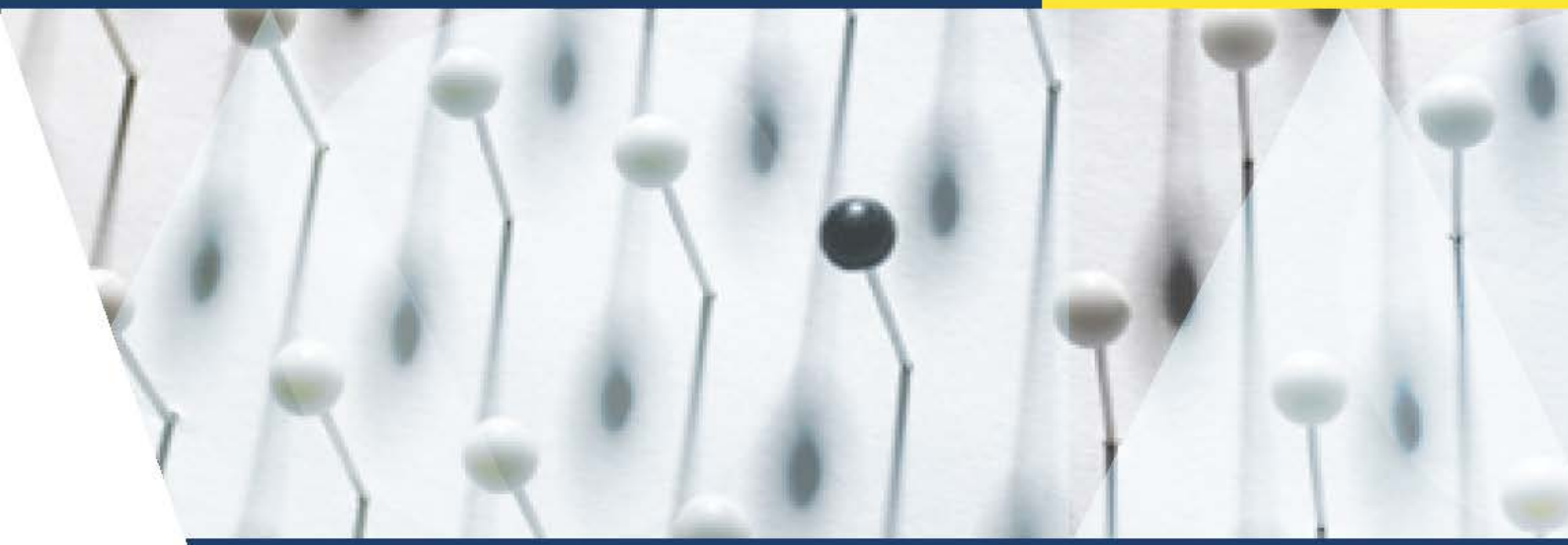
MANUAL



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

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

Dorëshkrimi i këtij Manuali u përfundua në prill të 2014-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.

Europe Direct është një shërbim që ju ndihmon të gjeni përgjigje për pyetjet që keni në lidhje me Bashkimin Evropian

Numri i telefonit pa pagesë (*)

00 800 67 89 10 11

(*) informacioni që ju jepet është pa pagesë, ashtu siç janë në përgjithësi edhe telefonatat (përveç disa operatorëve, kabinave telefonike ose hoteleve).

Fotografitë (kopertina dhe në brendësi): © iStockphoto

Më shumë informacion mbi Bashkimin Evropian mund të gjendet në internet (http://europa.eu).

Luksemburg: Zyra e publikimeve të Bashkimit Evropian, 2014

ISBN 978-92-871-9954-6 (CoE)

ISBN 978-92-9239-332-8 (FRA)

doi: 10.2811/53800

Printuar në Luksemburg

Printuar në letër të ricikluar pa përmbajtje klori (PCF)

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

Parathënie

Ky manual i së drejtës evropiane në fushën e mbrojtjes së të dhënave u përgatit bashkërisht me Agjencinë e së Drejtave Themelore të Bashkimit Evropian (ADTH) dhe Këshillin e Evropës, së bashku me Zyrën e Kancelarit të Gjykatës Evropiane të së Drejtave të Njeriut. Bëhet fjalë për manualin e tretë të një serie manualesh juridikë, të përgatitur bashkërisht nga ADTH-ja dhe Këshilli i Evropës. Në mars 2011, u publikua manuali i parë i së drejtës evropiane në fushën e mos-diskriminimit dhe në qershor 2013, u publikua një manuali i dytë, mbi të drejtën evropiane në fushën e azilit, kufijve dhe emigracionit.

Ne vendosëm të vazhdonim bashkëpunimin tonë me një subjekt tepër aktual, i cili na prek të gjithëve çdo ditë, domethënë mbrojtja e të dhënave personale. Evropa disponon një nga sistemet më proteksionist në këtë sferë, i cili mbështetet në Konventën 108 të Këshillit të Evropës, instrumentet e Bashkimit Evropian (BE), ashtu si edhe në jurisprudencën e Gjykatës Evropiane të së Drejtave të Njeriut (GjEDNj) dhe të Gjykatës së Drejtësisë së Bashkimit Evropian (GjDBE).

Synimi i këtij manuali është të rrisë ndërgjegjësimin dhe të përmirësojë njohuritë në lidhje me rregullat e mbrojtjes së të dhënave në shtetet anëtare të Bashkimit Evropian dhe të Këshillit të Evropës, duke shërbyer si një pikë kryesore referimi tek i cili mund të mbështeten lexuesit. Ky manual është konceptuar për juristët që nuk janë specialistë të fushës, gjyqtarët, autoritetet kombëtare të mbrojtjes së të dhënave dhe për persona të tjerë, të cilët punojnë në fushën e mbrojtjes së të dhënave.

Me hyrjen në fuqi të Traktatit të Lisbonës, në dhjetor të 2009-ës, Karta e të Drejtave Themelore të BE-së mori forcë ligjore dhe së bashku me të edhe e drejta për mbrojtje të së dhënave personale mori statusin e e një të drejte themelore më vete. Që të mbrohet kjo e drejtë themelore, është thelbësore të kuptohet më mirë Konventa 108 e Këshillit të Evropës dhe instrumentet e BE-së, të cilat hapën rrugën për mbrojtjen e të dhënave në Evropës, ashtu si edhe jurisprudenca e GjDBE-së dhe GjEDNj-së.

Do të dëshironim të falënderonim Institutin për të Drejtat e Njeriut Ludwig Boltzmann për kontributin e tij në hartimin e këtij manuali. Do të dëshironim gjithashtu të shprehnim mirënjohjen tonë për zyrën e Mbikëqyrësit Evropian të Mbrojtjes së të Dhënave për kontributin e saj gjatë fazës së hartimit. Falënderojmë veçanërisht njësinë e mbrojtjes së të dhënave të Komisionit Evropian, për mbështetjen e saj gjatë përgatitjes së këtij manuali.

Philippe Boillat

Drejtor i Përgjithshëm i të Drejtave të Njeriut
Dhe Sundimit të Ligjit të Këshillit të Evropës

Morten Kjaerum

Drejtor i Agjencisë për të Drejtat
Themelore të Bashkimit Evropian

Përmbajtja

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 Schengen

DUDNj Deklarata Universale e të Drejtave të Njeriut

EDPS Mbikëqyrësi Evropian i të Dhënave Personale

EFTA Shoqata evropiane e shkëmbimeve të lira

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

ENISA Agjencia Evropiane për Sigurinë e Rrjeteve dhe të informacionit

ENU Njësi kombëtare Europol-i

ESMA Autoriteti evropian i tregjeve financiare

eTEN Rrjetet Trans-evropiane të telekomunikacioneve

EuroPriSe Certifikimi Evropian i Mbrojtjes së të Dhënave

FRA Agjencia për të Drejtat Themelore të Bashkimit Evropian

GPS Sistem global lokalizimi

GjDBE Gjykata e Drejtësisë së Bashkimit Evropian (përpara dhjetorit 2009, Gjykata e Drejtësisë së Komunitetit Evropian, GjDKE)

GjEDNj Gjykata Evropiane e të Drejtave të Njeriut

HEE Hapësira Ekonomike Evropiane

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 nga përpunimi automatik i të dhënave personale (Këshilli i Evropës)

LTKiE Lista e traktateve të Këshillit të Evropës

MMK Menaxhimi i marrëdhënieve me klientët

MEA Mandat Evropian Arresti

N-SIS Sistem Kombëtar Informacioni Schengen

OECD Organizata për Bashkëpunim dhe Zhvillim Ekonomik

OJQ Organizatë jo-qeveritare

OKB Organizata e Kombeve të Bashkuara

PIN Numër identifikimi personal

PNR Të dhënat e pasagjerëve

SEPA Zona e Unifikuar e Pagesave në Euro

SID Sistem Informacioni Doganor

SIS Sistem Informacioni Schengen

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 ofron një panoramë të legjislacionit që zbatohet për mbrojtjen e të dhënave sa i përket Bashkimit Evropian (BE) dhe Këshillit të 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 juristë të tjerë, ashtu si edhe ata të cilët punojnë për organizma të tjerë, përfshirë edhe 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 kryesore referimi, si për të drejtën në fushën e mbrojtjes së të dhënave të BE-së, ashtu edhe të Konventës Evropiane të së Drejtave të Njeriut (KEDNj) dhe shpjegon se si rregullohet kjo fushë qoftë sipas legjislacionit të BE-së dhe atij të KEDNj-së, ashtu edhe të Konventës së KiE-së për Mbrojtjen e Personave nga Përpunimi Automatik i të Dhënave Personale (Konventa 108) dhe të instrumenteve të tjera ligjore të KiE-së. Secili kapitull, paraqet fillimisht një tabelë që përmbledh dispozitat ligjore në fuqi, përfshirë një përzgjedhje të rëndësishme, duke iu referuar jurisprudencës së të dy sistemeve juridike evropiane veç e veç. Më pas, paraqiten ligjet përkatëse, njëri pas tjetrit, për të treguar se si zbatohen për çdo çështje, me qëllim që lexuesi të kuptojë se ku përputhen e ku dallojnë të dy sistemet.

Tabelat në krye të secilit kapitull, rendisin tematikat e trajtuara në atë kapitull dhe citojnë dispozitat ligjore në fuqi dhe materiale të tjera të rëndësishme, sikurse jurisprudencën përkatëse. Rendi i tematikave mund të ndryshojë disi nga struktura e tekstit në kapitull, në rastet kur është parë e nevojshme për të prezantuar sa më saktë përmbajtjen e kapitullit. Tabelat mbulojnë si të drejtën e KiE-së ashtu edhe atë të BE-së, çka ndihmon lexuesit të gjejnë informacione thelbësore qa kanë lidhje me rastin e tyre specifik, sidomos kur janë subjekte vetëm të së drejtës së KiE-së.

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 kenë qasje në informacionin që i përket vendeve të tyre, duke vizituar drejtpërdrejt rubrikat e KiE-së. Juristët nga Shtetet Anëtare të BE-së duhet të përdorin të dyja rubrikat, duke qenë se këto shtete u nënshtrohen të dy rendeve juridike. 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.

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 të GjEDNj-së në lidhje me problematika të mbrojtjes së të dhënave.

E drejta e BE-së mbështetet në masa legjislative, në dispozitat përkatëse të traktateve dhe të Kartës së të Drejtave Themelore të Bashkimit Evropian, ashtu sikurse janë interpretuar nga jurisprudenca e Gjykatës së Drejtësisë së Bashkimit Evropian (GjDBE, ose siç njihej përpara 2009-ës, Gjykata Evropiane e Drejtësisë (GjED)).

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.

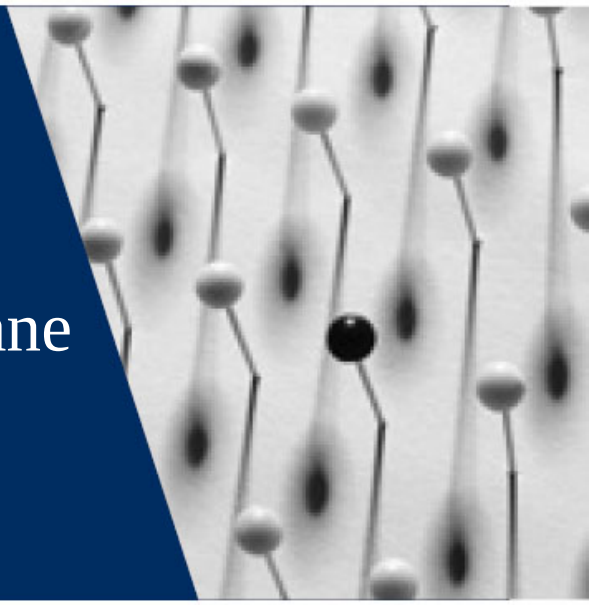
Gjithashtu, janë paraqitur shembuj konkretë dhe skenarë hipotetikë, brenda kutive me sfond blu, të cilat kanë për qëllim të ilustrojnë zbatimin në praktikë të rregullave evropiane në fushën e mbrojtjes së të dhënave, veçanërisht kur nuk ekziston jurisprudencë specifike të GjEDNj-së apo të GjDBE-së. Kutitë e tjera me sfond gri paraqesin shembuj të marrë nga burime të tjera, që s'janë as jurisprudenca e as legjislacioni.

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;
- Të drejtat e subjekteve të të dhënave dhe zbatimi i tyre;
- Qarkullimet ndërkufitare të të dhënave;
- Mbrojtja e të dhënave në kontekstin e policisë dhe drejtësisë penale;
- Ligje të tjera evropiane specifike në fushën e mbrojtjes së të dhënave.

1

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



BE	Çështje të trajtuara	KiE
E drejta për mbrojtje të të dhënave		
Direktiva 95/46/CE në lidhje me 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), OJ 1995 L281		GjEDNj, Neni 8 (e drejta për respektim të jetë private the familjare, të banesës dhe të korrespondencës) Konventa për mbrojtjen e personave nga përpunimi automatik i të dhënave personale (Konventa 108)
Ekuilibrimi i të drejtave		
GjDBE, çështje të bashkuara C-92/09 dhe C-93/09, *Volker und Markus Schecke GbR* dhe *Hartmut Eifert kundër Land Hessen*, 2010	**E përgjithshme**	
GjDBE, C-73/07, *Tietosuojavaltuutettu kundër Satakunnan Markkinapörssi Oy dhe Satamedia Oy*, 2008	**Liria e Shprehjes**	GjEDNj, *Axel Springer AG kundër Gjermanisë*, 2012 GjEDNj, *Mosley kundër Mbretërisë së Bashkuar*, 2011
	Liria e arteve Dhe shkencave	GjEDNj, *Vereinigung bildender Künstler kundër Austrisë*, 2007
GjDBE, C-275/06, *Productores de Música de España (Promusicae)kundër Telefónica de España SAU*,	**Mbrojtja e pronës**	

2008		
GjDBE, C-28/08 P, *European Commission kundër The Bavarian Lager Co. Ltd*, 2010	**Aksesi në dokumente**	GjEDNj, *Társaság a Szabadságjogokért kundër Hungarisë*, 2009

1.1. E drejta për mbrojtje të të dhënave

Pikat kryesore

- Sipas nenit 8 të KEDNj-së e drejta për mbrojtje nga mbledhja dhe përdorimi 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.
- E drejta e BE-së e ka rregulluar për herë të parë mbrojtjen e të dhënave nëpërmjet Direktivës për Mbrojtjen e të Dhënave.
- E drejta e BE-së e ka njohur mbrojtjen e të dhënave si të drejtë themelore.

Për herë të parë, është përcaktuar e drejta për mbrojtjen e sferës private të individit nga ndërhyrjet e të tjerëve, veçanërisht nga shteti, në një akt ligjor ndërkombëtar, në nenin 12 të Deklaratës Universale të së Drejtave të Njeriut (DUDNj) të Kombeve të Bashkuara (OKB) të vitit 1948, mbi respektimin e jetës private dhe familjare.[1] DUDNj-ja ndikoi edhe hartimin e akteve të tjera mbi të drejtat e njeriut në Evropë.

1.1.1. Konventa Evropiane e të Drejtave të Njeriut

Këshilli i Evropës u krijua pas përfundimit të Luftës së Dytë Botërore, për të bashkuar shtetet e Evropës, për të promovuar shtetin e së drejtës, demokracinë, të drejtat e njeriut dhe zhvillimet shoqërore. Për këtë qëllim, ai miratoi Konventën Evropiane të së Drejtave të Njeriut (KEDNj) në 1950-ën, e cila hyri në fuqi në 1953-shin.

Shtetet kanë detyrim ndërkombëtar të respektojnë KEDNj-në. Të gjitha shtetet anëtare të KiE-së kanë transpozuar tashmë ose i kanë dhënë fuqi ligjore KEDNj-në në të drejtën e tyre kombëtare, në mënyrë të tillë që t'u duhet të veprojnë në përputhje me dispozitat e Konventës.

Për t'u siguruar që Palët Kontraktuese të zbatojnë detyrimet e tyre në përputhje me KEDNj-në, u ngrit në 1959-ën në Strasburg të Francës, Gjykata Evropiane e të Drejtave të Njeriut (GjEDNj). GjEDNj-ja garanton që shtetet zbatojnë detyrimet e tyre në përputhje me Konventën, duke shqyrtuar padi nga individët, grupet e individëve, OJQ-të apo personat juridikë, të cilët pretendojnë shkelje të Konventës. Në 2013-ën, Këshilli i Evropës përfshinte 47 shtete anëtare, 28 prej të cilëve janë gjithashtu Shtete Anëtare të BE-së.

[1] Kombet e Bashkuara (OKB), Deklarata Universale e të Drejtave të Njeriut (DUDNj), 10 dhjetor 1948.

Për t'iu drejtuar GjEDNj-së nuk është e domosdoshme të jesh shtetas i një prej vendeve anëtare. GjEDNj-ja mund të shqyrtojë gjithashtu çështje të depozituara nga një ose më shumë shtete anëtare të KiE-së, kundër një shteti tjetër anëtar.

E drejta për mbrojtje të të dhënave personale bën pjesë tek të drejtat e mbrojtura sipas nenit 8 të KEDNj-së, i cili garanton të drejtën për respektim të jetës private dhe familjare, banesës dhe korrespondencës dhe përcakton kushtet sipas së cilëve lejohen kufizimet e kësaj të drejte.[2]

Në tërësinë e jurisprudencës së saj, GjEDNj-ja ka shqyrtuar temën e mbrojtjes së të dhënave në shumë rast, kryesisht në lidhje me përgjimin e komunikimeve[3], format e ndryshme të survejimit dhe mbrojtjen nga mbajtja e të dhënave nga ana e autoriteteve publike[5]. Gjykata ka qartësuar se neni 8 i KEDNj-së jo vetëm që detyron shtetet që të mos kryejnë veprime të cilat mund të shkelin këtë të drejtë të parashikuar nga Konventa, por i detyron në rrethana të caktuara, të garantojnë në mënyrë aktive respektimin e efektshëm të jetës private dhe familjare.[6] Shumë nga këto çështje do të paraqiten me hollësi në kapitujt përkatës.

1.1.2. Konventa 108 e Këshillit të Evropës

Lindja e teknologjive të informacionit në vitet 60, u shoqërua me një nevojë në rritje për rregulla më të detajuara për mbrojtjen e individëve, duke mbrojtur të dhënat e tyre (personale). Nga mesi i viteve 70, Komiteti i Ministrave të Këshillit të Evropës miratoi shumë rekomandime në lidhje me mbrojtjen e të dhënave personale, duke iu referuar nenit 8 të KEDNj-së.[7] Në vitin 1981, u përgatit për nënshkrim një Konventë për mbrojtjen e personave nga përpunimi automatik i të dhënave personale (Konventa 108).[8] Konventa 108 ishte dhe mbetet i vetmi akt ndërkombëtar me fuqi ligjore detyruese në fushën e mbrojtjes së të dhënave.

---

2 KiE, Konventa Evropiane e të Drejtave të Njeriut, STCE nr. 005, 1950.
3 Shih për shembull: GjEDNj, *Malone kundër Mbretërisë së Bashkuar*, nr. 8691/79, 2 gusht 1984; GjEDNj, Copland kundër Mbretërisë së Bashkuar, nr. 62617/00, 3 prill 2007.
4 Shih për shembull: GjEDNj, *Klass dhe të tjerët kundër Gjermanisë*, nr. 5029/71, 6 shtator 1978; GjEDNj, Uzun kundër Gjermanisë, nr. 35623/05, 2 shtator 2010.
5 Shih për shembull: GjEDNj, *Leander kundër Suedisë*, nr. 9248/81, 26 mars 1987; GjEDNj, S. Dhe Marper kundër Mbretërisë së Bashkuar, nr. 30562/04 dhe 30566/04, 4 dhjetor 2008.
6 Shih për shembull: GjEDNj, *I. kundër Finlandës*, nr. 20511/03, 17 korrik 2008; GjEDNj, K.U. kundër Finlandës, nr. 2872/02, 2 dhjetor 2008.
7 KiE, Komiteti i Ministrave (1973), Rezoluta (73) 22 mbi mbrojtjen e privatësisë së personave nga bankat e të dhënave elektronike në sektorin privat, 26 shtator 1973; KiE, Komiteti i Ministrave (1974), Rezoluta (74) 29 mbi mbrojtjen e privatësisë së personave nga bankat e të dhënave elektronike në sektorin publik, 20 shtator 1974.
8 KiE, Konventa për Mbrojtjen e Personave Përpunimi Automatik i të Dhënave Personale, Këshilli i Evropës, STCE nr. 108, 1981.

Konventa 108 zbatohet për të gjitha përpunimet e të dhënave personale, që kryhen si nga sektori privat ashtu edhe nga ai publik, si për shembull përpunimet që kryejnë autoritetet gjyqësore dhe ato të policisë. Ajo mbron personat nga abuzimet që mund të ndodhin gjatë mbledhjes dhe përpunimit të të dhënave personale dhe në të njëjtën kohë synon të rregullojë qarkullimin ndërkufitar të të dhënave personale. Sa i përket mbledhjes dhe përpunimit të të dhënave personale, parimet e përcaktuara në Konventë kanë të bëjnë veçanërisht me mbledhjen dhe përpunimin automatik të të dhënave në mënyrë të drejtë dhe të ligjshme, ruajtjen për qëllime legjitime të përcaktuara dhe jo për qëllime që nuk përputhen me këto të fundit e as të mos ruhen për një kohë më të gjatë se sa është e nevojshme. Këto parime kanë të bëjnë edhe me cilësinë e të dhënave, veçanërisht sa i takon faktit se ato duhet të jenë të përshtatshme, të rëndësishme, jo të tepërta (parimi i proporcionalitetit) dhe të sakta.

Përveç garancive që ofron në lidhje me mbledhjen dhe përpunimin e të dhënave personale, në mungesë të garancive të duhura ligjore, Konventa ndalon përpunimin e të dhënave "sensitive", sikundër janë raca, mendimet politike, të dhënat ne lidhje me shëndetin, bindjet fetare, jetën seksuale dhe të dhënat gjyqësore të një personi.

Konventa sanksionon ndër të tjera edhe të drejtën e personit për t'u informuar në lidhje me të dhënat e ruajtura të cilat kanë të bëjnë me të dhe aty ku është e nevojshme, të kërkojë korrigjimin e tyre. Kufizimet e të drejtave të parashtruara në Konventë, janë të mundshme vetëm kur prevalojnë interesa më të mëdha, si për shembull siguria ose mbrojtja kombëtare.

Edhe pse Konventa parashikon qarkullimin e lirë të të dhënave personale ndërmjet Shteteve Palë, ajo përcakton gjithashtu disa kufizime të këtyre qarkullimeve drejt shteteve ku kuadri ligjor nuk ofron mbrojtje ekuivalente.

Me qëllim që të zhvillohen më tej parimet e përgjithshme dhe rregullat e parashikuara në Konventën 108, Komiteti i Ministrave të KiE-së ka miratuar shumë rekomandime që nuk kanë fuqi ligjore detyruese (shih Kapitujt 7 dhe 8).

Të gjitha Shtetet Anëtare të BE-së kanë ratifikuar Konventën 108, e cila në 1999-ën u ndryshua, me qëllim që t'i mundësonte BE-së të aderonte në të.[9] Në 2001-shin, u miratua një Protokoll Shtesë i Konventës 108, i cili shton disa dispozita në lidhje me qarkullimet ndër-kufitare të të dhënave drejt palëve jo kontraktuese, të ashtuquajturit shtete të treta dhe në lidhje me krijimin e detyrueshëm të autoriteteve kombëtare mbikëqyrëse të mbrojtjes së të dhënave.[10]

---

[9] KiE, Ndryshimet në Konventën për Mbrojtjen e Personave nga Përpunimi Automatik i të Dhënave Personale (STCE nr. 108), që i mundësojnë Komunitetit Evropian të aderojë, miratuar nga Komiteti i Ministrave në Strasburg, më 15 qershor 1999; neni 23 (2) i Konventës 108 në variantin e ndryshuar.

[10] KiE, 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

Perspektivë

Në vijim të vendimit për të modernizuar Konventën 108, në vitin 2011 u zhvillua një konsultim publik, i cili bëri të mundur konfirmimin e dy objektivave kryesorë të punës: përforcimin e mbrojtjes së privatësisë në sektorin digjital dhe përmirësimin e mekanizmit të zbatimit të Konventës.

Konventa 108 është e hapur për aderim për shtetet që nuk janë anëtarë të KiE-së, përfshirë edhe vendet jo evropiane. Potenciali i saj si një standard universal dhe tipari i saj i hapur, mund të shërbejnë si bazë për promovimin e mbrojtjes së të dhënave në nivel botëror.

Deri më tani 45 nga 46 Palë Kontraktuese të Konventës 108 janë shtete anëtare të KiE-së. Uruguai, i pari vend jo evropian, aderoi në gusht të 2013-ës dhe Maroku, i cili është ftuar nga Komiteti i Ministrave që të aderojë në Konventën 108, është në fazën e zyrtarizmit të kërkesës.

1.1.3. E drejta e Bashkimit Evropian në fushën e mbrojtjes së të dhënave

E drejta e BE-së përbëhet nga traktatet dhe legjislacioni dytësor. Traktatet, konkretisht Traktati i Bashkimit Evropian (TBE) dhe Traktati i Funksionimit të Bashkimit Evropian (TFBE), janë miratuar nga të gjithë Shtetet Anëtare të BE-së dhe konsiderohen ndryshe "legjislacioni parësor i BE-së". Rregulloret, direktivat dhe vendimet e BE-së miratohen nga institucionet e BE-së, kompetencë e cila u është caktuar nga traktatet, shpesh konsiderohen si "legjislacioni dytësor i BE-së".

Akti juridik kryesor i BE-së në fushën e mbrojtjes së të dhënave është Direktiva 95/46/EC e Parlamentit Evropian dhe e Këshillit, e datës 24 tetor 1995, mbi mbrojtjen e personave nga përpunimi i të dhënave personale dhe mbi lëvizjen e lirë të këtyre të dhënave (*Direktiva për Mbrojtjen e të Dhënave*).[11]Direktiva u miratua në 1995-ën, në një kohë kur shumë Shtete Anëtare kishin miratuar më parë ligje kombëtare në fushën e mbrojtjes së të dhënave. Lëvizja e lirë e mallrave, kapitaleve, shërbimeve dhe njerëzve në tregun e brendshëm, imponte qarkullimin e lirë të dhënave, i cili mund të kryhej vetëm nëse Shtetet Anëtare mund të mbështeteshin në një nivel të njëtrajtshëm e të lartë të mbrojtjes së të dhënave.

---

[11] Direktiva e Mbrojtjes së të Dhënave, RZ1995 L 281, faqe 31.

Duke qenë se u miratua me qëllim që të harmonizonte[12] legjislacionet kombëtare në fushën e mbrojtjes së të dhënave, Direktiva ofron një shkallë saktësie të krahasueshme me atë të legjislacioneve kombëtare (të atëhershme) në fuqi të fushës së mbrojtjes së të dhënave. Për GjDBE-në: "Direktiva 95/46 ka për qëllim [...] të garantojë që niveli i mbrojtjes së të drejtave dhe lirive të individëve nga përpunimi i të dhënave personale të jetë ekuivalent në të gjitha Shtetet Anëtare. [...] Përafrimi i legjislacioneve kombëtare të zbatueshme në këtë fushë, nuk duhet të shkaktojë asnjë dobësim të mbrojtjes që gëzojnë, por përkundrazi, ky përafrim duhet të garantojë një nivel të lartë mbrojtjeje në BE. Kështu, [...] harmonizimi i këtyre legjislacioneve kombëtare nuk kufizohet në harmonizimin minimal të tyre, por në një harmonizim që parimisht është i plotë"[13]. Për rrjedhojë, Shtetet Anëtare të BE-së kanë hapësirë të kufizuar manovrimi sa i takon zbatimit të Direktivës.

Direktiva për Mbrojtjen e të Dhënave ka për qëllim t'i konkretizojë parimet e së drejtës për privatësi, që përfshinte më herët Konventa 108 dhe t'i zgjerojë ato. Fakti se në vitin 1995, të gjitha Shtetet Anëtare të BE-së ishin gjithashtu Palë Kontraktuese të Konventës 108, përjashton miratimin e rregullave kontradiktore në këto dy akte ligjore. Gjithsesi, Direktiva e Mbrojtjes së të Dhënave mbështetet mbi mundësinë që i jep neni 11 i Konventës 108, për të shtuar të tjera instrumente mbrojtjeje. Në mënyrë të veçantë, dispozita për mbikëqyrjen e pavarur, si një mjet për përmirësimin e përputhshmërisë me rregullat e mbrojtjes së të dhënave, ka rezultuar si një kontribut i rëndësishëm për funksionimin e efektshëm të legjislacionit evropian në fushën e mbrojtjes së të dhënave. (Rrjedhimisht, kjo karakteristikë u reflektua tek e drejta e KiE-së në 2001-shin, nëpërmjet Protokollit Shtesë të Konventës 108).

Zbatimi territorial i Direktivës për Mbrojtjen e të Dhënave shtrihet përtej 28 Shteteve Anëtare të BE-së, përfshirë edhe Shtetet të cilat nuk janë anëtare të BE, por bëjnë pjesë në Zonën Ekonomike Evropiane (ZEE)[14] – domethënë Islanda, Lihtenshteini dhe Norvegjia.

GjDBE-ja me seli në Luksemburg, ka kompetencën të përcaktojë nëse një Shtet Anëtar i ka përmbushur detyrimet e tij që rrjedhin nga Direktiva për Mbrojtjen e të Dhënave dhe të marrë vendim paraprak në lidhje me vlefshmërinë dhe interpretimin e Direktivës, me qëllim që të garantojë zbatim të efektshëm dhe uniform në Shtetet Anëtare. Një përjashtim i rëndësishëm nga zbatueshmëria e Direktivës për Mbrojtjen e të Dhënave është i ashtuquajturi përjashtim për ushtrimin e aktivitetit me karakter vetjak ose familjar, që nënkupton përpunimin e të dhënave personale nga individë për qëllime personale apo familjare.[15]Ky lloj përpunimi konsiderohet përgjithësisht si pjesë e lirive të individit.

---

[12] Shih për shembull, Direktiva e Mbrojtjes së të Dhënave, pikat 1, 4, 7 dhe 8.
[13] 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) kundër Administración del Estado*, 24 nëntor 2011, parag. 28-29.
[14] Marrëveshja e Zonës Ekonomike Evropiane, JO 1994 L 1, e cila hyri në fuqi më 1 janar 1994.
[15] Direktiva e Mbrojtjes së të Dhënave, neni 3, pika 2

Në përputhje me legjislacionin parësor të BE-së në fuqi në kohën e miratimin të Direktivës së Mbrojtjes së të Dhënave, fusha e zbatimit material kufizohet në çështjet e tregut të brendshëm. Përtej fushës së saj të zbatimit, janë veçanërisht çështjet e bashkëpunimit të policisë dhe drejtësisë penale. Mbrojtja e të dhënave në këto fusha mundësohet nga akte të tjera ligjore, të cilat përshkruhen me hollësi në Kapitullin 7.
Meqenëse Direktiva e Mbrojtjes së të Dhënave mund të përfshinte vetëm Shtetet Anëtare të BE-së, nevojitej një tjetër akt ligjor për të siguruar mbrojtjen e të dhënave gjatë përpunimit të të dhënave personale nga institucionet dhe organizmat e BE-së. Këtë funksion e ushtron Rregullorja (KE) nr. 45/2001 për mbrojtjen e personave nga përpunimi i të dhënave personale të institucioneve dhe organizmave të Komunitetit dhe për lëvizjen e lirë të këtyre të dhënave (*Rregullorja e Mbrojtjes së të Dhënave e Institucioneve të BE-së*).[16]

Gjithashtu, edhe në fushat që mbulohen nga Direktiva e Mbrojtjes së të Dhënave, shpesh nevojiten dispozita më të detajuara për mbrojtjen e të dhënave, për të pasur qartësinë e nevojshme për ekuilibrimin e interesave të tjera legjitime. Dy shembuj për këtë janë Direktiva 2002/58/KE për përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike (*Direktiva e privatësisë dhe komunikimeve elektronike*)[17]dhe Direktiva 2006/24/KE për ruajtjen e të dhënave të gjeneruara ose të përpunuara në kuadër të ofrimit të shërbimeve të komunikimit elektronik të aksesueshme nga publiku, ose të rrjeteve publike të komunikimit, që ndryshon Direktivën 2002/58/KE (*Direktiva e Ruajtjes së të Dhënave*, shfuqizuar më 8 prill 2014).[18] Shembuj të tjerë do të trajtohen në Kapitullin 8. Këto dispozita duhet të jenë në përputhje me Direktivën e Mbrojtjes së të Dhënave.

Karta e të Drejtave Themelore të Bashkimit Evropian

Traktatet fillestare të Komunitetit Evropian nuk i referoheshin të drejtave të njeriut apo mbrojtjes së tyre. Megjithatë, me paraqitjen e çështjeve tek Gjykata Evropiane e Drejtësisë (GjED) sikurse emërtohej atëherë, të cilat kishin të bënin me shkelje të së drejtave të njeriut, brenda fushës së zbatimit të së drejtës së BE-së, u zhvillua një qasje e re. Me qëllim që t'u jepte mbrojtje individëve, Gjykata përfshiu të drejtat themelore në të ashtuquajturit parime të përgjithshme të së drejtës evropiane. Sipas GjDBE-së, këto parime të përgjithshme reflektojnë esencën e mbrojtjes së të drejtave të njeriut, që garantohet nga kushtetutat kombëtare dhe nga traktatet e të drejtave të njeriut, veçanërisht nga KEDNj-ja. GjDBE-ja ka shprehur angazhimin e saj për të garantuar përputhshmëri me të drejtën e BE-së me këto parime.

---

[16] Rregullorja (CE) nr. 45/2001 e Parlamentit Evropian dhe e Këshillit e 18 dhjetorit 2000 për mbrojtjen e personave nga përpunimi i të dhënave personale të institucioneve dhe organizmave të Komunitetit dhe për lëvizjen e lirë të këtyre të dhënave, JO 2001 L 8.
[17] Direktiva 2002/58/CE e Parlamentit Evropian dhe e Këshillit e 12 korrikut 2002 për përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike (Direktiva e privatësisë dhe komunikimeve elektronike), JO 2002 L 201.
[18] Direktiva 2006/24/CE e Parlamentit Evropian dhe e Këshillit e 15 marsit 2006 për ruajtjen e të dhënave të gjeneruara ose të përpunuara në kuadër të ofrimit të shërbimeve të komunikimit elektronik të aksesueshme nga publiku ose të rrjeteve publike të komunikimit, që ndryshon Direktivën 2002/58/KE (*Direktiva e Ruajtjes së të Dhënave*,), JO 2006 L 105, shfuqizuar më 8 prill 2014.

E ndërgjegjshme për ndikimin e politikave të saj tek të drejtat e njeriut dhe duke u përpjekur t'i bënte qytetarët të ndjeheshin "më pranë" BE-së, në vitin 2000 Bashkimi Evropian shpalli Konventën e të Drejtave Themelore të Bashkimit Evropian (Karta). Kjo Kartë përfshin të gjithë gamën e të drejtave civile, politike, ekonomike dhe shoqërore të qytetarëve evropianë, duke sintetizuar traditat kushtetuese dhe detyrimet e përbashkëta ndërkombëtare për Shtetet Anëtare. Të drejtat e përshkruara në Kartë ndahen në 6 seksione: dinjiteti, liritë, barazia, solidariteti, të drejtat e qytetarëve dhe drejtësia.

Edhe pse fillimisht bëhej fjalë vetëm për dokument politik, Karta mori fuqi ligjore detyruese[19] si legjislacion parësor i BE-së (shih nenin 6 (1) të TBA-së) me hyrjen në fuqi të Traktatit të Lisbonës më 1 dhjetor 2009.[20]

Legjislacioni parësor i BE-së i jep gjithashtu Bashkimit kompetencën e përgjithshme të nxjerrë ligje për çështje që lidhen me mbrojtjen e të dhënave (neni 16 i TFBE-së).

Karta nuk garanton vetëm respektimin e jetës private dhe familjare (neni 7), por gjithashtu edhe të drejtën për mbrojtje të të dhënave (neni 8), duke e ngritur në mënyrë të qartë këtë të drejtë, në nivelin e një të drejte themelore në legjislacionin e BE-së. Institucionet e BE-së, ashtu sikundër Shtetet Anëtare, duhet të zbatojnë dhe garantojnë këtë të drejtë, edhe kur Shtetet Anëtare zbatojnë legjislacionin e Bashkimit (neni 51 i Kartës). Megjithëse u hartua shumë vite pas Direktivës për Mbrojtjen e të Dhënave, neni 8 i Kartës duhet trajtuar si mishërim i së drejtës pararendëse të 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 (1), por edhe i referohet parimeve thelbësore të mbrojtjes së të dhënave në nenin 8 (2). Si përfundim, neni 8 (3) i Kartës garanton që një autoritet i pavarur do të kontrollojë zbatimin e këtyre parimeve.

Perspektivë

Në janar të 2012-ës, Komisioni Evropian propozoi një paketë reformash në fushën e mbrojtjes së të dhënave, duke pohuar domosdoshmërinë e modernizimit të normave aktuale të mbrojtjes së të dhënave, për shkak të zhvillimeve të shpejta teknologjike dhe globalizimit. Paketa e reformave konsiston në një Rregullore të Përgjithshme të Mbrojtjes së të Dhënave,[21] e cila do të zëvendësojë Direktivën për Mbrojtjen e të Dhënave, ashtu si edhe një Direktivë të Përgjithshme të Mbrojtjes së të Dhënave[22] e cila do të sigurojë mbrojtjen e të dhënave në fushën e bashkëpunimit policor dhe gjyqësor për çështjet penale. Në kohën e publikimit të këtij manuali, vazhdojnë diskutimet për paketën e reformave.

---

[19] BE (2012), Karta e të Drejtave Themelore të Bashkimit Evropian, JO 2012 C 326.

[20] Shih variantet e konsoliduar të Komunitetit Evropian (2012), Traktati i Bashkimit Evropian, JO 2012 C 326; dhe i Komunitetit Evropian (2012), TFBE, JO 2012 C 326.

[21] Komisioni Evropian (2012), *Propozim për një Rregullore të Parlamentit Evropian dhe Këshillit për mbrojtjen e personave nga përpunimi i të dhënave personale dhe për lëvizjen e lirë të këtyre të dhënave (Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave)*, COM(2012) 11 përfundimtar, Bruksel, 25 janar 2012.

[22] Komisioni Evropian (2012), *Propozim për një Direktivë të Parlamentit Evropian dhe Këshillit për mbrojtjen e personave nga përpunimi i të dhënave personale të autoriteteve kompetente për qëllime të parandalimit, hetimit, zbulimit, ose gjykimit të veprave penale apo ekzekutimit të dënimeve penale dhe për lëvizjen e lirë të këtyre të Dhënave (Direktiva e Përgjithshme e Mbrojtjes së të Dhënave)*, COM(2012) 10 përfundimtar, Bruksel, 25 janar 2012.

1.2. Ekuilibrimi i të drejtave

Pika kryesore

- E drejta për mbrojtje të të dhënave nuk është një e drejtë absolute; ajo duhet të ekuilibrohet me të drejta të tjera.

Sipas nenit 8 të Kartës, e drejta themelore për mbrojtje të të dhënave " nuk është, gjithsesi, një e drejtë absolute, por duhet të trajtohet në raport me funksionin e saj në shoqëri".[23] Neni 52 (1) i Kartës pranon në këtë mënyrë se, ushtrimit të së drejtave të sanksionuara nga nenet 7 dhe 8 të Kartës, mund t'u bëhen kufizime, për sa kohë që këto të fundit janë të parashikuara me ligj, respektojnë thelbin e atyre të drejtave e lirive dhe bazuar në parimin e proporcionalitetit, janë të nevojshme dhe u përgjigjen në mënyrë të efektshme interesave të përgjithshme që njihen nga Bashkimi, apo nevojës për të mbrojtur të drejtat dhe liritë e të tjerëve.[24]

Në sistemin juridik të GjEDNj-së, mbrojtja e të dhënave garantohet nga neni 8 (e drejta për respektim të jetës private dhe familjare) dhe ashtu si në sistemin juridik të Kartës, kjo e drejtë duhet të zbatohet duke respektuar njëkohësisht edhe të drejtat e tjera konkurruese. Bazuar në nenin 8 (2) të KEDNj-së, "nuk duhet të ketë asnjë ndërhyrje nga autoritetet publike në ushtrimin e kësaj të drejte, përveçse kur kjo ndërhyrje është në përputhje me ligjin dhe kur përbën një masë të nevojshme në një shoqëri demokratike [...] për mbrojtjen e të drejtave dhe lirive të të tjerëve".

Rrjedhimisht, si GjEDNj-ja ashtu edhe GjDBE-ja janë shprehur në mënyrë të përsëritur se ekuilibrimi me të drejtat e tjera, është i nevojshëm kur zbatohet dhe interpretohet neni 8 i KEDNj-së dhe neni 8 i Kartës.[25] Shembuj të shumtë do të ilustrojnë mënyrën se si arrihet ky ekuilibrim.

1.2.1. Liria e shprehjes

Njëra nga të drejtat, e cila ka të ngjarë të përplaset me të drejtën për mbrojtje të të dhënave, është e drejta për lirinë e shprehjes.

---

[23] Shih për shembull, GjDBE, Çështje të bashkuara C-92/09 and C-93/09, *Volker dhe Markus Schecke GbR dhe Hartmut Eifert kundër Land Hessen*, 9 nëntor 2010, parag. 48.
[24] Ibidem, parag. 50.
[25] GjEDNj, *Von Hannover kundër Gjermanisë* (nr. 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) kundër Administración del Estado*, 24 nëntor 2011, parag. 48; GjDBE, C-275/06, *Productores de Música de España (Promusicae) kundër Telefónica de España SAU*, 29 janar 2008, parag. 68. Shih po ashtu Këshilli i Evropës (2013), Jurisprudenca e Gjykatës Evropiane të së Drejtave të Njeriut në lidhje me mbrojtjen e të dhënave personale, DP (2013) Jurisprudenca gjendet: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP 2013 Case Law_Eng_ FINAL.pdf.

Liria e shprehjes mbrohet nga neni 11 i Kartës ('Liria e shprehjes dhe informimit'). Kjo e drejtë përfshin 'lirinë e mendimit dhe lirinë për të marrë apo dhënë informacion ose ide, pa pasur ndërhyrje nga autoritetet publike dhe pa marrë parasysh kufijtë'. Neni 11 përkon me nenin 10 të KEDNj-së. Në bazë të nenit 52 (3) të Kartës, për aq sa parashikon të drejta që përputhen me të drejtat e garantuara nga KEDNj-ja, "kuptimi dhe qëllimi i këtyre të drejtave, duhet të jetë i njëjtë me ato të përcaktuara në Konventën në fjalë". Kufizimet që mund t'i bëhen në mënyrë legjitime të drejtës së garantuar nga neni 11 i Kartës, për rrjedhojë, nuk duhet të tejkalojnë ato të përcaktuara në nenin 10 (2) të KEDNj-së, çka do të thotë se duhet të jenë të parashikuara në ligj dhe të nevojshme në një shoqëri demokratike "për të mbrojtur [...] reputacionin ose të drejtat e të tjerëve". Ky koncept përfshin të drejtën për mbrojtje të të dhënave.

