhënave për qëllime statistikore dhe kërkimore

Pikat kryesore

- Të dhënat e mbledhura për qëllime statistikore, të kërkimit shkencor, ose historik, nuk mund të përdoren për asnjë qëllim tjetër.
- Të dhënat e mbledhura për qëllime legjitime, për çdo lloj qëllimi, mund të përdoren më tej për qëllime statistikore, shkencore, ose historike, me kusht që legjislacioni kombëtar të përcaktojë garanci të përshtatshme. Për këtë qëllim, duhet parashikuar anonimizimi, ose pseudonimizimi i të dhënave përpara transmetimit të tyre tek palë të treta.

E drejta e BE-së lejon përpunimin e të dhënave për qëllime statistikore dhe për qëllime të kërkimit shkencore, ose historik, në masën që të ekzistojnë garancitë e përshtatshme për mbrojtjen e të drejtave dhe lirive të subjekteve të të dhënave. Në këto garanci mund të përfshihet pseudonimizimi.[952] E drejta e BE-së, apo e drejta kombëtare mund të përcaktojnë disa kufizime të të drejtave të subjekteve të të dhënave, nëse këto të drejta kanë gjasa të pamundësojnë, ose të dëmtojnë rëndë përmbushjen e qëllimit legjitim kërkimor.[953] Kufizimet mund të prekin të drejtën e subjektit të të dhënave për akses, të drejtën e korrigjimit, të drejtën për kufizimin e përpunimit dhe të drejtën për të kundërshtuar.

Megjithëse të dhënat e mbledhura në mënyrë të ligjshme nga një kontrollues për çfarëdo qëllimi, mund të përdoren sërish nga kontrolluesi për qëllimet e veta statistikore dhe për qëllime kërkimi shkencor ose historik, të dhënat duhet të anonimizohen, ose të pseudonimizohen, në varësi të kontekstit, përpara se të transmetohen tek një palë e tretë për qëllime statistikore dhe të kërkimit shkencor ose historik, përveçse kur subjekti i të dhënave ka dhënë pëlqimin për këtë, ose nëse kjo është e parashikuar specifikisht në të drejtën kombëtare. Të dhënat që janë pseudonimizuar, ndryshe nga dhënat e anonimizuara, vijojnë të jenë subjekt i Rregullores së Përgjithshme të Mbrojtjes së të Dhënave.[954]

Kësisoj, rregullorja e trajton ndryshe kërkimin, në raport me rregullat e përgjithshme të mbrojtjes së të dhënave, me qëllim që të mos pengojë zhvillimin e tij dhe të mundësojë arritjen e objektivit të krijimit të një hapësire evropiane për kërkimin, sikurse përmendet në nenin 179 të TFBE-së. Ajo parashikon një interpretim të gjerë të përpunimit të të dhënave personale për qëllime të kërkimit shkencor, përfshirë zhvillimin dhe demonstrimin teknologjik, kërkimin themelor, kërkimin e aplikuar dhe kërkimin e

[949] Komisioni Evropian (2014), *Libër i Gjelbër në lidhje me Shëndetin në pajisjet e lëvizshme ("mHealth")*, COM(2014) 219 final, Bruksel, 10 prill 2014.
[950] *Ibid.*, fq. 8.
[951] Draft Code of Conduct on privacy for mobile health applications, 7 qershor 2016.
[952] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 89, pika 1.
[953] *Ibid.*, neni 89, pika 2.
[954] *Ibid.*, paragrafi 26 i preambulës.

financuar nga sektori privat. Ajo pranon gjithashtu rëndësinë e kryqëzimit të të dhënave që burojnë nga regjistrat për qëllime kërkimore dhe vështirësinë e mundshme të identifikimit të plotë, të qëllimit të përpunimit të mëtejshëm të të dhënave personale, për qëllime kërkimi shkencor, në momentin e mbledhjes së të dhënave.[955] Për këtë shkak, rregullorja lejon përpunimin e të dhënave për këto qëllime, pa pëlqimin e subjekteve të të dhënave, me kusht që të ekzistojnë garancitë përkatëse.

Një shembull i rëndësishëm i përdorimit të të dhënave për qëllime statistikore, janë statistikat zyrtare, që zhvillohen nga zyrat e statistikave në nivel kombëtar dhe të BE-së, sipas legjislacioneve kombëtare dhe të BE-së për statistikat zyrtare. Sipas këtyre legjislacioneve, qytetarët dhe shoqëritë tregtare janë zakonisht të detyruara të komunikojnë të dhëna tek autoritetet përkatëse të statistikave. Nëpunësit e zyrave të statistikave u nënshtrohet detyrimeve të veçanta të fshehtësisë profesionale, të cilat duhen zbatuar si duhet, pasi janë thelbësore për të krijuar nivel të lartë besimi tek qytetarët, i cili është i domosdoshëm për komunikimin e këtyre të dhënave tek autoritetet e statistikave.[956]

Rregullorja (KE) nr. 223/2009 mbi Statistikat Evropian (Rregullorja e Statistikave Evropiane) përcakton rregulla thelbësore për mbrojtjen e të dhënave në kuadrin e statistikave zyrtare dhe për rrjedhojë mund të konsiderohet po ashtu e rëndësishme për dispozitat në lidhje me statistikat zyrtare në nivel kombëtar.[957] Rregullorja zbaton parimin sipas së cilit aktiviteti i statistikave zyrtare kërkon bazë ligjore mjaft të saktë.[958]

[BOX TYPE 1]

Shembull: tek çështja *Huber k. Bundesrepublik Deutschland*,[959] një biznesmen austriak, i cili ishte vendosur në Gjermani, u ankua se mbledhja dhe mbajtja e të dhënave personale të shtetasve të huaj në një regjistër qendror (AZR), nga ana e autoriteteve gjermane, edhe për qëllime statistikore, shkelte të drejtat e tij të garantuara nga Direktiva e Mbrojtjes së të Dhënave. Duke vlerësuar se Direktiva 95/46 synon të garantojë nivel të barasvlershëm të mbrojtjes së të dhënave në të gjitha Shtetet Anëtare, GJDBE-ja u shpreh se që të sigurohet nivel i lartë mbrojtje në BE, koncepti i domosdoshmërisë së nenit 7, gërma (e), nuk mund të ketë kuptim të ndryshëm në Shtete Anëtare të ndryshme. Në fakt, ai është një concept i cili ka kuptimin e vet të pavarur në të drejtën e BE-së dhe duhet interpretuar në mënyrë të tillë që të reflektojë plotësisht objektivin e Direktivës 95/46. Duke theksuar se vetëm informacioni anonym mund të kërkohej për qëllime statistikore, GJDBE-ja vendosi se regjistri gjerman nuk ishte në pajtim me kriterin e domosdoshmërisë së përcaktuar në nenin 7, gërma (e).

Në kuadrin e **KiE-së**, përpunimi i mëtejshëm i të dhënave mund të kryhet për qëllime shkencore, historike, apo statistikore, kur i shërben interesit publik dhe duhet t'i nënshtrohet garancive të përshtatshme.[960] Të drejtat e subjekteve të të dhënave mund të kufizohen gjithashtu kur përpunohen të dhëna për qëllime statistikore, me kusht që të mos ekzistojë ndonjë risk i identifikueshëm për shkeljen e të drejtave dhe lirive të tyre.[961]

Rekomandimi për të Dhënat Statistikore, i publikuar më 1997, përfshin kryerjen e aktivitetit statistikor në sektorin publik dhe në atë privat.[962]

---

[955] *Ibid.*, parag. 33, 157 dhe 159 e preambulës.
[956] *Ibid.*, neni 90.
[957] Rregullorja (KE) nr. 223/2009 e Parlamentit Evropian dhe e Këshillit e 11 marsit 2009 mbi Statistikat Evropiane dhe që shfuqizon Rregulloren (KE, Euratom) nr. 1101/2008 të Parlamentit Evropian dhe të Këshillit mbi transmetitin e të dhënave që i nënshtrohen konfidencialitetit statistikor tek Zyra e Statistikave të Komuniteteve Evropiane, Rregulloren e Këshillit (KE) nr. 322/97 mbi Statistikat e Komunitetit dhe Vendimin 89/382/EEC të Këshillit, Euratom për ngritjen e Komitetit për Programet Statistikore të Komuniteteve Evropiane, FZ 2009 L 87, ndryshuar me Rregulloren (BE) 2015/759 të Parlamentit Evropian dhe Këshillit të 29 prillit 2015 që ndryshon Rregulloren (KE) nr. 223/2009 mbi Statistikat Evropiane, FZ 2015 L 123.
[958] Ky parim duhet saktësuar më tej në Kodin e praktikave të mira të Eurostat-it, që sipas nenit 11 të Rregullores së Statistikave Evropiane, duhet të japë orientime etike mbi mënyrën e kryerjes së statistikave zyrtare, përfshirë përdorimin e kujdesshëm të të dhënave personale.
[959] GJDBE, C-524/06, *Heinz Huber k. Bundesrepublik Deutschland* [ÇB], 16 dhjetor 2008; shih sidomos parag. 68.
[960] Konventa 108 e Modernizuar, neni 5, pika 4, gërma (b).
[961] *Ibid.*, neni 11, pika 2.
[962] Këshilli i Evropës, Komiteti i Ministrave (1997), Rekomandimi Rec(97)18 për shtetet anëtare për mbrojtjen e të dhënave personale të mbledhura dhe përpunuara për qëllime statistikore, 30 shtator 1997.

Të dhënat e mbledhura nga ana e një kontrolluesi për qëllime statistikore, nuk mund të përdoren për asnjë qëllim tjetër. Të dhënat që nuk janë mbledhur për qëllime statistikore, duhet të jenë në dispozicion për përdorim të mëtejshëm statistikor. Rekomandimi për të Dhënat Statistikore lejon gjithashtu komunikimin e të dhënave tek palët e treta, në masën që të bëhet vetëm për qëllime statistikore. Në këto raste, palët duhet të bien dakord dhe të përcaktojnë me shkrim shtrirjen e përdorimit të mëtejshëm legjitim për qëllime statistikore. Duke qenë se këto formalitete nuk mund të zëvendësojë pëlqimin e subjektit të të dhënave, duhen përcaktuar garanci shtesë të mjaftueshme në legjislacionin kombëtar, për të zvogëluar riskun e keqpërdorimit të të dhënave personale, si për shembull detyrimin për të anonimizuar apo pseudonimizuar të dhënat përpara transmetimit

Profesionistët e hulumtimeve statistikore duhet t'u nënshtrohen detyrimeve të veçanta për fshehtësi profesionale në legjislacionin kombëtar, ashtu sikundër funksionon për statistikat zyrtare. Ky kriter duhet të shtrihet si tek intervistuesit, ashtu edhe tek mbledhësit e tjerë të të dhënave personale, nëse ata janë të punësuar për mbledhjen e të dhënave nga subjektet e të dhënave, apo nga persona të tjerë.

Nëse një pyetësor statistikor i cili përdor të dhëna personale, nuk është i parashikuar në ligj, duhet të merret pëlqimi nga subjektet e të dhënave, për përdorimin e të dhënave në lidhje me ta, me qëllim që përpunimi të legjitimohet, ose të paktën t'u jepet mundësia për ta kundërshtuar. Nëse të dhënat personale mblidhen për qëllime statistikore nga intervistuesit, subjekteve të të dhënave duhet t'u bëhet qartësisht me dije nëse komunikimi i të dhënave është i detyrueshëm sipas legjislacionit kombëtar.

Nëse një pyetësor statistikor nuk mund të kryhet duke përdorur të dhëna anonime dhe të dhënat personale janë të nevojshme, të dhënat e mbledhura për këtë qëllim duhen anonimizuar sa më shpejt të jetë e mundur. Rezultatet e pyetësorëve statistikorë së paku nuk duhet të mundësojnë identifikimin e subjekteve të të dhënave, përveçse kur diçka e tillë qartazi nuk paraqet asnjë risk.

Pas kryerjes së analizës statistikore, të dhënat personale që janë përdorur duhen fshirë, ose anonimizuar. Në këtë rast, Rekomandimi për të Dhënat Statistikore këshillon që të dhënat identifikuese të mbahen veçmas nga të dhënat e tjera personale. Kjo nënkupton, për shembull, që si çelësi i enkriptimit, ashtu edhe lista me sinonimet identifikuese, të mbahen veçmas nga të dhënat e tjera.

9.5 Të dhënat financiare

Pikat kryesore

- Megjithëse të dhënat financiare nuk konsiderohen si të dhëna sensitive në kuptim të Konventës 108 të Modernizuar, apo të Rregullores së Përgjithshme të Mbrojtjes së të Dhënave, përpunimi i tyre kërkon masa të veçanta, për të garantuar saktësinë dhe sigurinë e të dhënave.
- Sistemet elektronike të pagesave duhet të kenë mbrojtje të integruar të të dhënave, d.m.th privatësi, ose mbrojtje të dhënash që në fazën e konceptimit dhe me parapërzgjedhje.
- Në këtë sferë mund të shfaqen problematika të veçanta për mbrojtjen e të dhënave, për shkak se është e domosdoshme që të përdoren mekanzima të përshtatshëm autentifikimi.

[For designer: BOX TYPE 1]

Shembull: tek çështja *Michaud k. Francës*,[963] kërkuesi, i cili ishte një avokat francez, kundërshtoi detyrimin që i vendoste legjislacioni francez, për të sinjalizuar dyshimet në lidhje me aktivitete të mundshme pastrimi parash nga klientët e tij. GJEDNJ-ja vërejti se detyrimi që u ngarkohej avokatëve për të sinjalizuar informacione në lidhje me persona të tretë tek autoritetet administrative, për të cilat ishin vënë në dijeni gjatë komunikimeve profesionale, përbënte ndërhyrje tek e drejta e avokatëve për respektim të korrespondencës dhe të jetës private, sipas nenit 8 të KEDNJ-së, pasi ky koncept përfshinte

[963] GJEDNJ, *Michaud k. Francës*, nr. 12323/11, 6 dhjetor 2012. Shih gjithashtu: GJEDNJ, *Niemietz k. Gjermanisë*, nr. 13710/88, 16 dhjetor 1992, parag. 29, dhe GJEDNJ, *Halford k. Mbretërisë së Bashkuar*, nr. 20605/92, 25 qershor 1997, parag. 42.

aktitivitetet me natyrë profesionale, ose tregtare. Megjithatë, ndërhyrja ishte në përputhje me ligjin dhe synonte përmbushjen e një qëllimi legjitim, konkretisht të mbrojtjes së rendit dhe parandalimit të veprave penale. Meqenëse avokatët i nënshtrohet detyrimit për të raportuar aktivitete të dyshimta vetëm në rrethana tepër specifike, GJEDNJ-ja vendosi se ky detyrim ishte proporcionale dhe se nuk ishte shkelur neni 8.

Shembull: tek çështja *M.N. dhe të Tjerët k. San Marinos,*[964] kërkuesi, shtetas italian, lidhi një marrëveshje trusti me një shoqëri që ishte nën hetim. Shoqëria iu nënshtrua një kontrolli, gjatë së cilit u konfiskuan kopje dokumentesh (elektronike). Kërkuesi iu drejtua gjykatës së San Marinos, me pretendimin se nuk kishte asnjë lidhje mes tij dhe veprave penale të dyshuara. Megjithatë, gjykata e shpalli të papranueshme kërkesën e tij, me arsyetimin se ai nuk ishte "palë e interesuar". GJEDNJ-ja u shpreh se kërkuesi kishte qenë në situatë shumë të pafavorshme për sa i përket mbrojtjes gjyqësore, krahasuar me një "palë të interesuar", por pavarësisht kësaj, të dhënat e tij u ishin nënshtruar kontrollit dhe konfiskimit. Gjykata vendosi kështu se ishte shkelur neni 8.

Shembull: tek çështja *G.S.B. k. Zvicrës,*[965] të dhënat e llogarisë bankare të kërkuesit u ishin dërguar autoriteteve fiskale të SHBA-ve, në bazë të marrëveshjes së bashkëpunimt administrativ midis Zvicrës dhe SHBA-ve. GJEDNJ-ja u shpreh se transmetimi i këtyre të dhënave nuk ishte në kundërshtim me nenin 8 të KEDNJ-së, pasi ndërhyrja tek e drejta e kërkuesit për privatësi ishte e parashikuar me ligj, synonte arritjen e një qëllimi legjitim dhe ishte proporcionale me interesin publik përkatës.

Zbatimi i kuadrit ligjor të përgjithshëm të mbrojtjes së të dhënave (sikurse është përcaktuar në Konventën 108) në kontekstin e pagesave, është zhvilluar nga **KiE-ja** në Rekomandimin Rec(90)19 të 1990-ës.[966] Ky rekomandim qartëson qëllimin e mbledhjes dhe përdorimit të ligjshëm të të dhënave në kuadër të pagesave, veçanërisht të atyre me anë të kartave të pagesës. Ai gjithashtu ofron për ligjvënësit kombëtarë rekomandime të hollësishme në lidhje me rregullat për komunikimin e të dhënave të pagesave tek palët e treta, afatet kohore të mbajtjes së të dhënave, transparencën, sigurinë e të dhënave dhe qarkullimet ndërkufitare të të dhënave, si dhe për mbikëqyrjen dhe mjetet juridike. KiE-ja ka hartuar gjithashtu një Opinion mbi transferimin e të dhënave fiskale,[967] i cili ofron rekomandime dhe elemente që duhen marrë parasysh për transferimin e të dhënave fiskale.

GJEDNJ-ja e autorizon transmetimin e të dhënave financiare në bazë të nenit 8 të KEDNJ-së, konkretisht të të dhënave të llogarisë bankare të një personi, nëse është e parashikuar në ligj, synon arritjen e një qëllimi legjitim dhe është proporcional me interesin publik përkatës.[968]

Në të drejtën e BE-së, sistemet e pagesave elektronike që përfshijnë përpunim të dhënash personale, duhet të jenë në përputhje me Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave, ndaj duhet që këto sisteme të sigurojnë mbrojtje të dhënash që në fazën e konceptimit dhe mbrojtje të dhënash me parapërzgjedhje. Mbrojtja e të dhënave që në fazën e konceptimit detyron kontrolluesit të marrin masat e duhura teknike dhe organizative, për të zbatuar parimet e mbrojtjes së të dhënave. Mbrojtja e të dhënave me parapërzgjedhje nënkupton se kontrolluesi duhet të garantojë që vetëm të dhënat personale që janë të nevojshme për një qëllim të caktuar, të mund të përpunohen me parapërzgjedhje (shih Seksionin 4.4). Për sa i takon të dhënave financiare, GJDBE-ja është shprehur se të dhënat fiskale të transferuara mund të përbëjnë të dhëna personale.[969] Grupi i Punës së Nenit 29 ka miratuar udhëzues për Shtetet Anëtare në lidhje me këtë, ku përfshihen kriteret për garantimin e rregullave të mbrojtjes së të dhënave, kur shkëmbehen automatikisht të dhëna personale për qëllime fiskale, me anë të mjeteve të

[964] GJEDNJ, *M.N. dhe të Tjerët k. San Marinos*, nr. 28005/12, 7 korrik 2015.
[965] GJEDNJ, *G.S.B. k. Zvicrës*, nr. 28601/11 22 dhjetor 2015.
[966] Këshilli i Evropës, Komiteti i Ministrave (1990), Rekomandimi nr. R(90)19 për mbrojtjen e të dhënave personale të përdorura për pagesa dhe veprime të tjera në lidhje me to, 13 shtator 1990.
[967] Këshilli i Evropës, Komiteti Konsultativ i Konventës 108 (2014), Opinion në lidhje me ndërlikimet për mbrojtjen e të dhënave nga mekanizmat e shkëmbimeve automatike ndërshtetërore të të dhënave administrative dhe fiskale, 4 qershor 2014.
[968] GJEDNJ, *G.S.B. k. Zvicrës*, nr. 28601/11, 22 dhjetor 2015.
[969] GJDBE, C-201/14, *Smaranda Bara dhe të Tjerët k. Casa Naţională de Asigurări de Sănătate dhe të Tjerët*, 1 tetor 2015, parag. 29.

automatizuara.[970] Përveç kësaj, janë miratuar një sërë instrumentesh juridike, që rregullojnë tregjet financiare dhe veprimtarinw e institucioneve të kreditit dhe shoqërive të investimeve.[971] Instrumente të tjera juridike ndihmojnë në luftën kundër abuzimit me informacionin tregtar dhe manipulimit të tregut.[972] Fushat kryesore që kanë ndikim tek mbrojtja e të dhënave janë:

- Mbajtja e regjistrave të transaksioneve financiare;
- Transferimi i të dhënave personale drejt shteteve të treta;
- Regjistrimi i bisedave telefonike apo komunikimeve elektronike, përfshirë kompetencën e autoriteteve kompetente për të kërkuar regjistrimet telefonike dhe të dhënave të trafikut;
- Përhapja e të dhënave personale, përfshirë edhe publikimin e sanksioneve;
- Kompetencat mbikëqyrëse dhe hetuese të autoriteteve kompetente, përfshirë inspektimet në terren dhe hyrjen në ambientet private për të konfiskuar dokumente;
- Mekanizmat për sinjalizimin e shkeljeve, d.m.th. skemat e bilbilfryrësve; dhe
- Bashkëpunimi ndërmjet autoriteteve kompetente të Shteteve Anëtare me Autoritetin Evropian të Tregjeve Financiare (ESMA).

Trajtohen gjithashtu konkretisht problematika të tjera në këto fusha, përfshirë mbledhjen e të dhënave në lidhje me gjendjen financiare të subjekteve të të dhënave[973], ose pagesat ndërkufitare nëpërmjet transfertave bankare, të cilat sjellin pashmangshmërisht qarkullime të dhënash personale.[974]

[970]Grupi i Punës i Nenit 29 (2015), Deklaratë e Grupit të Punës së Nenit 29 në lidhje me shkëmbimet automatike ndërshtetërore të të dhënave personale për qëllime fiskale, 14/EN ËP 230.

[971] Direktiva 2014/65/BE e Parlamentit Evropian dhe e Këshillit e 15 majit 2014 mbi tregjet e instrumenteve financiare dhe që ndryshon Direktivën 2002/92/KE dhe Direktivën 2011/61/BE, FZ 2014 L 173; Rregullorja (BE) nr. 600/2014 e Parlamentit Evropian dhe e Këshillit e 15 majit 2014 mbi tregjet e instrumenteve financiare dhe që ndryshon Rregulloren (BE) nr. 648/2012, FZ 2014 L 173; Direktiva 2013/36/BE e Parlamentit Evropian dhe e Këshillit e 26 qershorit 2013 mbi aksesin në veprimtarinë e institucioneve të kreditimit dhe mbikëqyrjen prudenciale të institucioneve të kreditit dhe shoqërive të investimit, që ndryshon Direktivën 2002/87/KE dhe që shfuqizon Direktivat 2006/48/KE dhe 2006/49/KE, FZ 2013 L 176.

[972] Rregulllorja (BE) nr. 596/2014 e Parlamentit Evropian dhe e Këshillit e 16 prillit 2014 mbi abuzimet e tregut (rregullorja e abuzimeve të tregut) dhe që shfuqizon Direktivën 2003/6/KE të Parlamentit Evropian dhe Këshillit dhe Direktivat e Komisionit 2003/124/KE, 2003/125/KE dhe 2004/72/KE, FZ 2014 L 173.

[973] Rregullorja (KE) nr. 1060/2009 e Parlamentit Evropian dhe e Këshillit e 16 shtatorit 2009 mbi agjencitë e vlerësimit të kredive, FZ 2009 L 302 dhe ndryshuar së fundmi me Direktivën 2014/51/BE të Parlamentit Evropian dhe Këshillit të 16 prillit 2014 që ndryshon Direktivat 2003/71/KE dhe 2009/138/KE dhe Rregulloret (KE) nr. 1060/2009, (BE) nr. 1094/2010 dhe (BE) nr. 1095/2010 në lidhje me kompetencat e Autoritetit Evropian Mbikëqyrës (Autoriteti Evropian i Sigurimeve dhe Pensioneve Profesionale) dhe Autoritetit Evropian Mbikëqyës (Autoriteti Evropian i Tregjeve Financiare), FZ 2014 L 153; Rregullorja (BE) nr. 462/2013 e Parlamentit Evropian dhe e Këshillit e 21 majit 2013 që ndryshon Rregulloren (KE) nr. 1060/2009 mbi agjencitë e vlerësimit të kredive, FZ 2013 L 146.

[974] Direktiva 2007/64/KE e Parlamentit Evropian dhe e Këshillit e 13 nëntorit 2007 mbi shërbimet e pagesave në tregun e brendshëm, që ndryshon Direktivat 97/7/KE, 2002/65/KE, 2005/60/KE dhe 2006/48/KE dhe që shfuqizon Direktivën 97/5/KE, FZ 2007 L 319, ndryshuar me Direktivën 2009/111/KE të Parlamentit Evropian dhe Këshillit të 16 shtatorit 2009 që ndryshon Direktivat 2006/48/KE, 2006/49/KE dhe 2007/64/KE në lidhje me bankat që kanë lidhje me institucione qendrore, disa çështje për fondet e veta, ekspozimet e mëdha, masat mbikëqyrëse, dhe administrimin e krizave, FZ 2009 L 302.

10 Sfidat moderne për mbrojtjen e të dhënave

Epoka digjitale, apo epoka e teknologjisë së informacionit, karakterizohet nga përdorimi tejet i përhapur i kompjuterëve, internetit dhe teknologjive digjitale, çka sjell mbledhje dhe përpunim sasish jashtëzakonisht të mëdha të të dhënave, përfshirë të dhënat personale. Mbledhja dhe përpunimi i të dhënave personale në një ekonomi të globalizuar nënkupton se qarkullimet ndëkufitare të të dhënave shumëfishohen. Ky përpunim mund të sjellë përparësi domethënëse dhe të prekshme në jetën e përditshme: motorët e kërkimit lehtësojnë qasjen në një vëllim të konsiderueshëm informacioni dhe njohurish, shërbimet e rrjeteve sociale u mundësojnë njerëzve në të gjithë botën që të komunikojnë, të shpehin mendime dhe të krijojnë ndërgjegjësim për çështje shoqërore, mjedisore dhe politike, ndërsa shoqëritë tregtare dhe konsumatorët përfitojnë nga teknikat efikase dhe të leverdishme të marketingut, të cilat nxisin ekonominë. Teknologjia dhe përpunimi i të dhënave personale janë gjithashtu mjete të domosdoshme për autoritetet shtetërore, në luftën e tyre kundër krimit dhe terrorizmit. Në të njëjtën masë, të dhënat masive, mbledhja, regjistrimi dhe analizimi i sasive të mëdha të informacionit me qëllim identifikimin e tendencave dhe parashikimin e sjelljeve, "mund të jetë një burim me vlerë të madhe për shoqërinë, për rritjen e prodhueshmërisë, për veprimtarinë e sektorit publik dhe pjesëmarrjen shoqërore".[975]

Pavarësisht përfitimeve të shumta, epoka digjitale paraqet gjithashtu sfida për privatësinë dhe mbrojtjen e të dhënave, për shkak se mblidhen dhe përpunohen sasi tepër të mëdha të dhënash personale, në mënyra gjithnjë e më të ndërlikuara e më pak transparente. Përparimi teknologjik ka sjellë zhvillim njësish të dhënash masive, që mund të kryqëzohen lehtësisht dhe të analizohen në mënyrë më të thelluar, për të evidentuar tendenca, ose për të marrë vendime mbështetur në algoritme, të cilat mund të japin informacion si asnjëherë më parë për sjelljet dhe jetën private të njerëzve.[976]

Teknologjitë e reja janë të fuqishme dhe mund të paraqesin rrezik tepër të madh nëse bien në duar të gabuara. Autoritetet shtetërore që kryejnë veprimtari përgjimi masiv, që mbështetet tek këto teknologji, përbëjnë një shembull të ndikimit të rëndë që mund të kenë këto teknologji tek të drejtat e personave. Në vitin 2013, sinjalizimet e Edward Snowden-it për përdorimin e programeve të përgjimit të internetit dhe telefonave në shkallë të gjerë, nga agjencitë informative të disa shteteve, shkaktoi shqetësim të madh në lidhje me rreziqet e veprimtarisë së përgjimit për privatësinë, qeverisjen demokratike dhe lirinë e shprehjes. Përgjimi masiv dhe teknologjitë që mundësojnë arkivimin dhe përpunimin e globalizuar të informacioneve personale, si dhe aksesi në të dhëna massive, mund të dëmtojnë vetë thelbin e së drejtës për provatësi.[977] Gjithashtu, ato mund të shkaktojnë pasoja negative për kulturën politike dhe të kenë ndikim shkurajues tek demokracia, krijimtaria dhe novacioni.[978] Thjesht frika se shteti mund të jetë duke gjurmuar dhe analizuar në mënyrë të pandërprerë sjelljen dhe veprimet e qytetarëve, mund t'i pengojë ata të shprehin mendime për çështje të caktuara dhe të sjellë si rezultat mobesim dhe kujdes.[979] Këto sfida kanë nxitur një sërë autoritetesh publike, qendrash kërkimore dhe organizatash të shoqërisë civile, që të analizojnë ndikimin e mundshëm të teknologjive të reja në shoqëri. Në vitin 2015, Mbikëqyrësi Evropian i Mbrojtjes së të Dhënave ndërmori disa iniciativa që synonin të vlerësonin ndikimin tek etika të të dhënave masive dhe Objekteve të Lidhura në Internet (*Internet of Things*). Më

---

[975] Këshilli i Evropës, Komiteti Konsultativ i Konventës 108, *Udhëzues për mbrojtjen e personave në lidhje me përpunimin e të dhënave personale në epokën e të dhënave masive*, T-PD(2017)01, Strasburg, 23 janar 2017.

[976] Parlamenti Evropian (2017), Rezolutë mbi ndërlikimet për të drejtat themelore nga të dhënat masiveL privatësia, mbrojtja e të dhënave, mos diskriminimi, siguria dhe zbatimi i ligjit (P8_TA-PROV(2017)0076, Strasburg, 14 mars 2017.

[977] Shih: OKB, Asambleja e Përgjithshme, *Raport i Raportuesit Special për nxitjen dhe mbrojtjen e të drejtave dhe lirive themelore të njeriut në luftën kundër terrorizmit*, Ben Emmerson, A/69/397, 23 shtator 2014, parag. 59. Shih gjithashtu: GJEDNJ, *Dokument tematik në lidhje me survejimin masiv,* korrik 2017.

[978] EDPS (2015), *Përballimi i sfidave të të dhënave masive*, Opinion 7/2015, Bruksel, 19 nëntor 2015.

[979] Shih sidomos: GJDBE, Çështje të bashkuara C-293/12 dhe C-594/12, *Digital Rights Ireland Ltd k. Minister for Communications, Marine and Natural Resources dhe të Tjerët* dhe *Kärntner Landesregierung dhe të Tjerët* [ÇB], 8 prill 2014, parag. 37.

kryesorja ndër to është ndgritja e Grupit Këshillimor për Etikën, i cili synon të nxisë "diskutime të hapura dhe të informuara mbi etikën digjitale, që t'i mundësojë BE-së të konkretizojë përfitimet e shoqërisë dhe ekonomisë nga teknologjia dhe njëkohësisht të përforcojë të drejtat dhe liritë e personave, sidomos së drejtave për privatësi dhe mbrojtje të të dhënave."[980]

Përpunimi i të dhënave personale është gjithashtu një mjet i fuqishëm në duart e shoqërive tregtare. Ai mundëson sot të zbulohet informacion në lidhje me shëndetin, apo gjendjen financiare të personave, informacion i cili përdoret më pas nga shoqëritë tregtare për të marrë vendime të rëndësishme për personat, si për shembull se cili prim sigurimi shëndetësor i përshtatet personit, apo aftësia paguese e kredisë. Teknikat e përpunimit të të dhënave mund të kenë po ashtu ndikim tek proceset demokratike, kur përdoren nga politikanët, apo shoqëritë tregtare për të ndikuar zgjedhjet, për shembull nëpërmjet "mikro-shënjestrimit" të komunikimeve me zgjedhësit. Me fjalë të tjera, fillimisht privatësia perceptohej si e drejta për mbrojtjen e personave nga ndërhyrja e pajustifikuar e autoriteteve publike, ndërsa në epokën moderne, ajo mund të kërcënohet edhe nga forcat e palëve private. Diçka e tillë ngre problematika që kanë të bëjnë me përdorimin e teknologjisë dhe analizës parashikuese, në vendimet që prekin jetën e përditshme të qyetarëve dhe rrisin nevojën për të garantuar që çdo përpunim të dhënash personale të respektojë kriteret e së drejtave themelore.

Mbrojtja e të dhënave është e lidhur pazgjidhshmërisht me ndryshimet teknokogjike, shoqërore dhe politike. Për këtë shkak, do të ishte e pamundur të hartohej një listë e plotë e sfidave të së ardhmes. Kapitulli në vijim shqyrton disa fusha të caktuara, që kanë të bëjnë me të dhënat masive, rrjetet sociale dhe Tregun Unik Digjital të BE-së. Nuk bëhet fjalë për një vlerësim shterrues të këtyre fushave, nga këndvështrimi i mbrojtjes së të dhënave, por për evidentimin e shumë ndërveprimeve të mundshme, midis veprimtarive njerëzore të reja, ose të ndryshuara, me mbrojtjen e të dhënave.

10.1 Të dhënat masive, algoritmet dhe inteligjenca artificiale

Pikat kryesore

- Risitë e jashtëzakonshme në fushën e teknologjisë së informacionit dhe komunikimit po formësojnë një mënyrë të re jetese, ku marrëdhëniet shoqërore, tregtare, shërbimet publike dhe private, janë ndërlidhur në rrugë digjitale, duke gjeneruar kësisoj sasi gjithnjë e më të mëdha të dhënash, ku një pjesë e madhe e tyre janë të dhëna personale.
- Qeveritë, ndërmarrjet dhe qytetarët veprojnë në një ekonomi gjithnjë e më shumë të bazuar tek shkëmbimi i të dhënave, në të cilat vetë të dhënat janë shndërruar në aset të vlefshëm.
- Koncepti i të dhënave masive nënkupton si të dhënat, ashtu edhe analizimin e tyre.
- Të dhënat personale që përpunohen me anë të analizimit të të dhënave masive, hyjnë në fushën e zbatimit të legjislacionit të BE-së dhe të KiE-së.
- Përjashtimet nga zbatimi i rregullave dhe të drejtave të mbrojtjes së të dhënave kufizohen në disa të drejta të caktuara dhe situata të veçanta, në të cilat ushtrimi i një të drejte do të ishte i pamundur, ose do të kërkonte përpjekje të shpërpjestuara nga ana e kontrolluesve të të dhënave.
- Vendimmarrja plotësisht e automatizuar është përgjithësisht e ndaluar, përveç disa rasteve të veçanta.
- Ndërgjegjësimi dhe kontrolli nga ana e qyetarëve është thelbësor, për të garantuar respektimin e të drejtave të tyre.