Marrëdhënia midis mbrojtjes së të dhënave personale dhe lirisë së shprehjes rregullohet nga neni 9 i Direktivës së Mbrojtjes së të Dhënave, të titulluar "Përpunimi i të dhënave personale dhe liria e shprehjes".[26] Sipas këtij neni, Shtetet Anëtare duhet të përcaktojnë përjashtimet apo kufizimet që lidhen me mbrojtjen e të dhënave dhe me të drejtën themelore për privatësi, të detajuar në kapitujt II, IV dhe VI të Direktivës. Përjashtimet duhen bërë vetëm për qëllime gazetarie, apo të shprehjes artistike ose letrare, të cilat i përfshin e drejta themelore e lirisë së shprehjes, vetëm për aq sa ato nevojiten për të pajtuar të drejtën për privatësi me normat që rregullojnë lirinë e shprehjes.

Shembull: Në çështjen *Tietosuojavaltuutettu kundër Satakunnan Markkinapörssi Oy dhe Satamedia Oy*, [27] GjDBE-së iu kërkua të interpretonte nenin 9 të Direktivës së Mbrojtjes së të Dhënave dhe të përkufizonte marrëdhënien midis mbrojtjes së të dhënave dhe lirisë së shtypit. Gjykatës iu desh të shqyrtonte publikimin nga ana e Markkinapörssi-t dhe Satamedia-s, të të dhënave tatimore të rreth 1.2 milion personave fizikë, të marra në mënyrë të ligjshme nga autoritetet tatimore finlandeze. Në mënyrë të veçantë, Gjykatës iu desh të verifikonte 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 aktiviteti i Satakunnan-it ishte "përpunim i të dhënave personale", ne kuptimin e nenit 3 (1) të Direktivës së Mbrojtjes së të Dhënave, Gjykata vijoi më pas me interpretimin e nenit 9 të Direktivës. Gjykata së pari vërejti 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. Ajo vuri më tej në dukje se për t'i vendosur këto dy të drejta themelore në ekuilibër, përjashtimet dhe kufizimet e së drejtës për mbrojtje të të dhënave, duhet të zbatohen vetëm për aq sa është e domosdoshme. Në ato rrethana, Gjykata vlerësoi se kryerja e këtyre aktiviteteve, sikurse i Markkinapörssi-t dhe Satamedia-s, 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 qëllimi i tyre është përhapja e informacionit, mendimeve apo ideve tek publiku, pavarësisht mjetit të përdorur për transmetim. Gjykata 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 vlerësimin në fjalë.

[26] Direktiva e Mbrojtjes së të Dhënave, neni 9.

[27] GjDBE, C-73/07, *Tietosuojavaltuutettu kundër Satakunnan Markkinapörssi Oy dhe Satamedia Oy*, 16 dhjetor 2008, parag. 56, 61 dhe 62.

Për sa i përket pajtueshmërisë së të drejtës për mbrojtje të të dhënave me të drejtën për lirinë e shprehjes, GjEDNj-ka ka marrë shumë vendime të rëndësishme.

Shembull: tek *Axel Springer AG kundër Gjermanisë,* [28] GjEDNj-ja u shpreh se ndalimi që i kishte bërë një gjykatë kombëtare pronarit të një gazete, i cili donte të publikonte një artikull në lidhje me arrestimin dhe dënimin e një aktori të mirënjohur, përbënte shkelje të nenit 10 të KEDNj-së. GjEDNj-ja ripohoi kriteret që ajo kishte përcaktuar në jurisprudencën e saj në rastet e ekuilibrimit të së drejtës për lirinë e shprehjes me të drejtën për respektim të jetës private:

- Së pari, nëse rasti i publikuar nga artikulli në fjalë përbënte interes të përgjithshëm: arrestimi dhe dënimi i një personi ishte fakt gjyqësor publik dhe për rrjedhojë me interes publik;

- Së dyti, nëse personi i përfshirë ishte figurë publike: personi i përfshirë ishte aktor mjaftueshëm i njohur, për t'i cilësuar si figurë publike;

- Së treti, në çfarë mënyre ishte marrë informacioni dhe nëse ishte i besueshëm ky i fundit: informacioni ishte dhënë nga zyra e prokurorit dhe saktësia e informacionit në të dy dokumentet e publikuara nuk kishte qenë objekt mosmarrëveshjeje midis palëve.

Për rrjedhojë, GjEDNj-ja vendosi se ndalimi i publikimit të vendosur ndaj gazetës, nuk ishin proporcionale në mënyrë të arsyeshme, në raport me qëllimin legjitim të mbrojtjes së jetës private të ankuesit. Gjykata doli me përfundimin se ishte shkelur neni 10 i KEDNj-së.

Shembull: tek çështja *Von Hannover kundër Gjermanisë (nr. 2),*[29] GjEDNj-ja nuk gjeti shkelje të së drejtës për respektim të jetës private bazuar në nenin 8 të KEDNj-së, kur u refuzua urdhri i Princeshës Caroline të Monakos për mospublikimin e një fotografie, ku ajo shfaqej me bashkëshortin gjatë pushimeve për ski. Fotografia shoqërohej nga një artikull, i cili, ndër të tjera, bënte me dije gjendjen jo të mirë shëndetësore të Princit Rainier-i. GjEDNj-ja doli në përfundimin se gjykata kombëtare e kishte ekuilibruar me kujdes të drejtën për lirinë e shprehjes së botuesit, me të drejtën për respektim të jetës private të ankuesit. Cilësimi nga ana e gjykatës kombëtare i sëmundjes së Princit Rainier-i si "ngjarje e historisë bashkëkohore", nuk mund të konsiderohej si e paarsyeshme dhe GjEDNj-ja vlerësoi se fotografia, e marrë në kuadër të artikullit, ka ndihmuar të paktën në një farë mase, në debatin me interes të përgjithshëm. Gjykata vendosi se nuk kishte shkelje të nenit 8 të KEDNj-së.

Në jurisprudencën e GjEDNj-së, një nga kriteret thelbësore që ka të bëjë me ekuilibrimin e këtyre të drejtave, është përcaktimi nëse shprehja e shqyrtuar ka kontribuuar ose jo në debatin me interes publik.

[28] GjEDNj, *Axel Springer AG kundër Gjermanisë* [GC], nr. 39954/08, 7 shkurt 2012, parag. 90 dhe 91.
[29] GjEDNj, *Von Hannover kundër Gjermanisë* (nr. 2) [GC], nr. 40660/08 dhe 60641/08, 7 shkurt 2012, parag. 118 dhe 124.

Shembull: tek *Mosley kundër Mbretërisë së Bashkuar*,[30] një gazetë e përjavshme publikoi fotografi intime të ankuesit. Ky i fundit pretendoi më pas se ishte shkelur neni 8 i KEDNj-së, pasi atij nuk i ishte dhënë mundësia të kërkonte më parë ndalimin e publikimit të fotove në fjalë, për shkak se nuk nuk ekzistonte një detyrim për njoftim paraprak nga ana e gazetës, në raste publikimi materialesh që mund të shkelin të drejtën për privatësi. Edhe pse përhapja e një materiali të tillë ishte përgjithësisht për qëllime zbavitjeje dhe jo informimi, padyshim që gëzonte mbrojtje nëpërmjet nenit 10 të KEDNj-së, mbi të cilin 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 *Biriuk kundër Lituanisë*,[31] ankuesi kërkonte dëmshpërblim nga një gazetë e përditshme, për shkak se kishte publikuar një artikull, në të cilin raportohej se personi ishte sieropozitiv. Me sa dukej, informacioni ishte konfirmuar nga mjekët e spitalit lokal. GjEDNj-ja vlerësoi se artikulli në fjalë nuk kontribuonte në asnjë lloj mënyre në debatin me interes të përgjithshëm dhe ritheksoi se mbrojtja e të dhënave personale, aq më tepër e të dhënave mjekësore, ishte e një rëndësie thelbësore për personin, në mënyrë që të gëzojë respektimin e jetës private dhe familjare të tij apo të saj, sikurse garantohet nga neni 8 i KEDNj-së. Gjykata i kushtoi rëndësi të veçantë faktit se, sipas artikullit, personeli mjekësor i spitalit kishte dhënë informacione mbi infektimin me virusin HIV të ankuesit, në shkelje të qartë të detyrimit që ata kanë të ruajtjes së sekretit mjekësor. Gjykata vendosi se ishte shkelur neni 8.

1.2.2. Aksesi në dokumente

E drejta e informimit, sipas nenit 11 të Kartës dhe nenit 10 të KEDNj-së, mbron jo vetëm të drejtën për të dhënë informacion, por edhe të *marrjes* së tij. Ndërgjegjësimi në lidhje me rëndësinë që ka transparenca e qeverisjes për funksionimin e një shoqërie demokratike, po vjen në rritje. Për rrjedhojë, gjatë dy dekadave të fundit, e drejta për të pasur akses në dokumentet që zotërohen nga autoritetet publike, është njohur si një e drejtë e rëndësishme e çdo qytetari të BE-së, ashtu si edhe çdo personi fizik apo juridik që ka vendbanimin ose selinë në një Shtet Anëtar.

Sipas së drejtës së KiE-së, referenca mund të merret nga parimet e përcaktuara në Rekomandimin për aksesin në dokumentet zyrtare, i cili frymëzoi hartuesit e Konventës për Aksesin në Dokumentet Zyrtare (Konventa 205).[32] **Tek e drejta e BE-së**, e drejta e aksesit në dokumente garantohet nga Rregullorja 1049/2001 mbi të drejtën e aksesit të publikut në dokumentet e Parlamentit Evropian, Këshillit dhe Komisionit (*Rregullorja e Akesit në Dokumente*).[33]

[30] GjEDNj, *Mosley kundër Mbretërisë së Bashkuar*, nr. 48009/08, 10 maj 2011, parag. 129 dhe 130.
[31] GjEDNj, *Biriuk kundër Lituanisë*, nr. 23373/03, 25 nëntor 2008.
[32] Këshilli i Evropës, Komiteti i Ministrave (2002), Rekomandimi Rek(2002)2 për Shtetet Anëtare mbi aksesin në dokumentet zyrtare, 21 shkurt 2002; Këshilli i Evropës, Konventa mbi Aksesin në Dokumentet Zyrtare, STCE nr. 205, 18 qershor 2009. Konventa nuk ka hyrë ende në fuqi.
[33] Rregullorja (KE) nr. 1049/2001 e Parlamentit Evropian dhe e Këshillit e 30 majit 2001 mbi të drejtën e aksesit të publikut në dokumentet e Parlamentit Evropian, Këshillit dhe Komisionit, JO 2001 L 145.

Neni 42 i Kartës dhe neni 15 (3) i TFBE-së e kanë zgjeruar këtë të drejtë aksesi "tek dokumentet e institucioneve, organizmave, zyrave dhe agjencive të Bashkimit, pavarësisht formës së tyre". Në përputhje me nenin (52) 2 të Kartës, e drejta e aksesit në dokumente ushtrohet gjithashtu në kushtet dhe brenda kufizimeve të përcaktuara në nenin 15 (3) të TFBE-së. Kjo e drejtë mund të përplaset me të drejtën për mbrojtje të të dhënave personale, në rastin kur aksesi në një dokument mund të zbulojë të dhëna personale të të tretëve. Për rrjedhojë, kërkesat për akses në dokumente ose informacionin që disponohet nga autoritetet publike, duhet të balancohen me të drejtën për mbrojtje të të dhënave të personave, të dhënat e të cilëve i përmbajnë dokumentet e kërkuara.

Shembull: tek çështja *Komisioni Evropian kundër Bavarian Lager-it,*[34] GjDBE-ja përcaktoi qëllimin e mbrojtjes së të dhënave personale në kontekstin e aksesit në dokumentet e institucioneve të BE-së dhe marrëdhënies midis Rregulloreve nr. 1049/2001 (*Rregullorja e Aksesit në Dokumente*) dhe 45/2001 (*Rregullorja e Mbrojtjes së të Dhënave*). 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*, favorizon prodhuesit vendas. Në përgjigjen ndaj ankesës së Bavarian Lager-it, Komisioni Evropian vendosi të niste një procedim ndaj 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. Me anë të 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 personave, sikundër garantohet nga Rregullorja e Mbrojtjes së të Dhënave. 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 datë 8 nëntor 2007 (çështja T-194/04, *Bavarian Lager kundër Komisionit*), 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 cënim të jetës private dhe nuk i rrezikonte aspak jetët private të tyre.

Pas apelimit të 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 disa raste të caktuara". Sipas GjDBE-së, kur një kërkesë bazuar në Rregulloren e Aksesit të Dokumenteve synon të përfitojë akses në dokumente në të cilat përfshihen të dhëna personale, dispozitat e Rregullores së Mbrojtjes së të Dhënave 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.

[34] GjDBE, C-28/08 P, *Komisioni Evropian kundër The Bavarian Lager Co. Ltd.*, 29 qershor 2010, parag. 60, 63, 76, 78 dhe 79.

Gjithashtu, sipas GjDBE-së, "duke qenë se Bavarian Lager-i nuk kishte parashtruar asnjë justifikim të shprehur dhe legjitim apo asnjë 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.

Sipas këtij vendimi, ndërhyrja tek e drejta për mbrojtje të të dhënave, për sa i takon aksesit në dokumente, nevojit arsye specifike dhe të justifikuar. E drejta për akses në dokumente, nuk mund të prevalojë automatikisht të drejtën për mbrojtje të të dhënave.[35]

Një aspekt i veçantë i kërkesës për akses u trajtua në çështjen në vijim nga GjEDNj-ja.

Shembull: tek çështja *Társaság a Szabadságjogokért kundër. Hungarisë,* [36] ankuesi, një OJQ që merrej me të drejtat e njeriut, kishte kërkuar nga Gjykata Kushtetuese aksesin në informacionet në lidhje me një çështje në pritje për t'u gjykuar. Pa u konsultuar më parë me deputetin, i cili e kishte dërguar çështjen në këtë gjykatë, kjo e fundit refuzoi kërkesën për akses, me arsyetimin se çështjet e depozituara pranë saj, nuk mund t'i komunikoheshin të tretëve pa autorizimin e ankuesit. Gjykatat vendase lanë në fuqi këtë vendim refuzimi, me arsyetimin se të tjera interesa legjitime, përfshirë aksesin në informacionin publik, nuk mund të prevalonin mbi mbrojtjen e këtyre lloj të dhënash personale. Ankuesi kishte vepruar si një "mbikëqyrës shoqëror", aktivitetet e së cilit meritonin mbrojtje të ngjashme me ato që gëzon shtypi. Në lidhje me lirinë e shtypit, GjEDNj-ja ka këmbëngulur vazhdimisht se publiku ka të drejtë të marrë informacion me interes të përgjithshëm. Informacioni i kërkuar nga ankuesi, ishte "gati dhe i disponueshëm" dhe nuk nevojitej asnjë mbledhje të dhënash. Në këto rrethana, shteti kishte detyrimin të mos pengonte qarkullimin e informacionit të kërkuar nga ankuesi. Me pak fjalë, GjEDNj-ja vlerësoi se pengesat që synojnë të ndalin aksesin në informacionin me interes për publikun, mund të pengojnë profesionistët e medias ose të fushave që kanë të bëjnë me të, që të kryejnë rolin e tyre thelbësor të "mbikëqyrësit shoqëror". Gjykata vendosi se kishte pasur shkelje të nenit 10.

E drejta e BE-së e përcakton me vendosmëri rëndësinë e transparencës. Parimi i transparencës është i sanksionuar në nenet 1 dhe 10 të TBE-së dhe në nenin 15 (1) të TFBE-së.[37] Sipas pikës 2 të Rregullores (KE) nr. 1049/2001, ajo u mundëson qytetarëve të marrin pjesë më nga afër në procesin vendimmarrës dhe garanton që administrata të gëzojë më tepër legjitimitet dhe të jetë më e efektshme dhe më e përgjegjshme kundrejt qytetarëve në një sistem demokratik.[38]

---

[35] Shih gjithsesi opinionin e detajuar të Mbikëqyrësit Evropian të Mbrojtjes së të Dhënave (EDPS) (2011), Aksesi i publikut në dokumente të cilat përmbajnë të dhëna personale, pas vendimit mbi Bavarian Lager-in, Bruksel, 24 mars 2011, i disponueshëm tek: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgrounddP/11-03-24_Bavarian_Lager_EN.pdf.

[36] GjEDNj, *Társaság a Szabadságjogokért kundër Hungarisë*, nr. 37374/05, 14 prill 2009; shih parag. 27, 36–38.

[37] BE (2012), Variantet e konsoliduara të Traktatit të Bashkimit Evropian dhe të TFBE-së, JO 2012 C 326.

[38] GjDBE, C-41/00 P, *Interporc Im- und Export GmbH kundër Komisionit të Komunitetit Evropian*, 6 mars 2003, parag. 39; dhe GjDBE, C-28/08 P, Komisioni Evropian kundër The Bavarian Lager Co. Ltd., 29 qershor 2010, parag. 54.

Në vijim të këtij arsyetimi, Rregullorja e Këshillit (KE) nr. 1290/2005 mbi financimin e politikave të përbashkëta bujqësore dhe Rregullorja e Komisionit (KE) nr. 259/2008 që përcakton rregullat e hollësishme për zbatimin e së parës, bëjnë të detyrueshëm publikimin e informacionit në lidhje me përfituesit e disa prej fondeve të BE-së në sektorin e bujqësisë dhe të shumave të akorduara për çdo përfitues.[39] Publikimi duhet të mundësojë kontrollin nga ana e publikut, sa i takon përdorimit të drejtë të fondeve publike nga ana e administratës. Proporcionaliteti i këtij publikimi është kundërshtuar nga shumë përfitues.

Shembull: tek çështja *Volker dhe Markus Schecke dhe Hartmut Eifert kundër Land Hessen,*[40] GjDBE-ja duhet të vlerësonte proporcionalitetin e publikimit, parashikuar nga legjislacioni i BE-së, të emrave të përfituesve të subvencioneve bujqësore të BE-së dhe të shumave të përfituara.

Gjykata 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 që përmbanin emrat e përfituesve të dy fondeve bujqësore të BE-së dhe shumën e saktë të përfituar, përbënte ndërhyrje në jetën e tyre private në përgjithësi dhe tek mbrojtja e të dhënave të tyre personale në veçanti.

Gjykata vlerësoi se ky cënim i neneve 7 dhe 8 të Kartës, ishte i parashikuar në ligj dhe përkonte me qëllimin e interesit të përgjithshëm, të njohur nga BE-ja dhe konkretisht me rritjen e transparencës mbi përdorimin e fondeve të komunitetit. Gjithsesi, GjDBE-ja u shpreh 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 (1) të Kartës. Kështu, Gjykata e shpalli pjesërisht të pavlefshëm legjislacionin e BE-së mbi publikimin e informacionit në lidhje me përfituesit e fondeve bujqësore evropiane.

1.2.3. Liria e arteve dhe shkencave

Një tjetër e drejtë, e cila duhet ekuilibruar me të drejtën për respektim të jetës private dhe për mbrojtje të të dhënave, është liria e arteve dhe shkencave, e cila garantohet nga neni 13 i Kartës. Kjo e drejtë buron kryesisht nga e drejta për lirinë e mendimit dhe të shprehjes dhe duhet ushtruar duke pasur parasysh nenin 1 të Kartës (Dinjiteti njerëzor). GjEDNj-ja e konsideron lirinë e arteve si të mbrojtur nga neni 10 i KEDNj-së.[41] Kjo e drejtë e garantuar nga neni 13 i Kartës, mundet gjithashtu të jetë subjekt kufizimesh, të cilat autorizohen nga neni 10 i KEDNj-së.[42]

[39] Rregullorja e Këshillit (KE) nr. 1290/2005 e 21 qershori 2005 mbi financimin e politikave të përbashkëta bujqësore, JO 2005 L 209; dhe Rregullorja e Komisionit (KE) nr. 259/2008 e 18 marsit 2008 që përcakton rregullat e hollësishme për zbatimin e rregullores së Këshillit (KE) nr. 1290/2005 mbi publikimin e informacionit në lidhje me përfituesit e fondeve që burojnë nga Fondi Evropian i Garancive Bujqësore (FEGB) dhe nga Fondi Evropian Bujqësor për Zhvillim Rural (FEBZhR), JO 2008 L 76.

[40] GjDBE, Çështje të bashkuara C-92/09 and C-93/09, *Volker dhe Markus Schecke GbR (C-92/09) dhe Hartmut Eifert (C-93/09) kundër Land Hessen*, 9 nëntor 2010, parag. 47–52, 58, 66–67, 75, 86 dhe 92.

[41] GjEDNj, *Müller dhe të Tjerët kundër Zvicrës*, nr. 10737/84, 24 maj 1988.

[42] Shpjegime në lidhje me Kartën e të Drejtave Themelore, JO 2007 C 303

Shembull: tek çështja *Vereinigung bildender Künstler kundër Austrisë,* [43] gjykatat austriake ndaluan shoqërinë ankuese që të vazhdonte të ekspozonte një pikturë, e cila përmbante fotografitë e disa figurave publike në pozicione seksuale. Një parlamentar austriak, fotografitë e të cilit ishin përdorur në pikturë, paditi shoqërinë ankuese, duke kërkuar urdhër ndalimi të ekspozimit të pikturës. Gjykata vendase pranoi kërkesën e tij dhe urdhëroi ndalimin. GjEDNj-ja u shpreh se neni 10 i KEDNj-së gjen zbatim në rastet e komunikimit të ideve të cilat fyejnë, tronditin 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 fotot e fytyrave të 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 tutje se "vështirë se piktura mund të kuptohej sikur i referohej detajeve të jetës private [të subjektit], por më së shumti qëndrimit të tij si politikan" dhe se "në këtë cilësi, [subjekti i pikturuar] duhet të tregonte me tepër tolerancë ndaj kritikës". Duke peshuar interesat e ndryshëm që luheshin, GjEDNj-ja vendosi se ndalimi i pakufizuar i ekspozimit të mëtejshëm të pikturës, ishte jo proporcional. Përfundimisht Gjykata vendosi se ishte shkelur neni 10 i KEDNj-së.

Sa i takon shkencës, legjislacioni evropian i mbrojtjes së të dhënave njeh vlerën e veçantë të shkencës në shoqëri. Rrjedhimisht, kufizimet e përgjithshme ndaj përdorimit të të dhënave personale, janë më pakta. Si Direktiva e Mbrojtjes së të Dhënave ashtu edhe Konventa 108 lejojnë ruajtjen e të dhënave për kërkime shkencore, kur këto nuk janë më të nevojshme për qëllimin fillestar të mbledhjes së tyre. Për më tepër, përdorimi i mëtejshëm i të dhënave personale për qëllime shkencore, nuk duhet të konsiderohet si qëllim i papajtueshëm. I takon legjislacioneve kombëtare të zhvillojnë dispozita më të hollësishme, përfshirë edhe ato në lidhje me masat e nevojshme të sigurisë, me qëllim që interesi për kërkimin shkencor të pajtohet me të drejtën për mbrojtje të të dhënave (shih gjithashtu paragrafët 3.3.3. dhe 8.4).

1.2.4. Mbrojtja e pronës

E drejta për mbrojtje të pronës sanksionohet nga neni 1 i Protokollit Shtesë të KEDNj-së dhe po ashtu nga neni 17 (1) i Kartës. Një aspekt i rëndësishëm i së drejtës së pronës, është mbrojtja e pronësisë intelektuale, e përmendur qartë në nenin 17 (2) të Kartës. Në rendin juridik të BE-së mund të gjenden direktiva të ndryshme, të cilat synojnë mbrojtjen e efektshme të pronësisë intelektuale dhe të së drejtës së autorit në veçanti. Pronësia intelektuale nuk mbulon vetëm pronësisë letrare dhe artistike, por edhe të patentave, markave dhe të drejta të tjera në lidhje me to.
Sikurse është qartësuar në të drejtën 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.[44] 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 cilët shfrytëzonin platformat e 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.

[43] GjEDNj, *Vereinigung bildender Künstler kundër Austrisë,* nr. 68345/01, 25 janar 2007; shih kryesisht parag. 26 dhe 34.

[44] GjEDNj, *Ashby Donald dhe të tjerët kundër Francës*, nr. 36769/08, 10 janar 2013.

Shembull: çështja *Promusicae kundër Telefónica de España*[45] kishte të bënte me refuzimin që i kishte bërë operatori i shërbimeve të internetit Telefónica që t'i jepte Promusicae-s, një organizate jo-fitimprurëse producentësh muzikorë dhe diskografikë, të dhënat personale të disa personave, të cilëve u kishte ofruar 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 shfrytëzimin të të cilave i posedonin anëtarët e Promusicae-s.

Gjykata spanjolle ia referoi çështjen GjDBE-së, për të verifikuar nëse këto të dhëna personale mund të komunikoheshin, bazuar në të drejtën e BE-së, në kuadër të procedimit civil për garantimin e mbrojtjes së efektshme të së drejtës së autorit. Gjykata u mbështet në Direktivat 2000/31, 2001/29 dhe 2004/48 si edhe referuar neneve 17 dhe 47 të Kartës. Gjykata arriti në përfundimin se këto tre direktiva, ashtu si edhe Direktiva mbi privatësinë dhe komunikimet elektronike (2002/58/KE), nuk i pengojnë Shtetet Anëtare që të përcaktojnë si të detyrueshëm komunikimin e të dhënave 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 pajtuar 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 të procedurave të efektshme të ankimit.

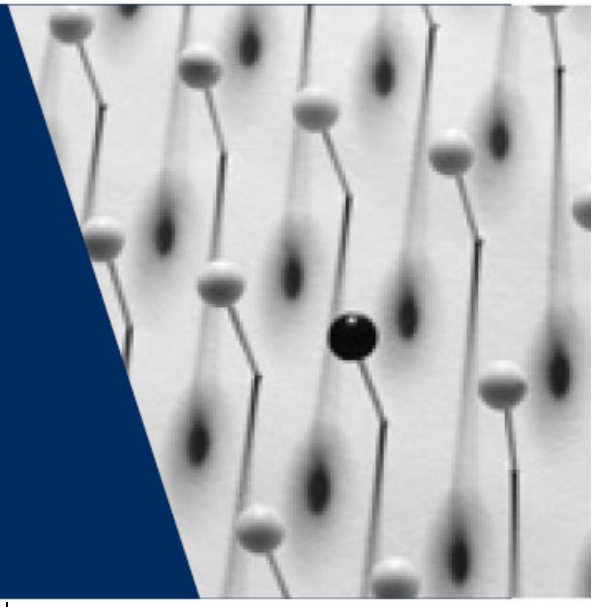
Gjykata doli në përfundimin se "Shtetet Anëtare, kur transpozojnë direktivat e lartpërmendura, duhet të kujdesen që të mbështeten në një interpretim të këtyre të fundit, të tillë që të bëjë të mundur ekuilibrimin e duhur të së drejtave të ndryshme themelore, të cilat mbrohen nga rendi juridik i Komunitetit. Në vijim, gjatë zbatimit të masave për transpozimin e këtyre direktivave, 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 të drejtat themelore të lartpërmendura, ose me parimet e tjera të përgjithshme të së drejtës së Komunitetit, sikurse me parimin e proporcionalitetit."[46]

[45] GjDBE, C-275/06, *Productores de Música de España (Promusicae) kundër Telefónica de España SAU*, 29 janar 2008, parag. 54 dhe 60.

[46] Po aty, parag. 65 dhe 68; shih gjithashtu GjDBE, C-360/10, *SABAM kundër Netlog N.V.*, 16 shkurt 2012.

2

Terminologjia e mbrojtjes së të dhënave



BE	Çështje të trajtuara	KiE
Të dhëna personale		
Direktiva e Mbrojtjes së të Dhënave, neni 2 (a) GjDBE, Çështje të bashkuara C-92/09 dhe C-93/09, *Volker dhe Markus Schecke GbR (C-92/09) dhe Hartmut Eifert (C-93/09) kundër Land Hessen*, 9 nëntor 2010 GjDBE, C-275/06, *Productores de Música de España (Promusicae) kundër Telefónica de España SAU*, 29 janar 2008	**Përkufizime ligjore**	Konventa 108, neni 2 (a) GjEDNj, *Bernh Larsen Holding AS dhe të tjerët kundër Norvegjisë*, nr. 24117/08, 14 mars 2013
Direktiva e Mbrojtjes së të Dhënave, neni 8 (1) GjDBE, C-101/01, *Bodil Lindqvist*, 6 nëntor 2003	**Kategori të veçanta të të dhënave personale** **(të dhënat sensitive)**	Konventa 108, neni 6
Direktiva e Mbrojtjes së të Dhënave, neni 6 (1) (e)	**Të dhëna të anonimizuara dhe të pseudonomizuara**	Konventa 108, neni 5 (e) Konventa 108, Raporti Shpjegues, neni 42
Përpunimi i të dhënave		
Direktiva e Mbrojtjes së të Dhënave, neni 2 (b) GjDBE, C-101/01, *Bodil Lindqvist*,6 nëntor 2003	**Përkufizime**	Konventa 108, neni 2 (c)
Përdoruesit e të dhënave		
Direktiva e Mbrojtjes së të Dhënave, neni 2 (d)	**Kontrolluesi**	Konventa 108, neni 2 (d) Rekomandimi mbi Profilizimin, neni 1 (g)*
Direktiva e Mbrojtjes së të dhënave, neni 2 (e)	**Përpunuesi**	Rekomandimi mbi Profilizimin, neni 1 (h)

GjDBE, C-101/01, *Bodil Lindqvist*, 6 nëntor 2003		
Direktiva e Mbrojtjes së të Dhënave, neni 2 (g)	**Marrësi**	Konventa 108, Protokolli Shtesë, neni 2(1)
Direktiva e Mbrojtjes së të Dhënave, neni 2 (f)	**Pala e tretë**	
Pëlqimi		
Direktiva e Mbrojtjes së të Dhënave, neni 2 (h) GjDBE, C-543/09, *Deutsche Telekom AG kundër Bundesrepublik Deutschland*, 5 maj 2011	**Përkufizime dhe norma për pëlqim të vlefshëm**	Rekomandimi mbi të Dhënat Mjekësore, neni 5 dhe rekomandime të ndryshme të mëtejshme

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

2.1. Të dhënat personale

Pikat kryesore

- Të dhënat janë të dhëna personale kur kanë lidhje me një person të identifikuar ose të identifikueshëm, subjektin e të dhënave.
- Personi është i identifikueshëm nëse mund të merret informacion shtesë pa përpjekje të paarsyeshme, që mundëson identifikimin e subjektit të të dhënave.
- Me autentifikim kuptohet procesi që synon të verifikojë që një person i caktuar zotëron një identitet të caktuar dhe/ose është i autorizuar të kryejë disa aktivitete të caktuara.
- Ekzistojnë kategori të veçanta të dhënash, të ashtuquajturat "të dhëna sensitive", të radhitura në Direktivën e Mbrojtjes së të Dhënave, për të cilat nevojitet mbrojtje më e madhe dhe për rrjedhojë janë subjekt i një regjimi ligjor specifik.
- Të dhënat janë të anonimizuara nëse nuk përmbajnë më asnjë identifikues, ndërsa janë të pseudonimizuara nëse identifikuesit janë të kriptuar.
- Ndryshe nga të dhënat e anonimizuara, të dhënat e pseudonimizuara janë të dhëna personale.

2.1.1. Aspektet kryesore të konceptit të të dhënave personale

Në kuadër të **së drejtës së BE-së** dhe të **së drejtës së KiE-së**, "të dhënat personale" përkufizohen si çdo lloj informacioni në lidhje me një person fizik, të identifikuar ose të identifikueshëm,[47] domethënë informacioni në lidhje me një person, identiteti i së cilit është haptazi i qartë ose të paktën mund të përcaktohet nëpërmjet marrjes së informacionit shtesë.

[47] Direktiva e Mbrojtjes së të Dhënave, neni. 2 (a); Konventa 108, neni. 2 (a).

Nëse të dhënat në lidhje me këtë person përpunohen, ky person quhet “subjekti i të dhënave”.

Personi

E drejta për mbrojtje të të dhënave buron nga e drejta për respektim të jetës private. Koncepti i jetës private lidhet me qeniet njerëzore. Prandaj, personat fizikë janë përfituesit parësorë të mbrojtjes së të dhënave. Për më tepër, sipas Opinionit të Grupit të Punës së Nenit 29, vetëm një *qenie njerëzore që jeton,* mbrohet nga legjislacioni evropian për mbrojtjen e të dhënave.[48]

Jurisprudenca e GjEDNj-së sa i takon nenit 8 të KEDNj-së, vë në dukje se mund të jetë e vështirë të ndahen krejtësisht çështjet e jetës private me ato profesionale.[49]

Shembull: tek çështje *Amann kundër Zvicrës*,[50] autoritetet kishin përgjuar një telefonatë pune të ankuesit. Bazuar në atë telefonatë, autoritetet hetuan ankuesin 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, cënonte jetën private të ankuesit. 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 ankuesit, 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.

Për më tepër, nëse çështjet që lidhen me jetën profesionale, mund të jenë gjithashtu subjekt i mbrojtjes së të dhënave, ngrihet pyetja nëse vetëm personat fizikë duhet të gëzojnë mbrojtje. Sipas KEDNj-së, të drejtat nuk u garantohen vetëm personave fizikë, por të gjithëve.

Jurisprudenca e GjEDNj-së përmban disa vendime gjyqësore, në lidhje me padi të depozituara nga persona juridikë, që pretendojnë shkelje të së drejtës për mbrojtje nga përdorimi i të dhënave të tyre, bazuar në nenin 8 të KEDNj-së. Gjithsesi, Gjykata shqyrtoi këto çështje bazuar mbi të drejtën për respektim të banesës dhe korrespondencës dhe jo mbi të drejtën e jetës private:

[48] Grupi i Punës së Nenit 29 (2007), Opinioni 4/2007 mbi konceptin e të dhënave personale, WP 136, 20 qershor 2007, fq. 22.
[49] Shih për shembull: GjEDNj, *Rotaru kundër Rumanisë* [GC], nr. 28341/95, 4 maj 2000, parag. 43; GjEDNj, *Niemietz kundër Gjermanisë*, 13710/88, 16 dhjetor 1992, parag. 29.
[50] GjEDNj, *Amann kundër Zvicrës* [GC], nr. 27798/95, 16 shkurt 2000, parag. 65.

Shembull: çështja *Bernh Larsen Holding AS dhe të Tjerët kundër Norvegjisë*[51] kishte të bënte me një ankesë të tre kompanive norvegjeze kundër vendimit të një autoriteti tatimor, i cili i urdhëronte t'u jepnin inspektorëve tatimorë një kopje të të gjitha të dhënave të një serveri kompjuterik, të cilin e përdornin të tre së bashku.

GjEDNj-ja vuri në dukje se një detyrim i tillë nga ana e kompanive ankuese, përbënte ndërhyrje në të drejtat e tyre për respektim të "banesës" dhe "korrespondencës", bazuar në nenin 8 të KEDNj-së. Gjithsesi Gjykata vlerësoi se autoritetet tatimore ofronin garanci të efektshme dhe të përshtatshme për të parandaluar çdo shkelje: kompanitë ankuese ishin njoftuar shumë kohë më përpara; ato ishin të pranishme dhe kishin mundësi të bënin vërejtje gjatë inspektimit në ambientet e tyre; dhe materialet e përdorura për inspektimin tatimor, do të shkatërroheshin pas përfundimit të tij. Në këto rrethana, ishte gjetur ekuilibri i drejtë midis së drejtës së kompanive ankuese për respektim të "banesës" dhe "korrespondencës" dhe interesit të tyre për mbrojtjen e privatësisë të të punësuarve të tyre, nga njëra anë, me interesin publik për të siguruar inspektim të efektshëm për qëllime të auditit tatimor, nga ana tjetër. Në këto kushte, Gjykata vendosi se nuk kishte pasur shkelje të nenit 8.

Sipas Konventës 108, synimi parësor i mbrojtjes së të dhënave janë personat fizikë; gjithsesi, palët kontraktuese mund ta shtrijnë mbrojtjen e të dhënave në legjislacionin e tyre kombëtar, edhe tek personat juridikë, si për shembull tek kompanitë tregtare dhe shoqatat.

E drejta e BE-së në fushën e mbrojtjes së të dhënave, në përgjithësi nuk mbulon personat juridikë, për sa i takon përpunimit të të dhënave që kanë të bëjnë me ta. Ligjbërësit kombëtarë janë të lirë të përcaktojnë norma në lidhje me këtë fushë.[52]

Shembull: tek çështja *Volker dhe Markus Schecke dhe Hartmut Eifert kundër Land Hessen-it*,[53] GjDBE-ja, duke iu referuar publikimit të të dhënave personale që kishin të bënin me përfituesit e ndihmës bujqësore, vuri në dukje 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 emërtesa ligjore e personit juridik, identifikon një apo më shumë persona fizikë. [...E] drejta për respektim të jetës private 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 [...]."[54]

[51] GjEDNj, *Bernh Larsen Holding AS dhe të Tjerët kundër Norvegjisë*, nr. 24117/08, 14 mars 2013. Gjithsesi, shih gjithashtu, GjEDNj, *Liberty dhe të Tjerët kundër Mbretërisë së Bashkuar*, nr. 58243/00, 1 korrik 2008.
[52] Direktiva e Mbrojtjes së të Dhënave, pika 24.
[53] GjDBE, Çështje të bashkuara C-92/09 and C-93/09, *Volker dhe Markus Schecke GbR (C-92/09) dhe Hartmut Eifert (C-93/09) kundër Land Hessen-it*, 9 nëntor 2010, parag. 53.
[54] Po aty, parag. 52.

Identifikueshmëria e një personi

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

- Një individ është i identifikuar në këtë informacion; ose
- Një individ, edhe pse nuk është i identifikuar, përshkruhet në këtë informacion në mënyrë të tillë që e bën të mundur zbulimin e subjektit të të dhënave, nëpërmjet kërkimeve të mëtejshme.

Të dyja llojet e informacioneve mbrohen në të njëjtën mënyrë nga legjislacioni evropian i mbrojtjes së të dhënave. GjEDNj-ja është shprehur në mënyrë të përsëritur se nocioni i "të dhënave personale" sipas KEDNj-së, është i njëjti si në Konventën 108, veçanërisht sa i takon normës sipas së cilës ato duhet të lidhen me persona të identifikuar apo të identifikueshëm.[55]

Përkufizimet ligjore të të dhënave personale, nuk qartësojnë më shumë kur një person konsiderohet si i identifikuar.[56] Në mënyrë të qartë, identifikimi kërkon elemente të cilat përshkruajnë personin në mënyrë të tillë që ai ose ajo të jetë i dallueshëm nga të gjithë personat e tjerë dhe që të mund të njihet si individ. Emri i personit është një shembull i dorës së parë i këtyre lloj elementesh të përshkrimit. Në raste të veçanta, identifikues të tjerë mund të kenë efekt të ngjashëm me emrin. Për shembull, për figurat publike, mjafton t'i referohemi pozicionit të personit, sikurse Presidenti i Komisionit Evropian.

Shembull: për çështjen *Promusicae*,[57] GjDBE-ja u shpreh se "nuk ka kundërshtim se komunikimi i kërkuar nga Promusicae-ja i emrave dhe adresave të disa përdoruesve [të një platforme të caktuar të shkëmbimit të skedarëve në internet], nënkupton vënien në dispozicion të të dhënave personale, të cilat janë informacione në lidhje me persona fizikë të identifikuar ose të identifikueshëm, në përputhje me përkufizimin e nenit 2 (a) të Direktivës 95/46 [...]. Ky komunikim informacioni, i cili sipas Promusicae-s, ruhet nga Telefónica, gjë që kjo e fundit nuk e mohon, përbën përpunim të dhënash personale, sipas kuptimit të paragrafit të parë të nenit 2 të Direktivës 2002/58, e lexuar në mënyrë të kombinuar me nenin 2 (b) të Direktivës 95/46".

Meqenëse shume emra nuk janë unikë, për përcaktimin e identitetit të një personi, mund të nevojiten identifikues të tjerë shtesë, për t'u siguruar që një person nuk ngatërrohet me dikë tjetër. Data dhe vendi i lindjes përdoren shpesh. Gjithashtu, numrat e personalizuar përdoren në shumë vende, me qëllim që qytetarët të dallohen më mirë nga njëri-tjetri. Të dhënat biometrike, sikurse gjurmët e gishtave, fotografitë digjitale apo skanimi i syrit, po bëhen gjithnjë e më të rëndësishme për identifikimin e personave në epokën teknologjike.

---

[55] Shih GjEDNj, *Amann kundër Zvicrës* [GC], nr. 27798/95, 16 shkurt 2000, parag. 65 e të tjerë.
[56] Shih gjithashtu GjEDNj, *Odièvre kundër Francës* [GC], nr. 42326/98, 13 shkurt 2003; dhe GjEDNj, *Godelli kundër Italisë*, nr. 33783/09, 25 shtator 2012.
[57] GjDBE, C-275/06, *Productores de Música de España (Promusicae) kundër Telefónica de España SAU*, 29 janar 2008, parag. 45.

Gjithsesi, me qëllim që legjislacioni evropian i mbrojtjes së të dhënave të jetë i zbatueshëm, nuk ka nevojë për identifikim të nivelit të lartë të subjektit të të dhënave; mjafton që ai të jetë i identifikueshëm. Personi konsiderohet i identifikueshëm nëse informacioni përmban elemente të identifikimit, nëpërmjet të cilëve personi mund të identifikohet, drejtpërdrejt ose tërthorazi.[58] Sipas pikës 26 të Direktivës së Mbrojtjes së të Dhënave, pika e referimit është nëse ka gjasa që përdoruesit e mundshëm të informacioneve të zotërojnë apo administrojnë mjete të arsyeshme për kryerjen e identifikimit; kjo përfshin edhe marrësit e tretë (shih paragrafin 2.3.2).

Shembull: një autoritet lokal kishte vendosur të mblidhte të dhëna në lidhje me automjetet, të cilat qarkullonin më shpejtësi të madhe në rrugët e qytetit, nëpërmjet fotografimit të mjeteve, duke regjistruar automatikisht kohën dhe vendndodhjen, me qëllim që t'ia përcillte ato të dhëna autoritetit kompetent, në mënyrë që ky i fundit të gjobiste ata që qarkullonin tej normave të lejuara të shpejtësisë. Një subjekt të dhënash depoziton një ankesë, me pretendimin se autoriteti lokal nuk kishte bazë ligjore për këtë lloj mbledhje të dhënash, duke iu referuar legjislacionit për mbrojtjen e të dhënave. Autoriteti lokal pretendonte se nuk mblidhte të dhëna personale. Numrat serialë të targave, sipas tij, janë të dhëna në lidhje me persona anonimë. Autoriteti lokal nuk ka kompetencë ligjore të hyjë në sistemin qendror të targave, për të zbuluar identitetin e pronësisë së mjetit apo drejtuesit.

Ky arsyetim nuk përputhet me pikën 26 të Direktivës së Mbrojtjes së të Dhënave. Duke qenë se qëllimi i mbledhjes së të dhënave është qartësisht identifikimi dhe gjobitja e kundërvajtësve, është lehtësisht e parashikueshme se do të kryhen orvatje për identifikimin e tyre. Edhe pse autoritetet lokale nuk kanë mjete për identifikimin e drejtpërdrejtë, ata do t'ua përcjellin të dhënat autoritetit kompetent, policisë, e cila i ka këto mjete. Gjithashtu, pika 26 përfshin qartësisht rastet kur parashikohet se marrësit e mëtejshëm të të dhënave, pra jo përdoruesit fillestarë, mund të përpiqen të identifikojnë individin. Bazuar në pikë 26, veprimi i autoriteti lokal përkon me mbledhjen e të dhënave në lidhje me një person të identifikueshëm dhe për rrjedhojë, kërkon bazë ligjore referuar legjislacionit të mbrojtjes së të dhënave.