[980] EDPS, Vendim i 3 dhjetorit 2015 për ngritjen e një grupi të jashtëm këshillimor mbi dimensionet etike të mbrojtjes së të dhënave ('Grupi Këshillimor mbi Etikën'), 3 dhjetor 2015, pika 5.

Në botën tonë gjithnjë e më të digjitalizuar, çdo veprim lë gjurmë digjitale, e cila mund të mblidhet, përpunohet dhe vlerësohet, ose analizohet. Falë teknologjive të reja të informacionit dhe komunikimit, gjithnjë e më tepër të dhëna mblidhen dhe regjistrohen.[981] Deri para pak kohësh, asnjë teknologji nuk kishte aftësinë të analizonte, ose vlerësonte këtë masë të dhënash, apo të nxirrte përfundime të dobishme prej tyre. Të dhënat ishin thjesht në numër tepër të lartë për t'u vlerësuar, tepër të ndërlikuara, të strukturuara keq dhe në evoluim tepër të shpejtë, për të identifikuar tendenca dhe zakone.

10.1.1 Përkufizimi i të dhënave masive, algoritmeve dhe inteligjencës artificiale

Të dhënat masive

Termi "të dhëna masive" (*big data*) është një shprehje e re, e cila i referohet disa koncepteve, në varësi të kontekstit. Përgjithësisht ajo nëkupton "aftësinë teknologjike në rritje për të mbledhur, përpunuar dhe ekstraktuar njohuri të reja dhe parashikuese, nga të dhëna në sasi, lloje dhe shpejtësi të mëdha".[982] Për rrjedhojë, koncepti i të dhënave masive përfshin qoftë të dhënat vetë, ashtu edhe analizimin e tyre.

Burimet e të dhënave janë të shumëllojshme dhe përfshijnë njerëzit dhe të dhënat e tyre personale, makineritë ose sensorët, informacionin për klimën, pamjet satelitore, fotografitë dhe videot digjitale, apo sinjalet e GPS-së. Megjithatë, një pjesë e madhe e të dhënave dhe e informacionit janë të dhëna personale, që nga emri, fotografija, adresa e postës elektronike, llogaria bankare, të dhënat e gjurmimit të GPS-së, postimet në rrjetet sociale, informacioni mjekësor, apo adresa e IP-së së kompjuterit.[983]

Të dhënat masive nënkuptojnë gjithashtu edhe **përpunimin**, analizimin dhe vlerësimin e masave të të dhënave dhe informacionit të disponueshëm, dmth ekstraktimi i informacioneve të dobishme për qëllime të analizimit të të dhënave masive. Kjo do të thotë se të dhënat dhe informacioni i mbledhur, mund të përdoren për qëllime të ndryshme nga ai i parashikuar fillimisht, p.sh. për tendenca statistikore, apo për shërbime më të përshtatura, sikurse është publiciteti. Në fakt, kur ekzistojnë teknologji që mundësojnë mbledhjen, përpunimin dhe vlerësimin e të dhënave masive, çdo lloj informacioni mund të kryqëzohet dhe të rivlerësohet: transaksionet financiare, aftësia paguese e kredisë, trajtimi mjekësor, konsumi privat, veprimtaria profesionale, gjurmimi dhe itinerary i ndjekur, përdorimi i internetit, kartat elektronike dhe telefonat inteligjentë, videopërgjimi, apo përgjimi i komunikimeve. Analizimi i të dhënave masive sjell një dimension të ri sasior të të dhënave, që mund të vlerësohen dhe përdoren në kohë reale, për shembull për të ofruar shërbime të përshtatura për konsumatorët.

Algoritmet dhe inteligjenca artificiale

Inteligjenca artificiale (IA) i referohet inteligjencës së makinerive, që veprojnë si "agjentë inteligjentë". Në cilësinë e agjentëve inteligjentë, disa lloj pajisjesh, me ndihmën e programeve kompjuterike, mund të perceptojnë mjedisin e tyre dhe të veprojnë sipas algoritmeve. Termi IA përdoret kur një makineri imiton funksionet njohëse, si të mësuarit dhe të zgjidhurit e problemeve, të cilat normalisht i mvishen personave fizikë.[984] Me qëllim që të imitojnë vendimmarrjen, teknologjitë dhe programet kompjuterike modern përdorin algoritme, të cilat i përdorin pajisjet për të marrë "vendime të automatizuara".

---

[981] Komisioni Evropian, Komunikatë e Komisionit për Parlamentin Evropian, Këshillin, Komitetin Ekonomik dhe Shoqëror Evropian dhe Komitetin e Rajoneve drejt një ekonomie të dhënash të begatë, COM(2014) 442 final, Bruksel, 2 korrik 2014.

[982] Këshilli i Evropës, Komiteti Konsultativ i Konventës 108, Udhëzues mbi mbrojtjen e personave në lidhje me përpunimin e të dhënave personale në epokën e të Dhënave Masive, 23 janar 2017, në fq. 2; Komisioni Evropian, Komisionit për Parlamentin Evropian, Këshillin, Komitetin Ekonomik dhe Shoqëror Evropian dhe Komitetin e Rajoneve drejt një ekonomie të dhënash të begatë, COM(2014) 442 final, Bruksel, 2 korrik 2014, në fq. 4; Unioni Ndërkombëtar i Telekomunikacioneve (2015), Rekomandimi Y.3600. Big Data – Cloud computing based requirements and capabilities.

[983] Dokument Tematik i Komisionit të BE-së mbi Reformën e BE-së në Fushën e Mbrojtjes së të Dhënave dhe të Dhënat Masive; Këshilli i Evropës, Komiteti Konsultativ i Konventës 108, Udhëzues mbi mbrojtjen e personave në lidhje me përpunimin e të dhënave personale në epokën e të Dhënave Masive, 23 janar 2017, në fq. 2.

[984] Stuart Russel dhe Peter Norvig, *Artificial Intelligence: A Modern Approach (2nd ed.)*, 2003, Upper Saddle River, New Jersey: Prentice Hall, fq. 27, 32–58, 968–972; Stuart Russel dhe Peter Norvig, *Artificial Intelligence: A Modern Approach (3rd ed.)*, 2009, Upper Saddle River, New Jersey: Prentice Hall, fq. 2.

Përkufizimi më i mirë për algoritmin është një procedurë hap pas hapi për përllogaritjen, përpunimin e të dhënave, vlerësimin, arsyetimin dhe vendimmarrjen e automatizuar.

Ashtu sikurse analizimi i të dhënave masive, Inteligjenca Artificiale dhe vendimmarrja e automatizuar që ajo prodhon, kërkon mbledhjen dhe përpunimin e sasive të mëdha të të dhënave. Këto të dhëna burojnë nga vetë pajisja (temperatura e frenave, karburanti, etj.), ose nga mjedisi përreth. Për shembull, profilizimi është një process që mund të mbështetet tek vendimmarrja e automatizuar sipas modeleve, apo faktorëve të parapërcaktuar.

[BOX TYPE 2]

Shembull: Profilizimi dhe publiciteti i shënjestruar

Profilizimi i bazuar tek të dhënat masive ka të bëjë me kërkimin e modeleve që pasqyrojnë "karakteristikat e një lloji personaliteti", për shembull, kur shoqëritë e blerjeve në internet ofrojnë "produkte të tjera që mund t'i pëlqeni", bazuar në informacionin e mbledhur nga produktet që klienti ka vendosur më parë në shportën e blerjeve. Sa më shumë të dhëna, aq më i qartë mozaiku. Për shembull, telefoni inteligjent përbën një pyetësor të fuqishëm, të cilin personat e plotësojnë sa herë që e përdorin, në mënyrë të ndërgjegjshme, ose jo.

Psikografia moderne, shkenca që studion personalitetin, përdor metodën OCEAN, bazuar në të cilat përcakton llojin e personalitetit që trajton. 'Pesë aspektet e mëdha' të personalitetit janë: Hapja (sa i hapur është personi kundrejt risive), Ndërgjegjshmëria (karakteri perfeksionist i një personi), Ekstraversioni (sa i shoqërueshëm është personi), Pëlqyeshmëria (sa i pëlqyeshëm është personi) dhe Neuroticizmi (sa emocional është personi). Ky informacion e profilizon personin, nevojat dhe frikat e tij, mënyrën se si do të sillet, etj. Kjo më pas plotësohet me informacion tjetër në lidhje me personin, të përftuar nga çdo burim tjetër i mundshëm, si nga ndërmjetësit e të dhënave, rrjetet sociale (përfshirë "pëlqimet" e postimeve dhe fotografive të publikuara), tek muzika e dëgjuar në internet, të dhënat e GPS-së dhe të dhënat e gjurmimit.

Më pas, bëhet krahasimi i masës së profileve që krijohen nëpërmjet teknikave të analizimit të të dhënave masive, me qëllim identifikimin e modeleve të ngjashme dhe përcaktimin e grupeve të personaliteteve. Kësisoj, përmbyset informacioni mbi sjelljet dhe qëndrimet e personaliteteve të caktuara. Falë aksesit tek të dhënat masive, testi i personalitetit modifikohet, meqenëse informacioni në lidhje me sjelljet dhe qëndrimet përdoret tashmë për të përshkruar personalitetin e personit. Duke zotëruar informacion të kryqëzuar në lidhje me "pëlqimet" në rrjetet sociale, të dhënat e gjurmimit, të muzikës së dëgjuar, apo filmave të shikuar, mund të ndërtohet një imazh i personalitetit të personit, çka i mundëson shoqërive tregtare t'i komunikojnë personit publicitet dhe/ose informacione të përshtatura me "personalitetin" e tij. Çka është më kryesorja, informacioni mund përpunohet në kohë reale.[985]

10.1.2 Ekuilibrimi i përfitimeve dhe risqeve të të dhënave masive

Teknikat moderne të përpunimit mund të trajtojnë sasi të mëdha të dhënash, të importojnë me shpejtësi të dhëna të reja, të kryejnë përpunim në kohë reale të informacioneve me kohë reagimi të shpejtë (madje edhe në rast kërkesash të ndërlikuara), të ofrojnë mundësinë e kërkesave të shumta dhe të njëkohëshme

[985] Teknikat e përpunimit dhe progamet e reja kompjuterike vlerësojnë në kohë reale informacionin në lidhje me shijet e personave, çfarë kërkojnë kur bëjnë blerje në internet, apo çfarë shtojnë tek shporta e blerjeve në internet dhe mund të ofrojnë "produkte" që mund të jenë me interes, bazuar në informacionin e mbledhur.

dhe të analizojnë lloje të ndryshme informacioni (fotografi, tekste, ose numra). Këto risi teknologjike bëjnë të mundur të strukturohen, përpunohen dhe vlerësohen masa të dhënash dhe informacioni në kohë reale.[986] Duke rritur në mënyrë eksponenciale sasinë e të dhënave të disponueshme dhe të analizuara, mund të arrihen tashmë rezultatet që nuk mund të arriheshin me një analizë në shkallë të ulët. Të dhënat masive kanë mundësuar zhvillimin e një fushe të re aktiviteti tregtar, në të cilin mund të shfaqen shërbime të reja, si për shoqëritë tregtare, ashtu edhe për konsumatorët. Vlera e të dhënave personale të qytetarëve të BE-së mund të arrijë në 1 triliard euro në vitin 2020.[987] Për rrjedhojë, të dhënat masive mund të ofrojnë **mundësi** të reja, që burojnë nga vlerësimi i të dhënave masive, për njohuri të reja shoqërore, ekonomike, apo shkencore, me dobi si për personat, ashtu edhe për shoqëritë tregtare dhe për qeveritë.[988]

Analizimi i të dhënave masive mund të zbulojë modele midis burimeve dhe grupeve të ndryshme të të dhënave, çka ofron njohuri të dobishme në sfera të tilla si shkenca dhe mjekësia. Shembuj të tillë për shembull janë në fushat e shëndetit, sigurisë ushqimore, sistemeve e transportit inteligjent, efikasitetit energjetik, apo planifikimit urban. Kjo analizë informacioni në kohë reale mund të përdoret për të përmirësuar sistemet ekzistuese. Në sferën e kërkimit, mund të përftohen njohuri të reja nëpërmjet kombinimit të sasive të mëdha të të dhënave dhe vlerësimeve statistikore, sidomos në disiplina ku deri më sot, një sasi e madhe e të dhënave vlerësoheshin manualisht. Mund të zhvillohen trajtime të reja, të përshtatura për çdo pacient, nëpërmjet krahasimit me tërësinë e informacioneve të disponueshme. Shoqëritë tregtare shpresojnë se analizimi i të dhënave masive do t'u mundësojë të kenë përparësi konkurrenciale, të kursejnë dhe të krijojnë sektorë të rinj tregtie, nëpërmjet një shërbimi klienti të drejtpërdrejtë dhe të personalizuar. Agjencitë qeveritare shpresojnë të arrijnë përmirësime në sferën e drejtësisë penale. Strategjia e Komisionit për Tregun Unik Digjital në Evropë e njeh potencialin e teknologjive dhe të shërbimeve të bazuara tek të dhënat, si dhe të dhënat masive si katalizatore të rritjes ekonomike, inovacionit dhe digjitalizimit në BE.[989]

Megjithatë, të dhënat masive mbartin gjithashtu **risqe**, të cilat lidhen përgjithësisht me tre cilësitë e tyre: vëllimin, shpejtësinë dhe shumëllojshmërinë e të dhënave të përpunuara.Vëllimi nënkupton sasinë e të dhënave të përpunuara, shumëllojshmëria ka të bëjë me numrin dhe diversitetin e llojeve të të dhënave, ndërsa shpejtësia nënkupton shpejtësinë e përpunimit të të dhënave. Problematikat për mbrojtjen e të dhënave shfaqen sidomos kur përdoret analizimi i të dhënave masive tek tërësi të mëdha të dhënash, për të ekstraktuar njohuri të reja dhe parashikuese për qëllime vendimmarrjeje në lidhje me persona dhe/ose grupe.[990] Risqet për mbrojtjen e të dhënave dhe privatësinë nga të dhënat masive janë theksuar në disa Opinione të EDPS-të dhe të Grupit të Punës së Nenit 29, në rezoluta të Parlamentit Evropian dhe në dokumente udhëzuese të Këshillit të Evropës.[991]

Risqet mund të të përfshijnë keqpërdorimin e të dhënave masive nga personat që kanë akses në informacione masive, për të manipuluar, diskriminuar, apo shtypur persona dhe grupe të caktuara të

---

[986] Zhvillimi i programeve kompjuterike për përpunimin e të dhënave masive është ende në hapat e parë. Sidoqoftë, kohët e fundit janë zhvilluar programe analitike, sidomos për analizimin e të dhënave dhe informacioneve masive në kohë reale, që lidhen me veprimtaritë e personave. Mundësia e analizimit dhe përpunimit të të dhënave masive në mënyrë të strukturuar, ka krijuar mjete të reja për profilizim dhe marketing të drejtpërdrejtë. Komisioni Evropian, Komunikatë e Komisionit për Parlamentin Evropian, Këshillin, Komitetin Ekonomik dhe Shoqëror Evropian dhe Komitetin e Rajoneve drejt një ekonomie të dhënash të begatë, COM(2014) 442 final, Bruksel, 2 korrik 2014; Komisioni i BE-së, Dokument Tematik i Komisionit mbi Reformën e Mbrojtes së të Dhënave të BE-së dhe të Dhënat Masive, si dhe Këshilli i Evropës, Udhëzues mbi mbrojtjen e personave në lidhje me përpunimin e të dhënave personale në epokën e të Dhënave Masive, 23 janar 2017, në fq. 2.

[987] Dokument Tematik i Komisionit të BE-së mbi Regormën e Mbrojtjes së të Dhënave në BE dhe të Dhënat Masive.

[988] Konferenca Ndërkombëtare e Komisionerëve të Mbrojtjes së të Dhënave dhe Privatësisë (2014), Rezolutë për të Dhënat Masive dhe Komisioni Evropian, Komunikatë e Komisionit për Parlamentin Evropian, Këshillit, Komitetin Ekonomik dhe Shoqëror Evropian dhe Komitetin e Rajoneve drejt një ekonomie të dhënash të begatë COM(2014) 442 final, Bruksel, 2 korrik 2014, në fq. 2; Komisioni i BE-së, Dokument Tematik i Komisionit mbi Reformën e Mbrojtes së të Dhënave të BE-së dhe të Dhënat Masive, si dhe Këshilli i Evropës, Udhëzues mbi mbrojtjen e personave në lidhje me përpunimin e të dhënave personale në epokën e të Dhënave Masive, 23 janar 2017, në fq. 1.

[989] Rezolutë e Parlamentit Evropian e 14 marsit 2017 mbi ndërlikimet që shkaktojnë të Dhënat Masive për të drejtat themelore, mbrojtjen e të dhënave, mos diskriminimin dhe zbatimin e ligjit (2016/2225 (INI)).

[990] Këshilli i Evropës, Komiteti Konsultativ i Konventës 108, Udhëzues mbi mbrojtjen e personave në lidhje me përpunimin e të dhënave personale në epokën e të Dhënave Masive, 23 janar 2017, në fq. 2.

[991] Shih për shembull: EDPS (2015), *Meeting the Challenges of big data*, Opinion 7/2015, 19 nëntor 2015; EDPS (2016), *Coherent enforcement of fundamental rights in the age of Big Data*, Opinion 8/2016, 23 shtator 2016; Parlamenti Evropian (2016), Rezolutë mbi ndërlikimet që shkaktojnë të Dhënat Masive për të drejtat themelore, mbrojtjen e të dhënave, mos diskriminimin dhe zbatimin e ligjit, P8_TA(2017)0076, Strasburg, 14 mars 2017; Këshilli i Evropës, Komiteti Konsultativ i Konventës 108, Udhëzues mbi mbrojtjen e personave në lidhje me përpunimin e të dhënave personale në epokën e të Dhënave Masive, T-PD(2017)01, Strasburg, 23 janar 2017.

shoqërisë.[992] Kur mblidhen, përpunohen dhe vlerësohen të dhëna personale, apo informacion masiv në lidhje me sjelljet individuale, shfrytëzimi i tyre mund të shkaktojë shkelje të rënda të të drejtave dhe lirive themelore, që shkojnë përtej së drejtës për privatësi. Nuk është e mundur që të matet saktë shkalla e mundshme e cënimit të privatësisë dhe të të dhënave personale. Parlamenti Evropian ka konstatuar mungesë metodologjie për kryerjen e një vlerësimi të provuar të ndikimit të përgjithshëm të të dhënave masive, por ka prova që tregojnë se analizimi i të dhënave masive mund të ketë ndikim horizontal të konsiderueshëm në sektorin publik dhe në atë privat.[993]

Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave përmban dispozita mbi të drejtën për të mos iu nënshtruar vendimmarrjes së automatizuar, përfshirë profilizimin.[994] Çështja e respektimit të privatësisë ngrihet kur ushtrimi i së drejtës për të kundërshton, kërkon ndërhyrje njerëzore, që t'u mundësojë subjekteve të të dhënave të shprehin këndvështrimin e tyre dhe të kundërshtojnë vendimin.[995] Këtu lindin sfidat që kanë të bëjnë me garantimin e një niveli të mjaftueshëm të mbrojtjes së të dhënave, nëse për shembull nuk ka asnjë mundësi për ndërhyrje njerëzore, ose kur algoritmi është tepër i ndërlikuar dhe sasia e të dhënave të përfshira është tejet e madhe për t'u bërë me dije personave justifikimin e disa vendimeve të caktuara dhe/ose informacion paraprak për t'u marrë pëlqimin. Një shembull i përdorimit të inteligjencës artificiale dhe vendimmarrjes automatike gjendet në zhvillimet e fundit për sa i përket aplikimeve për kredi hipotekore, ose procedurave të rekrutimit të punonjësve. Aplikimet refuzohen, ose kthehen mbrapsht me arsyetimin se aplikantët nuk përmbushin parametrat, ose faktorët e paracaktuar.

10.1.3 Problematika në lidhje me mbrojtjen e të dhënave

Për sa i përket mbrojtjes së të dhënave, problematikat kryesore kanë të bëjnë nga njëra anë me vëllimin dhe shumëllojshmërinë e të dhënave personale të përpunuara dhe nga ana tjetër me përpunimin dhe rezultatet e tij. Futja në përdorim e algoritmeve dhe programeve kompjuterike të ndërlikuara, për të transformuar të dhënat masive në burim për qëllime vendimmarrjeje, ndikon veçanërisht tek personat dhe grupet, kryesisht në rastet e profilizimit, ose etiketimit dhe së fundi ngre problematika të shumta për mbrojtjen e të dhënave.[996]

Identifikimi i kontrolluesve dhe përpunuesve dhe përgjegjësia e tyre

Të dhënat masive dhe inteligjenca artificiale ngrejnë pikëpyetje të shumta për sa i takon identifikimit të kontrolluesve dhe përpunuesve dhe përgjegjësisë së tyre: kur një sasi kaq e madhe të dhënash mblidhet dhe përpunohet, kush i ka në pronësi të dhënat? Kur të dhënat përpunohen nga makineri dhe programme kompjuterike inteligjente, kush është kontrolluesi? Saktësisht cilat janë përgjegjësitë e secilit aktor në përpunim? Si dhe për çfarë qëllimesh mund të përdoren të dhënat masive?

Çështja e përgjegjësisë në kontekstin e inteligjencës artificiale do të bëhet edhe më e mprehtë, kur një IA do të marrë vendim bazuar në përpunimin e të dhënave që ka zhvilluar vetë. Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave parashikon një kuadër ligjor për përgjegjësinë e kontrolluesit dhe përpunuesit të të dhënave. Përpunimi i paligjshëm i të dhënave personale sjell përgjegjësi për kontrolluesin e të dhënave dhe për përpunuesin e të dhënave.[997] Inteligjenca artificiale dhe vendimmarrja e automatizuar ngrejnë pikëpyetje se kush është përgjegjës për shkeljet që cënojnë privatësinë e subjekteve të të dhënave, kur kompleksiteti dhe sasia e të dhënave të përpunuara nuk mundësojnë të përcaktohet me siguri. Duke e konsideruar IA-në dhe algoritmet si produkte, lind problemi i përgjegjësisë personale, i cili rregullohet nga GDPR-ja dhe problemi i përgjegjësisë për

[992] Konferenca Ndërkombëtare e Komisionerëve të Mbrojtjes së të Dhënave dhe Privatësisë (2014), Rezolutë mbi të Dhënat Masive.
[993] Rezolutë e Parlamentit Evropian e 14 marsit 2017 mbi ndërlikimet që shkaktojnë të Dhënat Masive për të drejtat themelore, mbrojtjen e të dhënave, mos diskriminimin dhe zbatimin e ligjit (2016/2225 (INI)).
[994] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 22.
[995] *Ibid.*, neni 22, pika 3.
[996] Këshilli i Evropës, Komiteti Konsultativ i Konventës 108, *Udhëzues mbi mbrojtjen e personave në lidhje me përpunimin e të dhënave personale në epokën e të Dhënave Masive*, T-PD(2017)01, Strasburg, 23 janar 2017, në fq. 2.
[997] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, nenet 77–79 dhe neni 82.

produktin, i cili nuk rregullohet prej saj.[998] Për këtë nevojiten rregulla për përgjegjësinë, për mbushur boshllëkun midis përgjegjësisë personale dhe përgjegjësisë për produktin, në lidhje me robotikën dhe IA-në, duke përfshirë vendimmarrjen automatike.[999]

Ndikimi tek parimet e mbrojtjes së të dhënave

Natyra, analiza dhe përdorimi i të dhënave masive të përshkruar më lart, bien ndesh me zbatimin e disa prej parimeve tradicionale themelore të së drejtës evropiane në fushën e mbrojtjes së të dhënave.[1000] Këto sfida kanë të bëjnë kryesisht me parimet e ligjshmërisë, minimizimit të të dhënave, kufizimit të qëllimit dhe transparencës.

Parimi i minimizimit të të dhënave kërkon që të dhënat personale të jenë të përshtatshme, të rëndësishme dhe të kufizuara për sa i përket qëllimit të përpunimit të tyre. Megjithatë, model ii ekonomik i të dhënave masive mund të jetë antiteza e minimizimit të të dhënave, pasi ai kërkon gjithnjë e më shumë të dhëna, shpesh për qëllime të paqarta.

E njëjta vlen edhe për parimin e kufizimit të qëllimit, i cili kërkon që të dhënat të përpunohen për qëllime specifike dhe nuk mund të përdoren për qëllime që nuk pajtohen me qëllimin fillestar të mbledhjes së tyre, përveç rastit kur përpunimi mbështetet në një bazë juridike, si për shembull, por jo vetëm, pëlqimi i subjektit të të dhënave (shih Seksionin 4.1.1).

Së fundmi, të dhënat masive vënë në diskutim edhe parimin e saktësisë së të dhënave, meqenëse aplikacionet e të dhënave masive priren të mbledhin të dhëna nga një shumëllojshmëri burimesh, pa pasur mundësi të verifikojnë dhe/ose të ruajnë saktësinë e të dhënave të mbledhura.[1001]

Rregulla dhe të drejta të veçanta

Rregulli i përgjithshmë mbetet ai që të dhënat personale të përpunuara nëpërmjet analizimit të të dhënave masive, hyjnë në fushën e zbatimit të legjislacionit për mbrojtjen e të dhënave. Gjithsesi, në të drejtën e BE-së dhe atë të KiE-së janë integruar rregulla, ose përjashtime të veçanta, për raste të caktuara në lidhje përpunime të dhënash algoritmetike të ndërlikuara.

Në **të drejtën e KiE-së**, Konventa 108 e Modernizuar u jep të drejta të reja subjekteve të të dhënave, për t'u mundësuar kontroll më efikas tek të dhënat e tyre personale në epokën e të dhënave masive. Bëhet fjalë, për shembull, për nenin 9, pika 1, gërmat (a), (c) dhe (d) të Konventës së Modernizuar, mbi të drejtën për të mos iu nënshtruar një vendimi që prek subjektin në mënyrë të konsiderueshme, i cili bazohet krejtësisht në përpunim të automatizuar të të dhënave, pa marrë parasysh mendimin e tij, apo të saj; të drejtën për të marrë dijeni, me kërkesë, për arsyen e përpunimit të të dhënave, kur rezultatet e përpunimit zbatohen ndaj tij, apo ndaj saj, si dhe të drejtën për të kundërshtuar. Dispozita të tjera të Konventës 108 të Modernizuar, veçanërisht ato mbi transparencën dhe detyrimet e tjera, përbëjnë elemente plotësuese të mekanizmit mbrojtës që ka ngritur Konventa 108 e Modernizuar, për përballimin e sfidave digjitale.

Në **të drejtën e BE-së**, përtej rasteve të renditura në nenin 23 të GDPR-së, duhet garantuar **transparencë** në të gjitha përpunimet e të dhënave personale. Kjo merr rëndësi të veçantë sidomos për sa i përket shërbimeve në internet dhe për përpunime të tjera të automatizuara dhe të ndërlikuara të të dhënave, sikurse përdorimi i algoritmeve për vendimmarrje. Në këtë rast, karakteristikat e sistemeve të përpunimit të të dhënave duhet të bëjnë të mundur që subjektet e të dhënave të kuptojnë vërtet se çfarë po ndodh me të dhënat e tyre. Me qëllim që të garantojë përpunim të drejtë dhe transparent, Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave detyron kontrolluesin t'i japë subjektit të të dhënave informacion kuptimplotë mbi logjikën e përdorur për vendimmarrjen e automatizuar, përfshirë

---

[998] Parlamenti Evropian, Rregullat e së Drejtës Civile Evropiane në lidhje me Robotikën, Drejtoria e Përgjithshme e Politikave të Brendshme, (tetor 2016), fq. 14.

[999] Fjalim i Roberto Viola-s në seminarin mediatik mbi të Drejtën Evropiane në lidhje me Robotikën, në Parlamentin Evropian. (Fjalim 16/02/2017); Njoftim për shtyp i Parlamentit Evropian mbi kërkesën e Komisionit për një propozim në lidhje me rregullat e përgjegjësisë civile në sferën e robotikës dhe inteligjencës artificiale.

[1000] Këshilli i Evropës, Komiteti Konsultativ i Konventës 108, *Udhëzues mbi mbrojtjen e personave në lidhje me përpunimin e të dhënave personale në epokën e të Dhënave Masive*, T-PD(2017)01, Strasburg, 23 janar 2017.

[1001] EDPS (2016), *Coherent enforcement of fundamental rights in the age of Big Data*, Opinioni 8/2016, 23 shtator 2016, fq. 8.

profilizimin.[1002] Në Rekomandimin e tij mbi mbrojtjen dhe nxitjen e së drejtës së lirisë së shprehjes dhe së drejtës për jetë private në lidhje me neutralitetin e rrjetit, Komiteti i Ministrave të Këshillit të Evropës rekomandon që operatorët e shërbimeve të internetit "t'u japin përdoruesve informacion të qartë, të plotë dhe publikisht të disponueshëm rreth të gjitha praktikave të menaxhimit të trafikut, që mund të kenë ndikim tek aksesi dhe shpërndarja nga ana e përdoruesve të përmbajtjes, aplikacioneve, ose shërbimeve".[1003] Raportet që kanë të bëjnë me praktikat e menaxhimit të trafikut të internetit, që hartohen nga autoritetet kompetente të Shteteve Anëtare, duhen përgatitur në mënyrë të hapur dhe transparente dhe duhen vënë në dispozicion të publikut pa pagesë.[1004]

Pavarësisht nëse të dhënat janë mbledhur prej subjekteve të të dhënave, ose jo, kontrolluesit e të dhënave duhet t'u **japin** atyre jo thjesht **informacione** specifike në lidhje me të dhënat e mbledhura, apo përpunimin e planifikuar (shih Seksionin 6.1.1), por nëse është rasti edhe mbi ekzistencën e proceseve të vendimmarrjes së automatizuar, duke u dhënë "informacion kuptimplotë në për sa i përket logjikës së përdorur",[1005] objektivat dhe pasojat e mundshme të këtyre proceseve. Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave qartëson gjithashtu se (vetëm në rastet kur të dhënat personale nuk janë marrë nga vetë subjekti i të dhënave), se kontrolluesi nuk është i detyruar t'ia japë këto informacione subjektit të të dhënave në rast se "dhënia e këtyre informacioneve rezulton e pamundur, ose do të kërkonte përpjekje jo proporcionale".[1006] Gjithsesi, sikurse theksohet në *Uddhëzuesin mbi vendimmarrjen individuale të automatizuar dhe profilizimin për qëllime të Rregullores 2016/679* të Grupit të Punës së Nenit 29, kompleksiteti i përpunimit në vetvete nuk duhet ta pengojë kontrolluesin e të dhënave që t'i janë subjektit të të dhënave shpjegime të qarta mbi objektivat dhe metodën e analizimit të përdorur për përpunimin e të dhënave.[1007]

Të drejtat e subjekteve për **akses**, **korrigjim** dhe **fshirje** të të dhënave personale të tyre, ashtu si edhe e drejta për të **kufizuar** përpunimin, nuk e përfshijnë një përjashtim të tillë. Megjithatë, detyrimi i kontrolluesit të të dhënave për të njoftuar subjektin e të dhënave për çdo korrigjim, apo fshirje të të dhënave personale të tyre (shih Seksionin 6.1.4) mund të hiqet po ashtu, kur njoftimi "rezulton i pamundur, apo kërkon përpjekje jo proporcionale".[1008]

Referuar nenit 21 të GDPR-së (shih Seksionin 6.1.6), subjektet e të dhënave kanë gjithashtu të drejtën të **kundërshtojnë** çdo përpunim të të dhënave personale të tyre, përfshirë edhe rastet e analizimit të të dhënave masive. Paçka se kontrolluesit e të dhënave mund të përjashtohen nga ky detyrim nëse vërtetojnë se ekzistojnë interesa legjitime prevaluese, ata nuk përfitojnë nga ky përjashtim për përpunime për qëllime marketingu të drejtpërdrejtë.

Përjashtime të veçanta nga këto të drejta mund të përdoren nga kontrolluesit e të dhënave, kur përpunojnë të dhëna personale për qëllime arkivimi me interes publik, për qëllime kërkimi shkencor, ose historik, apo për qëllime statistikore.[1009]

Për sa i përket **profilizimit dhe vendimmarrjes së automatizuar**, GDPR-ja parashikon rregulla specifike: neni 22, pika 1 përcakton se subjekti i të dhënave "ka të drejtën të mos i nënshtrohet një vendimi të bazuar vetëm në një përpunim automatik duke përfshirë profilizimin, që prodhon efekte në lidhje me të". Sikundër nënvizohet në udhëzuesin e Grupit të Punës së Nenit 29, ky nen thekson një ndalim të përgjithshëm të vendimmarrjes krejtësisht të automatizuar.[1010] Kontrolluesit e të dhënave mund të përjashtohen nga ky ndalim vetëm në tre raste të caktuara: kur vendimi është: 1) i nevojshëm

[1002] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 13, pika, 2, gërma (f).
[1003] Këshilli i Evropës, Komiteti i Ministrave (2016), Rekomandimi CM/Rec(2016)1 I Komitetit të Ministrave për shtetet anëtare mbi mbrojtjen dhe nxitjen e lirisë së shprehjes dhe së drejtës për jetë private në lidhje me paanësinë e rrjetit, 13 janar 2016, parag. 5.1.
[1004] *Ibid.*, parag. 5.2.
[1005] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 13, pika 2, gërma f dhe neni 14, pika 2, gërma g.
[1006] *Ibid.*, neni 14, pika 5, gërma b.
[1007] Grupi i Punës së Nenit 29, *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*, wp251, 3 tetor 2017, fq. 14.
[1008] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 19.
[1009] *Ibid.*, neni 89, pikat 2 dhe 3.
[1010] Grupi i Punës së Nenit 29, *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*, wp251, 3 tetor 2017, fq. 9.

për përmbushjen e një kontrate midis subjektit të të dhënave dhe kontrolluesit, 2) autorizohet e drejta e BE-së ose e Shtetit Anëtar, ose 3) bazohet në pëlqimin e qartë.[1011]

Kontrolli nga ana e individëve

Kompleksiteti dhe mungesa e transparencës që karakterizojnë analizimin e të dhënave masive, mund të nxisin rishqyrtimin e rregullave të kontrollit nga ana e individëve tek të dhënat personale. Këto rregulla duhet të përshtaten me kontekstin shoqëror dhe teknologjik, duke marrë parasysh mungesën e njohurive nga ana e personave. Për rrjedhojë, mbrojtja e të dhënave në lidhje me të dhënat masive duhet të bazohet në një koncept më të gjerë të kontrollit mbi përdorimin e të dhënave, sipas së cilit kontrolli nga anan e personave evoluon drejt një procesi më kompleks vlerësimesh të shumta ndikimi të risqeve që burojnë nga përdorimi i të dhënave.[1012]

Cilësia e një aplikacioni të dhënash masive varet nga kapaciteti i tij për të parashikuar dëshirat, apo sjelljen e personave (apo konsumatorëve) që testohen. Modelet parashikuese aktuale që mbështeten tek analizimi i të dhënave masive, përmirësohen në mënyrë të pandërprerë. Zhvillimet e kohëve të fundit përfshijnë jo vetëm përdorimin e të dhënave për kategorizimin e personaliteteve (dmth sjelljes dhe qëndrimeve), por edhe analizimin e sjelljes nëpërmjet studimit të modeleve vokale dhe intensitetit me të cilin shkruhen mesazhet, apo duke matur temperaturën trupore. Gjithë ky informacion mund të krahasohet në kohë reale me njohuritë e përdtuara nga analizimi i të dhënave masive, për shembull për të vlerësuar aftësinë paguese të kredisë gjatë një takimi me një përfaqësues banke. Vlerësimi nuk bëhet bazuar në cilësitë e personit që aplikon për kredi, por në karakteristikat e sjelljes që nxirren nga analizimi dhe vlerësimi i informacionit të të dhënave masive, dmth fakti që kërkuesi i kredisë flet me zë të lartë, apo me zë miklues, gjuha e trupit të tij apo të saj, apo temperatura trupore.