Tek e drejta e KiE-së, identifikueshmëria kuptohet në mënyrë të ngjashme. Neni 1 (2) i Rekomandimit për të Dhënat e Pagesave,[59] për shembull nënvizon se personi nuk duhet të konsiderohet "i identifikueshëm", në rast se identifikimi kërkon një sasi kohore, kosto apo përpjekje fizike të paarsyeshme.

[58] Direktiva e Mbrojtjes së të Dhënave, neni 2 (a).

[59] KiE, Komiteti i Ministrave (1990), Rekomandim nr. R Rec(90) 19 për mbrojtjen e të dhënave personale, të përdorura për pagesa dhe veprime të tjera të lidhura me to, 13 shtator 1990.

Autentifikimi

Autentifikimi është procedura nëpërmjet së cilës një person mund të provojë se ai apo ajo zotëron një identitet të caktuar dhe/ose është i autorizuar të bëjë disa veprime, sikurse të hyjë në një zonë të sigurisë së lartë, ose të tërheqë para nga një llogari bankare. Autentifikimi mund të kryhet me anë të krahasimit të të dhënave biometrike, si për shembull me anë të fotografisë apo gjurmëve të gishtave në një pasaportë, me anë të të dhënave të personit kur ai prezanton veten e tij apo të saj, për shembull në një pikë kontrolli kufitar; ose me anë të pyetjeve për informacionin të cilin duhet ta dijë vetëm personi me identitet apo autorizim të caktuar, sikurse numrin e identifikimit personal (PIN) apo lejekalimin; ose me anë të paraqitjes së 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 në një kasafortë bankare. Përveç lejekalimeve ose kartave me çip, të cilat herë-herë shoqërohen me kode PIN, nënshkrimet elektronike janë instrumente veçanërisht të afta të identifikojnë ose autentifikojnë një person në komunikimet elektronike.

Natyra e të dhënave

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

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 përfshijnë informacionin që i përket jetës private të një personi, ashtu si edhe informacionin në lidhje me jetën profesionale apo publike të tij apo të saj.

Tek çështja *Amann*,[60] GjEDNj-ja e interpretoi termin "të dhëna personale" si jo të kufizuar thjesht në çështjet e sferës private së një individi (shiko paragrafin 2.1.1.). Ky kuptim i termit "të dhëna personale" është po ashtu i vlefshëm edhe për Direktivën e Mbrojtjes së të Dhënave:

Shembull: tek çështja *Volker and Markus Schecke dhe Hartmut Eifert kundër Land Hessen-it*, [61]GjDBE-ja theksoi se "sa i përket kësaj, nuk asnjë rëndësi nëse të dhënat e publikuara kanë të bëjnë me aktivitete të natyrës profesionale [...]. Gjykata Evropiane e të Drejtave të Njeriut është shprehur në lidhje me këtë pikë, duke iu referuar interpretimit të nenit 8 të Konventës, se termi "jetë private' nuk duhet interpretuar në mënyrë të kufizuar dhe se nuk asnjë arsye parimore për të justifikuar përjashtimin e aktiviteteve me natyrë [...] profesionale nga nocioni i jetës private".

---

[60] Shih GjEDNj, *Amann kundër Zvicrës*, nr. 27798/95, 16 shkurt 2000, parag. 65.

[61] GjDBE, Çështje të bashkuara C-92/09 dhe C-93/09, *Volker und Markus Schecke GbR dhe Hartmut Eifert kundër Land Hessen*, 9 nëntor 2010, parag. 59.

Të dhënat lidhen me personat nëse përmbajtja e informacionit zbulon tërthorazi të dhëna në lidhje me një person. Në disa raste, kur ka lidhje të ngushtë midis një objekti apo ngjarjeje – p.sh. një telefon celular, një auto-veturë, një aksident – nga njëra anë dhe një personi – p.sh. pronari, përdoruesi, viktima – nga ana tjetër, informacioni në lidhje me një objekt apo në lidhje me një ngjarje, duhet gjithashtu të konsiderohet e dhënë personale.

Shembull: tek çështja *Uzun kundër Gjermanisë,*[62] ankuesi dhe një person tjetër, ishin vënë nën përgjim nëpërmjet një pajisjeje me sistem global pozicionimi (GPS), të instaluar në automjetin e personit tjetër, për arsye të dyshimeve në lidhje me një sulm me lëndë shpërthyese. Në këtë rast, GjEDNj-ja vlerësoi se survejimi i ankuesit nëpërmjet GPS-it, përbënte ndërhyrje në jetën e tij private, bazuar në mbrojtjen e nenit 8 të KEDNj-së. Gjithsesi, survejimi me GPS kishte qenë në përputhje me ligjin, sikundër edhe proporcionale me qëllimin legjitim të hetimit të disa akuzave për tentativë vrasjeje dhe për rrjedhojë, ishte i nevojshëm në një shoqëri demokratike. Gjykata vendosi se nuk kishte pasur shkelje të nenit 8 të KEDNj-së.

Formati i të dhënave

Forma me të cilën ruhen ose përdoren të dhënat, nuk është e rëndësishme sa i takon zbatueshmërisë së legjislacionit të mbrojtjes së të dhënave. Komunikimet me shkrim apo me gojë, mund të përmbajnë të dhëna personale, e njëjta vlen edhe për imazhet,[63] përfshirë edhe pamjet[64] ose tingujt[65] e nxjerra nga televizioni me qark të mbyllur (CCTV). Informacionet e regjistruara elektronikisht, ashtu si edhe informacionet e shkruara në letër, mund të jenë të dhëna personale; edhe kampionët e qelizave të indeve njerëzore, mund të jenë të dhëna personale, për shkak se regjistrojnë ADN-në e personit.

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 të dhënave personale, të cilat për shkak të natyrës së tyre, mund të përbëjnë rrezik për subjektin e të dhënave kur përpunohen dhe për këtë shkak duhet të gëzojnë mbrojtje me të madhe. Ndaj, përpunimi i këtyre kategorive të veçanta të të dhënave ("të dhënave sensitive"), duhet lejuar vetëm nëse ofrohen garanci specifike.

---

[62] GjEDNj, *Uzun kundër Gjermanisë*, nr. 35623/05, 2 shtator 2010.
[63] GjEDNj, *Von Hannover kundër Gjermanisë*, nr. 59320/00, 24 qershor 2004; GjEDNj, *Sciacca kundër Italisë,* nr. 50774/99, 11 janar 2005.
[64] GjEDNj, *Peck kundër Mbretërisë së Bashkuar*, nr. 44647/98, 28 janar 2003; GjEDNj, *Köpke kundër Gjermanisë*, nr. 420/07, 5 tetor 2010.
[65] Direktiva e Mbrojtjes së të Dhënave, pikat 16 dhe 17; GjEDNj, *P.G. dhe J.H. kundër Mbretërisë së Bashkuar*, nr. 44787/98, 25 shtator 2001, parag. 59 dhe 60, GjEDNj, *Wisse kundër Francës*, nr. 71611/01, 20 dhjetor 2005.

Tek përkufizimi i të dhënave sensitive, si Konventa 108 (neni 6), ashtu edhe Direktiva e Mbrojtjes së të Dhënave (neni 8), radhisin kategoritë e mëposhtme:

- Të dhëna personale që tregojnë origjinën racore apo etnike;
- Të dhëna personale që tregojnë mendimet politike, fetare dhe besimet e tjera; dhe
- Të dhëna personale në lidhje me shëndetin ose jetën seksuale.

Shembull: tek *Bodil Lindqvist*,[66] GjDBE-ja u shpreh se "duke iu referuar faktit që një person ka plagosur këmbën dhe është me raport mjekësor, kjo duhet konsideruar si e dhënë personale në lidhje me shëndetin, në kuptimin e nenit 8 (1) të Direktivës 95/46."

Direktiva e Mbrojtjes së të Dhënave radhit gjithashtu "anëtarësinë në sindikata" si e dhënë sensitive, duke qenë se ky lloj informacioni mund të jetë indikator i fortë i bindjeve apo përkatësisë politike.

Konventa 108 vlerëson gjithashtu të dhënat personale në lidhje me dënimet penale, si të dhëna sensitive.

Neni 8 (7) i Direktivës së Mbrojtjes së të Dhënave detyron Shtetet Anëtare të BE-së "të përcaktojnë kushtet sipas së cilave një numër kombëtar identifikimi apo çdo lloj mjeti tjetër identifikues mund të jetë objekt përpunimi".

2.1.3. Të dhënat e anonimizuara dhe të pseudonimizuara

Sipas parimit të ruajtjes së kufizuar të të dhënave, të përcaktuar në Direktivën e Mbrojtjes së të Dhënave, ashtu si edhe në Konventën 108 (dhe i cili do të trajtohet më në hollësi në Kapitullin 3), të dhënat duhen të ruhen "më mënyrë të tillë që të mundësojnë identifikimin e subjekteve të të dhënave, për një kohë jo më të gjatë se sa është e nevojshme për përmbushjen e qëllimeve për të cilat u mblodhën të dhënat, apo për të cilat u përpunuan më tej."[67] Rrjedhimisht, të dhënat do të duhet të anonimizohen në rast se kontrolluesi dëshiron t'i ruajë edhe pasi ato bëhen të pavlefshme dhe nuk i shërbejnë më qëllimit fillestar.

Të dhënat e anonimizuara

Të dhënat konsiderohen të anonimizuara nëse të gjithë elementet identifikuese janë eliminuar nga një tërësi të dhënash personale. Asnjë element nuk duhet lënë në informacionin i cili mund të shërbejë për ri-identifikimin e subjektit/eve të përfshira, duke ushtruar përpjekje të arsyeshme.[68] Kur të dhënat janë anonimizuar me sukses, ato nuk konsiderohen më të dhëna personale.

---

[66] GjDBE, C-101/01, *Bodil Lindqvist*, 6 nëntor 2003, parag. 51.
[67] Direktiva e Mbrojtjes së të Dhënave, neni 6 (1) (e); dhe Konventa 108, neni 5 (e).
[68] Po aty, pika 26

Nëse të dhënat personale nuk i shërbejnë më qëllimit fillestar, por duhen ruajtur në një formë të personalizuar, për qëllime historike, statistikore ose shkencore, Direktiva e Mbrojtjes së të Dhënave dhe Konventa 108, e lejojnë këtë, me kusht që të ketë garanci të përshtatshme për mbrojtje nga abuzimet e mundshme.[69]

Të dhënat e pseudonimizuara

Informacionet personale përmbajnë elemente identifikuese, sikundër janë emri, datëlindja, gjinia dhe adresa. Kur informacionet personale janë të pseudonimizuara, elementet identifikuese zëvendësohen me një pseudonim. Pseudonimizimi arrihet për shembull me anë të enkriptimit të elementeve identifikuese tek të dhënat personale.

Të dhënat e pseudonimizuara nuk përmenden në mënyrë të qartë në përkufizimet ligjore të Konventës 108 dhe të Direktivës së Mbrojtjes së të Dhënave. Gjithsesi, në nenin 42 të Raportit Shpjegues të Konventës 108, përcaktohet se "detyrimi [...] në lidhje me afatet kohore të ruajtjes së të dhënave në formën e tyre nominative, nuk nënkupton se të dhënat duhet të ndahen në mënyrë të pakthyeshme nga emri i personit me të cilin ato lidhen, por vetëm se nuk duhet të jetë lehtësisht e mundshme të lidhen të dhënat me elementet identifikues." Ky efekt mund të përftohet duke pseudonimizuar të dhënat. Për cilindo që nuk zotëron çelësin e dekriptimit, të dhënat e pseudonimizuara mund të jetë e vështirë të identifikohen. Lidhja me identitetin ekziston ende me formën e pseudonimit, i cili shoqërohet me çelësin e dekriptimit. Për ata të cilët kanë të drejtë të përdorin çelësin e dekriptimit, ri-identifikimi është lehtësisht i mundshëm. Duhet kushtuar vëmendje e veçantë për të shmangur përdorimin e çelësave të enkriptimit nga persona të paautorizuar.

Duke qenë se pseudonimizimi i të dhënave është një nga mjetet më të rëndësishme për të përftuar mbrojtje të dhënash në shkallë të gjerë, logjika dhe efekti i një veprimi të tillë, duhet shpjeguar më në hollësi, në rastet kur nuk është e mundur të shmanget krejtësisht përdorimi i të dhënave personale.

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

"C.S 1967 është babai i një familjeje me katër fëmijë, dy djem dhe dy vajza"; ose
"324 është babai i një familjeje me katër fëmijë, dy djem dhe dy vajza"; ose
"YESz320I është babai i një familjeje me katër fëmijë, dy djem dhe dy vajza".

Përdoruesit të cilët kanë akses në të dhënat e pseudonimizuara, nuk kanë mundësi të identifikojnë "Charles Spencer-in, të lindur më 3 prill 1967" nga "324-a" ose nga "YESz320I-ja". Për rrjedhojë, të dhënat e psudonimizuara kanë të ngjarë të jenë më të mbrojtura nga keqpërdorimi.

---

[69] Po aty, neni 6, parag.1, pika e; dhe Konventa 108, neni 5, pika e.

Gjithsesi, shembulli i parë është më pak i sigurt. Nëse fjalia "C.S. 1967 është babai i një familjeje me katër fëmijë, dy djem dhe dy vajza" përdoret brenda një fshati të vogël, ku jeton Charles Spencer-i, atëherë z. Spencer mund të njihet lehtësisht. Metoda e pseudonimizimit, prek efikasitetin e mbrojtjes së të dhënave.

Të dhënat personale të cilat përmbajnë elemente identifikuese, përdoren në kontekste të ndryshme, si mënyrë për të mbajtur sekret identitetin e personave. Kjo mënyrë është veçanërisht e dobishme kur kontrolluesit e të dhënave kanë nevojë të binden se bëhet fjalë për të njëjtët subjekte të dhënash për të cilët interesohen, por nuk u nevojitet, ose nuk duhet t'u nevojitet, të njohin identitetin e vërtetë të subjekteve të të dhënave. Një rast i tillë mund të jetë për shembull kur një kërkues shkencor studion evoluimin e një sëmundjeje tek pacientët, identitetin e të cilëve e njohin vetëm në spitalin kur ata po trajtohen dhe nga i cili kërkuesi merr historikun e pseudonimizuar. Për këtë arsye, pseudonimizimi është një armë e fortë në arsenalin e teknologjive të cilat përmirësojnë mbrojtjen e privatësisë. Ai mund të veprojë si një element i rëndësishëm për zbatimin e privatësisë që nga konceptimi ("*privacy by design*"), e cila do të thotë që mbrojtja e të dhënave integrohet në rrjetet e sistemeve të përparuara të përpunimit të të dhënave.

2.2. Përpunimi i të dhënave

Pikat kryesore

- Termi "përpunim" i referohet kryesisht përpunimit automatik.
- Sipas së drejtës së BE-së, "përpunimi" i referohet gjithashtu edhe përpunimit manual në sistemet e strukturuara të arkivimit.
- Sipas së drejtës së KiE-së, kuptimi i termit "përpunim" mund të zgjerohet nga legjislacioni kombëtar, për të përfshirë në të edhe përpunimin manual.

Mbrojtja e të dhënave bazuar në Konventën 108 dhe në Direktivën e Mbrojtjes së të Dhënave, përqendrohet kryesisht në përpunimin automatik të të dhënave.

Sipas **së drejtës së KiE-së**, përkufizimi i përpunimit automatik pranon gjithsesi faktin se disa etapa të përdorimit manual të të dhënave personale, mund të nevojiten ndërmjet veprimeve të automatizuara. Në mënyrë të ngjashme, sipas së drejtës së BE-së, përpunimi automatik i të dhënave përkufizohet si "veprime të kryera mbi të dhënat personale, tërësisht ose pjesërisht me anë të mjeteve automatike".[70]

[70] Konventa 108, neni 2 (c); dhe Direktiva e Mbrojtjes së të Dhënave, neni 2 (b) dhe neni 3 (1).

Shembull: tek çështja *Bodil Lindqvist*,[71] GjDBE-ja u shpreh se:

"akti i të referuarit, në një faqe interneti, të disa personave dhe identifikimi i tyre me emër ose me mënyra të tjera, për shembull duke vënë në dispozicion numrat e tyre të telefonit apo informacion në lidhje me kushtet e tyre të punës apo si e kalojnë kohën e lirë, përbën "përpunim të të dhënave personale, tërësisht ose pjesërisht me anë të mjeteve automatike" sipas kuptimit të nenit 3 (1) të Direktivës 95/46."

Përpunimi manual i të dhënave kërkon gjithashtu mbrojtje të të dhënave.

Sipas **së drejtës së BE-së**, mbrojtja e të dhënave nuk është në asnjë mënyrë e kufizuar tek përpunimi automatik i të dhënave. Në përputhje me këtë, sipas së drejtës së BE-së, mbrojtja e të dhënave zbatohet edhe për përpunimin e të dhënave personale në një sistem manual arkivimi, që nënkupton fashikujt prej letre, të strukturuar në mënyrë specifike.[72] Arsyeja për këtë shtrirje të mbrojtjes së të dhënave është se:

- Fashikujt e letrës mund të strukturohen në mënyrë të tillë që të mundësojë gjetjen e informacionit shpejt dhe me lehtësi; dhe
- Ruajtja e të dhënave personale në fashikuj letre të strukturuara, e bën të lehtë shmangien nga kufizimeve të përcaktuara me ligj për përpunimin automatik të të dhënave.[73]

Sipas **së drejtës së KiE-së**, Konventa 108 rregullon kryesisht përpunimin e të dhënave në dosjet e automatizuara të të dhënave.[74] Gjithsesi, ajo parashikon mundësinë e shtrirjes së mbrojtjes mbi përpunimin manual tek legjislacioni kombëtar. Shumë Palë të Konventës 108 e kanë përdorur këtë mundësi dhe i kanë drejtuar Sekretarit të Përgjithshëm të KiE-së një deklaratë për këtë qëllim.[75] Shtrirja e mbrojtjes së të dhënave bazuar në një deklaratë të tillë, duhet t'i përkasë të gjitha përpunimeve manuale të të dhënave dhe nuk mund të kufizohet vetëm tek përpunimi në sistemet manuale të arkivimit.[76]

Ndërsa për sa i përket natyrës së veprimeve të përfshira të përpunimit, koncepti i këtij të fundit është gjithëpërfshirës, si bazuar tek e drejta e BE-së ashtu edhe tek e KiE-së: "përpunim i të dhënave personale" [...] do të thotë çdo veprim të kryer mbi të dhënat personale [...] sikurse mbledhja, regjistrimi, organizimi, ruajtja, përshtatja apo modifikimi, ekstraktimi, konsultimi, përdorimi, komunikimi nëpërmjet transmetimit, përhapja apo çfarëdo forme tjetër e vënies në dispozicion, krahasimi apo kombinimi, bllokimi, fshirja apo shkatërrimi"[77] Termi "përpunim" përfshin gjithashtu veprimet në kuadër të të cilave të dhënat kalojnë nga përgjegjësia e një kontrolluesi tek një kontrollues tjetër.

---

[71] GjDBE, C-101/01, *Bodil Lindqvist*, 6 nëntor 2003, parag. 27.
[72] Direktiva e Mbrojtjes së të Dhënave, neni 3 (1).
[73] Po aty, pika 27.
[74] Konventa 108, neni 2 (b).
[75] Shih deklaratat e bëra bazuar në Konventën 108, neni 3 (2) (c).
[76] Shih formulimin e Konventës 108, neni 3 (2).
[77] Direktiva e Mbrojtjes së të Dhënave, neni 2 (b). Gjithashtu shih Konventën 108, neni 2 (c).

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 saj 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", bazuar në përkufizimin e këtij termi në Konventën 108 dhe në Direktivë. 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 transferimin 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, transferimi i të dhënave do të përbënte përpunim të paligjshëm.

2.3. Përdoruesit e të dhënave personale

Pikat kryesore

- Referuar legjislacionit të mbrojtjes së të dhënave, cilido që vendos të përpunojë të dhënat personale të të tjerëve, është "kontrollues"; nëse disa persona e marrin këtë vendim së bashku, ata mund të jenë "kontrollues të përbashkët".
- "Përpunuesi" është një njësi ligjore më vete, që përpunon të dhëna personale për llogari të një kontrolluesi.
- Cilido që përfton të dhëna nga një kontrollues është "marrës".
- "Palë e tretë" është një person fizik ose juridik, i cili nuk vepron sipas udhëzimeve të kontrolluesit (dhe nuk është subjekti i të dhënave).
- "Palë e tretë marrëse" është personi apo njësia që është veçmas nga një kontrollues, por përfton të dhëna personale nga një kontrollues.

2.3.1. Kontrolluesit dhe përpunuesit

Pasoja më e rëndësishme e funksionit të kontrolluesit apo përpunuesit është përgjegjësia ligjore për respektim të detyrimeve përkatëse, të parashikuara në legjislacionin e fushës së mbrojtjes së të dhënave. Vetëm personat që mund të konsiderohen përgjegjës sipas legjislacionit të fushës, munden kështu të ushtrojnë këtë funksion. Në sektorin privat, ai zakonisht është një person fizik ose juridik; në sektorin publik është zakonisht një autoritet. Njësitë e tjera, sikurse organizmat apo institucionet pa identitet ligjor, mund të jenë kontrollues ose përpunues, vetëm kur dispozitat e veçanta ligjore e parashikojnë këtë.

Shembull: Kur seksioni i marketingut të shoqërisë Sunshine planifikon të përpunojë të dhëna për një studim të tregut, shoqëria Sunshine dhe jo seksioni i marketingut, do të jetë kontrolluesi i këtij përpunimi. Seksioni i marketingut nuk mund të jetë kontrolluesi, për arsye se nuk ka identitet ligjor të veçantë.

Në grupe shoqërish, shoqëria mëmë dhe secili filial, duke qenë se janë persona juridikë të veçantë, përbëjnë secili kontrollues ose përpunues më vete. Si rrjedhojë e këtij statusi ligjor të veçantë, për transferimin e të dhënave ndërmjet anëtarëve të një grupi shoqërish, nevojitet

bazë ligjore specifike. Nuk ekziston asnjë privilegj që të mundësojë shkëmbimin e të dhënave personale si të tillë, ndërmjet njësive të veçanta ligjore brenda grupit të shoqërive.

Në këtë kontekst, vlen të përmendet roli i individëve privatë. Sipas së drejtës së BE-së, individët privatë, kur përpunojnë të dhëna të të tretëve, në kuadër të aktivitetit me karakter thjesht personal apo familjar, nuk janë subjekt i rregullave të Direktivës së Mbrojtjes së të Dhënave, për këtë arsye nuk konsiderohen kontrollues.[78]

Gjithsesi, jurisprudenca ka vlerësuar se legjislacioni në fushën e mbrojtjes së të dhënave, gjen sidoqoftë zbatim në rastin kur një person privat publikon të dhëna në lidhje me të tretët, gjatë përdorimit të internetit.

Shembull: GjDBE-ja u shpreh për çështjen *Bodil Lindqvist*[79] se:

"akti i të referuarit, në një faqe interneti, të disa personave dhe identifikimi i tyre me emër ose me mënyra të tjera [...] përbën "përpunim të të dhënave personale, tërësisht ose pjesërisht me anë të mjeteve automatike" sipas kuptimit të nenit 3 (1) të Direktivës 95/46."[80]

Ky lloj përpunimi të dhënash personale nuk bën pjesë në aktivitetet thjesht personale apo familjare, të cilat janë jashtë fushës së zbatimit të Direktivës së Mbrojtjes së të Dhënave, duke qenë se ky përjashtim "duhet [...] të interpretohet si në lidhje vetëm me aktivitetet të cilat kryhen në kuadër të jetës private ose familjare të individëve, gjë që qartësisht nuk është rasti i përpunimit të të dhënave personale i cili konsiston në publikimin në internet, në mënyrë të tillë që ato të dhëna të jenë të disponueshme për një numër të pakufizuar njerëzish."[81]

Kontrolluesi

Sipas së drejtës së BE-së, kontrolluesi përkufizohet si dikush që "vetëm ose së bashku me të tjerë, përcakton qëllimet dhe mjetet e përpunimit të të dhënave personale".[82] Vendimi i kontrolluesit përcakton pse dhe si do të përpunohen të dhënat. **Sipas së drejtës së KiE-së**, përkufizimi i "kontrolluesit" përfshin gjithashtu që kontrolluesi vendos se cilat kategori të dhënash personale duhet të ruhen.[83]

Konventa 108, tek përkufizimi i saj i kontrolluesit, i referohet një aspekti tjetër të statusit të kontrolluesit, i cili duhet marrë në konsideratë. Ky përkufizim mbështetet në çështjen se cili mund të përpunojë në mënyrë të ligjshme, disa lloje të dhënash, për një qëllim të caktuar.

---

[78] Direktiva e Mbrojtjes së të Dhënave, Pika 12 dhe neni 3 (2) rreshti i fundit.
[79] GjDBE, C-101/01, *Bodil Lindqvist*, 6 nëntor 2003.
[80] Po aty, parag. 27.
[81] Po aty, parag. 47.
[82] Direktiva e Mbrojtjes së të Dhënave, neni 2 (d).
[83] Konventa 108, neni 2 (d).

Gjithsesi, në raste përpunimesh të dyshuara si të paligjshme dhe ku duhet gjetur kontrolluesi përgjegjës, do të konsiderohet kontrollues personi fizik apo juridik, si për shembull shoqëria apo autoriteti, i cili ka vendosur që të përpunohen ato të dhëna, pavarësisht nëse ka qenë ligjërisht i autorizuar të bëjë këtë përpunim ose jo.[84] Ndaj, kërkesa për fshirje duhet t'i dërgohet gjithnjë kontrolluesit "faktik".

Bashkë-kontrolluesi

Përkufizimi i "kontrolluesit" tek Direktiva e Mbrojtjes së të Dhënave parashikon se mund të ketë gjithashtu disa njësi ligjërisht të veçanta, të cilat së bashku apo në bashkëpunim me të tjerë, veprojnë si kontrollues. Kjo do të thotë se ata vendosin bashkërisht të përpunojnë të dhëna për një qëllim të përbashkët.[85] Gjithsesi kjo është e mundur ligjërisht vetëm në rastet kur një bazë ligjore specifike parashikon përpunim të përbashkët të dhënash për një qëllim të përbashkët.

Shembull: Një bazë të dhënash e klientëve "të këqinj" 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 e duhura në lidhje me historikun e kreditorit.

Rregulloret 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. Gjithsesi, nuk ka ende në dispozicion jurisprudencë përkatëse në nivel evropian dhe po ashtu nuk janë të qarta pasojat në lidhje me përgjegjësinë. Grupi i Punës së nenit 29 mbron idenë e një interpretimi më të gjerë të konceptit të bashkë-kontrolluesit, me qëllim që të krijohet një farë fleksibiliteti, që do të mundësonte të përballohej kompleksiteti në rritje i realitetit të tanishëm të përpunimeve të të dhënave.[86] Një çështje që përfshin Shoqatën Botërore të Telekomunikimit Financiar Ndër-bankar (SWIFT) është shembull në lidhje me qëndrimin e Grupit të Punës.

---

[84] Shih gjithashtu Opinionin 1/2010 të Grupit të Punës së Nenit 29 (2010) mbi konceptet e 'kontrolluesit' dhe 'përpunuesit', WP 169, Bruksel, 16 shkurt 2010, fq. 15.

[85] Direktiva e Mbrojtjes së të Dhënave, neni 2 (d).

[86] Opinioni 1/2010 i Grupit të Punës së Nenit 29 (2010) mbi konceptet e 'kontrolluesit' dhe 'përpunuesit', WP 169, Bruksel, 16 shkurt 2010, fq. 19.

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 ruheshin në një qendër shërbimesh kompjuterike në Shtetet e Bashkuara (SHBA), Departamentit të Thesarit të SHBA-së, pa një kërkesë të qartë të institucioneve bankare evropiane të cilat i përdornin. 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.[87] SWIFT-i, duke vendosur në lidhje me këtë komunikim të dhënash, kishte marrë në mënyrë të paligjshme funksionin e kontrolluesit; dukshëm, institucionet bankare nuk e kishin respektuar detyrimin e tyre për të mbikëqyrur përpunuesin e tyre dhe për rrjedhojë, nuk mund të çliroheshin krejtësisht nga përgjegjësia e tyre si kontrollues. Nga ky fakt, gjenerohet një situatë prej bashkë-kontrolluesi.

Përpunuesi

Përpunuesi përcaktohet **në të drejtën e BE-së** si dikush që përpunon të dhëna personale për llogari të kontrolluesit.[88] Aktivitetet që i besohen një përpunuesi, mund të kufizohen në një detyrë ose kontekst tepër specifik, ose mund të jenë mjaft të përgjithshme dhe të plota.

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

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. administrimi i punonjësve të tyre, shitjeve dhe kontabilitetit.

Shembuj: 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 veprimeve të përpunimit të të dhënave me qëllimin e përmbushjes së detyrimeve të tij si punëdhënës.

Marrëdhënia midis kontrolluesit dhe përpunuesit

Sikurse e pamë, kontrolluesi përkufizohet si ai që përcakton qëllimet dhe mjetet e përpunimit.

---

[87] Opinioni 10/2006 i Grupit të Punës së Nenit 29 (2006) mbi përpunimin e të dhënave personale nga Shoqata Botërore e Telekomunikimit Financiar Ndër-bankar (SWIFT), WP 128, Bruksel, 22 nëntor 2006.

[88] Direktiva e Mbrojtjes së të Dhënave, neni 2 (e).

Shembull: drejtuesi i shoqërisë Sunshine vendos që shoqëria Moonlight, e specializuar në analizën e tregut, duhet të kryejë një analizë të tregut të të dhënave të klientëve të Sunshine-it. Për rrjedhojë, edhe pse përcaktimi i mjeteve të përpunimit i delegohet Moonlight-it, shoqëria Sunshine mbetet kontrolluesi dhe Moonlight-i nuk është gjë tjetër veçse përpunuesi, duke qenë se sipas kushteve të kontratës, Moonlight-i nuk mund të përdorë të dhënat e klientëve të Sunshine-it përveçse 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 ketë mundësi të ndërhyjë tek vendimet e përpunuesit, për sa i takon mjeteve të përpunimit. Përgjegjësia e përgjithshme mbetet ende tek kontrolluesi, i cili duhet të mbikëqyrë përpunuesit, për t'u siguruar se vendimet e tyre respektojnë legjislacionin e mbrojtjes së të dhënave. Kontrata e cila do t'ia ndalonte kontrolluesit ndërhyrjen tek vendimet e përpunuesit, duhet të konsiderohet rrjedhimisht se gjeneron një situatë bashkë-kontrolluesi, ku të dyja palët ndajnë të njëjtat detyrime ligjore të një kontrolluesi.

Për më tepër, nëse një përpunues nuk respekton kufizimet e përdorimit të të dhënave, sikurse përcaktohet 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 u lejua përpunuesi të shkelë kontratën mes palëve. Në fakt, Grupi i Punës së Nenit 29 është i prirur t'i konsiderojë këto lloj rastesh si situatë bashkë-kontrolluesi, duke qenë se diçka e tillë gjeneron mbrojtje më të madhe të interesave të subjekteve të të dhënave.[89] Një pasojë e rëndësishme e situatës së bashkë-kontrolluesit është përgjegjësia e përbashkët dhe individuale për të gjitha dëmet e shkaktuara, gjë e cila do t'u ofronte subjekteve të të dhënave një shumëllojshmëri mjetesh ligjore.

Një problematikë tjetër e mundshme që mund të lindë ka të bëjë 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 interpretim i konceptit të kontrolluesit.[90]

Për arsye qartësie dhe transparence, hollësitë e marrëdhënies midis kontrolluesit dhe përpunuesit, duhet të përshkruhen në një kontratë të shkruar.[91] 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.[92]

---

[89] *Opinioni 1/2010* i Grupit të Punës së Nenit 29 (2010), mbi *konceptet e 'kontrolluesit' dhe 'përpunuesit'*, WP 169, Bruksel, 16 shkurt 2010, fq. 25; dhe *Opinioni 10/2006* i Grupit të Punës së Nenit 29 (2006) *mbi përpunimin e të dhënave personale nga Shoqata Botërore e Telekomunikimit Financiar Ndër-bankar (SWIFT)*, WP 128, Bruksel, 22 nëntor 2006.

[90], *Opinioni 1/2010* i Grupit të Punës së Nenit 29 (2010) *mbi konceptet e 'kontrolluesit' dhe 'përpunuesit'*, WP 169, Bruksel, 16 shkurt 2010, fq. 26.

[91] Direktiva e Mbrojtjes së të Dhënave, neni 17 (3) dhe (4).

[92] *Opinioni 1/2010* i Grupit të Punës së Nenit 29 (2010) *mbi konceptet e 'kontrolluesit' dhe 'përpunuesit'*, WP 169, Bruksel, 16 shkurt 2010, fq. 27.

Përpunuesit mund të duan të delegojnë disa detyra tek nën-përpunues të tjerë. Diçka e tillë është ligjërisht e lejueshme dhe ky delegim do të varet në hollësi nga klauzolat kontraktuese midis kontrolluesit dhe përpunuesit, duke përfshirë këtu edhe nëse nevojitet autorizimi i kontrolluesit për secilin rast, apo nëse thjesht bërja me dije është e mjaftueshme.

Sipas së drejtës së KiE-së, interpretimi i koncepteve të kontrolluesit dhe përpunuesit, sikurse u shpjegua më lartë, është plotësisht në përputhje më të, sikurse demonstrohet nga rekomandimet që janë hartuar mbështetur në Konventën 108.[93]

2.3.2. Marrësit dhe palët e treta

Ndryshimi midis këtyre dy kategorive të personave dhe njësive të cilat përshkruhen në Direktivën e Mbrojtjes së të Dhënave, konsiston kryesisht në marrëdhënien e tyre me kontrolluesin dhe rrjedhimisht, në autorizimin që u jepet për të pasur akses në të dhënat personale që ruan kontrolluesi.

"Palë e tretë" është dikush i cili ligjërisht është i ndryshëm nga kontrolluesi. Për këtë shkak, komunikimi i të dhënave një pale të tretë do të kërkojë gjithnjë bazë ligjore specifike. Në përputhje me nenin 2 (f) të Direktivës së Mbrojtjes së të Dhënave, 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". Kjo do të thotë se personat të cilët punojnë për një organizatë e cila është ligjërisht 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 që përpunojnë llogaritë e klientëve, nën autoritetin e drejtpërdrejtë të të bankës së saj qendrore, nuk do të konsiderohet "palë të treta".[94]

"Marrësi" është term më i gjerë se sa "pala e tretë". Në kuptimin e nenit 2 (g) të Direktivës së Mbrojtjes së të Dhënave, marrës do të thotë "një person fizik ose juridik, autoritet publik, agjenci apo çdo organizëm të cilit i komunikohen të dhëna, qoftë palë e tretë ose jo". Marrësi mund të jetë ose jo një person i ndryshëm nga kontrolluesi ose përpunuesi – dhe në këtë rast është palë e tretë – ose dikush i brendshëm tek kontrolluesi ose përpunuesi, sikundër mund të jetë një nëpunës 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 përfshirë në operacionet e përpunimit të kontrolluesit apo përpunuesit.

---

[93] Shih për shembull Rekomandimin e Profilizimit, neni 1.
[94] *Opinioni 1/2010* i Grupit të Punës së Nenit 29 (2010) *mbi konceptet e 'kontrolluesit' dhe 'përpunuesit'*, WP 169, Bruksel, 16 shkurt 2010, fq. 31.

Nga ana tjetër, një palë e tretë, e cila është ligjërisht e ndarë nga kontrolluesi apo përpunuesi, nuk është e autorizuar të përdorë të dhëna personale të përpunuara nga kontrolluesi, përveçse kur ka arsye ligjore specifike në raste të caktuara. Rrjedhimisht, "Marrësit palë të treta" të të dhënave do të kenë gjithmonë nevojë për bazë ligjore, në mënyrë që të përftojnë ligjërisht të dhëna personale.

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 bazuar në udhëzimet e tij.

Gjithsesi, nëse i njëjti punonjës vendos të përdorë të dhënat, tek të cilat ai ka akses në cilësinë e punonjësit të përpunuesit, për qëllimet e tij apo të saj dhe ua shet ato një shoqërie tjetër, në këtë rast punonjësi ka vepruar si palë e tretë. Ai ose ajo nuk është duke ndjekur më urdhrat e përpunuesit (punëdhënësit). Si palë e tretë, nëpunësi ka nevojë për një bazë ligjore për marrjen dhe shitjen e të dhënave. Në këtë shembull, sigurisht që punonjësi nuk disponon një bazë të tillë ligjore, kështu që veprimet e tij janë të paligjshme.

2.4. Pëlqimi

Pikat kryesore

- Pëlqimi, duke qenë baza ligjore për përpunimin e të dhënave personale, duhet të jetë i lirë, i informuar dhe specifik.
- Pëlqimi duhet të jetë dhënë në mënyrë të qartë. Pëlqimi mund të jepet ose shprehimisht ose i nënkuptuar, duke vepruar në mënyrë të tillë që nuk lë asnjë dyshim se subjekti i të dhënave është dakord me përpunimin e të dhënave të tij apo të saj.
- Për përpunimin e të dhënave sensitive që mbështetet në pëlqimin e subjektit, është i detyrueshëm pëlqimi i dhënë shprehimisht.
- Pëlqimi mund të revokohet në çdo kohë.

Pëlqim do të thotë "çdo shprehje e vullnetit të lirë, specifik dhe të informuar të subjektit të të dhënave."[95] Në shumë raste, përbën bazën ligjore të një përpunimi të ligjshëm të të dhënave (shih paragrafin 4.1).

2.4.1. Elementet që e bëjnë pëlqimin të vlefshëm

E drejta e BE-së përcakton tre elemente që e bëjnë pëlqimin të vlefshëm, synimi i të cilëve është të garantohet se subjektet e të dhënave pranojnë vërtet përdorimin e të dhënave të tyre:

- Subjekti i të dhënave nuk duhet të ketë qenë nën presion kur ka dhënë pëlqimin;
- Subjekti i të dhënave duhet të ketë qenë i informuar mjaftueshëm në lidhje me qëllimin dhe pasojat e dhënies së pëlqimit; dhe
- Fushëveprimi i pëlqimit duhet të jetë i arsyeshëm dhe konkret.

[95] Direktiva e Mbrojtjes së të Dhënave, neni 2 (h).

Sipas së drejtës në fushën e mbrojtjes së të dhënave, pëlqimi është i vlefshëm vetëm kur përmbushen të gjitha këto kërkesa.

Konventa 108 nuk përmban një përkufizim të pëlqimit: diçka e tillë i është lënë legjislacionit kombëtar. Gjithsesi, **sipas së drejtës së KiE-së,** elementet që e bëjnë pëlqimin të vlefshëm përkojnë me ato të shpjeguara më lart, sikurse përcaktohet nga rekomandimet që janë hartuar në përputhje me Konventën 108.[96] Normat për pëlqimin janë të njëjta si ato për një deklaratë të vlefshme qëllimi, bazuar në legjislacionin civil evropian.

Norma të tjera shtesë sipas legjislacionit civil, sikurse zotësia juridike, natyrisht që zbatohen edhe në kontekstin e mbrojtjes së të dhënave, duke qenë se këto kërkesa 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.

Pëlqimi mund të jepet në mënyrë eksplicite[97] ose jo. Pëlqimi i shprehur në mënyrë eksplicite nuk lë asnjë dyshim në lidhje me qëllimet e subjektit të të dhënave dhe mund të jepet si me gojë ashtu edhe me shkrim; pëlqimi i nënkuptuar varet nga rrethanat. Çdo pëlqim duhet të jepet në mënyrë të qartë.[98] Kjo do të thotë se nuk duhet të ketë asnjë dyshim të arsyeshëm se subjekti i të dhënave dëshiron të komunikojë miratimin e tij apo të saj për të lejuar përpunimin e të dhënave të tij apo të saj. Pëlqimi i nxjerrë thjesht nga pasiviteti, nuk do të përbënte pëlqim të qartë, për shembull. Kur të dhënat që do të përpunohen janë sensitive, pëlqimi eksplicit është i detyrueshëm dhe duhet të jetë i qartë.

Pëlqimi i lirë

Ekzistenca e një pëlqimi të lirë është i mundshëm vetëm "kur subjekti i të dhënave ka vërtet mundësi të bëjë zgjedhje dhe nuk ka rrezik mashtrimi, frikësimi, shtrëngimi apo pasoja negative të konsiderueshme nëse ai/ajo nuk e jep pëlqimin".[99]

---

[96] Shih për shembull, Konventa 108, Rekomandimi i të Dhënave Statistikore, pika 6.

[97] Direktiva e Mbrojtjes së të Dhënave, neni 8 (2).

[98] Po aty, neni 7 (a) dhe neni 26 (1).

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

Shembull: në shumë aeroporte, pasagjerët duhet të kalojnë nëpërmjet skanerëve të trupit, me qëllim që të hyjnë në zonat e nisjes së udhëtimit.[100] Duke qenë se të dhënat e pasagjerëve përpunohen gjatë skanimit, përpunimi duhet të jetë në përputhje me një nga bazat ligjore referuar nenit 7 të Direktivës së Mbrojtjes së të Dhënave (shih paragrafin 4.1.1). Kalimi nëpërmjet skanerëve të trupit, ndonjëherë u paraqitet pasagjerëve si një opsion, duke lënë të kuptohet se pëlqimi i tyre mund të justifikojë përpunimin. Gjithsesi, pasagjerët mund të druhen se kundërshtimi i tyre për të kaluar nëpërmjet skanerëve të trupit, mund të shkaktojë dyshime ose të bëhet shkak për kontrolle shtesë, sikurse janë kontrollet fizike. Shumë pasagjerë japin pëlqimin për kryerjen e skanimit, për shkak se duke e bërë këtë, ata shmangin probleme apo vonesa të mundshme. Mund të supozohet se ky lloj pëlqimi nuk është aq i lirë sa duhet.
Kështu, baza e sigurt ligjore mund të gjendet vetëm në një akt të ligjvënësit, në përputhje me nenin 7 (e) të Direktivës së Mbrojtjes së të Dhënave, prej të cilit buron detyrimi që kanë pasagjerët për të bashkëpunuar, për shkak të një interesi publik prevalues. Ky akt ligjor gjithsesi mund të lërë mundësinë e zgjedhjes ndërmjet skanimit dhe kontrollit manual fizik, por vetëm si pjesë e masave shtesë të kontrollit kufitar, të nevojshme në rrethana të veçanta. Kjo është ajo çka ka përcaktuar Komisioni Evropian në dy rregulloret e vitit 2011, të cilat trajtojnë skanerët e sigurisë.[101]

Pëlqimi i lirë mund të kërcënohet edhe në situata të vartësisë, kur ka pabarazi ekonomike domethënëse ose pabarazi të llojeve të ndryshme, midis kontrolluesit që merr pëlqimin dhe subjektit të të dhënave që jep pëlqimin.[102]

Shembull: një shoqëri e madhe planifikon të krijojë një regjistër të emrave të të gjithë punonjësve, funksionet e tyre në shoqëri dhe adresat e tyre të punës, me qëllimin e vetëm të përmirësimit të komunikimeve të brendshme të shoqërisë. Drejtuesi i personelit propozon të shtohet edhe një fotografi për secilin punonjës në regjistër, me qëllim që, për shembull, të lehtësohet njohja e kolegëve gjatë mbledhjeve. Përfaqësuesit e punonjësve kërkojnë që kjo të bëhet vetëm nëse secili punonjës jep pëlqimin.

Në këtë situatë, pëlqimi i një punonjësi duhet të njihet si bazë ligjore për përpunimin e fotografive në regjistër, pasi është e qartë se publikimi i një fotografie në regjistër nuk ka në vetvete pasoja negative dhe për më tepër, ka mundësi që punonjësi nuk do të duhet të përballet me ndonjë pasojë negative nga ana e punëdhënësit në rast se ai apo ajo nuk pranon që t'i publikohet fotografia në regjistër.

---

[100] Ky shembull është marrë po aty (99), fq. 15.

[101] Rregullorja e Komisionit (EU) nr. 1141/2011 e 10 nëntorit 2011 që ndryshon Rregulloren (EC) nr. 272/2009 që plotëson standardet themelore të përbashkëta në lidhje me sigurinë e aviacionit civil, sa i takon përdorimit të skanerëve të sigurisë në aeroportet e BE-së, JO 2011 L 293, dhe Rregullorja e Zbatimit (EU) e Komisionit nr. 1147/2011 datë 11 nëntor 2011 që ndryshon Rregulloren (EU) nr. 185/2010 që përcakton standardet themelore të përbashkëta në lidhje me sigurinë e aviacionit civil, sa i takon përdorimit të skanerëve të sigurisë në aeroportet e BE-së, JO 2011 L 294.

[102] Shih gjithashtu, *Opinionin 8/2001* e Grupit të Punës së Nenit 29 (2001) *mbi përpunimin e të dhënave personale në kontekstin e punësimit*, WP 48, Bruksel, 13 shtator 2001; dhe *Dokumentin e punës* së Grupit të Punës së Nenit 29 (2005), *mbi një interpretim të përbashkët të nenit 26 (1) të Direktivës 95/46/EC të datës 24 tetor 1995*, WP 114, Bruksel, 25 nëntor 2005.

Megjithatë, kjo nuk do të thotë se pëlqimi nuk mund të jetë kurrë i vlefshëm në rrethanat në të cilat mosdhënia e pëlqimit do të kishte pasoja negative. Në qoftë se për shembull, pasoja e mosdhënies së pëlqimit për t'u pajisur me një kartë klienti të një supermarketi është thjesht mos përfitimi i çmimeve më të ulëta për disa produkte, pëlqimi mbetet ende një bazë e vlefshme ligjore për përpunimin e të dhënave personale të atyre klientëve, të cilët kanë dhënë pëlqimin për t'u pajisur me këtë kartë. Nuk ekziston asnjë situatë vartësie ndërmjet kompanisë dhe klientit dhe pasojat për mosdhënien e pëlqimit nuk janë aq të rënda, sa të pengohet liria e zgjedhjes së subjektit të të dhënave.

Nga ana tjetër, në rastet kur produkte apo shërbime mjaft të rëndësishme mund të përfitohen vetëm dhe ekskluzivisht nëse palëve të treta u komunikohen disa të dhëna personale, pëlqimi i subjektit të të dhënave për komunikimin e të dhënave të tij apo të saj, përgjithësisht nuk mund të konsiderohet vendim i lirë dhe është për pasojë, i pavlefshëm në kuptimin e legjislacionit për mbrojtjen e të dhënave personale.

Shembull: Miratimi i shprehur i pasagjerëve për një shoqëri fluturimi që t'ua transferojnë të ashtuquajturat të dhëna të pasagjerëve (PNR), konkretisht të dhënat në lidhje me identitetin, mënyrën e të ushqyerit apo problemet shëndetësore, autoriteteve të emigracionit të një vendi të caktuar, nuk mund të konsiderohet si pëlqim i vlefshëm bazuar në legjislacionin për mbrojtjen e të dhënave, duke qenë se udhëtarët nuk kanë mundësi zgjedhjeje për sa kohë duan të vizitojnë atë vend. Nëse këto të dhëna duhen transferuar në mënyrë të ligjshme, përveç pëlqimit, nevojitet një bazë tjetër ligjore: me shumë gjasa një ligj special.

Pëlqimi i informuar

Subjekti i të dhënave duhet të ketë informacion të mjaftueshëm, përpara se të marrë vendimin e tij apo të saj. Nëse informacioni që i është dhënë është i mjaftueshëm ose jo, kjo mund të vendoset vetëm rast par rasti. Zakonisht, pëlqimi i informuar do të përfshijë një përshkrim të saktë dhe lehtësisht të kuptueshëm të objektit të çështjes për të cilën nevojitet pëlqimi si edhe të pasojave të dhënies apo mosdhënies së pëlqimit. Gjuha e përdorur për dhënien e informacionit, duhet të përshtatet për personat të cilëve parashikohet t'u drejtohet ky informacion.

Informacioni duhet gjithashtu të jetë lehtësisht i disponueshëm për subjektin e të dhënave. Aksesi dhe shikueshmëria e informacionit janë elemente të rëndësishme. Në ambientin e internetit, njoftimet informuese të përshkallëzuara mund të jenë një zgjidhje e mirë, duke qenë se bashkëlidhur me një variant të përmbledhur të informacionit, subjekti i të dhënave mund të ketë qasje në një variant tjetër më të zgjeruar.

Pëlqimi specifik

Pëlqimi duhet gjithashtu të jetë specifik, në mënyrë që të jetë i vlefshëm. Kjo gjë shkon paralelisht me cilësinë e informacionit që është dhënë në lidhje me objektin e pëlqimit. Në këtë kontekst, e rëndësishme do të jetë ajo çka përbën një pritshmëri të arsyeshme për një subjekt të zakonshëm të dhënash. Këtij të fundit i duhet marrë sërish pëlqimi kur operacionet

e përpunimit duhen shtuar ose ndryshuar, meqenëse nuk mund të parashikoheshin në mënyrë të arsyeshme gjatë kohës kur u mor pëlqimi fillestar.

Shembull: tek çështja *Deutsche Telekom AG,*[103] GjDBE-ja trajtoi problematikën në lidhje më një operator të shërbimeve të telekomunikacionit, i cili do të transmetonte të dhëna personale të abonentëve, në përputhje me nenin 12 të *Direktivës së privatësisë dhe komunikimeve elektronike*[104] dhe donte të dinte nëse i nevojitej të merrte sërish pëlqimin nga subjektet e të dhënave, duke qenë se në fillim, kur pëlqimi ishte marrë, nuk i kishin bërë me dije emrat e marrësve.

GjDBE-ja u shpreh se sipas atij neni, marrja sërish e pëlqimit përpara transmetimit të të dhënave, nuk ishte e nevojshme, për shkak se subjektet e të dhënave, referuar kësaj dispozite, kishin pasur mundësi të jepnin pëlqimin vetëm për qëllimin e përpunimit, i cili konsiston në publikimin e të dhënave të tyre dhe nuk kishin pasur mundësi të zgjidhnin ndërmjet regjistrave në të cilët do të publikoheshin këto të dhëna.

Sikurse theksoi Gjykata, "nga një interpretim kontekstual dhe sistematik të nenit 12 të Direktivës së privatësisë dhe komunikimeve elektronike rezulton se pëlqimi, sipas nenit 12 (2), lidhet me qëllimin e publikimit të të dhënave personale në një regjistër publik dhe jo me identitetin e një operatori të caktuar të një regjistri."[105] Gjithashtu "është vetë publikimi i të dhënave personale në një regjistër publik, me një qëllim të caktuar, i cili mund të rezultojë i dëmshëm për abonentin"[106] dhe jo cili është autori i publikimit.

2.4.2. E drejta për të revokuar pëlqimin në çdo kohë

Direktiva e Mbrojtjes së të Dhënave nuk përmend ndonjë të drejtë të përgjithshme për të revokuar pëlqimin në çdo kohë. Gjithsesi, supozohet në përgjithësi se kjo e drejtë ekziston dhe se duhet të jetë e mundur për subjektin e të dhënave që ta ushtrojë atë të drejtë sipas gjykimit të tij apo të saj. Nuk duhet të vendoset asnjë detyrim për të dhënë arsyet për revokimin dhe asnjë rrezik pasojash negative të shtuara apo përfitime të cilat mund të rrjedhin nga përdorimi i të dhënave për të cilin është rënë dakord më parë.

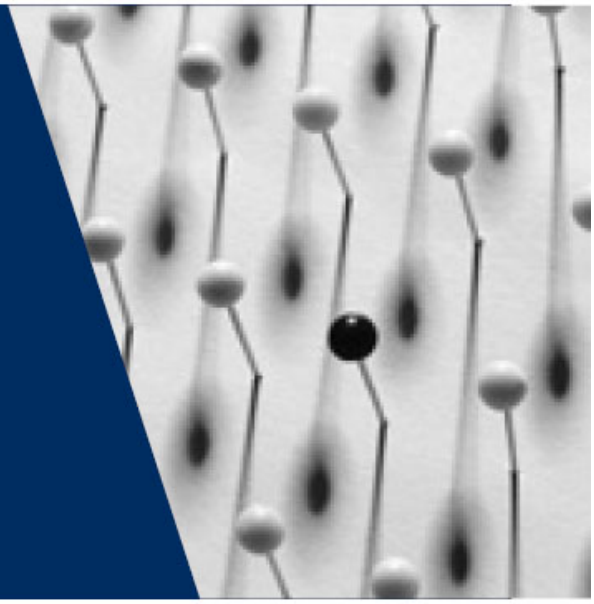
Shembull: Një klient pranon që t'i postojnë korrespondencë reklamuese, në adresën që ai apo ajo i ka dhënë kontrolluesit të të dhënave. Në rast se klienti revokon pëlqimin, kontrolluesi duhet të ndalë menjëherë dërgimin e postës reklamuese. Asnjë pasojë ndëshkuese nuk duhet të ndërmerret për këtë, si për shembull pagesë tarife.

Nëse klienti përfitonte 5% ulje nga kostoja e një dhome hoteli si shkëmbim për miratimin e dhënë për përdorimin e të dhënave të tij apo të saj për korrespondencë reklamuese, revokimi i pëlqimit për këtë të fundit në një fazë të mëvonshme, nuk duhet të sjellë si pasojë detyrimin për të kthyer mbrapsht uljet e përfituara.

[103] GjDBE, C-543/09, *Deutsche Telekom AG kundër Gjermanisë*, 5 maj 2011; shih veçanërisht parag. 53 and 54.
[104] 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, JO 2002 L 201 (Direktiva e privatësisë dhe komunikimeve elektronike).
[105] GjDBE, C-543/09, *Deutsche Telekom AG kundër Gjermanisë*, 5 maj 2011; shih veçanërisht parag. 61
[106] Po aty, shih veçanërisht parag. 62

3

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



BE	Çështje të trajtuara	KiE
Direktiva e Mbrojtjes së të Dhënave, neni 6 (1) (a) GjDBE, C-524/06, *Huber kundër Gjermanisë*, 16 dhjetor 2008 GjDBE, Çështje të bashkuara C-92/09 dhe C-93/09, *Volker dhe Markus Schecke GbR dhe Hartmut Eifert kundër Land Hessen-it*, 9 nëntor 2010	**Parimi i përpunimit të ligjshëm**	Konventa 108, neni 5 (a) dhe (b) GjEDNj, *Rotaru kundës Rumanisë* [GC], nr 28341/95, 4 maj 2000 GjEDNJ, *Taylor-Sabori kundër Mbretërisë së Bashkuar*, nr. 47114/99, 22 tetor 2002 GjEDNj, *Peck kundër Mbretërisë së Bashkuar*, nr. 44647/98, 28 janar 2003 GjEDNj, *Khelili kundër Zvicrës*, nr. 16188/07, 18 tetor 2011 GjEDNj, *Leander kundër Suedisë*, nr. 9248/81, 26 mars 1987
Direktiva e Mbrojtjes së të Dhënave, neni (6) (1) (b)	**Parimi i specifikimit dhe kufizimit të qëllimit**	Konventa 108, neni 5 (c)
	Parimet e cilësisë së të dhënave:	
Direktiva e Mbrojtjes së të Dhënave, neni 6 (1) (c)	**Rëndësia e të dhënave**	Konventa 108, neni 5 (c)
Direktiva e Mbrojtjes së të Dhënave, neni 6 (1) (d)	**Saktësia e të dhënave**	Konventa 108, neni 5 (d)
Direktiva e Mbrojtjes së të Dhënave, neni 6 (1) (e)	**Ruajtja e të dhënave për një afat kohor të kufizuar**	Konventa 108, neni 5 (e)
Direktiva e Mbrojtjes së të Dhënave, neni 6 (1) (e)	**Përjashtimi për qëllime kërkimore shkencore dhe statistikore**	Konventa 108, neni 9 (3)
Direktiva e Mbrojtjes së të Dhënave, neni 6 (1) (a)	**Parimi i përpunimit të drejtë**	Konventa 108, neni 5 (a) GjEDNj, *Haralambie kundër Rumanisë*, nr. 21737/03, 27 tetor 2009

		GjEDNj, *K.H. dhe të Tjerët kundër Sllovakisë*, nr. 32881/04, 28 prill 2009
Direktiva e Mbrojtjes së të Dhënave, neni 6 (2)	**Parimi i përgjegjshmërisë**	

Parimet e përcaktuara në nenin 5 të Konventës 108, përbëjnë esencën e së drejtës evropiane në fushën e mbrojtjes së të dhënave. Ato shfaqen gjithashtu edhe në nenin 6 të Direktivës së Mbrojtjes së të Dhënave, si një pikënisje për dispozita më të detajuara në nenet e mëtejshme të direktivës. Tërësia e akteve ligjore të mëvonshme, qofshin ato në nivel KiE-je apo BE-je, duhet të përputhen me këto parime, të cilat duhen pasur parasysh kur interpretohet legjislacioni. Çdo përjashtim dhe kufizim i këtyre parimeve kryesore, duhet të parashikohet në nivel kombëtar;[107] duhet të jenë të përcaktuara me ligj, për përmbushjen e një qëllimi legjitim dhe të jenë të nevojshme në një shoqëri demokratike. Të tre këto kushte duhen plotësuar.

3.1. Parimi i përpunimit të ligjshëm

Pikat kryesore

- Me qëllim që parimi i përpunimit të ligjshëm të jetë i kuptueshëm, është e nevojshme t'i referohemi kushteve për kufizime të ligjshme të së drejtës për mbrojtje të të dhënave, bazuar në nenin 52 (1) të Kartës dhe normave për ndërhyrje të justifikuar, sipas nenit 8 (2) të KEDNj-së.
- Në përputhje me këtë, përpunimi i të dhënave personale është i ligjshëm vetëm nëse:
- Është në përputhje me ligjin; dhe
- Synon përmbushjen e një qëllimi legjitim; dhe
- Është i nevojshëm në një shoqëri demokratike, për përmbushjen e qëllimit legjitim.

Sipas së drejtës së BE-së dhe KiE-së në fushën e mbrojtjes së të dhënave, parimi i përpunimit të ligjshëm është parimi i parë i cituar; ai është shprehur në terma thuajse identikë në nenin 5 të Konventës 108 dhe në nenin 6 të Direktivës së Mbrojtjes së të Dhënave.

Asnjë nga këto dispozita nuk përmban një përkufizim të asaj çka përbën "përpunim të ligjshëm". Me qëllim që të kuptohet ky term ligjor, është e nevojshme t'i referohemi ndërhyrjes së justifikuar sipas KEDNj-së, sikurse është interpretuar nga jurisprudenca e GjEDNj-së dhe kushteve për kufizime të ligjshme sipas nenit 52 të Kartës.

3.1.1. Normat për ndërhyrje të justifikueshme, sipas KEDNj-së

Përpunimi i të dhënave personale mund të përbëjë ndërhyrje tek e drejta për respektim të jetës private të subjektit të të dhënave. Gjithsesi, e drejta për respektim të jetës private nuk është absolute, por duhet ekuilibruar dhe përputhur me interesa të tjerë legjitimë, qofshin ato të personave të tjerë (interesa privatë) apo të shoqërisë në tërësi (interesa publikë).

Kushtet sipas së cilave shteti mund të ndërhyjë në mënyrë të justifikuara janë si vijon.

Në përputhje me ligjin

Bazuar në jurisprudencën e GjEDNj-së, ndërhyrja është në përputhje me ligjin nëse bazohet në një dispozitë të ligjit vendas, i cili duhet të ketë disa cilësi.

[107] Konventa 108, neni 9 (2), Direktiva e Mbrojtjes së të Dhënave, neni 13 (2).

Ligji duhet të jetë "i aksesueshëm nga personat e interesuar dhe i parashikueshëm sa i takon efekteve të tij".[108] Një normë është e parashikueshme "nëse është e formuluar me saktësi të mjaftueshme, që t'i mundësojë çdo individi – duke përfituar njëkohësisht, nëse është e nevojshme, edhe asistencën e duhur – të përshtatë sjelljen e tij".[109] "Shkalla e saktësisë që duhet të ketë "ligji" në këtë kontekst, do të varet nga çështja e trajtuar."[110]

Shembull: tek çështja *Rotaru kundër Rumanisë*,[111] GjEDNj-ja gjeti shkelje të nenit 8 të KEDNj-së, pasi legjislacioni rumun lejonte mbledhjen, regjistrimin dhe arkivimin në dosje sekrete, të informacioneve të rëndësishme për sigurinë kombëtare, pa përcaktuar kufizime në ushtrimin e këtyre kompetencave, të cilat u liheshin në dorë autoriteteve. Për shembull, e drejta kombëtare nuk përcaktonte llojin e informacionit që mund të përpunohej, kategoritë e njerëzve ndaj të cilëve mund të merreshin masa survejimi, rrethanat në të cilat këto masa mund të merreshin apo procedurat që duheshin ndjekur. Për shkak të këtyre mungesave në legjislacion, Gjykata vendosi se ligji kombëtar nuk zbatonte kërkesat për parashikueshmëri, sipas nenit 8 të KEDNj-së dhe se ai nen ishte shkelur.

Shembull: tek çështja *Taylor-Sabori kundër Mbretërisë së Bashkuar*,[112] ankuesi kishte qenë nën përgjim nga policia. Duke përdorur një "*pager* të klonuar" të ankuesit, policia kishte mundur të përgjonte mesazhet që i dërgoheshin atij. Ankuesi më pas ishte arrestuar me akuzën e trafikimit të lëndëve narkotike në bashkëpunim. Një pjesë e aktakuzës përbëhej nga shënimet e regjistruara njëkohësisht me mesazhet në *pager*-in e tij, të cilat ishin transkriptuar nga policia. Sidoqoftë, gjatë kohës që zhvillohej gjyqi ndaj ankuesit, nuk ekzistonte asnjë dispozitë në legjislacionin britanik që rregullonte interceptimin e komunikimeve të transmetuara nëpërmjet sistemit privat të telekomunikimeve. Për pasojë, ndërhyrja tek këto të drejta nuk ishte bërë "në përputhje me ligjin". GjEDNj-ja doli në përfundimin se ishte shkelur neni 8 i KEDNj-së.

Përmbushja e qëllimit legjitim

Qëllimi legjitim mund të jetë qoftë një nga interesat publike të cituara, qoftë të drejtat dhe liritë e të tjerëve.

Shembull: tek çështja *Peck kundër Mbretërisë së Bashkuar*,[113] ankuesi tentoi të vetëvritej në rrugë, duke prerë damarët, pa e ditur se një kamera vëzhgimi ishte duke e filmuar gjatë tentativës. Pasi policia, e cila ishte duke vëzhguar kamerat, e shpëtoi, ia kaloi filmimet e kamerës mediave, të cilat i publikuan pa e fshehur fytyrën e ankuesit. 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 ankuesit apo pa fshehur identitetin e tij. Gjykata vendosi se ishte shkelur neni 8 i KEDNj-së.

---

[108] GjEDNj, *Amann kundër Zvicrës* [GC], nr. 27798/95, 16 shkurt 2000, parag. 50; shih gjithashtu GjEDNj, *Kopp kundër Zvicrës*, nr. 23224/94, 25 mars 1998, parag. 55 dhe GjEDNj, *Iordachi dhe të Tjerët kundër Moldavisë*, nr. 25198/02, 10 shkurt 2009, parag. 50.

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

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

[111] GjEDNj, *Rotaru kundër Rumanisë* [GC], nr. 28341/95, 4 maj 2000, parag. 57; shih gjithashtu GjEDNj, *Shoqata për Integrim Evropian dhe të Drejtat e Njeriut dhe Ekimdzhiev kundër Bullgarisë*, nr. 62540/00, 28 qershor 2007; GjEDNj, *Shimovolos kundër Rusisë*, nr. 30194/09, 21 qershor 2011; dhe GjEDNj, *Vetter kundër Francës*, nr. 59842/00, 31 maj 2005.

[112] GjEDNj, *Taylor-Sabori kundër Mbretërisë së Bashkuar*, nr. 47114/99, 22 tetor 2002.

[113] GjEDNj, *Peck kundër Mbretërisë së Bashkuar*, nr. 44647/98, 28 janar 2003, sidomos parag. 85.

Ndërhyrja e nevojshme në një shoqëri demokratike

GjEDNj-ja theksoi se "nocioni i domosdoshmërisë nënkupton se ndërhyrja përkon me një nevojë të ngutshme shoqërore dhe sidomos se është proporcionale me qëllimin legjitim që kërkohet të përmbushet".[114]

Shembull: tek çështja *Khelili kundër Zvicrës,*[115] gjatë një pike kontrolli, policia i gjeti ankuesit 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. [...]". Ankuesi pretendoi se pas kontrollit, policia regjistroi emrin e saj në dosje si prostitutë, zanat të cilin ajo këmbëngulte se nuk e kryente. Ankuesi 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 ankuesit, dyshimet për ushtrim prostitucioni dukeshin tepër të dobëta dhe të përgjithshme, nuk mbështeteshin në fakte konkrete, duke qenë se ajo nuk ishte dënuar kurrë për ushtrim të paligjshëm prostitucioni dhe nuk mund të konsiderohej për rrjedhojë 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 ankuesin dhe rëndësinë e ndërhyrjes tek të drejtat e ankuesit, 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 çështja *Leander kundër Suedisë,*[116] 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 të kryera 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 (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 ankuesit, interesat e sigurisë kombëtare, prevalonin mbi ato individuale. Gjykata doli në përfundimin se nuk kishte pasur shkelje të nenit 8 të KEDNj-së.

3.1.2. Kushtet për kufizime të ligjshme sipas Kartës së BE-së

Struktura dhe formulimi i Kartës, është i ndryshëm nga ai i KEDNj-së. Karta nuk flet për ndërhyrje në të drejtat e garantuara, por përmban një dispozitë për kufizimin apo kufizimet e ushtrimit të së drejtave dhe lirive të njohura nga Karta.

[114] GjEDNj, *Leander kundër Suedisë*, nr. 9248/81, 26 mars 1987, parag. 58.
[115] GjEDNj, *Khelili kundër Zvicrës*, nr. 16188/07, 18 tetor 2011.
[116] GjEDNj, *Leander kundër Suedisë*, nr. 9248/81, 26 mars 1987, parag. 59 dhe 67

Sipas nenit 52 (1), kufizimet në ushtrimin e të drejtave dhe lirive të njohura nga Karta dhe rrjedhimisht në ushtrimin e së drejtës për mbrojtje të të dhënave personale, sikurse përpunimi i të dhënave personale, janë të pranueshme vetëm nëse:

- Janë të parashikuara në ligj; dhe
- Respektojnë thelbin e së drejtës për mbrojtje të të dhënave; dhe
- Janë të nevojshme, me kusht respektimin e proporcionalitetit; dhe
- Përputhen me objektivat e interesit të përgjithshëm të njohura nga Bashkimi ose me nevojën për të mbrojtur të drejtat dhe liritë e të tjerëve.

Shembuj: tek çështja *Volker dhe Markus Schecke,*[117] GjDBE-ja doli në përfundimin se duke përcaktuar detyrimin për të publikuar të dhëna personale në lidhje me secilin person fizik, i cili ishte përfitues ndihme [i disa fondeve bujqësore], pa bërë dallime bazuar në kritere të përshtatshme, sikurse periudha kohore gjatë së cilës ata persona kanë përfituar ndihmën, frekuenca e ndihmës, apo lloji dhe shuma e tyre, ishin tejkaluar kufijtë e përcaktuar nga parimi i proporcionalitetit.

Ndaj, GjDBE-ja e pa të arsyeshme të shpallte të pavlefshme disa dispozita të Rregullores së Këshillit (EC) nr. 1290/2005 dhe të shpallte pavlefshmërinë e Rregullores nr. 259/2008 në tërësinë e saj.[118]

Pavarësisht formulimit të ndryshëm, kushtet për përpunim të ligjshëm në nenin 52 (1) të Kartës, të kujtojnë ato të nenit 8 (2) të KEDNj-së. Në fakt, kushtet e radhitura në nenin 52 (1) të Kartës, duhet të konsiderohen si në përputhje me ato të nenit 8 (2) të KEDNj-së, sikundër neni 52 (3) i Kartës nënvizon, në fjalinë e tij të parë "për aq sa Karta përmban të drejta të cilat përkojnë me të drejtat e garantuara nga Konventa për Mbrojtjen e të Drejtave të Njeriut dhe Lirive Themelore, kuptimi dhe qëllimi i atyre të drejtave është i njëjtë me ato të përcaktuara në Konventën në fjalë."

Megjithatë, bazuar në fjalinë e fundit të nenit 52 (3), "kjo dispozitë nuk pengon legjislacionin e Bashkimit të ofrojë mbrojtje me shtrirje më të gjerë." Në kontekstin e krahasimit të nenit 8 (2) të KEDNj-së dhe fjalisë së parë të nenit 52 (3), kjo do të thotë vetëm që kushtet për ndërhyrje të justifikuar bazuar në nenin 8 (2) të KEDNj-së, janë normat minimale për kufizime të ligjshme të së drejtës për mbrojtje të të dhënave sipas Kartës. Për pasojë, për përpunimin e ligjshëm të të dhënave personale sipas së drejtës së BE-së, nevojitet minimalisht që kushtet e nenit 8 (2) të KEDNj-së të plotësohen; megjithatë, e drejta e BE-së mund të përcaktojë kërkesa të tjera për raste të veçanta.

Ngjashmëria e parimit të përpunimit të ligjshëm referuar së drejtës së BE-së, me dispozitat përkatëse të KEDNj-së, mbështetet gjithashtu nga neni 6 (3) i TBE-së, i cili përcakton se "të drejtat themelore që garantohen nga Konventa Evropiane për Mbrojtjen e të Drejtave të Njeriut dhe Lirive Themelore [...], bëjnë pjesë tek e drejta e Bashkimit, si parime të përgjithshme".

---

[117] GjDBE, Çështje të Bashkuara C-92/09 dhe C-93/09, *Volker dhe Markus Schecke GbR dhe Hartmut Eifert kundër Land Hessen-it,* 9 nëntor 2010, parag. 89 dhe 86.

[118] Rregullorja e Këshillit (EC) nr. 1290/2005 e 21 qershorit 2005 mbi financimin e politikave bujqësore të përbashkëta, JO 2005 L 209; Rregullorja 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 mbi publikimin e informacioneve mbi përfituesi e fondeve që burojnë nga Fondi Evropian i Garancive Bujqësore (FEGB) dhe Fondi Evropian Bujqësor për Zhvillim Rural (FEBZhR), JO 2008 L 76.

3.2. Parimi i specifikimit dhe kufizimit të qëllimit

Pikat kryesore

- Qëllimi i përpunimit të të dhënave duhet të jetë i përcaktuar në mënyrë të qartë dhe i bërë me dije përpara nisjes së përpunimit.
- Bazuar në të drejtën e BE-së, qëllimi i përpunimit duhet të përcaktohet në mënyrë të qartë; bazuar në të drejtën e KiE-së, kjo çështje i lihet për trajtim legjislacionit kombëtar.
- Përpunimi për qëllime të papërcaktuara nuk është në përputhje me të drejtën në fushën e mbrojtjes së të dhënave.
- Përpunimi i mëtejshëm i të dhënave, për qëllim tjetër, nevojit një kuadër ligjor shtesë, në rast se përpunimi i ri është i ndryshëm nga i pari.
- Transferimi i të dhënave tek palë të treta përbën qëllim të ri, për të cilin nevojitet kuadër ligjor shtesë.

Në thelb, parimi i specifikimit dhe kufizimit të qëllimit nënkupton që legjitimiteti i përpunimit të të dhënave personale varet nga qëllimi i përpunimit[119]. Qëllimi duhet të specifikohet dhe duhet bërë me dije nga kontrolluesi, përpara se të nisë përpunimi i të dhënave.[120] Bazuar në të drejtën e BE-së, duhet të bëhet ose me anë të një deklarate, me fjalë të tjera nëpërmjet njoftimit tek autoriteti përkatës mbikëqyrës, ose të paktën me anë të dokumentimit të brendshëm, i cili duhet të vihet në dispozicion nga kontrolluesi për inspektim nga ana e autoriteteve mbikëqyrëse dhe për akses nga ana e subjektit të të dhënave.

Përpunimi i të dhënave personale për qëllime të papërcaktuara dhe/ose të pakufizuara është i paligjshëm.

Çdo qëllim i ri përpunimi të dhënash, duhet të ketë kuadrin e vet ligjor përkatës dhe nuk mund të mbështetet në faktin se të dhënat ishin përftuar apo përpunuar fillimisht për një qëllim tjetër legjitim. Nga ana tjetër, përpunimi legjitim kufizohet tek qëllimi i vet parësor i specifikuar dhe për çdo qëllim të ri përpunimi nevojitet tjetër kuadër ligjor i veçantë. Komunikimi i të dhënave palëve të treta, duhet të trajtohet me kujdes, për shkak se përhapja përbën përgjithësisht qëllim të ri dhe rrjedhimisht ka nevojë për bazë ligjore, të ndryshme nga ajo për mbledhjen e të dhënave.

Shembull: Një shoqëri fluturimesh mbledh të dhënat e udhëtarëve 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 PNR-të, autoriteteve të emigrimit në aeroportin e mbërritjes, ato të dhëna po përdoren kështu 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.

[119] Konventa 108, neni 5 (b); Direktiva e Mbrojtjes së të Dhënave, neni 6 (1) (b).
[120] Shih gjithashtu, Opinionin 03/2013 e Grupit të Punës së Nenit 29 (2013) mbi kufizimin e qëllimit, WP 203, Bruksel, 2 prill 2013.

Kur trajton kuadrin dhe kufijtë e një qëllimi të caktuar, Konventa 108 dhe Direktiva e Mbrojtjes së të Dhënave drejtohen tek koncepti i përshtatshmërisë: përdorimi i të dhënave për qëllime të përshtatshme është i lejuar mbi bazën e kuadrit ligjor fillestar. Por, se çfarë do të thotë "përshtatshmëri", kjo nuk parashtrohet dhe lihet e hapur për interpretim rast pas rasti.

Shembull: shitja e të dhënave të klientëve të shoqërisë Sunshine, të cilat ishin mbledhur në kuadër të menaxhimit të marrëdhënieve me klientët (MMK), tek shoqëria Moonlight, e cila merret me marketing të drejtpërdrejtë dhe parashikon t'i përdorë këto të dhëna për të ndihmuar fushatat e marketingut të shoqërive të treta, përbën qëllim të ri, i cili nuk është në përputhje me MMK-në, pra me qëllimin fillestar të shoqërisë Sunshine të mbledhjes së të dhënave të klientëve. Për këtë, shitja e të dhënave tek shoqëria Moonlight kërkon bazën e vet ligjore.

Përkundër kësaj, përdorimi i të dhënave MMK nga ana e shoqërisë Sunshine, për qëllimet e veta të marketingut, që përfshin dërgimin e njoftimeve të marketingut tek klientët e vet, në lidhje me produktet që tregton, pranohet përgjithësisht si qëllim i përshtatshëm.

Direktiva e Mbrojtjes së të Dhënave përcakton në mënyrë të qartë se "përpunimi i mëtejshëm i të dhënave për qëllime historike, statistikore apo shkencore, duhet të konsiderohet si i përshtatshëm, me kusht që Shtetet Anëtare të parashikojnë garanci të mjaftueshme".[121]

Shembuj: shoqëria Sunshine ka mbledhur dhe ruajtur të dhëna MMK të klientëve të saj. Përdorimi i mëtejshëm i këtyre të dhënave nga ana e shoqërisë Sunshine, për qëllim të analizimit statistikor të sjelljes në raport me blerjen të klientëve të saj, është i lejuar, duke qenë se statistikat përbëjnë qëllim të përshtatshëm. Nuk nevojitet për këtë asnjë bazë ligjore shtesë, sikundër pëlqimi i subjekteve të të dhënave.

Nëse të njëjtat të dhëna do t'i transmetoheshin një pale të tretë, shoqërisë Starlight, për qëllime vetëm statistikore, transmetimi i të dhënave do të ishte i lejuar, pa bazë ligjore shtesë, por vetëm me masa sigurie të përshtatshme, si për shembull fshehja e identitetit të subjekteve të të dhënave, meqenëse identitetet zakonisht nuk nevojiten për qëllimet statistikore.

3.3. Parimi i cilësisë së të dhënave

Pikat kryesore

- Parimi i cilësisë së të dhënave duhet zbatuar nga kontrolluesi në të gjitha operacionet e përpunimit.
- Parimi i ruajtjes për afate kohore të kufizuara, detyron fshirjen e të dhënave, sapo ato nuk i shërbejnë më qëllimit për të cilin u mblodhën.
- Përjashtimet nga parimi i ruajtjes për afate kohore të kufizuara, duhet të parashikohen në ligj dhe duhet të ekzistojnë masa sigurie për mbrojtjen e subjekteve të të dhënave.

[121] Një shembull i këtyre dispozitave është Ligji i Austrisë për Mbrojtjen e të Dhënave (datenschutzgesetz), Fletorja Zyrtare Federale nr. 165/1999, parag. 46, varianti anglisht tek: www.dsk.gv.at/DocView.axd?CobId=41936.

3.3.1. Parimi i rëndësisë së të dhënave

Duhet të përpunohen vetëm ato lloje të dhënash të cilat janë "të përshtatshme, të rëndësishme dhe jo të tepërta në raport me qëllimin për të cilin ato janë mbledhur dhe/ose në vijim janë përpunuar".[122] Kategoritë e të dhënave të zgjedhura për përpunim, duhet të jenë të nevojshme për përmbushjen e qëllimit të përgjithshëm të deklaruar të operacioneve të përpunimit dhe kontrolluesi duhet ta kufizojë rreptësishtë mbledhjen e të dhënave vetëm tek informacionet të cilat janë drejtpërdrejtë të rëndësishme për qëllimin specifik që synon përpunimi.

Në shoqërinë bashkëkohore, parimi i rëndësisë së të dhënave ka një dimension tjetër: falë përdorimit të teknologjive speciale që përforcojnë mbrojtjen e privatësisë, ndonjëherë është e mundur të shmanget krejtësisht përdorimi i të dhënave personale, apo në vend të tyre të përdoren të dhëna të pseudonimizuara, zgjidhje e cila është e favorshme për respektimin e privatësisë dhe veçanërisht e përshtatshme në kuadër të sistemeve të përpunimit me shtrirje më të madhe.

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 kalohet përballë pajisjes lexuese të instaluar në autobus apo tramvaj. Të dhënat e lexuara nga pajisja, kontrollohen elektronikisht nëpërmjet një baze të dhënash që përmban emrat e njerëzve të cilët kanë blerë kartën e udhëtimit.

Ky lloj sistemi nuk përputhet plotësisht me parimin e rëndësisë së të dhënave: të kontrolluarit e 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 përdor cilat mjete dhe në çfarë kohe. Asnjë e dhënë personale nuk do të mblidhej, çka është zgjidhja optimale në kuptimin e parimit të rëndësisë, duke qenë se thelbi i këtij parimi është detyrimi për të minimizuar mbledhjen e të dhënave.

3.3.2. Parimi i saktësisë së të dhënave

Kontrolluesi i cili ruan informacione personale, nuk duhet t'i përdorë ato pa ndërmarrë më parë hapa për t'u bindur, me një farë sigurie të arsyeshme, se të dhënat janë të sakta dhe të përditësuara.

Detyrimi për të siguruar saktësinë e të dhënave duhet të shihet në kontekstin e qëllimit të përpunimit të të dhënave.

[122] Konventa 108, neni 5 (c); dhe Direktiva e Mbrojtjes së të Dhënave, neni 6 (1) (c).

Shembull: një shoqëri e shitjes së mobilieve kishte mbledhur identitetin dhe adresën e klientit, me qëllim që t'i dërgonte atij apo asaj faturën. Gjashtë muaj më vonë, e njëjta shoqëri dëshironte të niste një fushatë marketingu dhe të kontaktonte klientët e vjetër. Me qëllim që t'i kontaktonte, shoqëria kërkonte akses në regjistrin kombëtar të adresave të banimit, i cili përmban adresat e përditësuara, duke qenë se banorët janë ligjërisht të detyruar të informojnë regjistrin për adresat e tyre aktuale. Aksesi në të dhënat e regjistrit është i mundur vetëm për personat dhe njësitë të cilët apo të cilat kanë arsye të bazuara.

Në këtë situatë, shoqëria nuk mund të përdorë argumentin se të dhënat duhet të ruhen të sakta dhe të përditësuara, për të vërtetuar se ka të drejtë të mbledhë të dhënat e reja të adresave të të gjithë klientëve të saj të vjetër nga regjistri i adresave të banimit. Të dhënat ishin mbledhur për qëllime të dërgimit të faturës, për këtë arsye, adresa në kohën e kryerjes së shitjes është e rëndësishme. Nuk ka asnjë bazë ligjore për mbledhjen e të dhënave të reja të vendbanimit, duke qenë se marketingu nuk është interes që prevalon të drejtën për mbrojtje të të dhënave dhe për këtë shkak nuk mund të justifikojë aksesin në të dhënat e regjistrit.

Ka gjithashtu raste kur përditësimi i të dhënave të ruajtura është ligjërisht i ndaluar, pasi qëllimi i ruajtjes së të dhënave është kryesisht për dokumentimin e ngjarjeve.

Shembull: protokolli mjekësor i operacionit nuk duhet të ndryshohet, në fjalë të tjera nuk duhet "përditësuar", edhe nëse disa konkluzione të përmendura në protokoll, dalin më pas se kanë qenë të gabuara. Në këto rrethana, mund të bëhen vetëm shtesa tek komentet në protokoll, me kusht që ato të paraqiten në mënyrë të qartë si elemente të cilat janë shtuar në një fazë të mëvonshme.

Nga ana tjetër, ka situata kur verifikimi periodik i saktësisë së të dhënave, përfshirë edhe përditësimin, është domosdoshmëri absolute, për shkak të dëmit të mundshëm që mund të shkaktohet nëse të dhënat e subjektit të të dhënave do të mbeteshin të pasakta.

Shembull: nëse dikush dëshiron të nënshkruajë një kontratë me një institucion bankar, kjo e fundit zakonisht do të verifikojë besueshmërinë e klientit të mundshëm. Për ta bërë këtë, ekzistojnë baza të dhënash speciale, të cilat përmbajnë të dhëna në lidhje me historikun e kreditimit të individëve. Nëse kjo lloj baze të dhënash do të ofrojë të dhëna të pasakta apo jo të përditësuara në lidhje me një individ, ai person mund të përballet me probleme të mëdha. Për këtë arsye, kontrolluesit e këtyre bazave të të dhënave duhet të bëjnë përpjekje të veçanta për të përmbushur parimin e saktësisë.

Gjithashtu, të dhënat të cilat lidhen jo me faktet, por me dyshimet, si për shembull hetimet penale, mund të mblidhen dhe të ruhen nga kontrolluesi për aq kohë sa e përcakton kuadri ligjor për mbledhjen e këtij lloj informacioni dhe për sa kohë që krijimi i këtij dyshimi është i bazuar.

3.3.3. Parimi i kufizimit të kohëzgjatjes së ruajtjes së të dhënave

Neni 6, paragrafi (1), pika (e) e Direktivës së Mbrojtjes së të Dhënave dhe po ashtu edhe neni 5, pika (e) e Konventës 108, detyrojnë Shtetet Anëtare të garantojnë që të dhënat personale "ruhen në një formë e cila mundëson 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 mbledhur ose për të cilat janë përpunuar më tej." Për rrjedhojë, të dhënat duhet të fshihen, kur ato qëllime janë përmbushur.

Tek çështja *S. dhe Marper*, GjEDNj-ja doli në përfundimin se parimet thelbësore të instrumenteve përkatëse të Këshillit të Evropës dhe legjislacioni e praktika në fuqi e Palëve të tjera Kontraktuese, përcaktojnë që ruajtja e të dhënave të jetë proporcionale në raport me qëllimin e mbledhjes dhe e kufizuar në kohë, sidomos në sektorin e policisë.[123]

Sidoqoftë, kufizimi i kohëzgjatjes së ruajtjes së të dhënave personale gjen zbatim vetëm për të dhënat të cilat ruhen në një formë e cila mundëson identifikimin e subjekteve të të dhënave. Për këtë, ruajtja e ligjshme e të dhënave të cilat nuk nevojiten më, mund të bëhet duke anonimizuar ose pseudonimizuar të dhënat.

Ruajtja e të dhënave për t'i përdorur në të ardhmen për qëllime shkencore, historike apo statistikore, është qartësisht e përjashtuar nga parimi i kufizimit të kohëzgjatjes së ruajtjes së të dhënave tek Direktiva e Mbrojtjes së të Dhënave.[124] Megjithatë, kjo ruajtje e përdorim në vazhdimësi i të dhënave personale, duhet të shoqërohet me masa mbrojtjeje të posaçme.

3.4. Parimi i përpunimit të drejtë

Pikat kryesore

- Përpunim i drejtë nënkupton transparencën e përpunimit, sidomos në raport me subjektet e të dhënave.
- Kontrolluesit duhet t'i informojnë subjektet e të dhënave përpara përpunimit të të dhënave të tyre, të paktën në lidhje me qëllimin e përpunimit dhe mbi identitetin e adresën e kontrolluesit.
- Nuk duhet të kryhen përpunime sekrete dhe të fshehta të të dhënave personale, përveçse nëse lejohet shprehimisht me ligj.
- Subjektet e të dhënave kanë të drejtën e aksesit në të dhënat e tyre kudo që ato përpunohen.

Parimi i përpunimit të drejtë rregullon kryesisht marrëdhënien midis kontrolluesit dhe subjektit të të dhënave.

---

[123] GjEDNj, *S. dhe Marper kundër Mbretërisë së Bashkuar*, nr. 30562/04 dhe 30566/04, 4 dhjetor 2008; shih gjithashtu, për shembull: GjEDNj, *M.M. kundër Mbretërisë së Bashkuar*, nr. 24029/07, 13 nëntor 2012.

[124] Direktiva e Mbrojtjes së të Dhënave, neni 6 (1) (e).

3.4.1. Transparenca

Ky parim përcakton detyrimin për kontrolluesin që të mbajë të informuar subjektet e të dhënave, në lidhje me mënyrën se si po përdoren të dhënat e tyre.

Shembull: tek çështja *Haralambie kundër Rumanisë,*[125] ankuesi 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 vinin në dispozicion procedura të efektshme, për të mundësuar aksesin në këtë lloj 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 ankuesit për akses në dosjen e tij. Autoritet nuk i kishin ofruar ankuesit 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.

Operacionet e përpunimit duhet t'u shpjegohen subjekteve të të dhënave në mënyrë lehtësisht të kuptueshme, në mënyrë që ata të dinë se çfarë do të bëhet me të dhënat e tyre. Gjithashtu, subjekti i të dhënave ka të drejtën të dijë nga kontrolluesi, me kërkesën e tij, nëse të dhënat e tij apo të saj janë duke u përpunuar dhe nëse po, çfarë të dhënash.