Profilizimi dhe publiciteti i shënjestruar mund të mos jenë detyrimisht problematike, nëse personat janë **të ndërgjegjshëm** që janë subjekt reklamash të personalizuara. Profilizimi bëhet problematik kur përdoret për të manipuluar personat, për shembull për të kërkuar disa personalitete, apo grupe personash të caktuar për fushata politike. Për shembull, grupet e zgjedhësve të pavendosur mund të shënjestrohen me mesazhe politike të përshtatura me "personalitetin" dhe qëndrimet e tyre. Një problem tjetër mund të jetë përdorimi i këtij profilizimi për të refuzuar aksesin në mallra dhe shërbime për disa individë të caktuar. Një masë e mundshme për mbrojtjen nga abuzimi me të dhënat masive dhe informacionin personal është pseudonimizimi (shih Seksionin 2.1.1).[1013] Nëse të dhënat personale anonimizohen vërtet, dmth nuk mbetet asnjë informacion që mund të lërë gjurmë të cilat lidhen me subjektin e të dhënave, raste të tilla dalin jashtë fushës së zbatimit të Rregullores së Përgjithshme të Mbrojtjes së të Dhënave. Edhe pëlqimi i subjekteve të të dhënave dhe individëve për përpunimin e të dhënave masive, përbën gjithashtu sfidë për legjislacionin e mbrojtjes së të dhënave. Këtu hyn pëlqimi për t'iu nënshtruar publicitetit të personalizuar dhe profilizimit, që mund të justifikohen për qëllime të "vlerësimit të përvojës së klientit", dhe pëlqimi për përdorimin e masave të të dhënave personale për të përmirësuar dhe zhvilluar pajisjet analitike të bazuara tek informacioni. Dijenia, apo mungesa e dijenisë për përpunimin e të dhënave masive ngre shumë pikëpyetje, për sa i takon mjeteve më të cilat mund të ushtrojnë të drejtat e tyre subjektet e të dhënave, meqenëse përpunimi i të dhënave masive mund të mbështetet si tek informacioni i pseudonimizuar, ashtu edhe tek ai i anonimizuar që përpunohen me anë të algoritmeve. Ndërsa të dhënat e pseudonomizuara hyjnë në fushën e zbatimit të Rregullores së Përgjithshme të Mbrojtjes së të Dhënave, ajo nuk nuk zbatohet për të dhënat e anonimizuara. Kontrolli nga ana e personave mbi përpunimin e të dhënave personale dhe ndërgjegjësimi i tyre në lidhje me të, është thelbësor në kuadrin e analizimit të të dhënave masive. Pa këto, subjektet e të dhënave nuk do ta kenë të qartë se kush është kontrolluesi, e kush përpunuesi, duke mos mundur kësisoj të ushtrojnë me efikasitet të drejtat e tyre.

[1011] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 22, pika 2.
[1012] Këshilli i Evropës, Komiteti Konsultativ i Konventës 108, *Udhëzues mbi mbrojtjen e personave në lidhje me përpunimin e të dhënave personale në epokën e të Dhënave Masive*, T-PD(2017)01, Strasburg, 23 janar 2017.
[1013] *Ibid.*, fq. 2.

10.2 Web-et 2.0 dje 3.0: rrjetet sociale dhe Objektet e Lidhura në Internet

Pikat kryesore

- Shërbimet e Rrjeteve Sociale (SNS-të) janë platforma komunikimi në internet, të cilat u mundësojnë personave t'u bashkohen, apo të krijojnë rrjete përdoruesish që kanë interesa të përbashkëta.
- Objektet e Lidhura në Internet nënkupton lidhjen e objekteve në internet dhe ndërlidhjen e objekteve ndërmjet tyre.
- Pëlqimi i subjekteve të të dhënave është baza ligjore më e zakonshme për përpunim të ligjshëm të të dhënave nga kontrolluesit e të dhënave në rrjetet sociale.
- Përdoruesit e rrjeteve sociale janë përgjithësisht të mbrojtur nga "përjashtimi për aktivitete familjare"; megjithatë ky përjashtim mund të hiqet në situata të caktuara.
- Operatorët e rrjeteve sociale nuk mbrohen nga "përjashtimi për aktivitete familjare".
- Privatësia që në fazën e konceptimit dhe me parapërgjedhje janë thelbësore për të garantuar siguri të dhënash në këtë fushë.

10.2.1 Përkufizimi i web-eve 2.0 dhe 3.0

Shërbimet e Rrjeteve Sociale

Fillimisht, interneti u konceptua si një rrjet për ndërlidhjen e kompjuterëve dhe për të transmetuar mesazhe me kapacitete të kufizuara për shkëmbime të dhënash, ku faqet e internetit u ofronin personave thjesht mundësinë për të parë përmbajtjen e tyre në mënyrë pasive.[1014] Në epokën e Web-it 2.0, interneti u transformua në një forum ku përdoruesit ndërveprojnë, bashkëpunojnë dhe gjenerojnë të dhëna. Kjo epokë u karakterizua nga suksesi i jashtëzakonshëm dhe nga përdorimi tejet i përhapur i rrjeteve sociale, të cilat tashmë janë pjesë thelbësore e jetës së përditshme të miliona njerëzve.

Shërbimet e Rrjeteve Sociale (SNS-të), ndryshe "mediat sociale" mund të përkufizohen në mënyrë të përgjithshme si "platforma komunikimi në internet, që u mundësojnë personave t'u bashkohen, apo të krijojnë rrjete përdoruesit që kanë interesa të përbashkëta".[1015] Për t'iu bashkuar, apo për të krijuar një rrjet, personat ftohen të japin të dhënat personale dhe të krijojnë profilin e tyre. SNS-të u mundësojnë përdoruesve të gjenerojnë "përmbajtje" digjitale, duke nisur nga fotografitë dhe videot, tek lidhjet drejt gazetave dhe postimeve personale për shpehjen e mendimeve të tyre. Nëpërmjet këtyre platformave të komunikimit në internet, përdoruesit mund të ndërveprojë dhe të komunikojne me shumë përdorues të tjerë. Vlen të theksohet se rrjetet më të famshme SNS nuk kërkojnë asnjë tarifë regjistrimi. Në vend që t'u kërkojnë përdoruesve të paguajnë për t'iu bashkuar rrjetit, operatorët e SNS-ve krijojnë pjesën më të madhe të fitimeve nga publiciteti i shënjestruar. Publikuesit e reklamave mund të nxjerrin fitime të mëdha nga informacioni personal që zbulohet në mënyrë të përditshme në këto faqe interneti. Posedimi i informacionit mbi moshën, gjininë, vendndodhjen dhe interesat e përdoruesit, u mundëson atyre t'ua dërgojnë reklamat e tyre njerëzve "të duhur".

[1014] Komisioni Evropian (2016), *Advancing the Internet of Things in Europe*, SWD(2016) 110 final.
[1015] Grupi i Punës së Nenit 29 (2009), *Opinioni 5/2009 mbi rrjetet sociale në internet*, WP 163, 12 qershor 2009, fq. 4.

Komiteti i Ministrave të Këshillit të Evropës ka miratuar një Rekomandim mbi mbrojtjen e të drejtave të njeriut në lidhje me shërbimet e rrjeteve sociale,[1016] i cili trajton mbrojtjen e të dhënave në një kapitull të caktuar. Në vitin 2018, ai u plotësua me Rekomandimin mbi rolin dhe përgjegjësitë e ndërmjetësve të internetit.[1017]

[BOX TYPE 2]

Shembull: Nora është mjaft e lumtur, pasi partneri i saj i propozoi të martoheshin. Ajo dëshiron ta ndajë lajmin e mirë me miqtë dhe familjen dhe vendos të shkruajë një postim emocional në rrjetin social, për të shpehur gëzimin dhe për të ndryshuar statusin e marrëdhënies së saj në "e fejuar". Në ditët në vijim, kur ajo lidhet në llogarinë e saj, Norës i shfaqen reklama për fustane nusërie dhe dyqane lulesh. Përse ndodh kjo?

Kur krijojnë një reklamë në Facebook, shoqëritë e fustaneve të nusërisë dhe të luleve përzgjedhin disa parametra, në mënyrë që t'ua dërgojnë ato njerëzve si Nora. Kur në profilin e Norës thuhet se ajo është grua, e fejuar, me banim në Paris, pranë zonës ku ndodhen dyqanet e fustaneve dhe të luleve të cilat kanë vendosur reklamat, ajo menjëherë shikon ato reklama.

Objektet e Lidhura në Internet

Objektet e Lidhura në Internet (IoT) përbëjnë hapin e radhës së zhvillimit të internetit: epokën e Web-it 3.0. Falë Objekteve të Lidhura në Internet, pajisjet mund të lidhen dhe të ndërveprojnë me pajisje të tjera nëpërmjet internetit. Diçka e tillë u mundëson sendeve dhe njerëzve të ndërlidhen nëpërmjet rrjeteve të komunikimit, të raportojnë gjendjen e tyre dhe/ose gjendjen e mjedisit përreth tyre.[1018] Objektet e Lidhura në Internet dhe pajisjet e lidhura janë tashmë realitet, i cili pritet të zhvillohet në mënyrë të konsiderueshme në vitet e ardhshme, me krijimin dhe zhvillimin e mëtejshëm të pajisjeve inteligjente, që do të sjellin krijimin e qyteteve inteligjente, banesave inteligjente dhe bizneseve inteligjente.

[BOX TYPE 2]

Shembull: Objektet e Lidhura në Internet mund të jenë veçanërisht të dobishme për kujdesin shëndetësor. Disa shoqëri tregtare kanë krijuar tashmë pajisje, sensorë dhe aplikacione që mundësojnë monitorimin e shëndetit të pacientit. Nëpërmjet përdorimit të një butoni alarmi që mbahet në trup dhe sensorëve të tjerë me valë të instaluar në banesë, është e mundur të kontrollohet aktiviteti i përditshëm i të moshuarve që jetojnë të vetmuar dhe të lëshohen sinjale nëse vërehen çrregullime në programin e tyre të përditshëm. Për shembull, sensorët e rrëzimit përdoren gjerësisht nga të moshuarit. Këta sensore mund të zbulojnë rrëzimet me saktësi dhe të njoftojnë për këtë mjekun e personit dhe/ose familjen.

[1016] Këshilli i Evropës, Komiteti i Ministrave, Rekomandimi CM/Rec(2012)4 i Komitetit të Ministrave për shtetet anëtare mbi mbrojtjen e të drejtave të njeriut në lidhje me shërbimet e rrjeteve sociale, 4 prill 2012.
[1017] Këshilli i Evropës, Komiteti i Ministrave, Rekomandimi CM/Rec(2018)2 i Komitetit të Ministrave për shtetet anëtare mbi rolin dhe përgjegjësitë e ndërmjetësve të internetit, 7 mars 2018.
[1018] Komisioni Evropian, Dokument Pune i Shërbimeve të Komisionit, *Advancing the Internet of Things in Europe*, SWD(2016) 110, 19 prill 2016.

Shembull: Barcelona është një nga shembujt më të njohur të qyteteve inteligjente. Që prej vitit 2012, qyteti ka vënë në përdorim teknologji të përparuara, që synojnë krijimin e një sistemi inteligjent transporti publik, trajtimi mbetjesh, parkimi dhe ndriçimi rrugor. Për shembull, për përmirësimin e trajtimit të mbetjeve, qyteti përdor kosha inteligjentë, të cilët mundësojnë të kontrollohet niveli i mbetjeve, për të optimizuar itineraret e mbledhjes së mbeturinave. Kur koshat janë pothuajse të mbushur, ato transmetojnë sinjale nëpërmjet rrjetit të komunikimeve celulare, të cilat i dërgohen aplikacionit që përdoret nga shoqëria e menaxhimit të mbetjeve. Në këtë mënyrë, shoqëria mund të planifikojë itineraret më të mira për mbledhjen e mbeturinave, t'u japë përparësi dhe/ose të organizojë mbledhjen vetëm tek koshat që nevojitet të zbrazen.

10.2.2 Ekuilibrimi i përfitimeve dhe risqeve

Përhapja e gjerë dhe e sukseshme e SNS-ve gjatë dekadës së kaluar bën të mendohet se ato ofrojnë **përfitime të konsiderueshme**. Për shembull, publiciteti i shënjestruar, (si përshkruhet në shembullin përkatës), është një mënyrë tepër e përparuar që shoqëritë tregtare përdorin për t'iu afruar publikut të tyre, duke i ofruar një treg më konkret. Ai mund të jetë gjithashtu në interes të konsumatorëve, që reklamat të cilat u paraqiten, të jenë më të rëndësishme dhe më interesante për ta. Çka është më e rëndësishmja, shërbimet e rrjeteve sociale dhe mediat sociale mund të kenë ndikim pozitiv në shoqëri dhe në arritjen e ndryshimeve. Ato u mundësojnë përdoruesve të komunikojnë, ndërveprojnë, të organizojnë grupe dhe aktivitete për çështje që i prekin.

Edhe Objektet e Lidhura në Internet pritet të sjellin përfitime të konsiderueshme për ekonominë dhe janë pjesë e strategjisë së BE-së për zhvillimin e Tregut Digjital Unik. Vlerësohet se në vitin 2020, numri i objekteve të lidhura në internet në BE do të rritet në gjashtë milliard. Ky zgjerim ndërlidhjeje pritet të sjellë përfitime të rëndësishme ekonomike, nëpërmjet zhvillimit të shërbimeve dhe aplikacioneve novatore, kujdes shëndetësor më të mirë, njohuri tw pwrmirwsuara tw nevojave tw konsumatorwve dhe rritje efikasiteti.

Në të njëjtën kohë, për shkak të sasisë së jashtëzakonshme të informacioneve personale që krijojnë përdoruesit e mediave sociale dhe që më pas përpunohen nga operatorët e shërbimit, shtrirja e SNS-ve shoqërohet me **shqetësim në rritje**, për sa i përket mënyrave me të cilën mund të mbrohen privatësia dhe të dhënat personale. SNS-të mund të kërcënojnë të drejtën për jetë private dhe të drejtën e lirisë së shprehjes. Këto kërcënime mund të burojnë kryesisht nga: "mungesa e garancive juridike dhe procedurale për sa i përket proceseve që mund të çojnë në përjashtimin e përdoruesve; mbrojtja e papërshtatshme për fëmijët dhe të rinjtë nga materiale, ose sjellje të dëmshme; mungesa e respektit për të drejtat e të tjerëve; mungesa e konfigurimit të parapërzgjedhur për mbrojtjen e privatësisë; mungesa e transparencës në lidhje me qëllimet për të cilat mblidhen dhe përpunohen të dhënat personale".[1019] Legjislacioni evropian i mbrojtjes së të dhënave është përpjekur t'u përgjigjet sfidave që paraqesin mediat sociale për mbrojtjen e privatësisë dhe të dhënave. Parime të tilla si pëlqimi, mbrojtja e privatësisë dhe të dhënave që në fazën e konceptimit dhe me parapërzgjedhje dhe të drejtat e personave, janë me rëndësi të veçantë në kontekstin e mediave sociale dhe shërbimeve të rrjetit.