3.4.2. Krijimi i besimit

Kontrolluesit duhet t'ua dokumentojnë subjekteve të të dhënave dhe publikut të gjerë, se do të përpunojnë të dhëna në mënyrë të ligjshme dhe transparente. Asnjë përpunim nuk duhet të kryhet në mënyrë sekrete dhe nuk duhet të ketë pasoja negative të paparashikuara. Kontrolluesit duhet të sigurohen se abonentët, klientët apo qytetarët, janë të informuar në lidhje me përdorimin e të dhënave të tyre. Gjithashtu, për aq sa është e mundur, kontrolluesit duhet të veprojnë në mënyrë të tillë që përshtatet shpejt me dëshirat e subjektit të të dhënave, sidomos aty ku pëlqimi i tij apo i saj, përbën bazën ligjore për përpunimin e të dhënave.

Shembull: tek çështja *K.H. dhe të Tjerët kundër Sllovakisë,*[126] ankueset ishin tetë gra me origjinë etnike rome, të cilat ishin shtruar në dy spitale, në Sllovakinë lindore, gjatë shtatzënisë dhe lindjes. Më pas, asnjëra prej tyre nuk mundej të mbetej shtatzënë sërish, pavarësisht përpjekjesh të përsëritura. Gjykatat vendase urdhëruan spitalet të lejonin ankueset dhe përfaqësuesit e tyre të shihnin kartelat mjekësore dhe të bënin kopje me shkrim dore të fragmenteve të saj, por rrëzuan kërkesën e tyre për të fotokopjuar dokumentet, me pretendimin se kishin për qëllim të parandalonin abuzimin me to. Ndër detyrimet që kanë shtetet sipas nenit 8 të KEDNj-së, përfshihet domosdoshmërish detyrimi për t'i vënë në dispozicion subjektit të të dhënave kopje të kartelës së të dhënave në lidhje me të. I takonte shtetit të përcaktonte modalitetet për kopjimin e kartelave të të dhënave personale, ose, nëse ishte e përshtatshme, të demonstronte arsyet për refuzimin e tij. Në rastin e ankueseve, gjykatat vendase e justifikuan ndalimin për të kopjuar kartelat mjekësore, me nevojën për të mbrojtur informacionin përkatës nga abuzimi me të.

---

[125] GjEDNj, *Haralambie kundër Rumanisë*, nr. 21737/03, 27 tetor 2009.
[126] GjEDNj, *K.H. dhe të Tjerët kundër Sllovakisë*, nr. 32881/04, 28 prill 2009.

Megjithatë, GjEDNj-ja nuk arriti dot të kuptonte se në ç'mënyrë ankueset, të cilave gjithsesi u ishte dhënë akses në tërësinë e kartelave mjekësore, mund të abuzonin me informacionin që kishte lidhje po me to. Për më tepër, rreziku nga abuzimi mund të parandalohej me mënyra të tjera, përkundër ndalimit për të kopjuar kartelat e ankueseve, si për shembull duke kufizuar numrin e personave të autorizuar për të pasur akses në kartela. Shteti nuk kishte demonstruar ekzistencën e arsyeve të mjaftueshme, për t'u mohuar ankueseve aksesin në informacionet që kishin të bënin me shëndetin e tyre. Gjykata doli me përfundimin se kishte pasur shkelje të nenit 8.

Sa i takon shërbimeve të internetit, karakteristikat e sistemeve të përpunimit të të dhënave, duhet t'u mundësojnë subjekteve të të dhënave të kuptojnë realisht se çfarë po ndodh me të dhënat e tyre.

Përpunim i drejtë do të thotë gjithashtu se kontrolluesit janë të përgatitur të shkojnë përtej kërkesave minimale ligjore të detyrueshme të shërbimit ndaj subjektit të të dhënave, kur këtë e kërkojnë interesat legjitime të subjektit të të dhënave.

3.5. Parimi i përgjegjshmërisë

Pikat kryesore

- Parimi i përgjegjshmërisë nevojit zbatimin aktiv nga ana e kontrolluesve të masave për të nxitur dhe garantuar mbrojtjen e të dhënave në aktivitetet e tyre përpunuese.
- Kontrolluesit janë përgjegjës për përputhshmëri të operacioneve të tyre përpunuese me legjislacionin për mbrojtjen e të dhënave.
- Kontrolluesit duhet të jenë gjithnjë në gjendje t'u demonstrojnë subjekteve të të dhënave, publikut të gjerë dhe autoriteteve mbikëqyrëse, përputhshmërinë me dispozitat e mbrojtjes së të dhënave.

Organizata për Bashkëpunim dhe Zhvillim Ekonomik (OECD) ka miratuar në 2013-ën, një udhërrëfyes mbi privatësinë, i cili theksonte se kontrolluesit luajnë rol të rëndësishëm për funksionimin në praktikë të mbrojtjes së të dhënave. Udhërrëfyesi zhvillon parimin e përgjegjshmërisë në kuptimin që "një kontrollues të dhënash duhet të jetë i përgjegjshëm për përputhshmërinë e masave të cilat bëjnë të zbatueshme parimet [materiale] të cituara më lart."[127]

Ndërsa Konventa 108 nuk e përmend përgjegjshmërinë e kontrolluesve, duke ia lënë në thelb këtë çështje legjislacionit kombëtar, neni 6 (2) i Direktivës së Mbrojtjes së të Dhënave thekson se kontrolluesi duhet të garantojë përputhshmëri me parimet e cilësisë së të dhënave, të përshkruara në paragrafin 1.

[127] OECD (2013), Udhërrëfyesi në lidhje me Mbrojtjen e Privatësisë dhe qarkullimet ndër-kufitare të të dhënave personale, neni 14.

Shembull: një model legjislativ për të theksuar parimin e përgjegjshmërisë, janë ndryshimet[128] e 2009-ës që ka pësuar Direktiva e Privatësisë dhe Komunikimeve Elektronike (2002/58/EC). Sipas nenit 4 të variantit të ndryshuar, direktiva përcakton një detyrim për të zbatuar një politikë sigurie, domethënë "për të siguruar zbatimin e një politike sigurie në lidhje me përpunimin e të dhënave personale". Kështu, për sa i përket dispozitave të sigurisë, ligjvënësi ka vlerësuar si të nevojshme ndërfutjen e një norme eksplicite të zbatimit të një politike sigurie.

Sipas opinionit[129] të Grupit të Punës së nenit 29, thelbi i përgjegjshmërisë është detyrimi i kontrolluesit:

- Për të zbatuar masa të cilat – në rrethana normale – garantojnë që rregullat e mbrojtjes së të dhënave të respektohen në kontekstin e përpunimeve; dhe
- Për të pasur në dispozicion dokumentacionin i cili u vërteton subjekteve të të dhënave dhe autoriteteve mbikëqyrëse se çfarë masash janë marrë për të siguruar respektim të rregullave të mbrojtjes së të dhënave.

Kështu, parimi i përgjegjshmërisë detyron kontrolluesit të demonstrojnë në mënyrë aktive përputhshmërinë dhe jo thjesht të presin që subjektet e të dhënave dhe autoritetet mbikëqyrës të vënë në dukje mangësitë.

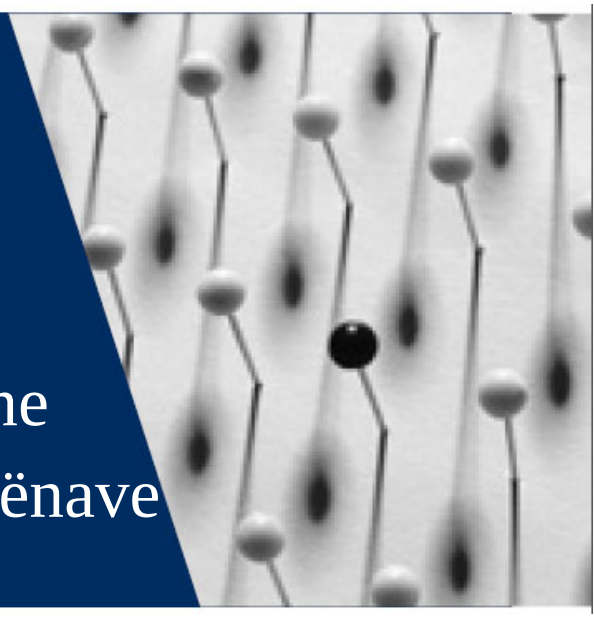
---

[128] Direktiva 2009/136/EC e Parlamentit Evropian dhe i Këshillit të 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, JO 2009 L 337, fq. 11.

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

4

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



BE	Çështje të trajtuara	KiE
Rregullat e përpunimit të ligjshëm të të dhënave jo sensitive		
Direktiva e Mbrojtjes së të Dhënave, neni 7 (a)	**Pëlqimi**	Rekomandimi i profilizimit, nenet 3.4 (b) dhe 3.6
Direktiva e Mbrojtjes së të Dhënave, neni 7 (b)	**Marrëdhëniet (para)kontraktuese**	Rekomandimi i profilizimit, neni 3.4 (b)
Direktiva e Mbrojtjes së të Dhënave, neni 7 (c)	**Detyrimet ligjore të kontrolluesit**	Rekomandimi i profilizimit, neni 3.4 (a)
Direktiva e Mbrojtjes së të Dhënave, neni 7 (d)	**Interesat jetikë të subjektit të të dhënave**	Rekomandimi i profilizimit, neni 3.4 (b)
Direktiva e Mbrojtjes së të Dhënave, neni 7 (e) dhe neni 8 (4) GjDBE, C-524/06, *Huber kundër Gjermanisë*, 16 dhjetor 2008	**Interesi publik dhe ushtrimi i autoriteti publik**	Rekomandimi i profilizimit, neni 3.4 (b)
Direktiva e Mbrojtjes së të Dhënave, neni 7 (f), neni 8 (2) dhe 8 (3) 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) kundër Administración del Estado*, 24 nëntor 2011	**Interesat legjitimë të të tretëve**	Rekomandimi i profilizimit, neni 3.4 (b)
Rregullat e përpunimit të ligjshëm të të dhënave sensitive		
Direktiva e Mbrojtjes së të Dhënave, neni 8 (1)	**Ndalimi i përgjithshëm i përpunimit**	Konventa 108, neni 6
Direktiva e Mbrojtjes së të Dhënave, neni 8 (2)-(4)	**Përjashtime nga ndalimi i përgjithshëm**	Konventa 108, neni 6
Direktiva e Mbrojtjes së të Dhënave, neni 8 (5)	**Përpunimi i të dhënave në lidhje me dënimet (penale)**	Konventa 108, neni 6

Direktiva e Mbrojtjes së të Dhënave, neni 8 (7)	**Numrat e identifikimit të përpunimit**	
Rregullat në lidhje me sigurinë e përpunimit		
Direktiva e Mbrojtjes së të Dhënave, neni 17	**Detyrimi për të garantuar sigurinë e përpunimit**	Konventa 108, neni 7 GjEDNj, *I. kundër Finlandës*, nr. 20511/03, 17 korrik 2008
Direktiva e Privatësisë dhe Komunikimeve Elektronike, neni 4 (2)	**Njoftimi për shkelje të të dhënave**	
Direktiva e Mbrojtjes së të Dhënave, neni 16	**Detyrimi për konfidencialitet**	
Rregullat në lidhje me transparencën e përpunimit		
	Transparenca në përgjithësi	Konventa 108, neni 8 (a)
Direktiva e Mbrojtjes së të Dhënave, nenet 10 dhe 11	**Informimi**	Konventa 108, neni 8 (a)
Direktiva e Mbrojtjes së të Dhënave, nenet 10 dhe 11	**Përjashtime nga detyrimi për të informuar**	Konventa 108, neni 9
Direktiva e Mbrojtjes së të Dhënave, nenet 18 dhe 19	**Njoftimi**	Rekomandimi i Profilizimit, neni 9.2 (a)
Rregullat në lidhje me nxitjen e përputhshmërisë		
Direktiva Mbrojtjes së të Dhënave, neni 20	**Kontrolli paraprak**	
Direktiva e Mbrojtjes së të Dhënave, neni 18 (2)	**Zyrtarët e mbrojtjes së të dhënave personale**	Rekomandimi i profilizimit, neni 8.3
Direktiva e Mbrojtjes së të Dhënave, neni 27	**Kodet e sjelljes**	

Parimet janë detyrimisht të natyrës së përgjithshme dhe zbatimi i tyre në situata konkrete lë një hapësirë të caktuar interpretimi dhe përzgjedhjeje mjetesh. Tek e **drejta e KiE-së,** i lihet Palëve të Konventës 108 qartësimi i kësaj hapësire interpretimi në legjislacionin e tyre vendas. Situata në **të drejtën e BE-së** është e ndryshme: për krijimin e një kuadri të mbrojtjes së të dhënave në tregun e brendshëm, është vlerësuar si e nevojshme të përcaktohen rregulla më të hollësishme në nivel BE-je, me qëllim që të harmonizohet niveli i mbrojtjes së të dhënave të legjislacioneve kombëtare të Shteteve Anëtare. Direktiva e Mbrojtjes së të Dhënave parashikon, bazuar në parimet e përcaktuara në nenin 6 të saj, një korpus normash të detajuara, të cilat duhen transpozuar besnikërisht në legjislacionin kombëtar. Për këtë arsye, shënimet e mëposhtme që kanë të bëjnë me normat e detajuara në fushën e mbrojtjes së të dhënave në nivel evropian, trajtojnë kryesisht të drejtën e BE-së.

4.1. Rregullat e përpunimit të ligjshëm

Pikat kryesore

- Të dhënat personale mund të përpunohen në mënyrë të ligjshme nëse:
- Përpunimi mbështetet në pëlqimin e subjektit të të dhënave; ose
- Përpunimi i të dhënave të subjekteve është i nevojshëm për interesat jetike të tyre; ose
- Shkaku për përpunimin janë interesat legjitimë të të tretëve, por vetëm për aq kohë sa nuk prevalohen nga interesat në lidhje me mbrojtjen e të drejtave themelore të

subjekteve të të dhënave.

- Përpunimi i ligjshëm i të dhënave sensitive i nënshtrohet një regjimi të veçantë dhe më rigoroz.

Direktiva e Mbrojtjes së të Dhënave përmban dy sete normash për përpunimin e ligjshëm të të dhënave: njëri për të dhënat jo sensitive (neni 7) dhe tjetri për të dhënat sensitive (neni 8).

4.1.1. Përpunimi i ligjshëm i të dhënave jo sensitive

Kapitulli II i Direktivës 95/46, i titulluar "Rregullat e përgjithshme të ligjshmërisë së përpunimeve të të dhënave personale" përcakton se, në varësi të përjashtimeve të parashikuara nga neni 13, të gjitha përpunimet e të dhënave personale duhet të përputhen pikë së pari me parimet e cilësisë së të dhënave, të përcaktuara në nenin 6 të Direktivës së Mbrojtjes së të Dhënave dhe së dyti, me një nga kriteret e nenit 7 që e bëjnë përpunimin të ligjshëm.[130] Ky nen shpjegon rastet kur përpunimet e të dhënave personale jo sensitive janë legjitime.

Pëlqimi

Sipas së drejtës së KiE-së, pëlqimi nuk përmendet në nenin 8 të KEDNj-së apo në Konventën 108. Gjithsesi, ai përmendet në jurisprudencën e GjEDNj-së dhe në disa rekomandime të KiE-së. **Sipas së drejtës së BE-së**, pëlqimi si bazë për përpunimin legjitim të të dhënave është përcaktuar në mënyrë solide në nenin 7 (a) të Direktivës së Mbrojtjes së të Dhënave dhe përmendet gjithashtu qartësisht në nenin 8 të Kartës.

Marrëdhëniet kontraktuese

Një tjetër bazë për përpunimin legjitim të të dhënave personale **sipas së drejtës së BE-së**, të përcaktuar në nenin 7 (b) të Direktivës së Mbrojtjes së të Dhënave, është "nëse nevojitet për përmbushur një kontratë, tek e cila subjekti është palë". Kjo dispozitë përfshin gjithashtu marrëdhëniet para-kontraktuese. Për shembull: një palë planifikon të lidhë një kontratë, por nuk e ka bërë ende këtë, për shkak se kanë mbetur disa verifikime për t'u bërë. Nëse një palë ka nevojë të përpunojë disa të dhëna për këtë qëllim, ky përpunim është legjitim për sa kohë që "kryhet me kërkesë të subjektit të të dhënave përpara lidhjes së një kontrate".

Sa i takon të drejtës së KiE-së, "mbrojtja e të drejtave dhe lirive të të tjerëve" përmendet në nenin 8 (2) të KEDNj-së si një arsye për ndërhyrje legjitime tek e drejta për mbrojtje të të dhënave.

---

[130] GjDBE, Çështje të bashkuara C-465/00, C-138/01 dhe C-139/01. *Rechnungshof kundër Österreichischer Rundfunk dhe të Tjerët dhe Neukomm dhe Lauermann kundër Österreichischer Rundfunk*, 20 maj 2003, parag. 65; GjDBE, C-524/06, *Huber kundër Gjermanisë*, 16 dhjetor 2008, parag. 48; 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) kundër Administración del Estado*, 24 nëntor 2011, parag. 26.

Detyrimet ligjore të kontrolluesit

E drejta e BE-së përmend në vijim qartësisht një tjetër kriter të legjitimimit të përpunimit të të dhënave, konkretisht nëse "është i nevojshëm për respektimin e një detyrimi ligjor të kontrolluesit" (neni 7 (c) i Direktivës së Mbrojtjes së të Dhënave. Ky nen i referohet kontrolluesve që veprojnë në sektorin privat; detyrimet ligjore të kontrolluesve të të dhënave të sektorit publik përcaktohen në nenin 7 (e) të direktivës. Ka shumë raste në të cilat kontrolluesit e sektorit privat janë të detyruar me ligj të përpunojnë të dhënat të të tjerëve; p.sh. mjekët dhe spitalet kanë detyrimin ligjor të ruajnë të dhënat e mjekimit të pacientëve të tyre për disa vite, punëdhënësit duhet të përpunojnë të dhënat e punonjësve të tyre për qëllime të sigurimeve shoqërore dhe të tatimeve dhe biznesi duhet të përpunojë të dhënat e klientëve të tyre për qëllime tatimore.

Në kontekstin e transferimit të detyrueshëm të të dhënave të pasagjerëve nga ana e shoqërive të fluturimit drejt autoriteteve të huaja të kontrollit të emigracionit, pyetja ngrihet në lidhje me faktin nëse detyrimet ligjore që burojnë nga një *legjislacion i huaj*, përbëjnë një bazë legjitime për përpunimin e të dhënave sipas së drejtës së BE-së (kjo çështje trajtohet me më shumë hollësi në paragrafin 6.2).

Detyrimet ligjore të kontrolluesit shërbejnë gjithashtu si bazë për përpunimin legjitim të të dhënave edhe **sipas së drejtës së KiE-së**. Sikurse është theksuar më parë, detyrimet ligjore të një kontrolluesi të sektorit publik, janë vetëm një rast specifik i interesave të të tjerëve, siç përmendet në nenin 8 (2) të KEDNj-së. Për këtë shkak, shembulli i mësipërm është gjithashtu i rëndësishëm nga pikëpamja e së drejtës së KiE-së.

Interesi jetik i subjektit të të dhënave

Sipas së drejtës së BE-së, neni 7 (d) i Direktivës së Mbrojtjes së të Dhënave parashikon se përpunimi i të dhënave personale është i ligjshëm nëse është "i nevojshëm për të mbrojtur interesat jetike të subjekteve të të dhënave". Këto interesa, të cilat kanë lidhje të ngushtë me mbijetesën e subjektit të të dhënave, mund të përbëjnë bazën për përdorimin legjitim, për shembull të të dhënave shëndetësore ose të personave të humbur.

Sipas së drejtës së KiE-së, interesat jetike të subjektit të të dhënave nuk përmenden në nenin 8 të KEDNj-së si shkak për ndërhyrje legjitime tek e drejta për mbrojtje të të dhënave. Gjithsesi, në disa prej rekomandimeve të KiE-së që plotësojnë Konventën 108 në fusha të caktuara, interesat jetike të subjektit të të dhënave përmenden qartësisht si kuadri për përpunimin legjitim të të dhënave.[131] Interesat jetike të subjektit të të dhënave konsiderohen qartësisht si të përfshira në grupin e arsyeve, që justifikojnë përpunimin e të dhënave: mbrojtja e të drejtave themelore nuk duhet të rrezikojë kurrë interesat jetike të personit të mbrojtur.

[131] Rekomandimi i profilizimit, neni 3.4 (b).

Interesi publik dhe ushtrimi i autoritetit publik

Duke iu referuar mënyrave të ndryshme të organizimit të aktiviteteve me karakter publik, neni 7 (e) të Direktivës së Mbrojtjes së të Dhënave përcakton se të dhënat personale mund të përpunohen ligjërisht nëse "është e nevojshme për përmbushjen e detyrës që kryhet për interesin publik ose për ushtrimin e autoritetit publik që gëzon kontrolluesi apo pala e tretë të cilës i komunikohen të dhënat [...]".[132]

Shembull: tek çështja *Huber kundër Gjermanisë*,[133] z. Huber, një shtetas austriak me banim në Gjermani, i kërkoi Zyrës Federale të Migracionit dhe Refugjatëve të fshinte të dhëna në lidhje me të, nga Regjistri Qendror i Shtetasve të Huaj (AZR-ja). Ky regjistër, i cili përmban të dhëna personale të shtetasve jo gjermanë të BE-së, që banojnë në Gjermani për më shumë se tre muaj, përdoret për qëllime statistikore dhe nga autoritetet e policisë e ato gjyqësore kur hetojnë dhe ndjekin aktivitetet penale ose ato që kërcënojnë sigurinë publike. Gjykata vendase kërkoi të dinte nëse përpunimi i të dhënave personale që kryhet në një regjistër sikurse Regjistri Qendror i Shtetasve të Huaj, tek i cili autoritetet publike kanë akses gjithashtu, ishte në përputhje me të drejtën e BE-së, duke qenë se një regjistër i tillë nuk ekzistonte për shtetasit gjermanë.

GjDBE-ja fillimisht vlerësoi se sipas nenit 7 (e) të direktivës, të dhënat personale mund të përpunohen në mënyrë të ligjshme, vetëm nëse përpunimi është i nevojshëm për përmbushjen e një detyre që kryhet në interes publik, ose për ushtrimin e një autoriteti publik.

Sipas Gjykatës, "duke pasur parasysh objektivin e sigurimit të një niveli të barasvlershëm të mbrojtjes në të gjitha Shtetet Anëtare, koncepti i domosdoshmërisë së përcaktuar në nenin 7 (e) të Direktivës 95/46 [...] nuk mund të ketë një kuptim që ndryshon nga një Shtet Anëtar në tjetrin. Ndaj, bëhet fjalë për një nocion autonom të së drejtës së Komunitetit, i cili duhet të interpretohet në mënyrë të tillë që të reflektojë objektivin e asaj direktive, sikurse përcaktohen në nenin 1 (1) të saj".[134]

Gjykata vërejti se e drejta e lëvizjes së lirë të një qytetari të Bashkimit në territorin e një Shteti Anëtar, në të cilin ai nuk është shtetasi tij, nuk është e pakushtëzuar, por mund t'i nënshtrohet kufizimeve dhe kushteve të përcaktuara nga Traktati dhe nga masat e miratuara me qëllim vënien e tij në zbatim. Kështu, nëse në parim, për një Shtet Anëtar, përdorimi i një regjistri si AZR-ja është legjitim, me qëllim mbështetjen e autoriteteve përgjegjëse për zbatimin e legjislacionin për të drejtën e qëndrimit, ky regjistër nuk duhet të përmbajë asnjë informacion tjetër përveç atij që është i nevojshëm për atë qëllim të veçantë. Gjykata përmbylli se një sistem i tillë për përpunimin e të dhënave personale pajtohet me të drejtën e BE-së vetëm nëse përmban të dhëna të nevojshme për zbatimin e atij legjislacioni dhe nëse natyra e tij e centralizuar e bën zbatimin e atij legjislacioni më të efektshëm. Gjykata vendase duhet të verifikojë nëse ato kushte janë plotësuar në atë rast. Nëse jo, ruajtja dhe përpunimi i të dhënave personale në një regjistër të tillë si AZR-ja, për qëllime statistikore, pavarësisht kuadrit të tij, nuk mund të konsiderohet si i nevojshëm, sipas kuptimit të nenit 7 (e) të Direktivës 95/46/EC.[135]

---

[132] Shih Direktivën e Mbrojtjes së të Dhënave, pikën 32.
[133] GjDBE, C-524/06, *Huber kundër Gjermanisë*, 16 dhjetor 2008
[134] Po aty, parag. 52.
[135] Po aty, parag. 54, 58, 59, 66-68.

Si përfundim, sa i takon çështjes së përdorimit të të dhënave të regjistrit për qëllimet e luftës kundër krimit, Gjykata u shpreh se ky objektiv "përfshin detyrimisht ndjekjen e krimeve dhe veprave penale të kryera, pavarësisht nacionalitetit të autorëve". Regjistri në fjalë nuk përmban të dhëna personale në lidhje me shtetasit e Shtetit Anëtar të përfshirë dhe ky ndryshim në trajtim përbën diskriminim, i cili ndalohet nga neni 18 i TFBE-së. Për këtë arsye, kjo dispozitë, sikurse interpretohet nga Gjykata, "pengon një Shtet Anëtar që të ngrejë një sistem të përpunimit të të dhënave personale posaçërisht për qytetarët e Bashkimit, të cilët nuk janë nënshtetas të atij Shteti Anëtar."[136]

Përdorimi i të dhënave personale nga autoritetet që veprojnë në sferën publike është gjithashtu subjekt i nenit 8 të KEDNj-së.

Interesat legjitimë të kontrolluesit apo palëve të treta

Subjekti i të dhënave nuk është i vetmi që ka interesa legjitimë. Neni 7 (f) i Direktivës për Mbrojtjen e të Dhënave parashikon se të dhënat personale mund të përpunohen në mënyrë të ligjshme nëse përpunimi është "i nevojshëm për qëllime të interesave legjitimë të kontrolluesit apo palëve të treta apo palëve tek të cilat komunikohet të dhënat, përveçse nëse këto interesa prevalohen nga interesat e të drejtave dhe lirive themelore të subjekteve të të dhënave, të cilat kërkojnë mbrojtje [...]".

Në gjykimin e çështjes në vijim, GjDBE-ja u shpreh në mënyrë eksplicite mbi nenin 7 (f) të direktivës:

Shembull: tek çështja ASNEF dhe FECEMD,[137] GjDBE-ja qartësoi se legjislacioni kombëtar nuk lejohet të shtojë kushte mbi ato të përmendura në nenin 7 (f) të Direktivës për Përpunimin e Ligjshëm të të dhënave. Kjo i referohej një situate kur legjislacioni spanjoll në fushën e mbrojtjes së të dhënave përmbante një dispozitë ku palë të tjera private mund të pretendonin se kishin interes legjitim të përpunonin të dhëna personale, vetëm nëse informacioni ishte bërë publik më parë.

Gjykata fillimisht vërejti se Direktiva 95/46/EC ka për qëllim të garantojë që niveli i mbrojtjes së të drejtave dhe lirive të individëve nga përpunimi i të dhënave personale, është ekuivalent në të gjitha Shtetet Anëtare. Por gjithashtu, përafrimi i legjislacioneve kombëtare në këtë fushë, nuk duhet të dobësojë mbrojtjen që ato ofrojnë, përkundrazi, ky përafrim duhet të ketë si qëllim të garantojë nivel të lartë të mbrojtjes në BE.[138] Në vijim, GjDBE-ja u shpreh se "neni 7 i Direktivës 95/46 përcakton një listë shteruese dhe të kufizuar të rasteve në të cilat përpunimi i të dhënave personale mund të konsiderohet i ligjshëm, bazuar në objektivin e saj për të garantuar nivel ekuivalent të mbrojtjes në të gjitha Shtetet Anëtare". Gjithashtu, "Shtetet Anëtare nuk mund të shtojnë parime të reja në lidhje me ligjshmërinë e përpunimit të të dhënave personale tek neni 7 i Direktivës 95/46 ose të përcaktojnë detyrime shtesë, të cilat sjellin si pasojë ndryshimin e qëllimit të një prej gjashtë parimeve të parashikuara në nenin 7."[139]

---

[136] Po aty, parag. 78 and 81.

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

[138] Po aty, parag. 28. Shih Direktivën e Mbrojtjes së të Dhënave, pikat 8 dhe 10.

[139] GjDBE, Çështje të bashkuara C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) dhe Federación de Comercio Electrónico y Marketing Directo (FECEMD) kundër Administración del Estado*, 24 nëntor 2011, parag. 30 dhe 32.

Gjykata pranoi se, në lidhje me ekuilibrimin, i cili është i nevojshëm bazuar në nenin 7 (f) të Direktivës 95/46/EC, "është e mundur të merret në konsideratë fakti se serioziteti i shkeljes së të të drejtave themelore të subjekteve të të dhënave, për shkak të përpunimit, mund të ndryshojë në varësi të faktit nëse të dhënat në fjalë ishin bërë publike më parë ose jo."

Bazuar në këto vlerësime, Gjykata doli në përfundimin se "neni 7 (f) i Direktivës 95/46 duhet të interpretohet si pengues i çdo rregulloreje kombëtare, e cila në mungesë të pëlqimit të subjektit të të dhënave dhe për të autorizuar përpunimin e të dhënave personale të tij të nevojshme për përmbushjen e interesit legjitim të kontrolluesit apo të të tretit ose të të tretëve të cilëve u janë komunikuar të dhënat, kërkon jo vetëm që të respektohen të drejtat dhe liritë themelore të subjektit të të dhënave, por edhe që të dhënat të jenë publike, duke përjashtuar në mënyrë kategorike dhe të përgjithësuar, çdo lloj përpunimi të dhënash që nuk nuk janë bërë publike më parë[140]".

Formulime të ngjashme mund të gjenden edhe në rekomandimet e KiE-së. Rekomandimi i Profilizimit e njeh si legjitim përpunimin e të dhënave personale për qëllime të profilizimit, nëse ai është i nevojshëm për interesat legjitimë të të tjerëve, "përveçse nëse këto interesa nuk prevalohen nga të drejtat dhe liritë themelore të subjekteve të të dhënave".[141]

4.1.2. Përpunimi i ligjshëm i të dhënave sensitive

E drejta e KiE-së ia lë në dorë legjislacionit kombëtar përcaktimin e mbrojtjes së përshtatshme për përdorimin e të dhënave sensitive, ndërsa **e drejta e BE-së,** në nenin 8 të Direktivës së Mbrojtjes së të Dhënave përfshin një regjim të detajuar për përpunimin e kategorive të të dhënave që tregojnë: origjinën racore apo etnike, mendimet politike, besimet fetare apo filozofike, anëtarësimin në sindikata apo informacion në lidhje me shëndetin apo jetën seksuale. Përpunimi i të dhënave sensitive, në parim, është i ndaluar.[142] Gjithsesi, ekziston një listë shteruese përjashtimesh përkundër këtij ndalimi, e cila mund të gjendet në nenin 8 (2) dhe (3) të Direktivës. Këto përjashtime përfshijnë pëlqimin eksplicit të subjektit të të dhënave, interesat jetikë të subjektit të të dhënave, interesat legjitimë të të tjerëve dhe interesin publik.

Përkundër rastit të përpunimit të të dhënave jo sensitive, një marrëdhënie kontraktuese me subjektin e të dhënave, nuk konsiderohet si bazë e përgjithshme për përpunimin legjitim të të dhënave sensitive. Për rrjedhojë, nëse të dhënat sensitive duhet të përpunohen në kuadër të një kontrate me subjektin e të dhënave, përdorimi i këtyre të dhënave nevojit pëlqimin përkatës eksplicit të subjektit të të dhënave, përveç miratimit të lidhjes së kontratës. Kërkesa eksplicite e subjektit të të dhënave, për mallra apo shërbime të cilat domosdoshmërish zbulojnë të dhëna sensitive, duhet gjithsesi të konsiderohet si ekuivalente me pëlqimin eksplicit.

Shembull: nëse një pasagjer i një shoqërie fluturimi, në kuadër të rezervimit të një fluturimi, kërkon nga shoqëria e fluturimit të vënë në dispozicion të tij një karrige me rrota dhe ushqim kosher, shoqëria e fluturimit lejohet të përdorë këto të dhëna dhe nëse pasagjeri nuk ka nënshkruar një klauzolë shtesë pëlqimi, ku të deklarojë se ai apo ajo pranon përdorimin e të dhënave të tij, të cilat zbulojnë informacion në lidhje me shëndetin dhe besimin e tij fetar.

[140] Po aty, parag. 40, 44, 48 dhe 49
[141] Rekomandimi i profilizimit, neni 3.4 (b).
[142] Direktiva e Mbrojtjes së të Dhënave, neni 8 (1).

Pëlqimi eksplicit i subjektit të të dhënave

Kushti i parë për përpunimin e ligjshëm të çdo të dhëne, pavarësisht nëse janë të dhëna sensitive ose jo, është pëlqimi i subjektit të të dhënave. Në rastin e të dhënave sensitive, ky pëlqim duhet të jetë eksplicit. Gjithsesi, legjislacioni kombëtar mund të përcaktojë se dhënia e pëlqimit për përdorimin e të dhënave sensitive nuk përbën bazë ligjore të mjaftueshme, për të lejuar përpunimin e tyre,[143] për shembull kur në disa raste të veçanta, përpunimi përfshin rreziqe të pazakonta për subjektin e të dhënave.

Në një rast të veçantë, edhe pëlqimi i nënkuptuar përbën bazë ligjore për përpunimin e të dhënave sensitive: neni 8 (2) i Direktivës parashikon se përpunimi nuk është i ndaluar, nëse ai ka lidhje me të dhëna të cilat janë bërë haptazi publike nga subjekti i të dhënave. Kjo dispozitë parashtron dukshëm se veprimi i subjektit të të dhënave për publikimin e të dhënave të tij apo të saj, duhet të interpretohet si pëlqim i nënkuptuar i subjektit të të dhënave për përdorimin e këtyre të dhënave.

Interesat jetikë të subjektit të të dhënave

Ashtu si në rastin e të dhënave jo sensitive, të dhënat sensitive mund të përpunohen për shkak të interesave jetikë të subjektit të të dhënave.[144]

Që përpunimi i të dhënave bazuar në të të jetë legjitim, është e nevojshme që të ketë qenë e pamundur për t'ia lënë subjektit të të dhënave që të vendosë, pasi, për shembull, subjekti i të dhënave ka qenë i pavetëdijshëm ose nuk ka qenë i pranishëm e nuk mund të kontaktohej.

Interesat legjitimë të të tjerëve

Ashtu si për të dhënat jo sensitive, interesat legjitimë të tjerëve mund të shërbejnë si bazë për përpunimin e të dhënave sensitive. Gjithsesi, për të dhënat sensitive dhe në përputhje me nenin 8 (2) të Direktivës së Mbrojtjes së të Dhënave, kjo gjen zbatim vetëm në rastet në vijim:

- Kur përpunimi është i nevojshëm për shkak të interesave jetikë të një personi tjetër[145], kur subjekti i të dhënave është i paaftë fizikisht apo juridikisht të japë pëlqimin e tij;
- Kur të dhënat sensitive janë të rëndësishme në fushën e punësimit, si për shembull të dhënat e shëndetit, sikurse në kontekstin e një vendi pune me rrezikshmëri të veçantë, apo të dhënat e besimit fetar, si për shembull në kontekstin e pushimeve;[146]
- Kur fondacionet, shoqatat apo organizma të tjera jo fitimprurëse me mision politik, filozofik, fetar apo sindikalist, përpunojnë të dhëna në lidhje me anëtarët e tyre ose financuesit apo palët e tjera të interesuara (këto të dhëna janë sensitive sepse kanë të ngjarë të zbulojnë bindjet fetare apo politike të personave të përfshirë);[147]
- Kur të dhënat sensitive përdoren në kontekstin e procedimeve ligjore në një gjykatë apo autoritet administrativ për vendosjen, ushtrimin apo mbrojtjen e një të drejte në rrugë gjyqësore.[148]

---

[143] Po aty, neni 8 (2) (a).
[144] Po aty, neni 8 (2) (c).
[145] Po aty.
[146] Po aty, neni 8 (2) (b).
[147] Po aty, neni 8 (2) (d).
[148] Po aty, neni 8 (2) (e).

- Gjithashtu, sipas nenit 8 (3) të Direktivës së Mbrojtjes së të Dhënave, kur të dhënat shëndetësore përdoren për ekzaminim mjekësor dhe mjekim nga stafi i kujdesit shëndetësor, menaxhimi i këtyre shërbimeve përfshihet në këtë përjashtim. Në cilësinë e një garancie të veçantë, personat konsiderohen "staf i kujdesit shëndetësor" vetëm nëse janë subjekt i detyrimit profesional për konfidencialitet.

Interesi publik

Gjithashtu, në përputhje me nenin 8 (4) të Direktivës së Mbrojtjes së të Dhënave, Shtetet Anëtare mund të parashikojnë qëllime të tjera sipas së cilave mund të përpunohen të dhënat sensitive, për sa kohë që:

- Përpunimi i të dhënave bëhet për arsye të interesit të rëndësishëm publik; dhe
- Parashikohet nga legjislacioni kombëtar ose bazohet në vendimin e autoriteti mbikëqyrës; dhe
- E drejta kombëtare ose vendimi i autoritetit mbikëqyrës përmban garancitë e nevojshme për mbrojtjen me efektshmëri të interesave të subjekteve të të dhënave.[149]

Një shembull domethënës janë sistemet e kartelave elektronike mjekësore, të cilat do të ngrihen së shpejti në shumë Shtete Anëtare. Këto sisteme mundësojnë që të dhënat e shëndetit, të mbledhura nga stafi i kujdesit shëndetësor gjatë trajtimit të pacientëve, t'u vihen në dispozicion edhe stafeve të tjera të kujdesit shëndetësor që trajtojnë atë pacient në shkallë të gjerë, zakonisht në nivel kombëtar.

Grupi i Punës së Nenit 29 ka dalë në përfundimin se ngritja e këtyre lloj sistemeve, nuk mund të bëhet bazuar në rregullat ekzistuese për përpunimin e të dhënave të pacientëve, duke iu referuar nenit 8 (3) të Direktivës së Mbrojtjes së të Dhënave. Duke supozuar se ekzistenca e këtyre kartelave elektronike mjekësore përbën interes publik të rëndësishëm, ky sistem mund të bazohet në nenin 8 (4) të Direktivës, çka nevojit bazë ligjore të qartë për ngritjen e tyre, që të përmbajë garancitë e nevojshme për të garantuar se sistemi po përdoret me siguri të plotë.[150]

4.2 Rregullat në lidhje me sigurinë e përpunimit

Pikat kryesore

- Rregullat në lidhje me sigurinë e përpunimit përfshijnë detyrimin e kontrolluesit dhe përpunuesit për të marrë masat e përshtatshme teknike dhe organizative, me qëllim që të parandalohet çdo ndërhyrje e paautorizuar në operacionet e përpunimit të të dhënave.
- Niveli i nevojshëm i sigurisë së të dhënave përcaktohet nga:
- Karakteristikat e sigurisë së disponueshme në treg, për çdo lloj të veçantë përpunimi; dhe
- Kostot;
- Natyra sensitive e të dhënave të përpunuara.
- Përpunimi i sigurt i të dhënave garantohet gjithashtu nga detyrimi i përgjithshëm që zbatohet për të gjithë personat, kontrolluesit ose përpunuesit, për të ruajtur konfidencialitetin e të dhënave.

[149] Po aty, neni 8 (4)

[150] Grupi i Punës së Nenit 29 (2007), *Dokument Pune mbi përpunimin e të dhënave personale në lidhje me shëndetin në kartelat elektronike mjekësore (DEM*), WP 131, Bruksel, 15 shkurt 2007.

Detyrimi që kanë kontrolluesit dhe përpunuesit për të marrë masat e përshtatshme për të garantuar sigurinë e të dhënave është pra i përcaktuar **në të drejtën e KiE-së në fushën e mbrojtjes së të dhënave** ashtu si edhe **në të drejtën e BE-së në fushën e mbrojtjes së të dhënave**.

4.2.1. Elementet e sigurisë së të dhënave

Sipas dispozitave përkatëse **në legjislacionin e BE-së**:

"Shtetet Anëtare duhet të garantojnë që kontrolluesi të marrë masat e përshtatshme teknike dhe organizative, për të mbrojtur të dhënat personale nga shkatërrimi aksidental apo i paligjshëm apo nga humbja aksidentale, modifikimi, përhapja apo aksesi i paautorizuar, sidomos aty ku përpunimi përfshin transmetimin e të dhënave në një rrjet dhe nga format e tjera të paligjshme të përpunimit".[151]

Një dispozitë e ngjashme ekziston edhe **në legjislacionin e KiE-së**:

"Duhen marrë masat e përshtatshme të sigurisë, për mbrojtjen e të dhënave personale që ruhen në skedarë të automatizuar të dhënash, nga shkatërrimi aksidental apo i paautorizuar apo humbja aksidentale, ashtu si edhe nga aksesi, modifikimi apo përhapja e paautorizuar."[152]

Shpesh janë hartuar edhe norma industriale, kombëtare dhe ndërkombëtare, të cilat synojnë përpunim të sigurt të të dhënave. Vula Evropiane e Privatësisë (EuroPriSe), për shembull, është një projekt eTen (Rrjetet Trans-Evropiane të Telekomunikacioneve) i BE-së, e cila ka shqyrtuar mundësitë për të certifikuar produktet, sidomos programet kompjuterike, si në përputhje me të drejtën evropiane në fushën e mbrojtjes së të dhënave. Agjencia Evropiane për Sigurinë e Rrjeteve dhe Informacionit (ENISA) u krijua për të përmirësuar kapacitetet BE-së, Shteteve Anëtare të BE-së dhe komunitetit të biznesit, për të parandaluar, trajtuar dhe për t'iu përgjigjur problemeve të sigurisë së rrjeteve dhe informacionit.[153] ENISA publikon rregullisht analiza të kërcënimeve aktuale ndaj sigurisë dhe këshilla në lidhje me mënyrën se si mund të zgjidhen ato.

Siguria e të dhënave nuk arrihet vetëm duke pasur pajisjet e duhura – pajisje elektronike dhe programe kompjuterike. Ajo nevojit gjithashtu rregulla organizative të brendshme të përshtatshme, të cilat, në rastin më të mirë, duhet të mbulojnë pikat në vijim:

- Informimi i rregullt i të gjithë punonjësve në lidhje me rregullat e sigurisë së mbrojtjes së të dhënave dhe detyrimeve të tyre sipas legjislacionit të mbrojtjes së të dhënave, sidomos në lidhje me detyrimet e tyre për konfidencialitet;
- Shpërndarje e qartë e përgjegjësive dhe një përcaktim i qartë i kompetencave në çështjet e përpunimit të të dhënave, veçanërisht në lidhje me vendimet për të përpunuar të dhëna personale dhe për të transferuar drejt palëve të treta;
- Përdorimi i të dhënave personale në përputhje me udhëzimet e personit kompetent ose në përputhje me rregullat e përgjithshme të përcaktuara;

---

[151] Direktiva e Mbrojtjes së të Dhënave, neni 17 (1).
[152] Konventa 108, neni 7.
[153] Rregullorja (EC) nr. 460/2004 e Parlamentit Evropian dhe e Këshillit e 10 marsit 2004 që krijon Agjencinë Evropiane të Sigurisë së Rrjeteve dhe të Informacionit, JO 2004 L 77.

- Mbrojtja e aksesit në ambiente dhe në pajisje elektronike e programeve kompjuterike të kontrolluesit ose përpunuesit, përfshirë kontrollet e autorizimeve për akses;
- Të garantuarit se autorizimet për akses në të dhënat personale, janë dhënë nga personi kompetent, nëpërmjet paraqitjes së dokumentacionit të përshtatshëm;
- Protokolle të automatizuara të aksesit në të dhënat personale, nëpërmjet pajisjeve elektronike dhe kontrolle të rregullta të këtyre protokolleve nga ana e shërbimit të kontrollit të brendshëm;
- Dokumentim i kujdesshëm për format e tjera të përhapjes, përveç aksesit automatik të të dhënave, me qëllim që të demonstrohet se nuk ka ndodhur asnjë transmetim i paligjshëm të dhënash.

Një element tjetër i rëndësishëm për masa të efektshme sigurie, është trajnimi dhe edukimi i përshtatshëm i anëtarëve të stafit në lidhje me sigurinë e të dhënave. Duhen përcaktuar gjithashtu procedura verifikimi, me qëllim që të garantohet se masat e duhura nuk ekzistojnë vetëm në letër, por se ato zbatohen dhe funksionojnë në praktikë (sikundër auditimet e brendshme dhe të jashtme).

Masat për përmirësimin e nivelit të sigurisë së kontrolluesit apo përpunuesit, përfshijnë instrumente të tilla sikurse janë zyrtarët e mbrojtjes së të dhënave personale, edukimi i punonjësve në lidhje me sigurinë, auditimet e brendshme, testimet e mundësisë së depërtimit dhe certifikimet e cilësisë.

Shembull: tek çështja *I. Kundër Finlandës,*[154] ankuesi nuk kishte mundësi të provonte që disa punonjës të tjerë të spitalit ku ajo kishte punuar, kishin pasur akses të paligjshëm në kartelën e saj shëndetësore. Për këtë arsye, pretendimi i saj për shkelje të së drejtës për mbrojtje të të dhënave, ishte rrëzuar nga gjykatat vendase. GjEDNj-ja doli në përfundimin se kishte pasur shkelje të nenit 8 të KEDNj-së, duke qenë se sistemi i regjistrimit të spitalit për kartelat shëndetësore "ishte i tillë që nuk mundësonte qartësimin retroaktiv të përdorimit të kartelave të pacientëve, duke qenë se tregonte vetëm pesë kërkimet më të fundit dhe se ky informacion fshihej sapo kartela kthehej në arkiv". Për Gjykatën, duke qenë se sistemi i regjistrimit të spitalit nuk kishte qenë në përputhje me kërkesat ligjore të së drejtës kombëtare, ishte elementi përcaktues, të cilit gjykatat vendase nuk i kishin dhënë rëndësinë e duhur.

Njoftimet për shkeljen e të dhënave

Në të drejtën e disa shteteve evropiane në fushën e mbrojtjes së të dhënave është ndërfutur një instrument i ri për të menaxhuar shkeljet e sigurisë së të dhënave. Ky instrument konsiston në detyrimin që kanë operatorët e shërbimeve të komunikimeve elektronike për t'ua njoftuar shkeljet e të dhënave viktimave të mundshme dhe autoriteteve mbikëqyrëse. Për operatorët e telekomunikacioneve, ky është detyrim sipas legjislacionit të BE-së.[155]

[154] GjEDNj, *I. kundër Finlandës*, nr. 20511/03, 17 korrik 2008.

[155] Shih Direktivën 2002/58/EC të Parlamentit Evropian dhe Këshillit të 12 korrikut 2002, në lidhje me përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike (*Direktiva e privatësisë dhe komunikimeve elektronike*), JO 2002 L 201, neni 4 (3), ndryshuar me Direktivën 2009/136/EC të Parlamentit Evropian dhe Këshillit të 29 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; shih gjithashtu Direktivën 2002/58/EC në lidhje me përpunimin e 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, JO 2009 L 337

Qëllimi i njoftimit të subjekteve të të dhënave për shkeljet e të dhënave, është që të shmangen dëmet: njoftimi për shkeljet e të dhënave dhe pasojat e tyre të mundshme, minimizojnë rrezikun e pasojave negative tek subjektet e të dhënave. Në raste neglizhence të rëndë, operatorët mund edhe të gjobiten. Do të jetë i nevojshëm përcaktimi paraprak i procedurave të brendshme, për menaxhimin me efikasitet dhe raportimin e shkeljeve të sigurisë, duke qenë se afati kohor për detyrimin për t'u raportuar subjekteve të të dhënave dhe/ose autoriteti mbikëqyrës, sipas legjislacionit kombëtar, është zakonisht shumë i shkurtër.

4.2.2. Konfidencialiteti

Tek e drejta e BE-së, përpunimi i sigurt i të dhënave garantohet gjithashtu nëpërmjet detyrimit të përgjithshëm që u vendoset të gjithëve, kontrolluesve dhe përpunuesve, për të ruajtur konfidencialitetin e të dhënave.

Shembull: Një punonjës i një shoqërie sigurimesh, merr një telefonatë në vendin e punës nga dikush që paraqitet si klient, i cili 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.

Neni 16 i Direktivës së Mbrojtjes së të Dhënave ka të bëjë vetëm me konfidencialitetin në kuadër të marrëdhënies midis kontrolluesit dhe përpunuesit. Nëse kontrolluesit duhet të ruajnë konfidencialitetin e të dhënave ose jo, në kuptimin që ato nuk duhet t'i përhapin tek palë të treta, trajtohet nga nenet 7 dhe 8 të Direktivës.

Detyrimi për konfidencialitet nuk mbulon situatat në të cilat të personi njihet me të dhënat në cilësinë e personit privat dhe jo si një punonjës i kontrolluesit apo përpunuesit. Në atë rast, neni 16 i Direktivës së Mbrojtjes së të Dhënave nuk gjen zbatim, duke qenë se në fakt, përdorimi i të dhënave personale nga individët privatë, përjashtohet krejtësisht nga qëllimi i Direktivës, për shkak se ky lloj përdorimi bën pjesë në të ashtuquajturin "përjashtim familjar".[156] Përjashtimi familjar është përdorimi i të dhënave personale "nga një person fizik gjatë kryerjes së aktivitetit krejtësisht personal apo familjar"[157] Gjithsesi, pas vendimit të GjDBE-së për çështjen *Bodil Lindqvist*,[158] ky përjashtim duhet të interpretohet ngushtësisht, sidomos sa i takon përhapjes së të dhënave. Në mënyrë të veçantë, përjashtimi familjar, nuk do të shtrihet tek publikimi i të dhënave personale për një numër të pakufizuar marrësish në internet (për më shumë hollësi në lidhje me çështjen, shih paragrafët 2.1.2, 2.2, 2.3.1 dhe 6.1).

Sipas së drejtës së KiE-së, detyrimi për konfidencialitet nënkuptohet tek nocioni i sigurisë së të dhënave, në nenin 7 të Konventës 108, i cili trajton sigurinë e të dhënave.
Për përpunuesit, konfidencialitet do të thotë se ata mund të përdorin të dhënat personale që u ka besuar kontrolluesi vetëm në përputhje me udhëzimet e kontrolluesit. Për punonjësit e një kontrolluesi apo përpunuesi, konfidencialiteti i detyron të përdorim të dhënat personale vetëm në përputhje me udhëzimet e eprorëve të tyre kompetentë.

[156] Direktiva e Mbrojtjes së të Dhënave, neni 3 (2), fjalia e dytë.
[157] Po aty.
[158] GjDBE, C-101/01, *Lindqvist*, 6 nëntor 2003.

Detyrimi për konfidencialitet duhet të përfshihet në çdo kontratë ndërmjet kontrolluesve dhe përpunuesve të tyre. Gjithashtu, kontrolluesit dhe përpunuesit do të duhet të marrin masa specifike për të përcaktuar një detyrim ligjor konfidencialiteti për punonjësit e tyre, e cila arrihet normalisht duke përfshirë klauzola konfidencialiteti në kontratën e punësimit të punonjësit.

Shkelja e detyrimeve profesionale për konfidencialitet, është e dënueshme nga legjislacioni penal në shumë Shtete Anëtare të BE-së dhe Palë të Konventës 108.

4.3. Rregullat në lidhje me transparencën e përpunimit

Pikat kryesore

- Përpara nisjes së përpunimit të të dhënave personale, kontrolluesi duhet të paktën të informojë subjektet e të dhënave mbi identitetin e kontrolluesit dhe qëllimin e përpunimit të të dhënave, përveçse nëse subjekti i të dhënave është i informuar më parë në lidhje me të.
- Kur të dhënat janë mbledhur nga palë të treta, detyrimi për të dhënë informacion nuk gjen zbatim nëse:
- Përpunimi i të dhënave parashikohet në ligj; ose
- Dhënia e informacion rezulton e pamundur ose do të kërkonte përpjekje të tepruara.
- Përpara nisjes së përpunimit të të dhënave personale, kontrolluesi duhet po ashtu:
- Të njoftojë autoritetin mbikëqyrës për operacionet përpunuese të parashikuara; ose
- Të dokumentojë përpunimin në mënyrë të brendshme, nëpërmjet një zyrtari të mbrojtjes së të dhënave personale të pavarur, nëse e drejta kombëtare parashikon një procedurë të tillë.

Parimi i përpunimit të drejtë kërkon transparencë të përpunimit. E drejta e KiE-së përcakton për këtë qëllim se çdo person duhet të ketë dijeni mbi ekzistencën e përpunimit të të dhënave, qëllimin e tij dhe kontrolluesit përgjegjës.[159] Mënyra se si duhet arritur kjo, i është lënë legjislacionit vendas. **E drejta e BE-së** është më specifike, meqenëse garanton transparencë për subjektin e të dhënave, me anë të detyrimit të kontrolluesit për të informuar subjektin e të dhënave dhe për publikun në përgjithësi me anë të njoftimit.

Sipas të dy sistemeve ligjore, përjashtimet dhe kufizimet nga detyrimet e kontrolluesit për transparencë, mund të mbulohen nga legjislacioni vendas, kur këto kufizime përbëjnë një mase të nevojshme për të garantuar disa interesa publike ose mbrojtjen e subjektit të të dhënave ose të së drejtave dhe lirive të të tjerëve, për aq sa është e nevojshme në një shoqëri demokratike.[160] Këto përjashtime, për shembull, mund të jenë të nevojshme në kuadër të hetimit të krimit, por mund të jenë po ashtu të justifikuara në rrethana të tjera.

4.3.1. Informimi

Në përputhje me të drejtën e KiE-së dhe të BE-së, kontrolluesit janë të detyruar të informojnë subjektin e të dhënave, përpara përpunimit që ata parashikojnë të kryejnë.[161]

[159] Konventa 108, neni 8 (a).
[160] Po aty, neni 9 (2) dhe Direktiva e Mbrojtjes së të Dhënave, neni 13 (1).
[161] Konventa 108, neni 8 (a); dhe Direktiva e Mbrojtjes së të Dhënave, neni 10 dhe 11.

Ky detyrim nuk varet nga kërkesa e subjektit të të dhënave, por duhet të respektohet në mënyrë proaktive nga kontrolluesi, pavarësisht nëse subjekti i të dhënave shfaq interes për informacionin ose jo.

Përmbajtja e informacionit

Informacioni duhet të përmbajë qëllimin e përpunimit, ashtu si edhe identitetin dhe të dhënat e kontaktit të kontrolluesit.[162] Direktiva e Mbrojtjes së të Dhënave përcakton që duhet të jepet informacion shtesë, kur kjo "është e nevojshme, duke pasur parasysh rrethanat specifike të mbledhjes së të dhënave, për t'i garantuar subjektit të të dhënave përpunim të drejtë". Nenet 10 dhe 11 të Direktivës, përcaktojnë ndër të tjera, kategoritë e të dhënave të përpunuara dhe marrësit e këtyre të dhënave, ashtu si edhe ekzistencën e së drejtës për akses në to dhe të së drejtës për të korrigjuar të dhënat. Kur të dhënat mblidhen nga subjektet e të dhënave, informacioni duhet të shpjegojë nëse përgjigjet ndaj pyetjeve janë të detyrueshme apo fakultative, ashtu si edhe pasojat e mundshme në rast mungese përgjigjeje.[163]

Nga këndvështrimi i legjislacionit të KiE-së, transmetimi i këtij lloj informacioni mund të konsiderohet si praktikë e mirë, referuar parimit të përpunimit të drejtë të të dhënave dhe në të njëjtën masë, është gjithashtu pjesë e së drejtës së KiE-së.

Parimi i përpunimit të drejtë kërkon që informacioni të jetë lehtësisht i kuptueshëm nga subjektet e të dhënave. Duhet përdorur një gjuhë e cila të jetë e përshtatshme për personat të cilëve u drejtohet. Niveli dhe lloji i gjuhës së përdorur duhet të jenë të ndryshme nëse i drejtohet një publiku të rriturish apo fëmijësh, publikut të përgjithshëm apo ekspertëve të lartë.

Disa subjekte të dhënash do të duan të informohen vetëm shkurtimisht mbi mënyrën se si dhe pse po përpunohen të dhënat e tyre, ndërkohë që të tjerë do të kërkojnë shpjegime më të hollësishme. Grupi i Punës së Nenit 29 e ka trajtuar në një opinion mënyrën se si ekuilibrohet ky aspekt i informimit të drejtë dhe mbështet idenë e njoftimeve të përshkallëzuara,[164] të cilat i mundësojnë subjektit të të dhënave të vendosë se cilin nivel shpjegimesh në detaje ai apo ajo preferon.

Koha kur duhet dhënë informacioni

Direktiva e Mbrojtjes së të Dhënave përmban dispozita lehtësisht të ndryshme në lidhje me kohën kur duhet dhënë informacioni, e cila varet nga koha kur të dhënat janë mbledhur nga subjekti i të dhënave (neni 10) apo nga një palë e tretë (neni 11). Në rastin kur të dhënat janë mbledhur nga subjekti i të dhënave, informacioni duhet dhënë si afat i fundit, në momentin e mbledhjes. Kur të dhënat janë mbledhur nga palët e treta, informacioni duhet dhënë si afat i fundit ose në momentin kur kontrolluesi regjistron të dhënat, ose përpara se sa të dhënat t'i komunikohen një pale të tretë për here të parë.

[162] Konventa 108, neni 8 (a); dhe Direktiva e Mbrojtjes së të Dhënave, neni 10 (a) dhe (b).
[163] Direktiva e Mbrojtjes së të Dhënave, neni 10 (c).
[164] Grupi i Punës së Nenit 29 (2004), *Opinioni 10/2004 mbi Dispozitat më të Harmonizuara në lidhje me Informimit*, WP 100, Bruksel, 25 nëntor 2004.

Përjashtime nga detyrimi për të informuar

Sipas së drejtës së BE-së, ekziston një përjashtim i përgjithshëm nga detyrimi për të informuar subjektin e të dhënave, në rastin kur subjekti i të dhënave është i informuar më parë.[165] Bëhet fjalë për situata në të cilat, në përputhje me rastin, subjekti i të dhënave do të ketë dijeni më parë që të dhënat e tij apo të saj do të përpunohen, për një qëllim të caktuar, nga një kontrollues i caktuar.

Neni 11 i Direktivës, i cili lidhet me detyrimin për të informuar subjektin e të dhënave kur të dhënat nuk janë mbledhur nga ai apo ajo, gjithashtu parashtron se nuk do të ketë një detyrim të tillë, veçanërisht për përpunimet për qëllime statistikore ose për qëllim historike apo të kërkimeve shkencore, kur:

- Dhënia e informacionit është e pamundur; ose
- Për të duhen bërë përpjekje të paarsyeshme; ose
- Regjistrimi apo komunikimi i të dhënave është përcaktuar shprehimisht në ligj.[166]

Vetëm neni 11 (2) i Direktivës së Mbrojtjes së të Dhënave thekson se subjektet e të dhëna nuk duhet të informohen në lidhje me përpunimet, nëse ato janë të përcaktuara me ligj. Duke pasur parasysh hipotezën ligjore të përgjithshme, sipas së cilës askush s'mund të thotë se nuk e njeh ligjin, mund të pohohet se, kur të dhënat mblidhen nga subjekti i të dhënave sipas nenit 10 të Direktivës, subjekti i të dhënave është i informuar. Por duke qenë se njohja e ligjit është thjesht supozim, parimi i përpunimit të drejtë do të kërkonte në përputhje me nenin 10, që subjekti i të dhënave të ishte i informuar edhe nëse përpunimi përcaktohet në ligj, sidomos për shkak se informimi i subjektit të të dhënave nuk është shumë i komplikuar, kur të dhënat mblidhen drejtpërdrejt nga subjekti i të dhënave.

Sa i takon së drejtës së KiE-së, Konventa 108 parashikon qartë përjashtimet nga neni 8 i saj. Sërish, përjashtimet e përcaktuara në nenet 10 dhe 11 të Direktivës së Mbrojtjes së të Dhënave mund të konsiderohen si shembuj të praktikave të mira për përjashtimet sipas nenit 9 të Konventës 108.

Mënyrat e ndryshme të dhënies së informacionit

Mënyra ideale për dhënien e informacionit do të ishte që ky i fundit t'i jepej subjektit të të dhënave me gojë ose me shkrim. Nëse të dhënat janë mbledhur nga subjekti i të dhënave, dhënia e informacionit duhet të shoqërojë paralelisht mbledhjen e të dhënave. Por kur të dhënat janë mbledhur nga të tretët, duke pasur parasysh vështirësitë praktike të qarta të kontaktimit personalisht të subjektit të të dhënave, informacioni mund të jepet gjithashtu nëpërmjet publikimit në mënyrë të përshtatshme.

Një nga mënyrat më efikase të dhënies së informacionit, do të ishte paraqitja e klauzolave informuese në faqen e internetit të kontrolluesit, në formën e politikave të privatësisë të faqeve të internetit. Gjithsesi, një pjesë e madhe e popullsisë nuk e përdor internetin dhe politikat e informimit të një shoqërie apo të një autoriteti publik, duhet ta kenë parasysh këtë fakt.

---

[165] Direktiva e Mbrojtjes së të Dhënave, nenet 10 dhe 11 (1).
[166] Po aty, pika 40 dhe neni 11 (2).

4.3.2. Njoftimi

E drejta kombëtare mund të detyrojë kontrolluesit të njoftojnë autoritetin kompetent mbikëqyrës në lidhje me përpunimet që ata kryejnë, në mënyrë që ato të mund të publikohen. E drejta kombëtare mund të përcaktojë gjithashtu që kontrolluesit të caktojnë një zyrtar të mbrojtjes së të dhënave personale, i cili të jetë përgjegjës veçanërisht për të mbajtur një regjistër të operacioneve përpunuese që kryhen nga kontrolluesi.[167] Ky regjistër i brendshëm duhet t'i vihet në dispozicion publikut me kërkesën e këtij të fundit.

Shembull: njoftimi, ashtu si edhe dokumentimi nga ana e zyrtarit të brendshëm të mbrojtjes së të dhënave personale, duhet të përshkruajë karakteristikat kryesore të përpunimit të të dhënave në fjalë. ai duhet të përmbajë informacionin në lidhje me kontrolluesin, qëllimin e përpunimit, bazën ligjore për përpunimin, kategoritë e të dhënave të përpunuara, palët e treta marrëse të mundshme dhe nëse parashikohet të kryhen qarkullime ndërkufitare të dhënash dhe nëse po, cilat.

Publikimi i njoftimeve nga ana e autoritetit mbikëqyrës, duhet të bëhet në formën e një regjistri special. Me qëllim që të përmbushë qëllimin e tij, aksesi në këtë regjistër duhet të jetë i lehtë dhe pa pagesë. E njëjta gjë vlen edhe për dokumentacionin që mban zyrtari i mbrojtjes së të dhënave personale të kontrolluesit.

Përjashtimet nga detyrimet për të njoftuar autoritetet kompetente mbikëqyrëse, ose të caktimit të një zyrtari të brendshëm të mbrojtjes së të dhënave, mund të përcaktohen nga legjislacioni kombëtar, për operacionet përpunuese, të cilat nuk kanë të ngjarë të paraqesin rrezik të veçantë për subjektet e të dhënave. Këto përjashtime renditen në nenin 18 (2) të Direktivës së Mbrojtjes së të Dhënave.[168]

4.4. Rregullat që ndihmojnë për respektimin e normave të mbrojtjes së të dhënave

Pikat kryesore

- Kur shtjellon parimin e përgjegjshmërisë, Direktiva e Mbrojtjes së të Dhënave përmend disa instrumente të cilat ndihmojnë për respektimin e normave të mbrojtjes së të dhënave:
  - Kontrolli paraprak i operacioneve përpunuese të parashikuara nga ana e autoritetit mbikëqyrës kombëtar;
  - Zyrtarët e mbrojtjes së të dhënave personale, të cilët ofrojnë ekspertizën e nevojshme në fushën e mbrojtjes së të dhënave;
  - Kodet e sjelljes, që specifikojnë rregullat e mbrojtjes së të dhënave që duhen zbatuar në një degë të një shoqërie, sidomos të një shoqërie tregtare.
- KiE-ja sugjeron instrumente të ngjashme për nxitjen e përputhshmërisë nëpërmjet Rekomandimit të Profilizimit.

[167] Po aty, neni 18 (2), fjalia e dytë.
[168] Po aty, neni 18 (2), fjalia e dytë.

4.4.1. Kontrolli paraprak

Sipas nenit 20 të Direktivës së Mbrojtjes së të Dhënave, autoriteti mbikëqyrës duhet të kontrollojë operacionet përpunuese, të cilat mund të krijojnë rreziqe specifike për të drejtat dhe liritë e subjekteve të të dhënave – qoftë për shkak të qëllimit, qoftë për shkak të rrethanave të përpunimit – përpara se përpunimi të nisë. Legjislacioni kombëtar duhet të përcaktojë cilat operacione përpunuese duhet t'i nënshtrohen kontrollit paraprak. Ky kontroll mund të sjellë ndalimin e përpunimeve, ose të ndryshojë karakteristikat e përpunimit që propozohet të kryhet. Neni 20 i Direktivës synon të garantojë që një përpunim që mbart rrezik të panevojshëm, të mos nisë, meqenëse autoriteti mbikëqyrës ka kompetencën t'i ndalojë këto lloj përpunimesh. Kushti i domosdoshëm që e bën këtë mekanizëm të efektshëm, është pikërisht që të njoftohet autoriteti mbikëqyrës. Me qëllim që të garantohet se kontrolluesit e përmbushin detyrimin tyre për të njoftuar, autoritetet mbikëqyrëse duhet kenë kompetenca shtrënguese, sikurse të mund t'u vendosin gjoba kontrolluesve.

Shembull: nëse një shoqëri kryen përpunime të cilat, në përputhje me legjislacionin kombëtar, janë subjekt i kontrollit paraprak, ajo kompani duhet të depozitojë dokumentacionin në lidhje me përpunimet e planifikuara pranë autoritetit mbikëqyrës. Shoqëria nuk lejohet të nisë operacionet përpunuese, përpara se të marrë përgjigje pozitive nga autoriteti mbikëqyrës.

Në disa Shtete Anëtare, legjislacioni kombëtar parashikon gjithashtu që operacionet përpunuese mund të nisin, në rast se nga ana e autoritetit mbikëqyrës nuk ka asnjë reagim, për një afat kohor të caktuar, për shembull, tre muaj.

4.4.2. Zyrtarët e Mbrojtjes së të dhënave

Direktiva e Mbrojtjes së të Dhënave e lejon legjislacionin kombëtar të parashikojë që kontrolluesi të caktojë një zyrtar, që të punojë si i ngarkuar për mbrojtjen e të dhënave personale,[169] i cili ka për qëllim të garantojë që të drejtat dhe liritë e subjekteve të të dhënave të mos preken negativisht nga operacionet përpunuese.[170]

Shembull: në Gjermani, sipas nenit 4f, paragrafi 1 of Ligjit Federal Gjerman për Mbrojtjen e të Dhënave (*Bundesdatenschutzgesetz*), shoqëritë private janë të detyruara të caktojnë një zyrtar të brendshëm të mbrojtjes së të dhënave, nëse kanë 10 apo më shumë persona të punësuar në mënyrë të përhershme, për përpunimet automatike të të dhënave personale.

Për të përmbushur këtë objektiv, pozicioni i zyrtarit të mbrojtjes së të dhënave nevojit një farë pavarësie brenda organizatës së kontrolluesit, sikurse theksohet në mënyrë eksplicite në Direktivë. Gjithashtu, do të jetë e rëndësishme që të gëzojë të drejta të përforcuara punësimi, për të shmangur pushim të mundshëm të pajustifikuar nga puna, me qëllim që të mbështetet funksionimi me efektivitet i pozicionit të të ngarkuarit me mbrojtjen e të dhënave.

[169] Po aty, neni 18 (2), fjalia e dytë.
[170] Po aty

Në mënyrë që të nxitet respektimi i së drejtës kombëtare në fushën e mbrojtjes së të dhënave, koncepti i zyrtarit të brendshëm për mbrojtjen e të dhënave është miratuar gjithashtu edhe në disa Rekomandime të KiE-së.[171]

4.4.3. Kodet e sjelljes

Me qëllim që të nxitet përputhshmëria ligjore, sektori i biznesit dhe sektorët e tjerë mund të hartojnë rregulla të hollësishme, të cilat rregullojnë aktivitetet e tyre përpunuese të zakonshme, duke kodifikuar praktikat më të mira. Ekspertiza e anëtarëve të sektorit do të ndihmojë në gjetjen e zgjidhjeve praktike dhe për rrjedhojë mund të vihet në zbatim. Sa i takon kësaj, Shtetet Anëtare, ashtu si edhe Komisioni Evropian – nxiten të promovojnë hartimin e kodeve të sjelljes, të cilat synojnë të ndihmojnë në zbatimin e duhur të dispozitave kombëtare, të miratuara nga Shtetet Anëtare në përputhje me këtë Direktivë, duke pasur parasysh karakteristikat e veçanta të sektorëve të ndryshëm.[172]

Me qëllim që të garantohet që këto kode sjelljeje të jenë në përputhje me dispozitat kombëtare të miratuara në zbatim të Direktivës së Mbrojtjes së të Dhënave, Shtetet Anëtare duhet të përcaktojnë një procedurë për vlerësimin e kodeve. Kjo procedurë normalisht kërkon pjesëmarrjen e autoritetit kombëtar, shoqatave të biznesit dhe të organizmave të tjera që përfaqësojnë kategori të tjera kontrolluesish.[173]

Projekt-kodet komunitare ashtu si ndryshimet apo zgjerimi i kodeve ekzistuese komunitare, mund të depozitohen pranë Grupit të Punës së nenit 29 për vlerësim. Pas miratimit nga ky Grup Pune, Komisioni Evropian mund të vijojë me promovimin e këtyre kodeve.[175]

Shembull: Federata Evropiane e Marketingut të Drejtpërdrejtë (FEDMA) hartoi një Kod Evropian të Sjelljes për përdorimin e të dhënave personale në marketingun e drejtpërdrejtë. Kodi iu paraqit me sukses Grupit të Punës së Nenit 29 dhe në 2010-ën iu bashkëngjit një shtojcë e dedikuar për komunikimet elektronike të marketingut.[175]

---

[171] Shih për shembull Rekomandimin e Profilizimit, neni 8.3.

[172] Shih Direktivën e Mbrojtjes së të Dhënave, neni 27 (1).

173 Po aty, neni 27 (2).

174 Po aty, neni 27 (3).

175 Grupi i Punës së nenit 29 (2010), *Opinioni 4/2010 mbi kodin evropian të sjelljes të FEDMA-s për përdorimin e të dhënave personale në marketingun e drejtpërdrejtë*, 13 korrik 2010.

5

Të drejtat e subjekteve të të dhënave dhe zbatimi i tyre

BE	Çështje të trajtuara	KiE
E drejta për akses		
Direktiva e Mbrojtjes së të Dhënave, neni 12 GjDBE, C-553/07, *College van burgemeester en wethouders van Rotterdam kundër M.E.E. Rijkeboer*, 7 maj 2009	**E drejta e aksesit në të dhënat që i përkasin një personi**	Konventa 108, neni 8 (b)
	E drejta për korrigjim, fshirje ose bllokim	Konventa 108, neni 8 (c) GjEDNj, *Cemalettin Canli kundër Turqisë*, nr. 22427/04, 18 nëntor 2008 GjEDNj, *Segerstedt-Wiberg dhe të Tjerët kundër Suedisë*, nr. 62332/00, 6 qershor 2006 GjEDNj, *Ciubotaru kundër Moldavisë*, nr. 27138/04, 27 prill 2010
E drejta për të kundërshtuar		
Direktiva e Mbrojtjes së të Dhënave, neni 14 (1) (a)	**E drejta për të kundërshtuar, për shkak të situatës së veçantë të subjektit të të dhënave**	Rekomandimi i Profilizimit, neni 5.3
Direktiva e Mbrojtjes së të Dhënave, neni 14 (1) (b)	**E drejta për të kundërshtuar përdorimin e mëtejshëm të të dhënave për qëllime marketingu**	Rekomandimi i Marketingut të Drejtpërdrejtë, neni 4.1
Direktiva e Mbrojtjes së të Dhënave, neni 15	**E drejta për të kundërshtuar vendimet e automatizuara**	Rekomandimi i Profilizimit, neni 5.5
Mbikëqyrja e Pavarur		
Karta, neni 8 (3) Direktiva e Mbrojtjes së të Dhënave, neni 28	**Autoritetet mbikëqyrëse kombëtare**	Konventa 108, Protokolli Shtesë, neni 1

Rregullorja e Mbrojtjes së të Dhënave të Institucioneve të BE—së, Kapitulli V Rregullorja e Mbrojtjes së të Dhënave GjDBE, C-518/07, *Komisioni Evropian kundër Republikës Federale Gjermane*, 9 mars 2010 GjDBE, C-614/10, *Komisioni Evropian kundër Republikës së Austrisë,* 16 tetor 2012 GjDBE, C-288/12, *Komisioni Evropian kundër Hungarisë*, 8 prill 2014		
Ankimi dhe sanksionet		
Direktiva e Mbrojtjes së të Dhënave, neni 12	**Kërkesa drejtuar kontrolluesit**	Konventa 108, neni 8 (b)
Direktiva e Mbrojtjes së të Dhënave, neni 28 (4) Rregullorja e Mbrojtjes së të Dhënave e Institucioneve të BE-së, neni 32 (2)	**Ankesat e depozituara pranë një autoriteti mbikëqyrës**	Konventa 108, Protokolli Shtesë, neni 1 (2) (b)
Karta, neni 47	**Gjykatat (në përgjithësi)**	KEDNj, neni 13
Direktiva e Mbrojtjes së të Dhënave, neni 28 (3)	**Gjykatat kombëtare**	Konventa 108, Protokolli Shtesë, neni 1 (4)
TFBE, neni 263 (4) Rregullorja e Mbrojtjes së të Dhënave e Institucioneve të BE-së, neni 32 (1) TFBE, neni 267	**GjDBE**	
	GjEDNj	KEDNj, neni 34
Ankimi dhe sanksionet		
Karta, neni 47 Direktiva e Mbrojtjes së të Dhënave, nenet 22 dhe 23 GjDBE, C-14/83, *Sabine von Colson dhe Elisabeth Kamann kundër Land Nordrhein-Westfalen*,	**Shkeljet e legjislacionit kombëtar të mbrojtjes së të dhënave**	KEDNj, neni 13 (vetëm për shtetet anëtare të KiE-së) Konventa 108, neni 10 GjEDNj, *K.U. kundër Finlandës*, nr. 2872/02, 2 dhjetor 2008

10 prill 1984 GjDBE, C-152/84, *M.H. Marshall kundër Southampton dhe South-West Hampshire Area Health Authority*, 26 shkurt 1986		GjEDNj, *Biriuk kundër Lituanisë*, nr. 23373/03, 25 nëntor 2008
Rregullora e Mbrojtjes së të Dhënave të Institucioneve të BE-së, nenet 34 dhe 49 GjDBE, C-28/08 P, *Komisioni Evropian kundër Thë Bavarian Lager Co. Ltd, 29 qershor 2010*	**Shkeljet e legjislacionit të BE-së nga ana e institucioneve dhe organizmave të BE-së**	

Efikasiteti i rregullave ligjore në përgjithësi dhe të drejtave të subjekteve të të dhënave në veçanti, varet kryesisht nga ekzistenca e mekanizmave të duhur për t'i zbatuar ato. Në të drejtën evropiane në fushën e mbrojtjes së të dhënave, e drejta kombëtare duhet t'i sigurojë subjektit të të dhënave mjetet për të mbrojtur të dhënat e tij apo të saj, si edhe të krijojë autoritete të pavarura mbikëqyrëse, për të ndihmuar subjektet e të dhënave gjatë ushtrimit të të drejtave të tyre dhe për të mbikëqyrur përpunimin e të dhënave personale. Gjithashtu, e drejta për ankim të efektshëm, sikurse garantohet nga KEDNj-ja dhe Karta, bën të detyrueshme që çdo person të ketë mundësi të ankohet në gjykatë.

5.1. Të drejtat e subjekteve të të dhënave

Pikat kryesore

- Sipas legjislacionit kombëtar, çdo person duhet të ketë të drejtën të kërkojë nga kontrolluesi konfirmimin nëse ai po përpunon ose jo të dhënat e tij apo të saj.
- Subjektet e të dhënave duhet të kenë të drejtën sipas legjislacionit kombëtar që:
  - Të kenë akses në të dhënat që u përkasin pranë kontrolluesit i cili përpunon këto të dhëna;
  - Të kërkojnë korrigjimin (ose sipas rastit bllokimin e përpunimit) nga kontrolluesi i cili përpunon të dhënat e tyre, nëse këto të dhëna janë të pasakta;
  - Sipas rastit, të kërkojnë nga kontrolluesi fshirjen apo bllokimin e të dhënave që u përkasin, nëse kontrolluesi përpunon të dhënat që u përkasin në mënyrë të paligjshme.
- Gjithashtu, subjektet e të dhënave kanë të drejtën të kundërshtojnë kontrolluesin në lidhje me:
  - Vendimet automatike (të cilat merren me ndihmën e të dhënave personale të përpunuara vetëm me mjete automatike);
  - Përpunimin e të dhënave që u përkasin, nëse ai çon në rezultate të pasakta;
  - Përdorimin e të dhënave që u përkasin për qëllime të marketingut të drejtpërdrejtë.

5.1.1. E drejta për akses

Sipas së drejtës së BE-së, neni 12 i Direktivës së Mbrojtjes së të Dhënave përmban elementet e së drejtës së subjekteve të të dhënave për akses, përfshirë të drejtën për të kërkuar nga kontrolluesi "që t'u konfirmojë nëse të dhënat e tyre janë duke u përpunuar dhe të paktën informacionin në lidhje me qëllimet e përpunimit, kategoritë e të dhënave të përfshira dhe

marrësit apo kategoritë e marrësve të cilëve u komunikohen të dhënat", ashtu si edhe "korrigjimin, fshirjen apo bllokimin e të dhënave, përpunimi i të cilave nuk përputhet me dispozitat e kësaj Direktive, veçanërisht për shkak të natyrës së pasaktë apo jo të plotë të të dhënave".

Sipas së drejtës së KiE-së, këto të drejta ekzistojnë dhe duhet të parashikohen nga legjislacioni kombëtar (neni 8 i Konventës 108). Në disa rekomandime të KiE-së, termi "akses" përdoret dhe asketet e ndryshme të së drejtës për akses përshkruhen dhe propozohen për zbatim në legjislacionin kombëtar, në të njëjtën mënyrë siç është cituar në paragrafin e mësipërm.

Sipas nenit 9 të Konventës 108 dhe nenit 13 të Direktivës së Mbrojtjes së të Dhënave, detyrimi i kontrolluesve për t'iu përgjigjur kërkesave të subjekteve të të dhënave për akses, mund të kufizohet si rezultat i interesave prevaluese ligjore të të tjerëve. Interesat prevaluese ligjore mund të përfshijnë interesa publike, sikurse siguria kombëtare, siguria publike dhe ndjekja e veprave penale, ashtu si edhe interesat private të cilat janë më shtrënguese se sa interesat në lidhje me mbrojtjen e të dhënave. Çdo përjashtim nga kufizimet, duhet të jetë i nevojshëm në një shoqëri demokratike dhe proporcionale në raport me qëllimin që synohet të arrihet. Në disa raste tepër të jashtëzakonshme, për shembull për shkak të indikacioneve mjekësore, vetë mbrojtja e subjektit të të dhënave mund të kërkojë kufizim të transparencës; kjo lidhet veçanërisht me kufizimin e së drejtës për akses të çdo subjekti të dhënash.

Kur të dhënat përpunohen vetëm për qëllime kërkimore shkencore apo statistikore, Direktiva e Mbrojtjes së të Dhënave lejon kufizimin e së drejtave për akses nga ana e legjislacionit kombëtar; gjithsesi me kusht që të ekzistojnë garancitë e përshtatshme ligjore. Në mënyrë të veçantë, duhet të garantohet që në kontekstin e këtij përpunimi, të mos merret asnjë masë apo vendim në lidhje me personat e caktuar dhe se "qartësisht të mos ekzistojë asnjë rrezik për shkelje të privatësisë së subjektit të të dhënave".[176] Dispozita të ngjashme përmban edhe neni 9 (3) i Konventës 108.

E drejta e subjektit për akses në të dhënat që i përkasin

Tek e drejta e KiE-së, e drejta e subjektit për akses në të dhënat që i përkasin, njihet në mënyrë eksplicite nga neni 8 i Konventës 108. GjEDNj-ja ka përcaktuar disa herë se ekziston një e drejtë për akses në informacionin që ka të bëjë me të dhënat personale që i përkasin subjektit, të ruajtura apo përdorura nga të tjerët dhe se kjo e drejtë buron nga nevoja për të respektuar jetën private.[177] Gjithsesi, tek çështja *Leander*,[178] GjEDNj-ja doli në përfundimin se e drejta për akses në të dhënat personale që ruhen nga autoritetet publike, mund të kufizohet në rrethana të caktuara.

Sipas së drejtës së BE-së, e drejta e subjektit për akses në të dhënat që i përkasin, njihet në mënyrë eksplicite nga neni 12 i Direktivës së Mbrojtjes së të Dhënave dhe si e drejtë themelore nga neni 8 (2) i Kartës.

[176] Direktiva e Mbrojtjes së të Dhënave, neni 13 (2).

[177] GjEDNj, *Gaskin kundër Mbretërisë së Bashkuar*, nr. 10454/83, 7 korrik 1989; GjEDNj, *Odièvre kundër Francës* [GC], nr. 42326/98, 13 shkurt 2003; GjEDNj, *K.H. dhe të Tjerët kundër Sllovakisë*, nr. 32881/04, 28 prill 2009; ECtHR, *Godelli kundër Italisë*, nr. 33783/09, 25 shtator 2012.

[178] GjEDNj, *Leander kundër Suedisë*, nr. 9248/81, 26 mars 1987.

Neni 12 (a) i Direktivës përcakton se Shtetet Anëtare duhet t'i garantojnë çdo subjekti të drejtën për akses në të dhënat e tyre personale dhe të drejtën e informimit. Në mënyrë të veçantë, çdo subjekt të dhënash ka të drejtën të marrë nga kontrolluesi konfirmimin nëse të dhënat në lidhje me të janë duke u përpunuar ose jo dhe informacion që të përmbajë të paktën pikat në vijim:

- Qëllimin e përpunimit;
- Kategoritë e të dhënave të përfshira;
- Të dhënat që janë objekt i përpunimit;
- Marrësit ose kategoritë e marrësve, të cilëve u komunikohen të dhënat;
- Çdo informacion të mundshëm në lidhje me origjinën e të dhënave, të cilat janë objekt i përpunimit;
- Logjikën e përdorur për çdo përpunim automatik të dhënave, në rastin e vendimeve automatike.

Legjislacioni kombëtar mund të parashikojë që kontrolluesi të japë edhe të tjera informacione, për shembull citimin e bazës ligjore që autorizon përpunimin e të dhënave.

Shembull: duke pasur akses në të dhënat që i përkasin, subjekti është në gjendje të përcaktojë nëse të dhënat janë të sakta ose jo. Për rrjedhojë, është e domosdoshme që subjekti i të dhënave të informohet në lidhje me kategoritë e të dhënave të përpunuara, ashtu si edhe në lidhje me përmbajtjen e të dhënave. Për këtë arsye, nuk mjafton vetëm që kontrolluesi t'i tregojë subjektit të të dhënave se ai po përpunon emrin, adresën, datëlindjen dhe sferën e interesave të tij apo të saj. Kontrolluesi duhet gjithashtu t'i komunikojë subjektit të të dhënave se ai po përpunon "emrin: N.N.; adresën: 1040 Vjenë, Schwarzenbergplatz 11, Austri; datëlindjen: 10.10.1974; dhe sferën e interesave (në përputhje me deklarimin e subjektit të të dhënave): muzika klasike." Elementi i fundit përmban për më tepër, informacion në lidhje me origjinën e të dhënave.

Informimi i subjektit të të dhënave në lidhje me të dhënat, të cilat janë objekt i përpunimit dhe komunikimi i të gjitha informacioneve të disponueshme, në lidhje me origjinën e tyre, duhet të jepen në formë të kuptueshme, e cila do të thotë që kontrolluesi është i detyruar t'i shpjegojë më me hollësi subjektit të të dhënave objektin e përpunimit. Për shembull, vetëm citimi i shkurtesave teknike apo termave mjekësore, në përgjigje të kërkesës për akses, përgjithësisht do të jetë e pamjaftueshme, edhe sikur të jenë ruajtur vetëm këto lloj akronimesh apo termash.

Informacioni në lidhje me origjinën e të dhënave të përpunuara nga kontrolluesi, duhet të jepet në përgjigje të kërkesës për akses, derisa ky informacion është i disponueshëm. Kjo dispozitë duhet të kuptohet duke iu referuar parimeve të përpunimit të drejtë dhe përgjegjshmërisë. Kontrolluesi nuk mund të shkatërrojë informacionin në lidhje me origjinën e të dhënave, në mënyrë që të përjashtohet nga detyrimi për ta komunikuar dhe as nuk duhet të injorojë normat e përgjithshme dhe nevojat e njohura për dokumentim në fushën e aktiviteteve të tij. Mosruajtja e asnjë dokumenti në lidhje me origjinën e të dhënave të përpunuara, përgjithësisht konsiderohet si mosrespektim i detyrimit të kontrolluesit referuar së drejtës për akses.

Kur kryhen vlerësime automatike, duhet të shpjegohet logjika e përgjithshme e vlerësimit, përfshirë edhe kriteret e veçanta të cilat janë marrë në konsideratë, gjatë vlerësimit të subjektit të të dhënave.

Direktiva nuk qartëson nëse e drejta për akses në informacion ka të bëjë me të shkuarën dhe nëse po, cilës periudhë të së shkuarës. Në lidhje me këtë, sikurse theksohet në praktikën gjyqësore të GjDBE-së, e drejta e subjektit për akses në të dhënat që i përkasin, nuk mund të kufizohet padrejtësisht nga afatet kohore. Subjekteve të të dhënave u duhen dhënë mundësi të arsyeshme, për të përftuar informacione në lidhje me përpunimet e kryera në të shkuarën.

Shembull: tek çështja *Rijkeboer,*[179] GjDBE-së iu kërkua të përcaktonte nëse, sipas nenit 12 (a) të Direktivës, e drejta për akses e një personi tek informacioni në lidhje me marrësit, apo kategoritë e marrësve të të dhënave personale dhe në lidhje me përmbajtjen e të dhënave të komunikuara, mund të kufizohet në një vit, i paraprin kërkesës së tij apo të saj për akses.

Për të përcaktuar nëse neni 12 (a) i Direktivës autorizon kufizime të tilla kohore, Gjykata vendosi ta interpretonte atë nen bazuar në qëllimet e Direktivës. Gjykata fillimisht theksoi se e drejta për akses është e nevojshme, për t'i mundësuar subjektit të të dhënave të ushtrojë të drejtën për të kërkuar nga kontrolluesi korrigjimin, fshirjen apo bllokimin e të dhënave të tij (neni 12 (b)), ose për t'i njoftuar palët e treta, të dhënat e të cilëve janë komunikuar në lidhje me atë korrigjim, fshirje apo bllokim (neni 12 (c)). E drejta për akses është gjithashtu e nevojshme për t'i mundësuar subjektit të të dhënave që të ushtrojë të drejtën e tij apo të saj, për të kundërshtuar përpunimin e të dhënave personale që i përkasin (neni 14), apo të drejtën për t'u ankuar në rast dëmtimi (neni 22 dhe 23).