Për sa i përket Objekteve të Lidhura në Internet, vëllimi i jashtëzakonshëm i të dhënave personale që gjenerohen nga pajisjet e ndryshme të ndërlidhura, sjell gjithashtu risqe për privatësinë dhe mbrojtjen e të dhënave. Paçka se transparenca është parim i rëndësishëm në të drejtën evropiane të mbrojtjes së të dhënave, nisur nga moria e pajisjeve të lidhura, nuk është gjithnjë e qartë se cila mund të mbledhë,

[1019] Këshilli i Evropës, Rekomandimi Rec(2012)4 për shetetet anëtare mbi mbrojtjen e të drejtave të njeriut në lidhje me shërbimet e rrjeteve sociale, 4 prill 2012.

aksesojë dhe përdorë të dhënat e mbledhura nga Objektet e Lidhura në Internet.[1020] Megjithatë, në të drejtën e BE-së dhe atë të KiE-së, parimi i transparencës përcakton një detyrim për kontrolluesit, që të mbajnë të informuar subjektet e të dhënave, me gjuhë të qartë dhe të thjeshtë, për mënyrën se si përdoren të dhënat e tyre. Risqet, rregullat, garancitë dhe të drejtat në kuadrin e përpunimit të të dhënave personale të tyre, duhet t'u bëhen të qarta personave përkatës. Numri i Objekteve të Lidhura në Internet dhe i aktiviteteve të përpunimit dhe sasia e të dhënave të përfshira, mund të shkelin po ashtu kriterin e dhënies së pëlqimit të qartë dhe të informuar për përpunimin e të dhënave, kur përpunimi bazohet tek pëlqimi. Shpesh personat nuk e kuptojnë si funksionon teknikisht përpunimi e rrjedhimisht as pasojat e pëlqimit që japin.

Një tjetër çështje shqetësuese është siguria, duke pasur parasysh se pajisjet e lidhura janë tepër të brishta ndaj risqeve të sigurisë. Pajisjet e lidhura kanë nivele të ndryshme sigurie. Meqenëse veprojnë jashtë infrastrukturës së zakonshme të TI-s, ato mund të mos kenë fuqi përpunuese dhe kapacitet regjistrimi të përshtatshëm për të mbajtur program sigurie, apo për të zbatuar teknika të tilla si enkriptimi, pseudonimizimi, apo anonimizmi për të mbrojtjur informacionet personale të përdoruesve.

[BOX TYPE 2]

Shembull: në Gjermani, autoriteti rregullator vendosi të ndalonte një lodër të lidhur në internet, pas shqetësimeve në lidhje me ndikimin e lodrës tek respektimi i jetë private të fëmijëve. Autoriteti rregullator vlerësoi se një kukull e quajtur Kajla, e cila lidhej në internet, ishte në fakt një pajisje përgjimi të fshehtë. Kukulla funksiononte duke dërguar pyetjet zanore të fëmijës që luante me të tek një aplikacion i një pajisjeje digjilate, i cili e përkthente në tekst dhe kërkonte përgjigjen në internet. Aplikacioni i dërgonte më pas përgjigjen kukullës, e cila ia përcillte fëmijës me zë. Nëpërmjet kësaj kukulle, komunikimet e fëmijës, ashtu si edhe të të rriturve pranë saj, mund të regjistroheshin dhe të transmetoheshin tek aplikacioni. Nëse prodhuesi i kukullës nuk aplikonte masa të përshtatshme sigurie, kukulla mund të përdorej nga gjithkush për të dëgjuar bisedat.

10.2.3 Problematika në lidhje me mbrojtjen e të dhënave

Pëlqimi

Në Evropë, përpunimi i të dhënave personale është i ligjshëm vetëm nëse lejohet nga legjislacioni evropian për mbrojtjen e të dhënave. Për operatorët e SNS-ve, pëlqimi i subjekteve të të dhënave përbën zakonisht bazën ligjore për përpunimin e të dhënave. Pëlqimi duhet dhënë në mënyrë të lirë dhe specifike, të informuar dhe të qartë (shih Seksionin 4.1.1).[1021] 'I dhënë lirisht' në thelb nënkupton se subjektet e të dhënave duhet të kenë mundësi zgjedhjeje reale. Pëlqimi është 'specifik' dhe 'i informuar' kur është i kuptueshëm dhe i drejtohet qartësisht dhe saktësisht fushës, qëllimeve dhe pasojave të përpunimit të të dhënave. Në kontekstin e rrjeteve sociale, mund të ngrihen pikëpyetje nëse pëlqimi është i lirë, specifik dhe i informuar për të gjitha llojet e përpunimit që kryejnë operatorët e SNS-ve dhe palët e treta.

[BOX TYPE 3]

Shembull: për t'u anëtarësuar dhe për të hyrë në një rrjet social, personat shpesh janë të detyruar të pranojnë lloje të ndryshme përpunimi të të dhënave personale të tyre, jo rrallë pa marrë shpjegimet e duhura, apo të drejtë zgjedhjeje tjetër. Një shembull i tillë është kur duhet të japin pëlqimin që t'u

[1020] Mbikëqyrësi Evropian i Mbrojtjes së të Dhënave (2017), *Understanding the Internet of Things.*
[1021] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 4 dhe neni 7; Konventa 108 e Modernizuar, neni 5.

dërgohen reklama bazuar tek sjellja, në mënyrë që të regjistrohen në një rrjet social. Sikurse thekson Grupi i Punës së Nenit 29 në Opinion e tij mbi përkufizimin e pëlqimit, "duke pasur parasysh rëndësinë që kanë marrë disa rrjete sociale, disa kategori përdoruesish (si për shembull adoleshentët), pranojnë t'u dërgohen reklama bazuar tek sjellja, vetëm që të shmangin rrezikun e përjashtimit nga një pjesë e ndërveprimeve shoqërore. Përdoruesit duhet t'i mundësohet të japë pëlqimin e lirë dhe specifik për marrjen e reklamave bazuar tek sjellja, në mënyrë të pavarur nga aksesi i tij në shërbimin e rrjetit social."[1022]

Sipas Rregullores së Përgjithshme të Mbrojtjes së të Dhënave, në parim, të dhënat personale të fëmijëve nën moshën 16 vjeç, nuk mund të përpunohen mbi bazën e pëlqimit të tyre.[1023] Nëse pëlqimi për përpunimin është i nevojshëm, ai duhet dhënë nga prindi, apo kujdestari i fëmijës. Fëmijët kanë nevojë për mbrojtje të veçantë, nisur nga fakti se ata mund të jenë më pak të ndërgjegjshëm për risqet dhe pasojat që mbart përpunimi i të dhënave. Ky element ka rëndësi të madhe në kontekstin e rrjeteve sociale, pasi fëmijët janë më të brishtë ndaj pasojave negative të përdorimit të këtyre rrjeteve, sikurse janë ngacmimet, përndjekja dhe vjedhja e identitetit në internet.

Siguria dhe privatësia/mbrojtja e të dhënave që në fazën e konceptimit dhe me parapërzgjedhje

Përpunimi i të dhënave personale mbart në vetvete risqe për sigurinë, për shkak të mundësisë së përhershme për shkelje sigurie, të cilat shkaktojnë shkatërrim aksidental, apo të paligjshëm, humbje, modifikim, akses, apo përhapje të paautorizuar të të dhënave personale të përpunuara. Në legjislacionin evropian të mbrojtjes së të dhënave, kontrolluesi dhe përpunuesit janë të detyruar të zbatojnë masat e përshtatshme teknike dhe organizative, për të parandaluar çdo ndërhyrje të paautorizuar tek operacionet e përpunimit të të dhënave. Edhe operatorët e shërbimeve të rrjeteve sociale që hyjnë në fushën e zbatimit të rregullave evropiane të mbrojtjes së të dhënave, duhet ta zbatojnë këtë detyrim.

Parimet e privatësë dhe mbrojtjes së të dhënave që në fazën e konceptimit dhe me papapërzgjedhje detyrojnë kontrolluesit të garantojnë sigurinë që në fazën e konceptimit të produkteve të tyre dhe të zbatojnë në mënyrë automatike parametrat e përshtatshme të mbrojtjes së privatësisë dhe të dhënave. Kjo nënkupton që kur një person vendos të regjistrohet në një rrjet social, operatori i shërbimit nuk duhet t'ua vërë automatikisht në dispozicion të gjitha informacionet e përdoruesit të ri të shërbimit, të gjithë përdoruesve të tij. Gjatë regjistrimit, parametrat e parapërzgjedhur të mbrojtjes së privatësisë dhe të dhënave duhet të jenë vendosur në mënyrë të tillë që informacioni të jetë i disponueshëm vetëm për kontaktet e zgjedhur nga personi. Zgjerimi i aksesit tek njerëz të tjerë jashtë asaj liste, duhet të jetë i mundur vetëm pasi përdoruesi të kryejë manualisht ndryshimin e parametrave të parapërzgjedhur të mbrojtjes së privatësisë dhe të dhënave. Diçka e tillë mund të ketë gjithashtu ndikim në rastet kur ndodh një shkelje ndaj të dhënave, pavarësisht masave të sigurisë që janë zbatuar. Në këto raste, operatorët e shërbimit duhet të njoftojnë përdoruesit e prekur, nëse shkelja ka gjasa të shkaktojë rrezik të lartë për të drejtat dhe liritë e subjekteve të të dhënave.[1024]

Mbrojtja e privatësisë dhe të dhënave që në fazën e konceptimit dhe me parapërzgjedhje janë tepër të rëndësishme në kontekstin e SNS-ve, pasi përveç risqeve të aksesit të paautorizuar që mbartin shumica e llojeve të përpunimit, shkëmbimi i informacioneve personale në rrjetet sociale mbart edhe risqe të tjera shtesë për sigurinë. Shpesh këto burojnë nga fakti që personat nuk kuptojnë se *kush* mund të ketë akses në informacionet e tyre dhe se si këta persona mund ta përdorin atë. Me përdorimin e përhapur të mediave sociale, numri i incidenteve të vjedhjes së identitetit dhe të viktimave të tyre është rritur.

[BOX TYPE 2]

[1022] Grupi i Punës së Nenit 29 (2011), *Opinioni 15/2011 mbi përkufizimin e pëlqimit*, WP 187, 13 korrik 2011, fq. 18.
[1023] Shih Rregulloren e Përgjithshme të Mbrojtjes së të Dhënave, nenin 8. Shtetet Anëtare të BE-së mund të përcaktojnë në ligj një moshë më të ulët, në masën që ajo të mos jetë më e ulët se 13 vjeç.
[1024] *Ibid*., neni 34.

Shembull: vjedhja e identitetit është një fenomen në të cilin një person merr në posedim informacion, të dhëna, apo dokumente që i përkasin një personi tjetër (viktimës) dhe hiqet më pas sikur është viktima, për të përfituar mallra dhe sërbime në emër të viktimës. Marrim për shembull Polin, i cili ka një llogari në një rrjet social. Poli është mësues dhe anëtar aktiv i komunitetit të tij, tepër i shoqërueshëm dhe aspak i shqetësuar për parametrat e mbrojtjes së privatësisë dhe të të dhënave personale të llogarisë së tij në median sociale. Ai ka një listë të madhe kontaktesh, ku madje një pjesë janë persona që ai as nuk i njeh personalisht. Meqenëse ai punon në një shkollë të madhe dhe është mjaft i famshëm, pasi është trajner i ekipit të futbollit të shkollës, ai mendon se këta persona ka shumë mundësi të jetë prindër, ose miq të shkollës. Adresa e postës elektronike dhe datëlindja e Polit janë publikuar në llogarinë e tij në median sociale. Gjithashtu, Poli poston rregullisht fotografi të qenit të tij të quajtur Tobi, me diçitura të llojit "Unë dhe Tobi duke bërë vrapin e mëngjesit". Poli nuk i ka rënë në të, se një nga pyetjet më të shpeshta që përdoren për mbrojtjen e llogarisë së postës elektronike, apo të llogarisë së telefonit cellular, është "si e quajnë kafshën tuaj shtëpiake". Duke përdorur informacionin që është publikuar në profilin e Polit në rrjetin social, Niku ia del me lehtësi të piratojë llogaritë e Polit.

Të drejtat e personave

Operatorët e SNS-së duhet të respektojnë të drejtat e personave (shih Seksionin 6.1), duke përfshirë të drejtën për t'u informuar në lidhje me qëllimin e përpunimit dhe se sim und të përdoren të dhënat personale për qëllime marketingu të drejtpërdrejtë. Personave duhet t'u jepet gjithashtu e drejta e aksesit tek të dhënat personale që ata kanë gjeneruar në platformën e rrjetit social dhe të kërkojnë fshirjen e tyre. Edhe kur personat kanë dhënë pëlqimin për përpunimin e të dhënave personale dhe kanë ngarkuar informacione nëpërmjet internetit, ata duhet të kenë mundësinë të kërkojnë "të harrohen", nëse ata nuk dëshirojnë më të përdorin shërbimin e rrjetit social. E drejta për transferueshmërinë e të dhënave u mundëson gjithashtu përdoruesve të marrin një kopje të të dhënave personale që ata i kanë dhënë operatorëve të shërbimeve të rrjeteve sociale, në format të strukturuar, të përdorur gjerësisht dhe të lexueshëm nga pajisje automatike dhe t'i transferojë të dhënat e tij nga një operator rrjeti social tek një tjetër.[1025]

Kontrolluesit

Një çështje e vështirë që ngrihet shpesh në kontekstin e mediave sociale ka të bëjë me identifikimin e kontrolluesit, që do të thotë: cili është personi që ka detyrimin dhe përgjegjësinë për të zbatuar rregullat e mbrojtjes së të dhënave. Operatorët e shërbimit të rrjeteve sociale konsiderohen si kontrollues nga legjislacioni evropian i mbrojtjes së të dhënave. Kjo është e lehtë për t'u kuptuar nisur nga fakti se përkufizimi i "kontrolluesit" është i gjerë dhe gjithashtu pasi këta operatorë shërbimesh përcaktojnë qëllimin dhe mjetet për përpunimin e të dhënave personale që shkëmbehen nga personat. Sipas së drejtës së BE-së, nëse ata u ofrojnë shërbime subjekteve të të dhënave brenda BE-së, kontrolluesit janë të detyruar të zbatojnë dispozitat e Rregullores së Përgjithshme të Mbrojtjes së të Dhënave, edhe nëse ata nuk janë të vendosur në BE.

Megjithatë, a mund të konsiderohen edhe përdoruesit e shërbimeve të rrjeteve sociale si kontrollues? Kur personat përpunojnë të dhëna personale "në kuadrin e një aktiviteti thjesht personal, apo familjar", rregullat e mbrojtjes së të dhënave nuk zbatohen. Kjo njihet në të drejtën evropiane të mbrojtjes së të dhënave si "përjashtimi për aktivitetin familjar". Sidoqoftë, në disa raste, një përdorues i shërbimit të një rrjeti social mund të mos përfshihet në përjashtimin për aktivitetin familjar.

Përdoruesit i shkëmbejnë vullnetarisht informacionet e tyre personale në internet. Megjithatë, informacioni i shkëmbyer në internet shpesh përfshin informacione personale të personave të tjerë.

[BOX TYPE 2]

[1025] Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave, neni 20.

Shembull: Poli ka një llogari në një platformë rrjeti social tepër të famshëm. Poli po përpiqet të bëhet aktor, ndaj përdor llogarinë e tij për të publikuar fotografi, video dhe postime, me anë të të cilave bën të ditur pasionin e tij për artin. Fama është e rëndësishme për të ardhmen e tij, prandaj ai ka vendosur që profile i tij të mos jetë i disponueshëm vetëm për listën e të njohurve të tij të afërt, por për të gjithë përdoruesit e internetit, qofshin ata të regjistruar në rrjet, ose jo. A mund të publikojë Poli fotografi dhe video të tij me shoqen e tij Sara, pa pëlqimin e saj? Sara është mësuese në shkollë fillore dhe përpiqet ta mbajë jetën e saj private larg syve të punëdhënësit, nxënësve dhe prindërve të saj. Imagjinoni që Sara, e cila nuk përdor rrjetet sociale, zbulon nga miku i tyre i përbashkët, Niku, se një fotografi e saj në një festë me Polin, është postuar në internet. Në këtë rast, përpunimi i të dhënave nga ana e Polit, del jashtë fushës së zbatimit të së drejtës së BE-së, pasi përfshihet në "përjashtimin për aktivitetin familjar".

Gjithsesi, mbetet thelbësore që përdoruesit të ndërgjegjësohen dhe të jenë të vetdijshëm që ngarkimi i informacioneve që kanë të bëjnë me persona të tjerë, pa pëlqimin e tyre, mund të shkelë të drejtat e këtyre personave për privatësi dhe mbrojtje të të dhënave. Edhe kur gjen zbatim përjashtimi për aktivitetin familjar, për shembull nëse një përdorues ka një profil, i cili është publik vetëm për një listë kontaktesh të përzgjedhura nga vetë ai apo ajo, publikimi i informacioneve në lidhje me të tjerët, sërish mund ta ngarkojë me përgjegjësi përdoruesin. Paçka se rregullat e mbrojtjes së të dhënave nuk zbatohen, nëse aplikohet përjashtimi për aktivitetin familjar, përgjegjësia mund të burojë nga zbatimi i normave të tjera kombëtare, siç janë ato për shpifjen, apo prekjen e dinjitetit. Së fundmi, vetëm përdoruesit e rrjeteve sociale janë të mbrojtur nga përjashtimi për aktivitetin familjar: kontrolluesit dhe përpunuesit që ofrojnë mjetet për këtë lloj përpunimi privat, hyjnë në fushën e zbatimit të së drejtës së BE-së për mbrojtjen e të dhënave.[1026]

Nëse miratohet reforma e Direktivës mbi privatësinë dhe komunikimet elektronike, rrregullat në lidhje me mbrojtjen e të dhënave, privatësinë dhe sigurinë që zbatohen për operatorët e shërbimeve të telekomunikimit sipas kuadrit ligjor të tanishëm, do të gjejnë zbatim edhe për komunikimet midis pajisjeve elektronike dhe për shërbimet e komunikimeve elektronike, duke përfshirë për shembull shërbimet me akses të drejtpërdrejtë (*over-the-top*).