Për të siguruar efekt të dobishëm të dispozitave të mësipërme, Gjykata vlerësoi se "ajo e drejtë, duhet detyrimisht të shtrihet në të shkuarën. Sikur kjo të mos ishte e saktë, subjekti i të dhënave nuk do të kishte mundësi të ushtronte me efektivitet të drejtën e tij, për të kërkuar korrigjimin, fshirjen apo bllokimin e të dhënave që ai pretendon se janë të paligjshme, apo të pasakta, ose për të proceduar ligjërisht dhe për të përftuar zhdëmtim për dëmin e pësuar".

E drejta për korrigjim, fshirja apo bllokim të të dhënave

"Çdo person duhet të ketë mundësi të ushtrojë të drejtën për akses në të dhënat në lidhje me të, të cilat janë objekt përpunimi, me qëllim që të verifikojë saktësinë e të dhënave dhe ligjshmërinë e përpunimit."[180] Në përputhje me këto parime, subjektet e të dhënave duhet të gëzojnë të drejtën sipas legjislacionit kombëtar, për të kërkuar nga kontrolluesi korrigjimin, fshirjen apo bllokimin e të dhënave të tyre, nëse mendojnë se përpunimi i tyre nuk respekton dispozitat e Direktivës, sidomos për shkak të natyrës së pasaktë apo të mangët të të dhënave.[181]

Shembull: tek çështja *Cemalettin Canli kundër Turqisë,*[182] GjEDNj-ja gjeti shkelje të nenit 8 të KEDNj-së, në një raport policor të pasaktë në kuadër të një procedimi penal.

Ankuesi ishte përfshirë dy herë në një procedim penal, për shkak se dyshohej se ishte anëtarësuar në organizata të jashtëligjshme, por nuk ishte dënuar kurrë.

[179] GjDBE, C-553/07, *College van burgemeester en wethouders van Rotterdam kundër M. E. E. Rijkeboer*, 7 maj 2009.
[180] Direktiva e Mbrojtjes së të Dhënave, pika 41.
[181] Po aty, neni 12 (b).
[182] GjEDNj, *Cemalettin Canli kundër Turqisë*, nr. 22427/04, 18 nëntor 2008, parag. 33, 42 dhe 43; GjEDNj, *Dalea kundër Francës*, nr. 964/07, 2 shkurt 2010.

Kur ankuesi ishte arrestuar sërish dhe akuzuar për një vepër tjetër penale, policia i paraqiti gjykatës penale një raport të titulluar "*formular informacioni në lidhje me vepra të tjera penale"*, në të cilin ankuesi paraqitej si anëtar i dy organizatave të jashtëligjshme. Kërkesa e ankuesit për të ndryshuar raportin dhe dosjen policore nuk ishte pranuar. GjEDNj-ja vlerësoi se informacioni në raportin policor ishte brenda fushës së nenit 8 të KEDNj-së, meqenëse informacioni publik mund t'i përkasë edhe fushës së "jetës private", kur ai mblidhet dhe ruhet në mënyrë sistematike në skedarët që mbajnë autoritetet. Gjithashtu, raporti i policisë ishte i pasaktë dhe hartimi e depozitimi i tij në një gjykatë penale, nuk ishte bërë në përputhje me ligjin. Gjykata vendosi se ishte shkelur neni 8.

Shembull: tek çështja *Segerstedt-Wiberg dhe të Tjerët kundër Suedisë,* [183] ankuesit ishin anëtarësuar në disa parti politike të caktuara liberale dhe komuniste. Ata dyshonin se disa informacione në lidhje me ta, ishin regjistruar në dosjet policore të sigurisë. GjEDNj-ja vlerësoi se ruajtja e të dhënave në fjalë kishte bazë ligjore dhe synonte përmbushjen e një qëllimi legjitim. Sa i takon disa ankuesve, GjEDNj-ja deklaroi se ruajtja e vazhdueshme e të dhënave, përbënte një ndërhyrje jo proporcionale në jetët e tyre private. Për shembull, në rastin e z. Schmid, autoritetet ruanin një informacion se në 1969-ën, ai kishte bërë thirrje për rezistencë të dhunshme ndaj kontrolleve policore gjatë demonstratave. GjEDNj-ja vlerësoi se ky informacion, nuk përmbushte asnjë interes të rëndësishëm për sigurinë kombëtare, veçanërisht sa i takon natyrës së tij historike. GjEDNj-ja doli në përfundimin se kishte pasur shkelje të nenit 8 të KEDNj-së për katër nga pesë ankuesit.

Në disa raste, do të ishte e mjaftueshme për subjektin e të dhënave që ky i fundit thjesht të kërkojë korrigjimin, për shembull, të shkronjave të emrit, ndryshimit të adresës ose numrit të telefonit. Gjithsesi, nëse këto kërkesa lidhen me çështje ligjore, sikurse identiteti ligjor i subjektit të të dhënave, ose vendbanimi i saktë për dorëzimin e dokumenteve ligjore, kërkesat për korrigjim mund të mos jenë të mjaftueshme dhe kontrolluesi ka të drejtë të kërkojë prova për pasaktësinë e pretenduar. Kjo e fundit nuk duhet ta ngarkojë në mënyrë të paarsyeshme subjektin e të dhënave që të paraqesë prova, duke i penguar subjektet e të dhënave që të korrigjojnë të dhënat në lidhje me ta. GjEDNj-ja gjeti shkelje të nenit 8 të KEDNj-së në disa raste, ku ankuesit nuk kishin mundur të kundërshtonin saktësinë e informacionit që ruhet në regjistrat sekretë.[184]

Shembull: tek çështja *Ciubotaru kundër Moldavisë,*[185] ankuesi nuk kishte mundur të ndryshonte origjinën etnike në regjistrat zyrtarë, nga moldav në rumun, për shkak se nuk e kishte shoqëruar me prova kërkesën e tij për ndryshim. GjEDNj-ja e konsideroi të pranueshme që shtetet të kërkojnë prova objektive, gjatë regjistrimit të identitetit etnik të një personi. Kur një pretendim i tillë mbështetej në arsye krejtësisht subjektive dhe të pabazuara, autoritetet mund të refuzonin. Gjithsesi, pretendimi i ankuesit ishte mbështetur në më shumë se sa perceptimin subjektiv të etnisë së tij: ai kishte mundur të demonstronte lidhje të verifikueshme në mënyrë objektive me grupin etnik rumun, sikurse gjuhën, emrin, afinitetin dhe të tjera. Gjithsesi, sipas legjislacionit vendas, ankuesi ishte i detyruar të paraqiste prova që prindërit e tij i përkisnin grupit etnik rumun.

[183] GjEDNj, *Segerstedt-Wiberg dhe të tjerët kundër Suedisë*, nr. 62332/00, 6 qershor 2006, parag. 89 dhe 90; shih gjithashtu, për shembull: GjEDNj, *M.K. kundër Francës*, nr. 19522/09, 18 prill 2013
[184] GjEDNj, *Rotaru kundër Rumanisë*, nr. 28341/95, 4 maj 2000.
[185] GjEDNj, *Ciubotaru kundër Moldavisë*, nr. 27138/04, 27 prill 2010, parag. 51 dhe 59.

Duke iu referuar fakteve historike të Moldavisë, një kërkesë e tillë kishte krijuar pengesë të pakapërcyeshme për regjistrimin e identitetit etnik, të ndryshëm prej atij të regjistruar nga autoritetet sovjetike për prindërit e tij. Duke penguar ankuesin që të përfitonte shqyrtimin e pretendimit të tij, bazuar në prova të verifikueshme në mënyrë objektive, shteti nuk kishte zbatuar detyrimin e tij pozitiv për t'i garantuar ankuesit respektim të efektshëm të jetës së tij private. Gjykata doli në përfundimin se kishte pasur shkelje të nenit 8 të KEDNj-së.

Gjatë gjykimit të çështjeve civile apo procedimeve përpara një autoriteti publik, për të vendosur nëse të dhënat janë të sakta ose jo, subjekti i të dhënave mund të kërkojë që të vihet një shënim ose një koment në dosjen e tij personale, me qëllim që të vihet në dukje fakti se personi ka kundërshtuar saktësinë e të dhënave dhe se është në pritje të një vendimi zyrtar. Gjatë kësaj periudhe, kontrolluesi nuk duhet t'i paraqesë të dhënat si të sigurta apo përfundimtare, veçanërisht palëve të treta.

Kërkesa e subjektit të të dhënave për fshirjen e të dhënave shpesh mbështetet në pretendimin se përpunimi i të dhënave nuk ka bazë ligjore. Pretendime të tilla shpesh lindin kur pëlqimi është revokuar, ose kur disa të dhëna nuk janë më të nevojshme për të përmbushur qëllimin e mbledhjes së të dhënave. Barra e provës se përpunimi i të dhënave është i ligjshëm, i takon kontrolluesit, duke qenë se është përgjegjës për legjitimitetin e përpunimit. Mbështetur në parimin e përgjegjshmërisë, kontrolluesi duhet të jetë gjithnjë në gjendje të demonstrojë se ekziston një bazë ligjore e sigurt për përpunimin e të dhënave, pa të cilën përpunimi duhet të ndërpritet.

Nëse përpunimi i të dhënave kundërshtohet për shkak të pretendimit se të dhënat janë të pasakta, ose janë objekt përpunimi të paligjshëm, subjekti i të dhënave, në përputhje me parimin e përpunimit të drejtë, mund të kërkojë që të dhënat në fjalë të bllokohen. Kjo nuk do të thotë se të dhënat fshihen, por se kontrolluesi nuk duhet të përdorë të dhënat gjatë periudhës së bllokimit. Diçka e tillë do të ishte e nevojshme veçanërisht kur vazhdimi i përdorimit të të dhënave të pasakta apo të ruajtura në mënyrë të paligjshme, mund të dëmtojë subjektin e të dhënave. Legjislacioni kombëtar duhet të parashikojë më tepër hollësi, sa i takon periudhës kur lind detyrimi për të bllokuar përdorimin e të dhënave dhe mbi mënyrën se si duhet të ushtrohet ai.

Gjithashtu, subjektet e të dhënave kanë të drejtën të kërkojnë nga kontrolluesi njoftimin e bërë palëve të treta për çdo bllokim, korrigjim apo fshirje, në rast se ato palë të treta kanë përftuar të dhëna përpara këtyre përpunimeve. Meqenëse komunikimi i të dhënave tek palët e treta duhet të jetë i dokumentuar nga kontrolluesit, duhet të jetë e mundshme të identifikohen marrësit e të dhënave dhe të kërkohet fshirja e tyre. Gjithsesi, nëse të dhënat janë publikuar gjatë kësaj kohe, për shembull në internet, mund të jetë e pamundur të fshihen të dhënat në çdo rrethanë, duke qenë se marrësit e të dhënave nuk mund të identifikohen. Në përputhje me Direktivën e Mbrojtjes së të Dhënave, kontaktimi i marrësve të të dhënave me qëllim korrigjimin, fshirjen apo bllokimin e të dhënave, është i detyrueshëm, "përveçse nëse diçka e tillë është e pamundur apo kërkon përpjekje të tepruara".[186]

[186] Direktiva e Mbrojtjes së të Dhënave, neni 12 9c), gjysmë fjalia e fundit.

5.1.2. E drejta për të kundërshtuar

E drejta për të kundërshtuar përfshin të drejtën për të kundërshtuar vendimet individuale automatike, të drejtën për të kundërshtuar për shkak të situatës së veçantë të subjektit të të dhënave dhe të drejtën për të kundërshtuar përdorimin e mëtejshëm të të dhënave për qëllime marketingu të drejtpërdrejtë.

E drejta për të kundërshtuar vendimet individuale automatike

Vendimet automatike janë vendime të cilat merren duke përdorur të dhëna personale, të cilat janë përpunuar vetëm me mjete automatike. Duke qenë se këto vendime kanë gjasa të ndikojnë në mënyrë të konsiderueshme në jetët e individëve, meqenëse ato lidhen për shembull me besueshmërinë e kreditimit, rendimentin profesional, sjelljen apo besueshmërinë në përgjithësi, nevojitet mbrojtje e veçantë, me qëllim që të shmangen pasojat e papërshtatshme. Direktiva e Mbrojtjes së të Dhënave parashikon se vendimet automatike nuk duhet të përcaktojnë çështje që janë të rëndësishme për individët dhe bën të detyrueshme që individët të kenë të drejtën për të rishikuar vendimin automatik.[187]

Shembull: një shembull praktik i rëndësishëm i vendimmarrjes automatike është klasifikimi i kredisë. Për të përcaktuar me shpejtësi besueshmërinë e një klienti të ardhshëm, në lidhje me kreditimin, disa lloj të dhënash sikurse profesioni dhe situata familjare mblidhen nga klienti dhe kombinohen me të dhënat në lidhje me klientin, të cilat janë të disponueshme nga burime të tjera, sikundër nga sistemet e informacionit të kreditimit. Këto të dhëna inkuadrohen në një algoritëm vlerësimi, i cili përllogarit vlerën e përgjithshme, që përfaqëson besueshmërinë e kreditimit të klientit të mundshëm. Në këtë mënyrë, nëpunësi i shoqërisë mund të marrë vendim brenda pak sekondash, nëse subjekti i të dhënave është i pranueshëm si klient apo jo.

Gjithsesi, në përputhje me Direktivën, Shtetet Anëtare duhet të përcaktojnë nëse një person mund t'i nënshtrohet një vendimi individual automatik, nëse interesat e subjektit të të dhënave nuk rrezikohen, për shkak se vendimi është në favor të tij, apo mbrohen nga mjete të tjera të përshtatshme.[188] **E drejta e KiE-së,** parashikon gjithashtu një të drejtë kundërshtimi të vendimeve automatike, sikurse shihet në Rekomandimin e Profilizimit.[189]

E drejta për të kundërshtuar për shkak të situatës së veçantë të subjektit të të dhënave

Nuk ekziston ndonjë e drejtë e përgjithshme për subjektin e të dhënave që të kundërshtojë përpunimit e të dhënave personale që i përkasin.[190] Sidoqoftë, neni 14 (a) i Direktivës së Mbrojtjes së të Dhënave njeh të drejtën e subjektit të të dhënave për të kundërshtuar, për arsye shtrënguese dhe legjitime, për shkak të situatës së tij të veçantë. Një e drejtë e ngjashme njihet edhe në Rekomandimin e Profilizimit të KiE-së.[191]

---

[187] Po aty, neni 15 (1).
[188] Po aty, neni 15 (2).
[189] Rekomandimi i Profilizimit, neni 5 (5).
[190] Shih gjithashtu GjEDNj, *M.S. kundër Suedisë*, nr. 20837/92, 27 gusht 1997, ku të dhënat mjekësore ishin komunikuar pa pëlqim dhe pa mundësi për të kundërshtuar; ose GjEDNj, *Leander kundër Suedisë*, nr. 9248/81, 26 mars 1987; ose GjEDNj, *Mosley kundër Mbretërisë së Bashkuar*, nr. 48009/08, 10 maj 2011.
[191] Rekomandimi i Profilizimit, neni 5 (3).

Këto dispozita synojnë gjetjen e ekuilibrit të duhur, midis së drejtave të subjektit të të dhënave për mbrojtje të të dhënave dhe të drejtave legjitime të të tjerëve për përpunimin e të dhënave të subjektit.

Shembull: një bankë ruan për shtatë vite të dhënat e klientëve, të cilët nuk respektojnë pagesat e kredive të tyre. Një klient, të dhënat e të cilit ruhen në një bazë të dhënash, aplikon për një kredi tjetër. Kryhen verifikimet në bazën e të dhënave dhe vlerësimi i situatës financiare dhe klientit i refuzohet dhënia e kredisë. Gjithsesi, klienti mund të kundërshtojë të dhënat personale të regjistruara në bazën e të dhënave dhe të kërkojë fshirjen e të dhënave, nëse ai apo ajo mund të provojë se vonesa në pagesa ishte thjesht rezultat i një gabimi, që ishte korrigjuar menjëherë sapo klienti ishte vënë në dijeni.

Nëse kundërshtimi pranohet, të dhënat në fjalë nuk mund të vazhdojnë të përpunohen nga kontrolluesi. Sidoqoftë, përpunimet e të dhënave, të kryera tek të dhënat e subjektit përpara se ai të kundërshtonte, mbeten legjitime.

E drejta për të kundërshtuar përdorimin e mëtejshëm të të dhënave për qëllime marketingu të drejtpërdrejtë

Neni 14 (b) i Direktivës së Mbrojtjes së të Dhënave parashikon një të drejtë specifike për të kundërshtuar përdorimin e të dhënave të dikujt për qëllime të marketingut të drejtpërdrejtë. Kjo e drejtë përcaktohet edhe në Rekomandimin e Profilizimit të KiE-së.[192] Ky lloj kundërshtimi duhet të bëhet i ditur përpara se të dhënat t'i vihen në dispozicion palëve të treta për qëllime të marketingut të drejtpërdrejtë. Për rrjedhojë, subjektit të të dhënave i duhet dhënë mundësia të kundërshtojë përpara se të dhënat të transferohen.

5.2. Mbikëqyrja e pavarur

Pikat kryesore

- Me qëllim që të garantohet mbrojtje e efektshme të dhënash, duhen ngritur autoritetet e pavarura të mbikëqyrjes bazuar në legjislacionin kombëtar.
- Autoritetet mbikëqyrëse të pavarura duhet të veprojnë në pavarësi të plotë, e cila duhet garantuar nga ligji organik dhe të pasqyrohet në strukturën organizative specifike të autoritetit mbikëqyrës.
- Autoritetet mbikëqyrëse kanë detyra specifike, ndër të tjera:
- Të monitorojnë dhe mbështesin mbrojtjen e të dhënave në nivel kombëtar;
- Të këshillojnë subjektet e të dhënave dhe kontrolluesit, ashtu si edhe qeverinë dhe publikun e gjerë;
- Të shqyrtojnë ankesat dhe të ndihmojnë subjektin e të dhënave në rastet e shkeljeve të pretenduara të së drejtave për mbrojtje të të dhënave;
- Të mbikëqyrin kontrolluesit dhe përpunuesit;
- Të ndërhyjnë nëse është e nevojshme duke:
  - Paralajmëruar, këshilluar apo edhe gjobitur kontrolluesit dhe përpunuesit,
  - Urdhëruar korrigjimin, bllokimin apo fshirjen e të dhënave,
  - Urdhëruar ndalimin e përpunimit;
- T'ia referojnë çështjen gjykatës.

[192] KiE, Komiteti i Ministrave (1985), Rekomandimi Rec(85)20 drejtuar shteteve anëtare mbi mbrojtjen e të dhënave personale të përdorura për qëllime të marketingut të drejtpërdrejtë, 25 tetor 1985, neni 4 (1).

Direktiva e Mbrojtjes së të Dhënave detyron ekzistencën e mbikëqyrjes së pavarur, si një mekanizëm i rëndësishëm për të garantuar mbrojtje të efektshme të të dhënave. Direktiva paraqiti një instrument për zbatimin e mbrojtjes së të dhënave, i cili fillimisht nuk ekzistonte në Konventën 108 apo në Udhëzuesin mbi Privatësinë të OECD-së.

Meqenëse mbikëqyrja e pavarur rezultoi të ishte e domosdoshme, për garantimin e një mbrojtjeje të efektshme të të dhënave, një dispozitë e re e Udhëzuesit mbi Privatësinë të OECD-së, në variantin e tij të rishikuar, miratuar në 2013-ën, u bën thirrje Shteteve Anëtare të "krijojnë dhe sigurojnë funksionimin e autoriteteve të ngarkuara për mbrojtjen e të dhënave personale, të cilat të disponojnë kompetencat, burimet dhe ekspertizën teknike të nevojshme për të ushtruar funksionet me efektivitet dhe për të marrë vendimet e tyre në mënyrë objektive, të paanshme dhe koherente".[193]

Tek e drejta e KiE-së, Protokolli Shtesë i Konventës 108 e ka bërë të detyrueshme ngritjen e autoriteteve të mbikëqyrjes. Neni 1 i këtij Protokolli përcakton kuadrin ligjor për autoritetet mbikëqyrëse të pavarura, të cilin Palët Kontraktuese duhet ta vënë në zbatim në legjislacionin e tyre kombëtar. Ky nen përdor formulime të ngjashme, për të përshkruar detyrat dhe kompetencat e këtyre autoriteteve, sikurse ato të përdorura në Direktivën e Mbrojtjes së të Dhënave. Në parim, autoritetet mbikëqyrëse duhet rrjedhimisht të funksionojnë në të njëjtën mënyrë, në kuadër të së drejtës së BE-së dhe të KiE-së.

Tek e drejta e BE-së, kompetencat dhe struktura organizative e autoriteteve mbikëqyrëse janë përcaktuar fillimisht në nenin 28 (1) të Direktivës së Mbrojtjes së të Dhënave. Rregullorja e Mbrojtjes së të Dhënave të Institucioneve të BE-së[194] krijon Mbikëqyrësin Evropian të Mbrojtjes së të Dhënave (EDPS), autoritetin përgjegjës për përpunimin e të dhënave nga organet dhe institucionet e BE-së. Kur përcakton rolin dhe përgjegjësitë e autoritetit mbikëqyrës, kjo rregullore mbështetet mbi eksperiencën e përftuar që prej miratimit të Direktivës së Mbrojtjes së të Dhënave.

Pavarësia e autoriteteve të mbrojtjes së të dhënave garantohet nga neni 16 (2) i TFBE-së dhe neni 8 (3) i Kartës. Kjo dispozitë e fundit e konsideron kontrollin nga një autoritet i pavarur si një element thelbësor të së drejtës themelore për mbrojtje të të dhënave. Gjithashtu, Direktiva e Mbrojtjes së të Dhënave u kërkon Shteteve Anëtare të krijojnë autoritetet mbikëqyrëse, për të monitoruar zbatimin e Direktivës në pavarësi të plotë.[195] Jo vetëm që legjislacioni, bazuar në të cilin krijohet organi mbikëqyrës, duhet të përmbajë dispozita specifike për garantimin e pavarësisë, por edhe struktura specifike organizative e autoritetit duhet të demonstrojë pavarësi.

Në 2010-ën, GjDBE-ja trajtoi për herë të parë një çështje të sferës së pavarësisë së autoriteteve mbikëqyrëse të mbrojtjes së të dhënave.[196] Shembujt në vijim ilustrojnë arsyetimin e saj.

---

[193] OECD (2013), *Udhëzuesi mbi mbrojtjen e privatësisë dhe qarkullimeve ndërkufitare të të dhënave personale*, parag. 19 (c).

[194] Rregullorja (EC) nr. 45/2001 e Parlamentit Evropian dhe e Këshillit, datë 18 dhjetor 2000 mbi mbrojtjen e personave nga përpunimi i të dhënave personale nga ana e institucioneve dhe organet e Komunitetit dhe mbi lëvizjen e lirë të këtyre të dhënave, JO 2001 L8, nenet 41-48.

[195] Direktiva e Mbrojtjes së të Dhënave, neni 28 (1), fjalia e fundit; Konventa 108, Protokolli Shtesë, neni 1 (3).

[196] Shih FRA (2010) *Të drejtat themelore: sfidat dhe arritjen në 2010-n*, Raporti vjetor 2010, fq. 59. FRA-ja e trajtoi këtë çështje në hollësi të shumta tek raporti i saj mbi *Mbrojtjen e të Dhënave në Bashkimin Evropian: roli i Autoriteteve Kombëtare të Mbrojtjes së të Dhënave*, i cili u publikua në maj të 2010-ës.

Shembull: tek çështja *Komisioni Evropian kundër Gjermanisë*,[197] Komisioni Evropian i kishte kërkuar GjDBE-së të deklaronte se Gjermania kishte transpozuar në mënyrë të pasaktë normën për "pavarësi të plotë" të autoriteteve përgjegjëse, për garantimin e mbrojtjes së të dhënave dhe në këtë mënyrë nuk kishte respektuar detyrimet që rrjedhin nga neni 28 (1) i Direktivës së Mbrojtjes së të Dhënave. Në këndvështrimin e Komisionit, problemi qëndronte tek fakti se Gjermania kishte vendosur nën mbikëqyrjen e shtetit, autoritetet mbikëqyrëse për monitorimin e përpunimit të të dhënave personale nga sektori jo publik, në disa shtete të ndryshme federale (*Länder*).

Vlerësimi i Gjykatës në lidhje me vlefshmërinë e ankesës, varej nga fushëveprimi i normës së pavarësisë që përmbante ai nen dhe për rrjedhojë, në interpretimin e dispozitës.

Gjykata theksoi se fjalët "në pavarësi të plotë" të nenit 28 (1) të Direktivës duhet të interpretohen bazuar në formulimin e kësaj dispozite, ashtu si edhe në objektivat dhe strukturën e Direktivës së Mbrojtjes së të Dhënave.[198] Gjykata nëvizoi se autoritetet mbikëqyrëse ishin "rojtarët" e të drejtave në lidhje me përpunimin e të dhënave personale të garantuara në Direktivë dhe në këtë mënyrë, krijimi i tyre në Shtetet Anëtare konsiderohet "si një element thelbësor i mbrojtjes së individëve nga përpunimi i të dhënave personale"[199] Gjykata arriti në përfundimin se "gjatë kryerjes së detyrave të tyre, autoritetet mbikëqyrëse duhet të veprojnë në mënyrë objektive dhe të paanshme. Për këtë qëllim, ato duhet të jenë të mbrojtura nga ndikim i jashtëm, përfshirë edhe atë të drejtpërdrejtë apo të tërthortë nga ana e shtetit apo Länder-it dhe jo vetëm nga ndikimi i organeve të mbikëqyrura".[200]

GjDBE-ja gjithashtu u shpreh se kuptimi i termit "në pavarësi të plotë" duhet të interpretohet mbështetur në pavarësinë e EDPS-së, siç e përcakton atë Rregullorja e Mbrojtjes së të Dhënave të Institucioneve të BE-së. Sikurse theksoi Gjykata, neni 44 (2) qartëson konceptin e pavarësisë, duke shtuar se, gjatë ushtrimit të detyrës së tij, EDPS-ja nuk mund të kërkojë apo të marrë udhëzime nga askush. Kjo përjashton mbikëqyrjen nga ana e shtetit të autoritetit të pavarur të mbikëqyrjes së mbrojtjes së të dhënave.[201]

Për rrjedhojë, GjDBE-ja vlerësoi se institucionet gjermane të mbrojtjes së të dhënave në nivel shteti federal, përgjegjëse për monitorimin e përpunimit të të dhënave personale nga organizmat jo publikë, nuk ishin të pavarura sa duhet, për shkak se ato ishin subjekt i mbikëqyrjes nga ana e shtetit.

Shembull: tek çështja *Komisioni Evropian kundër Austrisë*,[202] GjDBE-ja vuri në dukje probleme të ngjashme, që kishin të bënin me pozicionin e disa anëtarëve dhe stafit të Autoritetit Austriak të Mbrojtjes së të Dhënave (Komisioni i Mbrojtjes së të Dhënave, DSK). Gjykata vendosi në lidhje me këtë çështje se legjislacioni austriak e pengonte Autoritetin Austriak të Mbrojtjes së të Dhënave që të ushtronte funksionet e tij në pavarësi të plotë, sipas kuptimit të Direktivës së Mbrojtjes së të Dhënave. Pavarësia e autoritetit austriak nuk garantohej mjaftueshëm, për shkak se personeli i DSK-së sigurohej nga Kancelaria Federale, e cila edhe e mbikëqyrte DSK-në dhe kishte të drejtën të informohej në çdo kohë për punën që kryente.

[197] GjDBE, C-518/07, *Komisioni Evropian kundër Republikës Federale të Gjermanisë*, 9 mars 2010, parag. 27.
[198] Po aty, parag. 17 dhe 29.
[199] Po aty, parag. 23.
[200] Po aty, parag. 25.
[201] Po aty, parag. 27.
[202] GjDBE, C-614/10, *Komisioni Evropian kundër Republikës së Austrisë*, 16 tetor 2012, parag. 59 dhe 63.

Shembull: tek çështja *Komisioni Evropian kundër Hungarisë*,[203] GjDBE-ja vuri në dukje se "norma [...] sipas së cilës duhet të garantohet që çdo autoritet mbikëqyrës ka mundësi të ushtrojë detyrën që i është besuar, në pavarësi të plotë, nënkupton detyrimin e Shtetit Anëtar në fjalë që të respektojë mandatin e parashikuar". Gjykata theksoi gjithashtu se "duke ndërprerë para kohe mandatin e autoritetit mbikëqyrës për mbrojtjen e të dhënave personale, Hungaria nuk kishte përmbushur detyrimet e saj sipas Direktivës 95/46/EC [...]."

Sipas legjislacionit kombëtar, autoritetet mbikëqyrëse kanë kompetencat dhe të drejtat për të:[204]

- Këshilluar kontrolluesit dhe subjektet e të dhënave në lidhje me të gjitha çështjet e mbrojtjes së të dhënave;
- Hetuar përpunimet dhe rrjedhimisht për të ndërhyrë në to;
- Paralajmëruar apo këshilluar kontrolluesit;
- Urdhëruar korrigjimin, bllokimin, fshirjen apo shkatërrimin e të dhënave;
- Pezulluar përkohësisht apo përfundimisht përpunimin;
- Referuar çështjen gjykatës.

Për të ushtruar funksionet e tij, autoriteti mbikëqyrës duhet të ketë akses në të gjitha të dhënat personale dhe informacionet e nevojshme për një hetim, ashtu si edhe akses në të gjitha ambientet tek të cilat kontrolluesi ruan informacionin përkatës.

Ka dallime të konsiderueshme ndërmjet juridiksioneve sa i takon procedurave dhe efekteve ligjore të konstatimeve të një autoriteti mbikëqyrës. Ato mund të variojnë nga rekomandime të ngjashme me ato të një avokati populli, tek vendimet e ekzekutueshme menjëherë. Për këtë arsye, kur analizohet efektiviteti i mjeteve juridike të një juridiksioni, këto instrumente duhet të vlerësohen në kontekstin e tyre.

5.3. Mjetet e ankimit dhe sanksionet

Pikat kryesore

- Sipas Konventës 108 ashtu si edhe sipas Direktivës së Mbrojtjes së të Dhënave, legjislacioni kombëtar duhet të sigurojë mjetet e duhura të ankimit dhe sanksionet ndaj shkeljeve të së drejtës për mbrojtje të të dhënave.
- E drejta për mjete të efektshme ankimi nevojit, sipas së drejtës së BE-së, që legjislacioni kombëtar të sigurojë mjetet e ankimit gjyqësor, ndaj shkeljeve të të drejtave për mbrojtje të të dhënave, pavarësisht mundësisë për t'iu drejtuar një autoriteti mbikëqyrës.
- Legjislacioni kombëtar duhet të parashikojë sanksione të efektshme, ekuivalente, proporcionale dhe frenuese.
- Përpara se t'i drejtohet gjykatës, personi duhet t'i drejtohet fillimisht kontrolluesit. Ndërsa, nëse është gjithashtu e detyrueshme që t'i drejtohet autoritetit mbikëqyrës përpara gjykatës, kjo është lënë të rregullohet nga e drejta kombëtare.
- Subjektet e të dhënave mund të ankohen tek GjEDNj-ja për shkeljet e legjislacionit të mbrojtjes së të dhënave, si një instancë e fundit dhe sipas disa kushteve.
- Gjithashtu, subjektet e të dhënave mund t'i drejtohen edhe GjDBE-së, por vetëm në disa raste tepër të kufizuara.

[203] GjDBE, C-288/12, *Komisioni Evropian kund Hungarisë*, 8 prill 2014, parag. 50 dhe 67.
[204] Direktiva e Mbrojtjes së të Dhënave, neni 28; shih gjithashtu Konventa 108, Protokolli Shtesë, neni 1.

Të drejtat që burojnë nga legjislacioni në fushën e mbrojtjes së të dhënave, mund të ushtrohen vetëm nga personi, të drejtat e së cilit janë cënuar; domethënë një person i cili është, ose të paktën pretendon të jetë, subjekti i të dhënave. Këta persona, në ushtrimin e të drejtave të tyre, mund të përfaqësohen nga subjekte të cilët plotësojnë normat e nevojshme sipas legjislacionit kombëtar. Të miturit duhet të përfaqësohen nga prindërit apo kujdestarët e tyre. Përpara autoriteteve mbikëqyrëse, personi mund të përfaqësohet gjithashtu edhe nga shoqatat, qëllimi ligjor i të cilave është promovimi i së drejtave për mbrojtje të të dhënave.

5.3.1. Kërkesat drejtuar kontrolluesit

Të drejtat e përmendura në pikën 3.2 duhet të ushtrohen fillimisht në raport me kontrolluesin. Duke iu drejtuar drejtpërdrejtë autoritetit mbikëqyrës kombëtar apo gjykatës, do të ishte e pavlerë, meqenëse autoriteti vetëm mund të këshillojë që t'i drejtohet kontrolluesit fillimisht dhe gjykata nuk do ta pranonte kërkesën. Normat formale, për një kërkesë drejtuar kontrolluesit, e cila të jetë ligjërisht e vlefshme, sidomos nëse kërkesa duhet të jetë me shkrim, duhet të përcaktohen nga legjislacioni kombëtar.

Subjekti të cilit i është paraqitur kërkesa në cilësinë e kontrolluesit, duhet t'i përgjigjet kërkesës, edhe nëse nuk është kontrolluesi. Në çdo rast, përgjigja i duhet kthyer subjektit të të dhënave brenda afatit kohor të përcaktuar nga legjislacioni kombëtar, edhe nëse bëhet fjalë thjesht për të bërë me dije se asnjë e dhënë nuk po përpunohet në lidhje me aplikuesin. Në përputhje me dispozitat e nenin 12 (a) të Direktivës së Mbrojtjes së të Dhënave dhe nenit 8 (b) të Konventës 108, ajo kërkesë duhet trajtuar "pa vonesa të tepruara". Për rrjedhojë, legjislacioni kombëtar duhet të parashikojë një periudhë për përgjigjen, e cila të jetë e shkurtër sa duhet, po që gjithsesi t'i mundësojë kontrolluesit që të trajtojë kërkesën në mënyrën adekuate.

Përpara se t'i përgjigjet kërkesës, subjekti të cilit i është drejtuar në cilësinë e kontrolluesit, duhet të dijë identitetin e aplikuesit, me qëllim që të përcaktojë nëse ai apo ajo është vërtet personi i cili apo e cila pretendon të jetë, duke shmangur në këtë mënyrë një shkelje të rëndë të konfidencialitetit. Kur normat për përcaktimin e identitetit nuk rregullohen në mënyrë specifike nga legjislacioni kombëtar, ato duhet të vendosen nga kontrolluesi. Sidoqoftë, parimi i përpunimit të drejtë detyron kontrolluesit, të mos parashikojnë kushte tepër të vështira, për bërjen me dije të identitetit (dhe autenticitetit të kërkesës, sikurse u trajtua në paragrafin 2.1.1).

Legjislacioni kombëtar duhet të trajtojë gjithashtu çështjen nëse kontrolluesi, përpara se t'u përgjigjet kërkesave, mund të kërkojë pagesën e një tarife nga ana e aplikuesit: neni 12 (a) i Direktivës dhe neni 8 (b) i Konventës 108 parashikon se përgjigja ndaj kërkesave për akses duhet të jepet "pa shpenzime [...] të tepruara". Legjislacioni kombëtar në shume shtete evropiane parashikon se përgjigjet e kërkesave, në kuadër të legjislacionit të mbrojtjes së të dhënave, duhet të jepen pa pagesë, për sa kohë që përgjigjet nuk kërkojnë përpjekje të tepruara dhe të pazakonta; nga ana tjetër, e drejta kombëtare i mbron përgjithësisht kontrolluesit nga abuzimet me të drejtën për përgjigje ndaj kërkesave.

Nëse personi, institucioni apo organizmi të cilit i është drejtuar aplikuesi në cilësinë e kontrolluesit nuk e mohon që është i tillë, brenda periudhës së parashikuar në ligj, subjekti duhet të:

- Trajtojë kërkesën dhe të informojë aplikuesin në lidhje me mënyrën se si e ka trajtuar kërkesën; ose
- Të informojë aplikuesin pse kërkesa e tij apo e saj nuk do të trajtohet.

5.3.2. Ankesat e depozituara pranë një autoriteti mbikëqyrës

Çdo person që ka depozituar një kërkesë për akses, apo ka kundërshtuar një përpunim të një kontrolluesi, nuk merr përgjigje në kohën e duhur dhe të kënaqshme, mund t'i drejtohet autoritetit kombëtar mbikëqyrës me kërkesë për asistencë. Në kuadër të procedimit pranë autoritetit mbikëqyrës, duhet të qartësohet nëse personi, institucioni apo organizmi të cilit i është drejtuar aplikuesi, kishte në të vërtetë detyrimin për të trajtuar kërkesën dhe nëse trajtimi i saj ishte i saktë dhe i mjaftueshëm. Autoriteti mbikëqyrës duhet ta informojë aplikuesin në lidhje me rezultatin e procedimit.[205] Efektet ligjore të rezultateve të procedimeve, nga ana e autoriteteve mbikëqyrëse kombëtare, varen nga legjislacioni kombëtar: nëse vendimet e autoriteteve mund të jenë ligjërisht ekzekutive, domethënë që ato janë të ekzekutueshme nga autoriteti kompetent, ose nëse është e nevojshme që të bëhet ankim në gjykatë, në rast se kontrolluesi nuk zbaton vendimet e autoritetit mbikëqyrës (mendimin ligjor, paralajmërimin, etj.).

Nëse e drejta për mbrojtje të të dhënave e garantuar nga neni 16 i TFBE-së është shkelur nga institucionet dhe organet e BE-së, subjekti i të dhënave mund të depozitojë ankesë pranë EDPS-së,[206] autoritetit të pavarur mbikëqyrës për mbrojtjen e të dhënave, në përputhje me Rregulloren e Mbrojtjes së të Dhënave të Institucioneve të BE-së, e cila përcakton detyrat dhe kompetencat e EDPS-së. Në mungesë të përgjigjes nga EDPS-ja brenda gjashtë muajve, ankesa duhet konsideruar se është refuzuar.

Kundër vendimeve të autoritetit mbikëqyrës kombëtar, duhet të ekzistojë mundësia për t'u ankuar në gjykatë. Kjo është e vlefshme si për subjektin e të dhënave, ashtu edhe për kontrolluesit, të cilat kanë qenë palë të një procedimi nga një autoritet mbikëqyrës.

Shembull: Komisioneri i Informimit të Mbretërisë së Bashkuar publikoi një vendim më 24 korrik 2013, në të cilin kërkonte nga policia e Hertfordshire-it, të ndalonte përdorimin e sistemit të gjurmimit të targave të automjeteve, të cilin e konsideronte të paligjshëm. Të dhënat e mbledhura nga kamerat ruheshin si në bazën e të dhënave të policisë lokale, ashtu edhe në një bazë qendrore të të dhënave. Fotografitë e targave ruheshin për dy vite dhe fotografitë e automjeteve për 90 ditë. Argumentimi mbështetej tek fakti se përdorimi me shtrirje kaq të madhe i kamerave dhe formave të tjera të survejimit, nuk ishte proporcional në raport me problemin që synonte të zgjidhte.

[205] Direktiva e Mbrojtjes së të Dhënave, neni 28 (4).
[206] Rregullorja (EC) nr. 45/2001 e Parlamentit Evropian dhe e Këshillit e datës 18 dhjetor 2000 mbi mbrojtjen e personave nga përpunimi i të dhënave personale nga ana e institucioneve dhe organizmave të Komunitetit dhe mbi lëvizjen e lirë të këtyre të dhënave, JO 2001 L 8.

5.3.3. Ankesa e paraqitur në gjykatë

Sipas Direktivës së Mbrojtjes së të Dhënave, çdo person që i ka paraqitur kërkesë një kontrolluesi sipas legjislacionit të mbrojtjes së të dhënave dhe është i pakënaqur me përgjigjen e kontrolluesit, duhet të ketë mundësi të paraqesë ankesë pranë një gjykate kombëtare.[207]

Nëse është e detyrueshme t'i drejtohet fillimisht një autoriteti mbikëqyrës, përpara se të ankohet në gjykatë, këtë e përcakton legjislacioni kombëtar. Gjithsesi, në shumicën e rasteve, do të ketë më shumë përparësi për personat që ushtrojnë të drejtën për mbrojtje të të dhënave, t'i drejtohen së pari autoritetit mbikëqyrës, meqenëse shqyrtimi i kërkesave për asistencë nuk është burokratik dhe është pa pagesë. Ekspertiza e dokumentuar në vendimin e autoritetit mbikëqyrës (mendimi ligjor, paralajmërimi, etj.), mund të ndihmojë gjithashtu subjektin e të dhënave që të kërkojë të drejtat e tij apo të saj në gjykatë.

Sipas së drejtës së KiE-së, shkeljet e pretenduara të së drejtës për mbrojtje të të dhënave, që kanë ndodhur në nivel kombëtar të një Pale Kontraktuese të KEDNj-së dhe që përbëjnë në të njëjtën kohë shkelje të nenit 8 të KEDNj-së, mund gjithashtu të dërgohen për shqyrtim në GjEDNj, pasi të jenë shteruar të gjitha mjetet ligjore të brendshme. Ankimi pranë GjEDNj-së për shkelje të nenit 8 të KEDNj-së, duhet gjithashtu të përmbushë disa kritere të tjera pranueshmërie (nenet nga 34-37 të KEDNj-së).[208]

Edhe pse aplikimet pranë GjEDNj-së mund të drejtohen vetëm kundër Palëve Kontraktuese, ato mund të kenë të bëjnë gjithashtu në mënyrë të tërthortë me veprimet apo mosveprimet e individëve, për aq sa Palët Kontraktuese nuk kanë përmbushur detyrimet e tyre pozitive sipas KEDNj-së dhe nuk kanë garantuar mbrojtje të mjaftueshme nga shkeljet e të drejtës për mbrojtje të të dhënave në legjislacionin përkatës kombëtar.

Shembull: tek çështja *K. U. Kundër Finlandës,*[209] ankuesi, që ishte i mitur, u ankua se në një faqe interneti për takime, ishte postuar në emër të tij një njoftim me natyrë seksuale. Identiteti i personit i cili kishte postuar informacionin, nuk ishte bërë me dije nga ana e operatorit të shërbimit të internetit, për shkak të detyrimeve në lidhje me konfidencialitetin, sipas legjislacionit finlandez. Ankuesi pretendoi se legjislacioni finlandez nuk ofronte mbrojtje të mjaftueshme, ndaj veprimeve të tilla të një individi, i cili publikonte në internet informacione të dëmshme në lidhje me ankuesin. GjEDNj-ja përcaktoi se shtetet nuk janë të detyruara vetëm të mos ndërhyjnë në mënyrë arbitrare në jetën private të individëve, por mund t'i nënshtrohen edhe detyrimeve pozitive që kanë të bëjnë me "marrjen e masave që synojnë të garantojnë respektim të jetës private, deri tek sfera e marrëdhënieve të individëve ndërmjet tyre". Në rastin e ankuesit, për mbrojtjen praktike dhe të efektshme të tij, duheshin marrë disa masa reale për të identifikuar e ndjekur penalisht autorin. Por, shteti nuk e kishte siguruar një mbrojtje të tillë dhe GjEDNj-ja doli në përfundimin se ishte shkelur neni 8 i KEDNj-së.

---

[207] Direktiva e Mbrojtjes së të Dhënave, neni 22.
[208] KEDNj, nenet 34-37, të disponueshme në adresën: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.
[209] GjEDNj, *K.U. kundër Finlandës,* nr. 2872/02, 2 dhjetor 2008.