[1026] *Ibid*., paragrafi 18 i preambulës.

Lexime plotësuese

Kapitulli 1

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Vjenë, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C. 'Four fundamental rights: finding the balance', *International Data Privacy Law*, Vol. 6, nr. 3, fq. 195–209.

González Fuster, G. dhe Gellert, G. (2012), 'The fundamental right of data protection in the European Union: in search of an uncharted right', *International Review of Law, Computers and Technology*, Vol. 26 (1), fq. 73–82.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C. dhe Nouwt, S. (Eds.) (2009), *Reinventing Data Protection*, Springer.

Hijmans, H. (2016), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Springer.

Hustinx, P. (2016), 'EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation'.

Kranenborg, H. (2015), 'Google and the Right to be Forgotten', *European Data Protection Law Review*, Vol. 1, nr. 1, fq. 70–79.

Lynskey, O. (2014), 'Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order', *International and Comparative Law Quarterly*, Vol. 63, nr. 3, fq. 569–597.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Oksford, Oxford University Press.

Kokott, J. dhe Sobotta, C. (2013), 'The distinction between privacy and data protection in the case law of the CJEU and the ECtHR', *International Data Privacy Law*, Vol. 3, nr. 4, fq. 222–228.

EDRi, *An introduction to data protection*, Bruksel.

Frowein, J. dhe Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. and Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Munich, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. dhe Bates, E. (2009), *Law of the European Convention on Human Rights*, Oksford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Mynih, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oksford, Oxford University Press.

Nowak, M., Januszewski, K. and Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerp, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. and Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Bruksel, Emile Bruylant.

Simitis, S. (1997), 'Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?', *Neue Juristische Wochenschrift*, nr. 5, fq. 281–288.

Warren, S. dhe Brandeis, L. (1890), 'The right to privacy', *Harvard Law Review,* Vol. 4, nr. 5, fq. 193–220.

White, R. dhe Ovey, C. (2010), *The European Convention on Human Rights*, Oksford, Oxford University Press.

Kapitulli 2

Acquisty, A., dhe Gross R. (2009), 'Predicting Social Security numbers from public data', *Proceedings of the National Academy of Science*, 7 korrik 2009.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oksford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., dhe Blondel V. D. (2013), 'Unique in the Crowd: the Privacy Bounds of Human Mobility', *Nature Scientific Reports*, Vol. 3, 2013.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer.

Morgan, R. dhe Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, Londër, Sweet & Maxwell.

Ohm, P. (2010), 'Broken promises of privacy: Responding to the surprising failure of anonymization', *UCLA Law Review*, Vol. 57, nr. 6, fq. 1701–1777.

Samarati, P. dhe Sweeney, L. (1998), 'Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression', Raport Teknik SRI-CSL-98-04.

Sweeney, L. (2002), 'K-Anonymity: A Model for Protecting Privacy' *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, Vol. 10, nr. 5, fq. 557–570.

Tinnefeld, M., Buchner, B. dhe Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Mynih, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice*.

Kapitujt 3 deri 6

Brühann, U. (2012), 'Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr' in: Grabitz, E., Hilf, M. and Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Mynih, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Kadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrucken, Éditions universitaires européennes.

Curren, L. and Kaye, J. (2010), 'Revoking consent: a 'blind spot' in data protection law?', *Computer Law & Security Review*, Vol. 26, nr. 3, fq. 273–283.

Dammann, U. dhe Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. dhe Papakonstantinou, V. (2012), 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis', *Computers & Law Magazine of SCL*, Vol. 22, nr. 6, fq. 1–5.

De Hert, P. dhe Papakonstantinou, V. (2012), 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', *Computer Law & Security Review*, Vol. 28, nr. 2, fq. 130–142.

Feretti, Federico (2012), 'A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after the Lisbon treaty: Taking rights seriously', *European Review of Private Law*, Vol. 20, nr. 2, fq. 473–506.

FRA (European Union Agency for Fundamental Rights) (2010), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)*, Luksemburg, Publications Office of the European Union (Publications Office).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Conference edition), Vjenë, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luksemburg, Publications Office.

Irish Health Information and Quality Authority (2010), Guidance on Privacy Impact Assessment in Health and Social Care.

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I. dhe Saxby, S. (2011), '30 years on – The review of the Council of Europe Data Protection Convention 108', *Computer Law & Security Review*, Vol. 27, nr. 3, fq. 223–231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*.

Kapitulli 7

European Data Protection Supervisor (2014), Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies.

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. dhe Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, Oksford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oksford, Oxford University Press.

Article 29 Working Party (2005), *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*.

Kapitulli 8

Blasi Casagran, C. (2016) *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, Londër, Routledge.

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,* Berlin, Springer.

Europol (2012), *Data Protection at Europol*, Luksemburg, Publications Office.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Hagë, Eurojust.

De Hert, P. dhe Papakonstantinou, V. (2012), 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis', *Computers & Law Magazine of SCL*, Vol. 22, nr. 6, fq. 1–5.

Drewer, D. dhe Ellermann, J. (2012), 'Europol's data protection framework as an asset in the fight against cybercrime', *ERA Forum*, Vol. 13, nr. 3, fq. 381–395.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlin, Springer.

Gutwirth, S., Poullet, Y. dhe De Hert, P. (2010), *Data protection in a profiled world*, Dordreht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. dhe Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordreht, Springer.

Konstadinides, T. (2011), 'Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem', *European Law Review*, Vol. 36, nr. 5, fq. 722–776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of External Relations, CLEER Dokument pune 2013/2.

Kapitulli 9

Büllesbach, A., Gijrath, S., Poullet, Y. dhe Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. dhe Poullet, Y. (2012), *European data protection: In good health?*, Dordreht, Springer.

Gutwirth, S., Poullet, Y. dhe De Hert, P. (2010), *Data protection in a profiled world*, Dordreht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. dhe Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordreht, Springer.

Konstadinides, T. (2011), 'Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem', *European Law Review*, Vol. 36, nr. 5, fq. 722–776.

Rosemary, J. dhe Hamilton, A. (2012), *Data protection law and practice*, Londër, Sweet & Maxwell.

Kapitulli 10

El Emam, K. dhe Álvarez, C. (2015), 'A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques', *International Data Privacy Law*, Vol. 5, nr. 1, fq. 73–87.

Mayer-Schönberger, V. dhe Cate, F. (2013), 'Notice and consent in a world of Big Data', *International Data Privacy Law*, Vol. 3, nr. 2, fq. 67–73.

Rubistein, I. (2013), ‘Big Data: The End of Privacy or a New Beginning?’, *International Data Privacy Law*, Vol. 3, nr. 2, fq. 74–87.

Jurisprudencë

Jurisprudencë e përzgjedhur e Gjykatës Evropiane të së Drejtave të Njeriut

Aksesi tek të dhënat personale

Gaskin k. Mbretërisë së Bashkuar, nr. 10454/83, 7 korrik 1989

Godelli k. Italisë, nr. 33783/09, 25 shtator 2012

K.H. dhe të Tjerët k. Sllovakisë, nr. 32881/04, 28 prill 2009

Leander k. Suedisë, nr. 9248/81, 26 mars 1987

M.K. k. Francës, nr. 19522/09, 18 prill 2013

Odièvre k. Francës [ÇB], nr. 42326/98, 13 shkurt 2003

Ekuilibrimi i mbrojtjes së të dhënave me lirinë e shprehjes dhe me të drejtën e informimit

Axel Springer AG k. Gjermanisë [ÇB], No. 39954/08, 7 shkurt 2012

Bohlen k. Gjermanisë, nr. 53495/09, 19 shkurt 2015

Coudec dhe Hachette Filipacchi Associés k. Francës [ÇB], nr. 40454/07, 10 nëntor 2015

Magyar Helsinki Bizottság k. Hungarisë [ÇB], nr. 18030/11, 8 nëntor 2016

Müller dhe të Tjerët k. Zvicrës, nr. 10737/84, 24 maj 1988

Vereinigung bildender Künstler k. Austrisë, nr. 68354/01, 25 janar 2007

Von Hannover k. Gjermanisë (nr. 2) [ÇB], nr. 40660/08 dhe 60641/08, 7 shkurt 2012

Satakunnan Markkinapörssi Oy dhe Satamedia Oy k. Finlandës, nr. 931/13, 27 qershor 2017

Ekuilibrimi i mbrojtjes së të dhënave me lirinë e besimit fetar

Sinan Işık k. Turqisë, nr. 21924/05, 2 shkurt 2010

Sfidat e mbrojtjes së të dhënave në internet

K.U. k. Finlandës, nr. 2872/02, 2 dhjetor 2008

Pëlqimi i subjektit të të dhënave

Elberte k. Letonisë, nr. 61243/08, 13 janar 2015

Sinan Işık k. Turqisë, nr. 21924/05, 2 shkurt 2010

Y kv. Turqisë, nr. 648/10, 17 shkurt 2015

Korrespondenca

Amann k. Zvicrës [ÇB], nr. 27798/95, 16 shkurt 2000

Association for European Integration snd Human Rights dhe Ekimdzhiev k. Bullgarisë, nr. 62540/00, 28 qershor 2007

Bernh Larsen Holding AS dhe të Tjerët k. Norvegjisë, nr. 24117/08, 14 mars 2013

Cemalettin Canli k. Turqisë, nr. 22427/04, 18 nëntor 2008

D.L. k. Bullgarisë, nr. 7472/14, 19 maj 2016

Dalea k. Francës, nr. 964/07, 2 shkurt 2010

Gaskin k. Mbretërisë së Bashkuar, nr. 10454/83, 7 qershor 1989

Haralambie k. Rumanisë, nr. 21737/03, 27 tetor 2009

Khelili k. Zvicrës, nr. 16188/07, 18 tetor 2011

Leander k. Suedisë, nr. 9248/81, 26 mars 1987

Malone k. Mbretërisë së Bashkuar, nr. 8691/79, 2 gusht 1984

Rotaru k. Rumanisë [ÇB], nr. 28341/95, 4 maj 2000

S. dhe Marper k. Mbretërisë së Bashkuar [ÇB], nr. 30562/04 dhe 30566/04, 4 dhjetor 2008

Shimovolos k. Rusisë, nr. 30194/09, 21 qershor 2011

Silver dhe të Tjerët k. Mbretërisë së Bashkuar, nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 mars 1983

The Sunday Times k. Mbretërisë së Bashkuar, nr. 6538/74, 26 prill 1979

Bazat e të dhënave të dosjeve penale

Aycaguer k. Francës, nr. 8806/12, 22 qershor 2017

B.B. k. Francës, nr. 5335/06, 17 dhjetor 2009

Brunet k. Francës, nr. 21010/10, 18 shtator 2014

M.K. k. Francës, nr. 19522/09, 18 prill 2013

M.M. k. Mbretërisë së Bashkuar, nr. 24029/07, 13 nëntor 2012

Siguria e të dhënave

Haralambie k. Rumanisë, nr. 21737/03, 27 tetor 2009

K.H. dhe të Tjerët k. Sllovakisë, nr. 32881/04, 28 prill 2009

Bazat e të dhënave të ADN-së

S. dhe Marper k. Mbretërisë së Bashkuar [ÇB], nr. 30562/04 dhe 30566/04, 4 dhjetor 2008

Të dhënat e GPS-së

Uzun k. Gjermanisë, nr. 35623/05, 2 shtator 2010

Të dhënat e shëndetit

Avilkina dhe të Tjerët k. Rusisë, nr. 1585/09, 6 qershor 2013

Biriuk k. Lituanisë, nr. 23373/03, 25 nëntor 2008

I k. Finlandës, nr. 20511/03, 17 korrik 2008

L.H. k. Letonisë, nr. 52019/07, 29 prill 2014

L.L. k. Francës, nr. 7508/02, 10 tetor 2006

M.S. k. Suedisë, nr. 20837/92, 27 gusht 1997

Szuluk k. Mbretërisë së Bashkuar, nr. 36936/05, 2 qershor 2009

Y k. Turqisë, nr. 648/10, 17 shkurt 2015

Z k. Finlandës, nr. 22009/93, 25 shkurt 1997

Identiteti

Ciubotaru k. Moldavisë, nr. 27138/04, 27 prill 2010

Godelli k. Italisë, nr. 33783/09, 25 shtator 2012

Odièvre k. Francës [ÇB], nr. 42326/98, 13 shkurt 2003

Informacioni që lidhet me veprimtaritë personale

G.S.B. k. Zvicrës, nr. 28601/11, 22 dhjetor 2015

M.N. dhe të Tjerët k. San Marinos, nr. 28005/12, 7 korrik 2015

Michaud k. Francës, nr. 12323/11, 6 dhjetor 2012

Niemietz k. Gjermanisë, nr. 13710/88, 16 dhjetor 1992

Përgjimi i komunikimeve

Amann k. Zvicrës [ÇB], nr. 27798/95, 16 shkurt 2000

Brito Ferrinho Bexiga Villa-Nova k. Portugalisë, nr. 69436/10, 1 dhjetor 2015

Copland k. Mbretërisë së Bashkuar, nr. 62617/00, 3 prill 2007

Halford k. Mbretërisë së Bashkuar, nr. 20605/92, 25 qershor 1997

Iordachi dhe të Tjerët k. Moldavisë, nr. 25198/02, 10 shkurt 2009

Kopp k. Zvicrës, nr. 23224/94, 25 mars 1998

Liberty dhe të Tjerët k. Mbretërisë së Bashkuar, nr. 58243/00, 1 korrik 2008

Malone k. Mbretërisë së Bashkuar, nr. 8691/79, 2 gusht 1984

Mustafa Sezgin Tanrıkulu k. Turqisë, nr. 27473/06, 18 korrik 2017
Pruteanu k. Rumanisë, nr. 30181/05, 3 shkurt 2015
Szuluk k. Mbretërisë së Bashkuar, nr. 36936/05, 2 qershor 2009

Detyrimet për titullarët e të drejtave

B.B. k. Francës, nr. 5335/06, 17 dhjetor 2009
I k. Finlandës, nr. 20511/03, 17 korrik 2008
Mosley k. Mbretërisë së Bashkuar, nr. 48009/08, 10 maj 2011

Të dhënat personale

Amann k. Zvicrës [ÇB], nr. 27798/95, 16 shkurt 2000
Uzun k. Gjermanisë, nr. 35623/05, 2010
Bernh Larsen Holding AS dhe të Tjerët k. Norvegjisë, nr. 24117/08, 14 mars 2013

Fotografitë

Sciacca k. Italisë, nr. 50774/99, 11 janar 2005
Von Hannover k. Gjermanisë, nr. 59320/00, 24 qershor 2004

E drejta për t'u harruar

Segerstedt-Wiberg dhe të Tjerët k. Suedisë, nr. 62332/00, 6 qershor 2006
Satakunnan Markkinapörssi Oy dhe Satamedia Oy k. Finlandës, nr. 931/13, 27 qershor 2017

E drejta për të kundërshtuar

Leander k. Suedisë, nr. 9248/81, 26 mars 1987
M.S. k. Suedisë, nr. 20837/92, 27 gusht 1997
Mosley k. Mbretërisë së Bashkuar, nr. 48009/08, 10 maj 2011
Rotaru k. Rumanisë [ÇB], nr. 28341/95, 4 maj 2000
Sinan Işık k. Turqisë, nr. 21924/05, 2 shkurt 2010

Kategoritë sensitive të të dhënave

Brunet k. Francës, nr. 21010/10, 18 shtator 2014
I k. Finlandës, nr. 20511/03, 17 korrik 2008
Michaud k. Francës, nr. 12323/11, 6 dhjetor 2012
S. dhe Marper k. Mbretërisë së Bashkuar [ÇB], nr. 30562/04 dhe 30566/04, 4 dhjetor 2008

Mbikëqyrja dhe zbatimi i ligjit (roli i aktorëve të ndryshëm, përfshirë autoritetet mbikëqyrëse)

I k. Finlandës, nr. 20511/03, 17 korrik 2008

K.U. k. Finlandës, nr. 2872/02, 2 dhjetor 2008

Von Hannover k. Gjermanisë, nr. 59320/00, 24 qershor 2004

Von Hannover k. Gjermanisë (nr. 2) [ÇB], nr. 40660/08 dhe 60641/08, 7 shkurt 2012

Metodat e mbikëqyrjes

Allan k. Mbretërisë së Bashkuar, nr. 48539/99, 5 nëntor 2002

Association for European Integration and Human Rights dhe Ekimdzhiev k. Bullgarisë, nr. 62540/00, 28 qershor 2007

Bărbulescu k. Rumanisë [ÇB], nr. 61496/08, 5 shtator 2017

D.L. k. Bullgarisë, nr. 7472/14, 19 maj 2016

Dragojević k. Kroacisë, nr. 68955/11, 15 janar 2015

Karabeyoğlu k. Turqisë, nr. 30083/10, 7 qershor 2016

Klass dhe të Tjerët k. Gjermanisë, nr. 5029/71, 6 shtator 1978

Rotaru k. Rumanisë [ÇB], nr. 28341/95, 4 maj 2000

Szabó dhe Vissy k. Hungarisë, nr. 37138/14, 12 janar 2016

Taylor-Sabori k. Mbretërisë së Bashkuar, nr. 47114/99, 22 tetor 2002

Uzun k. Gjermanisë, nr. 35623/05, 2 shtator 2010

Versini-Campinchi dhe Crasnianski k. Francës, nr. 49176/11, 16 qershor 2016

Vetter k. Francës, nr. 59842/00, 31 maj 2005

Vukota-Bojić k. Zvicrës, nr. 61838/10, 18 tetor 2016

Roman Zakharov k. Rusisë [ÇB], nr. 47143/06, 4 dhjetor 2015

Video-përgjimi

Köpke k. Gjermanisë, nr. 420/07, 5 tetor 2010

Peck k. Mbretërisë së Bashkuar, nr. 44647/98, 28 janar 2003

Kampionët vokalë

Wisse k. Francës, nr. 71611/01, 20 dhjetor 2005

P.G. dhe J.H. k. Mbretërisë Bashkuar, nr. 44787/98, 25 shtator 2001

Jurisprudencë e përzgjedhur e Gjykatës së Drejtësisë së Bashkimit Evropian

Jurisprudencë në lidhje me Direktivën e Mbrojtjes së të Dhënave

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde k. Rīgas pašvaldības SIA 'Rīgas satiksme'*, 4 maj 2017
[Parimi i përpunimit të ligjshëm: interesi legjitim që ndiqet nga një palë e tretë]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce k. Salvatore Manni*, 9 mars 2017

[E drejta për fshirje të të dhënave personale; e drejta për të kundërshtuar përpunimin]

Çështje të bashkuara C-203/15 dhe C-698/15, *Tele2 Sverige AB k. Post- och telestyrelsen* dhe *Secretary of State for the Home Department k. Tom Watson dhe të Tjerët* [ÇB], 21 dhjetor 2016

[Konfidencialiteti i komunikimeve elektronike; operatorët e shërbimeve të komunikimeve elektronike; detyrimi në lidhje me mbajtjen e përgjithshme dhe pa dallim të të dhënave të trafikut dhe të vendndodhjes; mungesë shqyrtimi paraprak nga një gjykatë, apo autoritet administrativ i pavarur; Karta e të Drejtave Themelore të Bashkimit Evropian; pajtueshmëria me të drejtën e BE-së]

C-582/14, *Patrick Breyer k. Bundesrepublik Deutschland*, 19 tetor 2016
[Përkufizimi i 'të dhënave personale'; adresat e protokollit të internetit (IP); mbajtja e të dhënave nga një operator i shërbimeve të medias në internet; legjislacioni kombëtar që nuk lejon të merret parasysh interesi legjitim që ndjek kontrolluesi]

C-362/14, *Maximilian Schrems k. Data Protection Commissioner* [ÇB], 6 tetor 2015
[Parimi i përpunimit të ligjshëm; të drejtat themelore; pavlefshmëria e Vendimit të Portit të Sigurt; kompetencat e autoriteteve mbikëqyrëse të pavarura]

C-230/14, *Weltimmo s. r. o. k. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 tetor 2015
[Kompetencat e autoriteteve mbikëqyrëse kombëtare]

C-201/14, *Smaranda Bara dhe të Tjerët k. Casa Naţională de Asigurări de Sănătate dhe të Tjerët*, 1 tetor 2015
[E drejta për t'u informuar në lidhje me përpunimin e të dhënave personale]

C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 11 December 2014
[Koncepti i "përpunimit të të dhënave" dhe ai i "kontrolluesit"]

C-473/12, *Institut professionnel des agents immobiliers (IPI) k. Geoffrey Englebert dhe të Tjerët*, 7 nëntor 2013
[E drejta për t'u informuar në lidhje me përpunimin e të dhënave personale]

T-462/12 R, *Pilkington Group Ltd k. Komisionit Evropian*, Urdhër i Presidentit të Gjykatës së Përgjithshme, 11 mars 2013

C-342/12, *Worten – Equipamentos para o Lar SA k. Autoridade para as Condições de Trabalho (ACT)*, 30 maj 2013
[Koncepti i 'të dhënave personale'; regjistrimi i orëve të punës; parimet që kanë të bëjnë me cilësinë e të dhënave dhe kriteret që legjitimojnë përpunimin e të dhënave; aksesi nga autoriteti kombëtar kompetent për monitorimin e kushteve të punës; detyrimi i punëdhënësit për të vënë në dispozicion regjistrin e orëve të punës, për të mundësuar që të konsultohet në mënyrë të menjëhershme]

Çështje tw bashkuara C-293/12 dhe C-594/12, *Digital Rights Ireland Ltd k. Minister for Communications, Marine and Natural Resources dhe të Tjerët* dhe *Kärntner Landesregierung dhe të Tjerët* [ÇB], 8 prill 2014

[Shkelja e legjislacionit parësor të BE-së nga Direktiva e Mbajtjes së të Dhënave; përpunimi i ligjshëm; kufizimi i qëllimit dhe mbajtjes]

C-288/12, *Komisioni Evropian k. Hungarisë* [ÇB], 8 prill 2014

[Legjitimiteti i shkarkimit nga detyra të mbikëqyrësit kombëtar të mbrojtjes së të dhënave]

Çështje të bashkuara C-141/12 dhe C-372/12, *YS k. Minister voor Immigratie, Integratie en Asiel* dhe *Minister voor Immigratie, Integratie en Asiel k. M dhe S*, 17 korrik 2014

[Fusha e zbatimit të së drejtës për akses të subjektit të të dhënave; mbrojtja e personave në lidhje me përpunimin e të dhënave personale; koncepti i 'të dhënave personale'; të dhëna që kanë të bëjnë me kërkuesin e një leje qëndrimi dhe analiza ligjore që përmban një dokument administrativ përgatitor i vendimit; Karta e të Drejtave Themelore të Bashkimit Evropian]

C-131/12, *Google Spain SL, Google Inc. k. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [ÇB], 13 maj 2014

[Detyrimet e operatorëve të motorëve të kërkimit që të mos shfaqin të dhëna personale tek rezultatet e kërkimit, me kërkesë të subjektit të të dhënave; zbatueshmëria e Direktivës së Mbrojtjes së të Dhënave; koncepti i "përpunimit të të dhënave"; kuptimi i "kontrolluesve"; ekuilibrimi i mbrojtjes së të dhënave me lirinë e shprehjes; e drejta për t'u harruar]

C-614/10, *Komisioni Evropian k. Republikës së Austrisë* [ÇB], 16 tetor 2012

[Pavarësia e autoritetit kombëtar mbikëqyrës]

Çështje të bashkuara C-468/10 dhe C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) dhe Federación de Comercio Electrónico y Marketing Directo (FECEMD) k. Administración del Estado*, 24 nëntor 2011

[Zbatimi i saktë i nenit 7, gërma (f) të Direktivës së Mbrojtjes së të Dhënave – "interesat legjitime të të tjerëve" – në legjislacionin kombëtar]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) k. Netlog NV*, 16 shkurt 2012

[Detyrimi i operatorëve të rrjeteve sociale për të parandaluar përdorimin e paligjshëm të punimeve muzikore dhe audio-vizive nga përdoruesit e rrjeteve]

C-70/10, *Scarlet Extended SA k. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 nëntor 2011

[Shoqëria e informacionit; e drejta e autorit; interneti; programet kompjuterike 'peer-to-peer'; operatorët e shërbimeve të internetit; instalimi i një sistemi filtrimi të komunikimeve elektronike për të parandaluar shkëmbimin e skedarëve që shkelin të drejtën e autorit; mungesa e një detyrimi të përgjithshëm për të monitoruar informacionin e transmetuar]

C-543/09, *Deutsche Telekom AG k. Bundesrepublik Deutschland*, 5 maj 2011

[Domosdoshmëria e ripërtëritjes së pëlqimit]

Çështje të bashkuara C-92/09 dhe C-93/09, *Volker und Markus Schecke GbR dhe Hartmut Eifert k. Land Hessen* [ÇB], 9 nëntor 2010

[Koncepti i të "dhënave personale"; proporcionaliteti i detyrimit ligjor për publikimin e të dhënave personale të përfituesve të disa fondeve bujqësore të BE-së]

C-553/07, *College van burgemeester en wethouders van Rotterdam k. M. E. E. Rijkeboer*, 7 maj 2009

[E drejta e subjektit të të dhënave për akses]

C-518/07, *Komisioni Evropian k. Republikës Federale të Gjermanisë* [ÇB], 9 mars 2010

[Pavarësia e autoritetit mbikëqyrës kombëtar]

C-73/07, *Tietosuojavaltuutettu k. Satakunnan Markkinapörssi Oy dhe Satamedia Oy* [ÇB], 16 dhjetor 2008

[Koncepti i 'veprimtarisë gazetareske' në kuptim të nenit 9 të Direktivës së Mbrojtjes së të Dhënave]

C-524/06, *Heinz Huber k. Bundesrepublik Deutschland* [ÇB], 16 dhjetor 2008
[Legjitimiteti i mbajtjes së të dhënave në lidhje me të huajt në regjistrin e statistikave]

C-275/06, *Productores de Música de España (Promusicae) k. Telefónica de España SAU* [ÇB], 29 janar 2008
[Koncepti i "të dhënave personale"; detyrimi i operatorëve të aksesit në internet për të komunikuar identitetin e përdoruesve të programit të shkëmbimit të skedarëve KaZaA, shoqatës për mbrojtjen e pronësisë intelektuale]

C-101/01, *Criminal proceedings kundër Bodil Lindqvist*, 6 nëntor 2003
[Kategoritë e veçanta të të dhënave personale]

Çështje të Bashkuara C-465/00, C-138/01 and C-139/01, *Rechnungshof k. Österreichischer Rundfunk dhe të Tjerët* dhe *Christa Neukomm dhe Jospeh Lauermann k. Österreichischer Rundfunk*, 20 maj 2003
[Proporcionaliteti i detyrimit ligjor për të publikuar të dhënat personale në lidhje me pagat e punonjësve të disa kategorive të caktuara të institucioneve përkatëse të sektorit publik]

C-434/16, *Peter Nowak k. Data Protection Commissioner*, Opinion i Avokatit të Përgjithshëm Kokott, 20 korrik 2017

[Koncepti i të dhënave personale; aksesi tek teza vetjake e provimit; korrigjimet e bëra nga personi që kontrollon provimin]

C-291/12, *Michael Schwarz k. Stadt Bochum*, 17 tetor 2013

[Kërkesë për një vendim paragjyqësor; fusha e lirisë, sigurisë dhe drejtësisë; pasaporta biometrike; gjurmët e gishtave; baza ligjore; proporcionaliteti]

Jurisprudencë në lidhje me Direktivën 2016/681

Opinioni 1/15 i Gjykatës (Dhoma e Madhe), 26 korrik 2017
[Baza ligjore; projekt-marrëveshje midis Kanadasë dhe Bashkimit Evropian mbi transferimin dhe përpunimin të të dhënave të Regjistrit të Emrave të Pasagjerëve; pajtueshmëria e projekt-marrëveshjes me nenin 16 TFBE dhe nenet 7 dhe 8 dhe nenin 52, pika 1 të Kartës së të Drejtave Themelore të Bashkimit Evropian]

Jurisprudencë në lidhje me Rregulloren e Mbrojtjes së të Dhënave të Institucioneve të BE-së

C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) k. European Food Safety Authority (EFSA), Komisioni Evropian,* 16 korrik 2015
[Aksesi në dokumente]

C-28/08 P, *Komisioni Evropian k. The Bavarian Lager Co. Ltd.* [ÇB], 29 qershor 2010
[Aksesi në dokumente]

Jurisprudencë në lidhje me Direktivën 2002/58/KE

C-536/15, *Tele2 (Netherlands) BV dhe të Tjetrët k. Autoriteit Consument en Markt (AMC)*, 15 mars 2017

[Parimi i mosdiskriminimit; vënia në dispozicion e të dhënave personale që kanë të bëjnë me abonentët, për qëllime të ofrimit të shërbimeve të informacionit telefonik të aksesueshme nga publiku dhe të numratorëve; pëlqimi i abonentëve; jepet dallimi sipas Shtetit Anëtar, në të cilin janë të aksesueshme shërbimet e informacionit telefonik të aksesueshme nga publiku dhe të numratorëve]

Çështje të bashkuara C-203/15 and C-698/15, *Tele2 Sverige AB k. Post- och telestryrelsen* dhe *Secretary of State for the Home Department k. Tom Watson dhe të Tjerët* [ÇB], 21 dhjetor 2016

[Konfidencialiteti i komunikimeve elektronike; operatorët e shërbimeve të komunikimeve elektronike; detyrimi në lidhje me mbajtjen e përgjithshme dhe pa dallim të të dhënave të trafikut dhe të vendndodhjes; mungesë shqyrtimi paraprak nga një gjykatë, apo autoritet i pavarur administrativ; Karta e të Drejtave Themelore të Bashkimit Evropian; pajtueshmëria me të drejtën e BE-së]

C-70/10, *Scarlet Extended SA k. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 nëntor 2011

[Shoqëria e informacionit; e drejta e autorit; interneti; programet kompjuterike 'peer-to-peer'; operatorët e shërbimit të internetit; instalimi i një sistemi të filtrimit të komunikimeve elektronike për të penguar shkëmbimin e skedarëve që shkelin të drejtën e autorit; mungesë detyrimi të përgjithshëm për monitorimin e informacioneve të transmetuara]

C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB k. Perfect Communication Sweden AB*, 19 prill 2012

[E drejta e autorit dhe të drejta që lidhen me të; përpunimi i të dhënave nga interneti; shkelja e një të drejtë ekskluzive; audio-librat e vënë në dispozicion me anë të një serveri FTP, nëpërmjet internetit nga një adresë IP, të caktuar nga një operator shërbimi interneti; urdhëresë për një operator shërbimi internet, ku i kërkohet të japë emrin dhe adresën e përdoruesit të adresës IP]

Shumë informacion në lidhje me Agjencinë e Bashkimit Evropian për të Drejtat Themelore genden në faqen zyrtare në internet të FRA-së, në adresën fra.europa.eu.

Më shumë informacion mbi jurisprudencën e Gjykatës Evropian të së Drejtave të Njeriut gjendet në faqen zyrtare të Gjykatës: echr.coe.int. Portali i kërkimit HUDOC ofron akses në çështjet e gjykuara dhe vendimet në gjuhën angleze dhe/ose frënge, përkthimet në gjuhë të tjera, përmbledhje ligjore, njoftime për shtyp dhe informacione të tjera në lidhje me punën e Gjykatës.

Si të përfitoni botime të Këshillit të Evropës

Botimet e Këshillit të Evropës publikojnë punime në të gjitha sferat e veprimtarië së Organizatës, përfshirë të drejtat e njeriut, shkenca jkuridike, shëndeti, etika, çështjet shoqërore, mjedisi, arsimii, kultura, sportet, rinia dhe trashëgimia arkitekturore. Librat dhe botimet elektronike nga katalogu i përmasave të mëdha mund të porositen në internet (http://book.coe.int/).

Një dhomë virtuale leximi i mundëson përdoruesve të shohin ekstrakte të punimeve kryesore të sapo botuara, ose tekste të plota të disa dokumenteve zyrtare pa pagesë.

Informacione si edhe teksti i plotë i Konventave të Këshillit të Evropës mund të gjendet në faqen zyrtare në internet të Zyrës së Traktateve: http://conventions.coe.int/.

Zhvillimi i shpejtë i teknologjive të informacionit thekson domosdoshmërinë për mbrojtje më rigoroze të të dhënave personale, e drejtë e cila garantohet si nga instrumentet e Bashkimit Evropian (BE), ashtu edhe nga ato të Këshillit të Evropës (KiE). Mbrojtja e kësaj të drejte të rëndësishme përballet me sfida të reja dhe domethënëse, pasi zhvillimet teknologjike zgjerojnë kufijtë e fushave të ndryshme, sikurse të mbikëqyrjes, përgjimit të komunikimeve dhe arkivimit të të dhënave. Ky manual është konceptuar në mënyrë të tillë që t'u mundësojë juristëve që nuk janë të specializuar për mbrojtjen e të dhënave të marrin njohuri për këtë fushë të re të së drejtës. Manuali ofron gjithashtu një vështrim të përgjithshëm të kuadrit ligjor përkatës të BE-së dhe të KiE-së dhe shpjegon jurisprudencën themelore, duke përmbledhur vendimet e Gjykatës së Drejtësisë së Bashkimit Evropian dhe Gjykatës Evropiane të së Drejtave të Njeriut. Gjithashtu, ai paraqet edhe shembuj praktikë, mbështetur në situata të hamendësuara, në lidhje me problemet e ndryshme që shfaqen në këtë fushë në zhvillim të vazhdueshëm.

AGJENCIA E BASHKIMIT EVROPIAN PËR TË DREJTAT THEMELORE

Schwarzenbergplatz 11 - 1040 Vjenë - Austri

Tel. +43 (1) 580 30-0 - Fax +43 (1) 580 30-699

fra.europa.eu - info@fra.europa.eu - @EURightsAgency

GJYKATA EVROPIANE E TË DREJTAVE TË NJERIUT

KËSHILLI I EVROPËS

67075 Strasburg Cedex - Francë

Tel. +33 (0) 3 88 41 20 18 - Fax +33 (0) 3 88 41 27 30

echr.coe.int - publishing@echr.coe.int - @ECHRPublication

MBIKËQYRËSI EVROPIAN I MBROJTJES SË TË DHËNAVE

Rue Wiertz 60 – 1047 Bruksel – Belgjikë

Tel. +32 2 283 19 00

www.edps.europa.eu – edps@edps.europa.eu – logo@EU_EDPS