Shembull: tek çështja *Köpke kundër Gjermanisë,*[210] ankuesja kishte qenë e dyshuar për vjedhje në vendin e saj të punës dhe për këtë arsye i ishte nënshtruar video-survejimit të fshehtë. GjEDNj-ja doli në përfundimin se "nuk kishte asnjë provë se autoritetet kombëtare nuk kishin kërkuar të gjenin ekuilibrin, brenda hapësirës së vlerësimit të tyre, midis së drejtës së ankueses për respektim të jetës së saj private, sipas nenit 8 dhe interesit të punëdhënësit të saj, për mbrojtjen e pronës së tij dhe interesit publik, për administrimin e drejtësisë në mënyrën e duhur". Për rrjedhojë, ankesa u refuzua.

Nëse GjEDNj-ja konstaton se një Shtet Palë ka shkelur cilëndo nga të drejtat e sanksionuara nga KEDNj-ja, Shteti Palë është i detyruar të zbatojë vendimin e GjEDNj-së. Masat për zbatimin e vendimit së pari duhet të ndalin shkeljen dhe të zhdëmtojnë, aq sa është e mundur, pasojat negative për ankuesin. Zbatimi i vendimeve mund të kërkojë gjithashtu masa të përgjithshme, për të parandaluar shkeljet, të ngjashme me ato të gjetura nga Gjykata, qoftë nëpërmjet ndryshimeve në legjislacion, të jurisprudencës apo masa të tjera.

Kur GjEDNj-ja konstaton shkelje të KEDNj-së, neni 41 i KEDNj-së parashikon ajo mund t'i akordojë dëmshpërblim të drejtë ankuesit, me shpenzimet e Shtetit Palë.

Sipas së drejtës së BE-së,[211] viktimat e shkeljeve të legjislacionit kombëtar të mbrojtjes së të dhënave, i cili transpozon legjislacionin e BE-së në fushën e mbrojtjes së të dhënave, në disa raste mund t'i dërgojnë çështjet e tyre përpara GjDBE-së. Parashikohen dy raste të mundshme kur ankesa e një subjekti, në lidhje me shkeljen e të drejtave për mbrojtje të të dhënave të tij apo të saj, mund të dërgohet për procedim nga ana e GjDBE-së.

Në rastin e parë, subjekti i të dhënave do të duhej të ishte viktima e drejtpërdrejtë e një akti administrativ apo rregullator të BE-së, i cili shkel të drejtën e tij për mbrojtje të të dhënave. Sipas nenit 263 (4) të TFBE-së:

"çdo person fizik apo juridik mund [...] të fillojë proces kundër një akti që i drejtohet atij personi, ose i cili është në interes të drejtpërdrejtë të atij personi dhe kundër një akti rregullator, i cili është në interes të drejtpërdrejtë të atij personi dhe i cili nuk nënkupton masa zbatuese."

Kështu, viktimat e një përpunimi të paligjshëm të dhënash nga ana e një organizmi të BE-së, mund të ankohen drejtpërdrejtë në Gjykatën e Përgjithshme të GjDBE-së, i cili është organi që ka kompetencën për të gjykuar çështje që kanë të bëjnë me Rregulloren e Mbrojtjes së të Dhënave të BE-së. Personi mund të ankohet edhe drejtpërdrejtë tek GjDBE-ja, nëse statusi ligjor i tij preket drejtpërdrejt nga një dispozitë ligjore e BE-së.

Rasti i dytë ka të bëjë me kompetencën e GjDBE-së (Gjykatës së Drejtësisë) për të nxjerrë vendime paraprake, në përputhje me nenin 267 të TFBE-së.

---

[210] GjEDNj, *Köpke kundër Gjermanisë* (dec.), nr. 420/07, 5 tetor 2010.

[211] BE (2007) Traktati i Lisbonës që ndryshon Traktatin e Bashkimit Evropian dhe Traktatin për Themelimin e Komunitetit Evropian, nënshkruar në Lisbonë, 13 dhjetor 2007, JO 2007 C 306. Shih gjithashtu versionin e konsoliduar të Traktatit të Bashkimit Evropian, JO 2012 C 326 dhe të TFBE-së, JO 2012 C 326.

Subjektet e të dhënave, në kuadër të procedimeve kombëtare, mund t'i kërkojnë gjykatës kombëtare që t'i drejtohet për qartësime Gjykatës së Drejtësisë për interpretimin e Traktateve të BE-së dhe për interpretimin e vlefshmërinë e akteve të institucioneve, organeve, zyrave dhe agjencive të BE-së. Këto qartësime njihen si vendime paraprake. Ky lloj vendimi nuk përbën apelim të drejtpërdrejtë për ankuesin, por i mundëson gjykatave kombëtare të sigurohen se po kryejnë interpretimin e saktë të legjislacionit të BE-së.

Nëse një palë në procedimin përpara gjykatave kombëtare kërkon referimin e një çështjeje në GjDBE, vetëm ato gjykata kombëtare të cilat janë të shkallës më të lartë, vendimet e të cilave janë të formës së prerë, janë të detyruara ta zbatojnë.

Shembull: tek çështja *Kärntner Landesregierung dhe të tjerët,*[212] Gjykata Kushtetuese Austriake i paraqiti GjDBE-së pyetje në lidhje me vlefshmërinë e neneve nga 3 deri 9 të Direktivës 2006/24/EC (*Direktiva e Ruajtjes së të Dhënave, shfuqizuar më 8 prill 2014*) mbështetur në nenet 7, 9 dhe 11 të Kartës dhe nëse disa dispozita të Ligjit Federal Austriak mbi Telekomunikacionet, i cili transpozon Direktivën e Ruajtjes së të Dhënave, ishin në kundërshtim me disa aspekte të Direktivës së Mbrojtjes së të Dhënave dhe të Rregullores së Mbrojtjes së të Dhënave të Institucioneve të BE-së.

Z. Seitlinger, njëri nga ankuesit e çështjes së gjykuar në Gjykatën Kushtetuese, deklaroi se e përdorte telefonin, internetin dhe adresën elektronike si në lidhje me punën, ashtu edhe me jetën private. Për këtë arsye, informacioni që ai dërgon dhe merr, kalon nëpërmjet rrjeteve publike të telekomunikacionit. Bazuar në Ligjin Austriak të Telekomunikacioneve të vitit 2003, ofruesi i shërbimeve të telekomunikacionit të tij, është ligjërisht i detyruar të mbledhë dhe ruajë të dhëna në lidhje me përdorimin e rrjetit nga ana e z. Seitlinger. Ky i fundit kishte kuptuar se kjo mbledhje e ruajtje të dhënash personale, nuk ishte në asnjë mënyrë e nevojshme për qëllime teknike, të transmetimit të informacionit në rrjet nga pika A në pikën B. Në fakt, mbledhja dhe ruajtja e këtyre të dhënave, nuk ishte as tërthorazi e nevojshme për qëllime të faturimit. Sigurisht, z. Seitlinger nuk kishte dhënë pëlqimin, për përdorimin e të dhënave të tij personale. E vetmja arsye për mbledhjen dhe ruajtjen e këtyre të dhënave të tepërta, ishte Ligji Austriak i Telekomunikacioneve i vitit 2003.

Për këtë arsye, z. Seitlinger, iu drejtua Gjykatës Kushtetuese të Austrisë me pretendimin se detyrimet ligjore që i ishin përcaktuar operatorit të tij të shërbimeve të telekomunikacionit, ishin në shkelje të së drejtave themelore të tij sipas nenit 8 të Kartës së BE-së.

GjDBE-ja nxjerr vendim vetëm në lidhje me elementet në përbërje të kërkesës për vendim paraprak që i është drejtuar. Vendimi në lidhje me çështjen fillestare, mbetet në juridiksionin e gjykatave kombëtare.

Në parim, Gjykata e Drejtësisë duhet t'u përgjigjet pyetjeve që i janë drejtuar. Ajo nuk mund të refuzojë të shprehet në mënyrë paragjykimore, me arsyetimin se përgjigja nuk do të ishte as e rëndësishme dhe as në kohën e duhur, në raport me çështjen fillestare. Gjithsesi, ajo mund të refuzojë çështjen nëse kjo e fundit nuk është në kompetencën e saj.

[212] GjDBE, Çështje të bashkuara, C-293/12 dhe C-594/12, *Digital Rights Ireland dhe Seitling dhe të Tjerët*, 8 prill 2014.

Si përfundim, nëse të drejtat për mbrojtje të të dhënave, të cilat sanksionohen nga neni 16 i TFBE-së, shkelen nga një institucion apo organ i BE-së gjatë përpunimit të të dhënave personale, subjekti i të dhënave mund t'i drejtohet Gjykatës së Përgjithshme të GjDBE-së (neni 32 (1) dhe (4) i Rregullores së Mbrojtjes së të Dhënave të Institucioneve të BE-së). Në të njëjtën mënyrë veprohet edhe për vendimet e EDPS-së që kanë të bëjnë me shkelje të tilla (neni 32 (2) i Rregullores së Mbrojtjes së të Dhënave të Institucioneve të BE-së).

Megjithëse Gjykata e Përgjithshme e GjDBE-së është kompetente për të dhënë vendime për çështjet që mbulon Rregullorja e Mbrojtjes së të Dhënave të Institucioneve të BE-së, nëse një person në cilësinë e pjesëtarit të stafit të një institucioni apo organi të BE-së kërkon të bëjë padi, duhet t'i drejtohet Tribunalit të Shërbimit Civil të BE-së.

Shembull: çështja *Komisioni Evropian kundër The Bavarian Lager Co. Ltd* [213] ilustron mjetet juridike që mund të përdoren, kundër veprimeve apo vendimeve në fushën e mbrojtjes së të dhënave të institucioneve dhe organeve të BE-së.

Bavarian Lager-i kërkoi nga Komisioni Evropian akses të plotë në proces-verbalin e një mbledhjeje të këtij të fundit, e cila kishte trajtuar çështje ligjore me rëndësi për shoqërinë. Komisioni e kishte refuzuar kërkesën për akses të shoqërisë, duke u mbështetur në interesat prevalues të mbrojtjes së të dhënave.[214] Kundër këtij vendimi, Bavarian Lager-i kishte bërë padi në GjDBE, në zbatim të nenit 32 të Rregullores së Mbrojtjes së të Dhënave të Institucioneve të BE-së; me konkretisht, padia ishte bërë pranë Gjykatës së Shkallës së Parë (paraardhësja e Gjykatës së Përgjithshme). Në vendimin e saj mbi çështjen T-194/04, *Bavarian Lager kundër Komisionit,* Gjykata e Shkallës së Parë anuloi vendimin e Komisionit për të refuzuar kërkesën për akses. Komisioni Evropian e apeloi vendimin në Gjykatën e Drejtësisë së GjDBE-së. Vendimi i Gjykatës së Drejtësisë (Dhoma e Madhe) rrëzoi vendimin e Gjykatës së Shkallës së Parë dhe konfirmoi refuzimin e Komisionit Evropian ndaj kërkesës për akses.

5.3.4. Sanksionet

Sipas së drejtës së KiE-së, neni 10 i Konventës 108 parashikon se sanksionet dhe mjetet e përshtatshme të ankimit, për shkeljet e dispozitave të legjislacionit vendas, të cilat bëjnë të zbatueshme parimet themelore të mbrojtjes së të dhënave, të sanksionuara në Konventën 108, duhet të përcaktohen nga secila Palë.[215] **Sipas së drejtës së BE-së,** neni 24 i Direktivës së Mbrojtjes së të Dhënave vendos se Shtetet Anëtare "duhet të marrin masat e përshtatshme, për të garantuar zbatim të plotë të dispozitave të kësaj Direktive dhe në mënyrë të veçantë duhet të përcaktojnë sanksionet, që duhet vendosur në rast shkeljeje të dispozitave të miratuara [...]".

Të dy instrumentet juridike u japin Shteteve Anëtare një hapësirë te gjerë vlerësimi sa i takon përzgjedhjes së sanksioneve dhe mjeteve të përshtatshme të ankimit.

---

[213] GjDBE, C-28/08 P, *Komisioni Evropian kundër The Bavarian Lager Co. Ltd*, 29 qershor 2010.

[214] Për një analizë të argumentit, shih: EDPS (2011), Aksesi i publikut në dokumentet që përmbajnë të dhëna personale pas vendimin mbi the Bavarian Lager, Bruksel, EDPS, në adresën: www.secure.edps.europa.eu/EDPSËEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_ Lager_EN.pdf.

[215] GjEDNj, *I. kundër Finlandës*, nr. 20511/03, 17 korrik 2008; GjEDNj, K.U. kundër Finlandës, nr. 2872/02, 2 dhjetor 2008.

Asnjë nga instrumentet juridike nuk jep këshilla të veçanta, në lidhje me natyrën apo llojin e sanksionit të përshtatshëm, as shembuj të tyre.

Gjithsesi:

"*edhe pse Shtetet Anëtare të BE-së gëzojnë një hapësirë vlerësimi për përcaktimin e masave më të përshtatshme, për garantimin e të drejtave që u njeh legjislacioni i BE-së, në përputhje me parimin e bashkëpunimit të drejtë, sikurse përshkruhet në nenin 4 (3) të TFBE-së, duhen respektuar kërkesat minimale të efektivitetit, ekuivalencës, proporcionalitetit dhe parandalueshmërisë."*[216]

GjDBE-ja ka theksuar në mënyrë të përsëritur se legjislacioni kombëtar nuk është krejtësisht i lirë për të përcaktuar sanksionet.

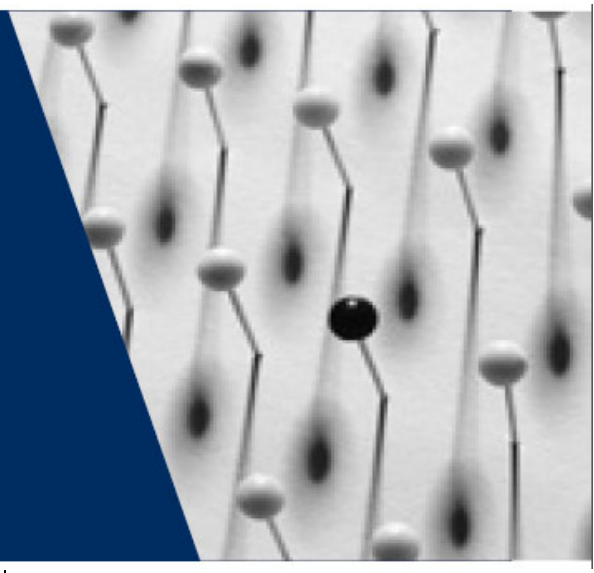
Shembull: tek çështja *Von Colson dhe Kamann kundër Land Nordrhein-Westfalen*,[217] GjDBE-ja u shpreh se Shtetet Anëtare të cilëve u drejtohet Direktiva, janë të detyruar të miratojnë në sistemet e tyre ligjore kombëtare, të gjitha masat e nevojshme, për t'u siguruar se ai është plotësisht i efektshëm, në përputhje me objektivin që ajo synon të arrijë. Gjykata vendosi se, edhe pse u takon Shteteve Anëtare të zgjedhin rrugët dhe mjetet për të garantuar zbatimin e Direktivës, ajo liri nuk ndikon në detyrimin që bie mbi to. Veçanërisht, mjetet ligjore të ankimit duhet t'i mundësojnë individit të ndjekë dhe ushtrojë të drejtën në fjalë, deri në arritjen e efektit të saj thelbësor. Me qëllim që të arrihet mbrojtja e vërtetë dhe e efektshme, mjetet ligjore të ankimit duhet të jenë pikënisja e procedurave penale dhe/ose e masave kompensuese, të cilat çojnë në sanksione me efekte frenuese.

Sa i takon sanksioneve kundër shkeljeve të legjislacionit të BE-së nga institucionet dhe organet e BE-së, për shkak të qëllimit të veçantë të Rregullores së Mbrojtjes së të Dhënave të BE-së, sanksionet parashikohen vetëm në formën e masave disiplinore. Sipas nenit 49 të Rregullores, "çdo shkelje e detyrimeve në përputhje me këtë Rregullore, qoftë me qëllim apo nga pakujdesia, e ngarkon funksionarin apo nëpunësin e Komunitetit Evropian me përgjegjësi disiplinore (...)".

[216] FRA (2012), Opinion i Agjencisë së Bashkimit Evropian e të Drejtave Themelore mbi paketën e propozuar të reformës së mbrojtjes së të dhënave, 2/2012, Vjenë, 1 tetor 2012, fq. 27.
[217] GjDBE, C-14/83, *Sabine von Kolson dhe Elisabeth Kamann kundër Land Nordrhein-Westfalen*, 10 prill 1984.

6

Qarkullimet ndërkufitare të të dhënave



BE	Çështje të trajtuara	KiE
Qarkullimet ndërkufitare të të dhënave		
Direktiva e Mbrojtjes së të Dhënave, neni 25 (1) GjDBE, C-101/01, *Bodil Lindqvist*, 6 nëntor 2003	**Përkufizim**	Konventa 108, Protokolli Shtesë, neni 2 (1)
Qarkullimet e lira të të dhënave		
Direktiva e Mbrojtjes së të Dhënave	**Ndërmjet Shteteve Anëtare të BE-së**	
	Ndërmjet Palëve Kontraktuese të Konventës 108	Konventa 108 Protokolli Shtesë, neni 12 (2)
Direktiva e Mbrojtjes së të Dhënave, neni 25	**Drejt shteteve të treta me nivel të mjaftueshëm të mbrojtjes së të dhënave**	Konventa 108, Protokolli Shtesë, neni 2 (1)
Direktiva e Mbrojtjes së të Dhënave, neni 26 (1)	**Drejt shteteve të treta në raste të veçanta**	Konventa 108, Protokolli Shtesë, neni 2 (2) (a)
Qarkullimet e kufizuara të të dhënave drejt shteteve të treta		
Direktiva e Mbrojtjes së të Dhënave, neni 26 (2) Direktiva e Mbrojtjes së të Dhënave, neni 26 (4)	**Klauzolat kontraktuese**	Konventa 108, Protokolli Shtesë, neni 2 (2) (b) Udhëzuesi për përgatitjen e klauzolave kontraktuese
Direktiva e Mbrojtjes së të Dhënave, neni 26 (2)	**Rregullat e detyrueshme të korporatave**	
Shembuj: BE-SHBA Marrëveshja mbi PNR-të BE-SHBA Marrëveshja mbi SWIFT-in	**Marrëveshje ndërkombëtare speciale**	

Direktiva e Mbrojtjes së të Dhënave nuk parashikon vetëm qarkullimin e lirë të të dhënave ndërmjet Shteteve Anëtare, por përmban gjithashtu edhe dispozita në lidhje me kërkesat që duhen përmbushur për transferimin e të dhënave personale drejt shteteve të treta, jashtë BE-së. KiE-ja po ashtu njohu rëndësinë e zbatimit të rregullave për qarkullimet ndërkufitare të të dhënave drejt shteteve të treta dhe miratoi Protokollin Shtesë të Konventës 108 në vitin 2001.

Ky Protokoll miratoi aspektet normative kryesore, në lidhje me qarkullimet ndërkufitare të të dhënave, nga palët kontraktuese të Konventës dhe Shtetet Anëtare të BE-së.

6.1. Natyra e qarkullimeve ndërkufitare të të dhënave

Pikat kryesore

- Qarkullimi ndërkufitar i të dhënave është një transferim të dhënash, drejt një marrësi i cili është subjekt i një juridiksioni të huaj.

Neni 2 (1) i Protokollit Shtesë të Konventës 108 e përshkruan qarkullimin ndërkufitar të të dhënave si një transferim të dhënash personale, drejt një marrësi i cili është subjekt i një juridiksioni të huaj. Neni 25 (1) i Direktivës së Mbrojtjes së të Dhënave rregullon "transferimin e të dhënave personale drejt një shteti të tretë, të cilat janë duke iu nënshtruar përpunimit apo kanë për qëllim të përpunohen pas transferimit [...]". Ky lloj transferimi të dhënash lejohet vetëm në përputhje me rregullat e përcaktuara në nenin 2 të Protokollit Shtesë të Konventës 108, ashti si dhe për Shtetet Anëtare të BE-së, në nenet 25 dhe 26 të Direktivës së Mbrojtjes së të Dhënave.

Shembull: tek çështja *Bodil Lindqvist*,[218] GjDBE-ja vendosi se "veprimi që konsiston në referimin në një faqe interneti të disa personave dhe identifikimin e tyre me emër apo me mënyra të tjera, për shembull nëpërmjet numrit të telefonit apo informacionit në lidhje me kushtet e tyre të punës dhe si e kalojnë kohën e lirë, përbën "përpunim të dhënash personale, plotësisht ose pjesërisht me pajisje automatike", sipas kuptimit të nenit 3 (1) të Direktivës 95/46".

Në vijim, Gjykata theksoi se Direktiva përcakton gjithashtu rregulla specifike, të cilat synojnë t'u lejojnë Shtetet Anëtare të monitorojnë transferimin e të dhënave personale drejt shteteve të treta.

Gjithsesi, duke pasur parasysh nga njëra anë nivelin e zhvillimit të internetit, në kohën kur është hartuar Direktiva dhe nga ana tjetër mungesën në të të kritereve të zbatueshme, në lidhje me përdorimin e internetit, "nuk mund të prezumohet se legjislatori komunitar kishte për qëllim të përfshinte në nocionin e "transferimit të të dhënave drejt një shteti të treta" ngarkimin [...] e të dhënave në një faqe interneti, edhe nëse ato të dhëna për rrjedhojë bëhen të aksesueshme për personat në shtetet e treta, të cilët zotërojnë pajisjet teknike për t'i aksesuar ato."

Përndryshe, nëse Direktiva do të "interpretohej në kuptimin që sa herë që ngarkohen të dhëna personale në një faqe interneti, ka transferim të dhënash drejt shteteve të treta, ai transferim do të përbënte detyrimisht transferim drejt të gjitha shtetet e treta, ku ekzistojnë pajisjet teknike të nevojshme për akses në internet. Në këtë mënyrë, regjimi special i parashikuar [nga direktiva] do të shndërrohej domosdoshmërish në regjim me fushë të përgjithshme, sa i takon operacioneve në internet. Në fakt, sa herë që Komisioni do të konstatonte (...) se vetëm një shtet i tretë nuk garanton nivel mbrojtjeje të mjaftueshme, Shtetet Anëtare do të ishin të detyruara të pengonin çdo ngarkim të të dhënave personale në internet."

Parimi sipas së cilit thjesht publikimi i të dhënave (personale) nuk konsiderohet si qarkullim ndërkufitar të dhënash, zbatohet gjithashtu për regjistrat publikë *online*, apo masmediat, sikurse gazetat (elektronike) dhe televizionet.

[218] GjDBE, C-101/01, *Bodil Lindqvist*, 6 nëntor 2003, parag. 27, 68 dhe 69.

Vetëm komunikimi i cili i drejtohet marrësve specifikë mund të plotësojë kriteret e "qarkullimit ndërkufitar të të dhënave".

6.2. Qarkullimet e lira të të dhënave ndërmjet Shteteve Anëtare ose ndërmjet Palëve Kontraktuese

Pikat kryesore

- Transferimi i të dhënave personale drejt një shteti tjetër anëtar të Zonës Ekonomike Evropiane ose drejt një Pale tjetër Kontraktuese të Konventës 108, duhet të jetë i përjashtuar nga çdo lloj kufizimi.

Në përputhje me nenin 12 (2) të Konventës 108, **sipas së drejtës së KiE-së,** duhet të ketë qarkullim të lirë të të dhënave personale ndërmjet Palëve të Konventës. Legjislacioni kombëtar nuk mundet të kufizojë eksportimin e të dhënave personale drejt një Pale Kontraktuese përveçse:

- Kur e imponon natyra e veçantë e të dhënave[219]; ose
- Kufizimi është i nevojshëm për të parandaluar shmangien nga dispozitat ligjore kombëtare mbi qarkullimin ndërkufitar të të dhënave drejt palëve të treta.[220]

Sipas së drejtës së BE-së, kufizimet apo ndalimet e qarkullimit të lirë të të dhënave ndërmjet Shteteve Anëtare për arsye të mbrojtjes së të dhënave, janë të ndaluara nga neni 1 (2) i Direktivës së Mbrojtjes së të Dhënave. Zona e qarkullimit të lirë të të dhënave është zgjeruar me Marrëveshjen e Zonës Ekonomike Evropiane (EEA),[221] e cila bën pjesë të tregut të brendshëm Islandën, Lihtenshtejnin dhe Norvegjinë.

Shembull: nëse një filial i një grupi ndërkombëtar shoqërish, i cili është i vendosur në Shtete të ndryshme Anëtare të BE-së, midis të tjerësh në Sllloveni dhe në Francë, transferon të dhëna personale nga Sllovenia drejt Francës, ky lloj qarkullimi të dhënash nuk duhet të kufizohet apo ndalohet nga legjislacioni kombëtar slloven.

Por nëse i njëjti filial slloven dëshiron të transferojë të njëjtat të dhëna personale, drejt kompanisë mëmë në Shtetet e Bashkuara, eksportuesi slloven i të dhënave duhet të respektojë procedurat e përcaktuara në legjislacionin slloven, në fushën e qarkullimeve ndërkufitare të të dhënave drejt shteteve të treta, të cilat nuk kanë nivel të mjaftueshëm mbrojtjeje, përveç rastit kur kompania mëmë ka miratuar Parimet e Privatësisë "Safe Harbor"("Porti i Sigurt"), i cili është një kod sjelljeje vullnetar, për garantimin e një niveli të mjaftueshëm të mbrojtjes së të dhënave (shih pikën 6.3.1).

[219] Konventa 108, neni 12 (3) (a).
[220] Po aty, neni 12 (3) (b).
[221] Vendim i Këshillit dhe Komisionit, datë 13 dhjetor 1993, mbi arritjen e Marrëveshjes së Zonës Ekonomike Evropiane ndërmjet Komuniteteve Evropiane, Shteteve të tyre Anëtare dhe Republikës së Austrisë, Republikës së Finlandës, Republikës së Islandës, Principatës së Lihtenshtejnit, Mbretërisë së Norvegjisë, Mbretërisë së Suedisë dhe Konfederatës Zvicerane, JO 1994 L 1.

Gjithsesi, qarkullimet ndërkufitare të të dhënave drejt Shteteve Anëtare të EEA-së, për qëllime që s'kanë të bëjnë me tregun e brendshëm, sikurse për hetimin e krimeve, nuk i nënshtrohen dispozitave të Direktivës së Mbrojtjes së të Dhënave dhe për rrjedhojë nuk i përfshin parimi i qarkullimit të lirë të të dhënave. Sa i përket së drejtës së KiE-së, të gjitha fushat përfshihen në objektin e Konventës 108 dhe të Protokollit Shtesë të Konventës 108, edhe pse Palët Kontraktuese mund të parashikojnë përjashtime. Të gjithë anëtarët e EEA-së janë gjithashtu Palë të Konventës 108.

6.3. Qarkullimet e lira të të dhënave drejt vendeve të treta

Pikat kryesore

- Transferimi i të dhënave personale drejt vendeve të treta përjashtohet nga çdo kufizim në përputhje me legjislacionin kombëtar të fushës së mbrojtjes së të dhënave nëse:
  - Është certifikuar niveli i mjaftueshëm i mbrojtjes së të dhënave në territorin e marrësit; ose
  - Është i domosdoshëm për interesat specifikë të subjektit të të dhënave ose interesave prevalues legjitimë të të tjerëve, veçanërisht interesave të rëndësishëm publikë.
- Nivel i mjaftueshëm i mbrojtjes së të dhënave në një vend të tretë, do të thotë se parimet themelore të mbrojtjes së të dhënave janë zbatuar, në mënyrë të efektshme në legjislacionin e brendshëm të atij vendi.
- Sipas së drejtës së BE-së, niveli i mjaftueshëm i mbrojtjes së të dhënave në një vend të tretë, vlerësohet nga Komisioni Evropian. Sipas së drejtës së KiE-së, modalitetet e vlerësimit të nivelit të mjaftueshëm rregullohen nga legjislacioni kombëtar.

6.3.1. Qarkullimi i lirë i të dhënave për shkak të nivelit të mjaftueshëm të mbrojtjes

Sipas së drejtës së KiE-së, legjislacioni kombëtar mund të lejojë qarkullimin e lirë të të dhënave drejt shteteve jo kontraktuese, nëse shteti apo organizata garanton nivel të mjaftueshëm mbrojtjeje për transferimin e parashikuar të të dhënave.[222] Legjislacioni i brendshëm përcakton se si duhet vlerësuar niveli i mbrojtjes së të dhënave në një vend të huaj dhe personat që do të kryejnë vlerësimin.

Sipas së drejtës së BE-së, qarkullimi i lirë i të dhënave drejt shteteve të treta që kanë nivel të mjaftueshëm të mbrojtjes së të dhënave, parashikohet në nenin 25 (1) të Direktivës së Mbrojtjes së të Dhënave. Kërkesa për mjaftueshmëri dhe jo për ekuivalencë, mundëson respektimin e mënyrave të ndryshme, me anë të së cilave mund të garantohet mbrojtja e të dhënave. Në përputhje me nenin 25 (6) të Direktivës, Komisioni Evropian është kompetent për të vlerësuar nivelin e mbrojtjes së të dhënave në vendet e huaja, nëpërmjet një vendimi në lidhje me nivelin e mjaftueshëm të mbrojtjes së të dhënave dhe konsultimit për vlerësimin e bërë me Grupin e Punës së Nenit 29, i cili ka dhënë kontribut thelbësor në interpretimin e neneve 25 dhe 26.[223]

---

[222] Konventa 108, Protokolli Shtesë, neni 2 (1).

[223] Shih për shembull, Grupi i Punës së Nenit 29 (2003*), Dokument pune në lidhje me transferimet e të dhënave personale drejt shteteve të treta: zbatimi i nenit 26 (2) të Direktivës së Mbrojtjes së të Dhënave të BE-së për rregullat e detyrueshme të korporatave për transferimet ndërkombëtare të të dhënave*, WP 74, Bruksel, 3 qershor 2003; dhe Grupi i Punës së Nenit 29 (2005), *dokument pune në lidhje me interpretimin e unifikuar të nenit 26 (1) të Direktivës 95/46/EC, datë 24 tetor 1995*, WP 114, Bruksel, 25 nëntor 2005.

Vendimi i Komisionit Evropian për nivelin e mjaftueshëm të të dhënave ka forcë ligjore detyruese. Nëse Komisioni Evropian publikon vendimin në lidhje me nivelin e mjaftueshëm të një vendi në Fletoren Zyrtare të Bashkimit Evropian, të gjitha shtetet anëtare të EEA-së dhe organet përkatëse, janë të detyruara të zbatojnë vendimin, çka nënkupton se të dhënat mund të qarkullojnë me këtë vend pa procedura verifikimi apo autorizimi nga ana e autoriteteve kombëtare.[224]
Komisioni Evropian ka mundësi gjithashtu të bëjë vlerësimin e disa pjesëve të sistemit juridik të një vendi, ose të kufizohet vetëm në disa tema të veçanta. Për shembull, Komisioni ka dhënë një vendim në lidhje me nivelin vetëm sa i takon të drejtës tregtare private të Kanadasë.[225] Ekzistojnë gjithashtu disa vendime mbi nivelin në lidhje me transferimet, mbështetur në marrëveshjet ndërmjet BE-së dhe shteteve të huaja. Këto vendime kanë të bëjnë posaçërisht me një lloj të vetëm transferimi të dhënash, sikurse transmetimi i të dhënave të pasagjerëve nga ana e shoqërive të fluturimit, drejt autoriteteve të huaja të kontrollit kufitar, kur shoqëria kryen fluturime nga BE-ja drejt disa destinacioneve jashtë BE-së (shih pikën 6.4.3). Një praktikë e kohëve të fundit në lidhje me transferimin e të dhënave, mbështetur në marrëveshje speciale midis BE-së dhe vendeve të treta, lë përgjithësisht mënjanë vendimet për nivelin e mbrojtjes së të dhënave, me pretendimin se marrëveshja vetë ofron nivel të mjaftueshëm të mbrojtjes së të dhënave.[226]

Një prej vendimeve më të rëndësishme të nivelit të mbrojtjes së të dhënave, nuk konsiston në fakt në një tërësi dispozitash ligjore.[227] Përkundrazi, ka të bëjë me rregulla që ngjasojnë më së shumti me një Kod Sjelljeje, i cili njihet si Parimet e Privatësisë "Safe Harbour". Këto parime u hartuan nga BE-ja së bashku me SHBA-të, për shoqëritë tregtare të SHBA-ve. Përputhshmëria me parimet e "Safe Harbour"-it arrihet nëpërmjet angazhimit vullnetar, i cili shprehet nëpërmjet një deklarate para Komisionit të Tregtisë së SHBA-ve dhe dokumentimit të saj në një listë që e publikon po ai departament. Duke qenë një nga elementet më të rëndësishme të nivelit të mjaftueshëm të mbrojtjes së të dhënave është efektshmëria e zbatimit të mbrojtjes së të dhënave, Marrëveshja "Safe Harbour" parashikon gjithashtu edhe një farë mbikëqyrjeje nga ana e shtetit: mund të aderojnë në parimet e Safe Harbour-it vetëm ato shoqëri të cilat janë objekt i mbikëqyrjes së Komisionit Federal të Tregtisë së SHBA-ve.

6.3.2. Qarkullimi i lirë i të dhënave në raste të veçanta

Sipas së drejtës së KiE-së, neni 2 (2) i Protokollit Shtesë të Konventës 108 lejon transferimin e të dhënave personale drejt vendeve të treta, të cilat nuk ofrojnë nivel të mjaftueshëm të mbrojtjes së të dhënave, për sa kohë që transferimi parashikohet nga legjislacioni i brendshëm dhe është i nevojshëm për:

[224] Për një listë të përditësuar në vazhdimësi, të vendeve të cilat kanë përfituar një vendim mjaftueshmërie të mbrojtjes së të dhënave, shih faqen zyrtare të Komisionit Evropian, Drejtoria e Përgjithshme e Drejtësisë, tek: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.
[225] Komisioni Evropian (2002), Vendimi 2002/2/EC, datë 20 dhjetor 2001 në përputhje me Direktivën 95/46/EC të Parlamentit Evropian dhe Këshillit në lidhje me mbrojtjen e mjaftueshme të të dhënave personale, që garanton Ligji për Mbrojtjen e Informacionit Personal dhe Dokumentacionit Elektronik të Kanadasë, JO 2002 L 2.
[226] Për shembull, Marrëveshjen midis Shteteve të Bashkuara të Amerikës dhe Bashkimit Evropian në lidhje me përdorimin dhe transferimin e të Dhënave të Pasagjerëve drejt Departamentit të Sigurisë Kombëtare të Shteteve të Bashkuara (OJ 2012 L 215, fq. 5–14) ose Marrëveshjen midis Bashkimit Evropian dhe Shteteve të Bashkuara të Amerikës në lidhje me përpunimin dhe transferimin e të Dhënave të Komunikimit Financiar nga Bashkimi Evropian drejt Shteteve të Bashkuara për qëllime të Programit të Survejimit të Financimit të Terrorizmit, JO 2010 L 8, fq. 11-16.
[227] Komisioni Evropian (2000), Vendimi i Komisionit 2000/520/EC datë 26 korrik 2000 në përputhje me Direktivën 95/46/EC të Parlamentit Evropian dhe Këshillit në lidhje me nivelin e mjaftueshëm të mbrojtjes që ofrojnë parimet e privatësisë "*safe harbour*" dhe "pikëpyetjeve më të shpeshta" në lidhje me to, të publikuara nga ana e Departamentit të Tregtisë së SHBA-ve, JO 2000 L 215.

- Interesat specifikë të subjektit të të dhënave; ose
- Interesat legjitimë prevalues të të tjerëve, veçanërisht interesat e rëndësishëm publikë.

Sipas së drejtës së BE-së, neni 26 (1) i Direktivës së Mbrojtjes së të Dhënave përmban dispozita të cilat janë të ngjashme me ato të Protokollit Shtesë të Konventës 108.

Sipas Direktivës, interesat e subjektit të të dhënave mund të justifikojnë qarkullimin e lirë të të dhënave drejt një vendi të tretë nëse:

- Subjekti i të dhënave ka dhënë pëlqimin e tij të qartë për eksportimin e të dhënave; ose
- Subjekti i të dhënave hyn – ose përgatitet të hyjë – në një marrëdhënie kontraktuese e cila përcakton në mënyrë të qartë se të dhënat do të transferohen tek një marrës jashtë vendit; ose
- Është lidhur një marrëveshje midis kontrolluesit të të dhënave dhe një pale të tretë, për interesat e subjektit të të dhënave; ose
- Transferimi është i domosdoshëm për mbrojtjen e interesave jetikë të subjektit të të dhënave.
- Për transferimin e të dhënave nga regjistrat publikë; ky është një shembull i interesave prevalues të publikut të gjerë, që të ketë mundësi aksesi në informacionet që mbahen në regjistrat publikë.

Interesat legjitimë të të tjerëve, mund të justifikojnë qarkullimin e lirë ndërkufitar të të dhënave:[228]

- Për shkak të një interesi të rëndësishëm publik, të ndryshëm nga ai për sigurinë kombëtare apo publike, meqenëse ato nuk mbulohen nga Direktiva e Mbrojtjes së të Dhënave; ose
- Për të konstatuar, ushtruar apo mbrojtur një të drejtë në rrugë gjyqësore.

Rastet e sipërpërmendura duhet të kuptohen si përjashtime nga rregulli sipas së cilit transferimi i lirë i të dhënave drejt vendeve të tjera, nevojit nivel të mjaftueshëm të mbrojtjes së të dhënave në vendin marrës. Përjashtimet duhet të interpretohen në mënyrë shteruese. Kjo është theksuar në mënyrë të përsëritur nga Grupi i Punës së Nenit 29 në kontekstin e nenit 26 (1) të Direktivës së Mbrojtjes së të Dhënave, veçanërisht nëse pëlqimi paraqitet si baza e transferimit të të dhënave.[229] Grupi i Punës së Nenit 29 ka dalë në përfundimin se rregullat e përgjithshme në lidhje me kuptimin ligjor të pëlqimit, gjenin gjithashtu zbatim për nenin 26 (1) të Direktivës. Nëse për shembull në kontekstin e marrëdhënieve të punës, nuk mund të thuhet me siguri se pëlqimi i dhënë nga punëmarrësi ka qenë pëlqim vërtet i lirë, atëherë transferimet e të dhënave nuk mund të mbështeten në nenin 26 (1) (a) të Direktivës. Në raste të tilla, gjen zbatim neni 26 (2), i cili u kërkon autoriteteve kombëtare të mbrojtjes së të dhënave që të japin autorizim për transferimet e të dhënave.

[228] Direktiva e Mbrojtjes së të Dhënave, neni 26 (1) (d).
[229] Shih veçanërisht Grupi i Punës së Nenit 29 (2005), *Dokument pune në lidhje me interpretimin uniform të nenit 26 (1) të Direktivës 95/46/EC, datë 24 tetor 1995,* WP 114, Bruksel, 25 nëntor 2005.

6.4. Qarkullimet e kufizuara të të dhënave drejt vendeve të treta

Pikat kryesore

- Përpara se të eksportohen të dhëna drejt vendeve të treta, të cilat nuk kanë nivel të mjaftueshëm të mbrojtjes së të dhënave, kontrolluesi mund të jetë i detyruar t'ia paraqesë për shqyrtim qarkullimin e parashikuar të të dhënave autoritetit mbikëqyrës.
- Kontrolluesi i cili dëshiron të eksportojë të dhëna, duhet të demonstrojë dy elemente gjatë procedurës së shqyrtimit:
  - Ekzistencën e një baze ligjore për transferimin e të dhënave drejt marrësit; dhe
  - Ekzistencën e masave që garantojnë mbrojtje të mjaftueshme të të dhënave në territorin e marrësit.
- Masat që përcaktojnë nivelin e mjaftueshëm të mbrojtjes së të dhënave të marrësit mund të përfshijnë:
  - Klauzolat kontraktuese midis kontrolluesit i cili eksporton të dhënat dhe marrësit të huaj të të dhënave; ose
  - Rregullat e detyrueshme të korporatave, që zbatohen përgjithësisht për transferimet e të dhënave brenda një grupi shoqërish shumëkombëshe.
- Transferimet e të dhënave drejt autoriteteve të huaja mund të rregullohen gjithashtu me anë të një marrëveshje speciale ndërkombëtare.

Direktiva e Mbrojtjes së të Dhënave dhe Protokolli Shtesë i Konventës 108 i lejojnë legjislacionit kombëtar të përcaktojë regjime për qarkullimet ndërkufitare të të dhënave drejt shteteve të treta, të cilat nuk kanë nivel të mjaftueshëm të mbrojtjes së të dhënave, nëse kontrolluesi ka lidhur marrëveshje speciale për të siguruar garanci të mjaftueshme të mbrojtjes së të dhënave në territorin e marrësit dhe nëse kontrolluesi mund t'i paraqesë provat në lidhje me të pranë autoritetit kompetent. Kjo normë përmendet në mënyrë eksplicite vetëm në Protokollin Shtesë të Konventës 108; gjithsesi, ajo konsiderohet gjithashtu procedurë standarde sipas Direktivës së Mbrojtjes së të Dhënave.

6.4.1. Klauzolat kontraktuese

Si **e drejta e KiE-së** ashtu edhe **e drejta e BE-së**, i përmendin klauzolat kontraktuese midis kontrolluesit që eksporton të dhënat dhe marrësit në një vend të tretë, si një mjet i mundshëm për të garantuar nivel të mjaftueshëm të mbrojtjes së të dhënave në vendin e marrësit.

Në **nivel BE-je**, Komisioni Evropian me mbështetjen e Grupit të Punës së Nenit 29 hartoi klauzola kontraktuese standarde, të cilat u certifikuan zyrtarisht nëpërmjet një Vendimi të Komisionit, si provë për mbrojtje të mjaftueshme të dhënash.[230] Meqenëse vendimet e Komisionit janë detyruese për të gjitha Shtetet Anëtare, autoritetet kombëtare përgjegjëse për monitorimin e qarkullimeve ndërkufitare të të dhënave duhet t'i njohin këto klauzola kontraktuese standarde në procedurat e tyre.[231] Kështu, nëse kontrolluesi i cili eksporton të dhëna dhe marrësi nga një vend i tretë bien dakord dhe nënshkruajnë këto klauzola, ky fakt duhet të jetë provë e mjaftueshme për autoritetin mbikëqyrës mbi ekzistencën e garancive të mjaftueshme.

[230] Direktiva e Mbrojtjes së të Dhënave, neni 26 (4).
[231] TFBE, neni 288.

Ekzistenca e klauzolave kontraktuese standarde në kuadrin ligjor të BE-së nuk i ndalon kontrolluesit që të formulojnë të tjera klauzola kontraktuese *ad hoc*. Gjithsesi, atyre u duhet të sigurojnë të njëjtin nivel mbrojtjeje, sikurse klauzolat kontraktuese standarde. Karakteristikat më të rëndësishme të klauzolave kontraktuese standarde janë:

- Një klauzolë e palës së 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 të jetë subjekt i procedurave të autoritetit mbikëqyrës kombëtar dhe/ose gjykatave në raste mosmarrëveshjesh, të kontrolluesit eksportues të të dhënave.

Aktualisht, një kontrolluesi i cili parashikon të transferojë të dhëna personale drejt një kontrolluesi tjetër, mund të përzgjedhë midis dy grupeve të klauzolave kontraktuese.[232] Për transferimet nga kontrolluesi drejt përpunuesit ekziston vetëm një grup klauzolash kontraktuese standarde.[233]

Sa i përket **së drejtës së KiE-së**, Komiteti Konsultativ i Konventës 108 ka përgatitur një udhëzues për hartimin e klauzolave kontraktuese.[234]

6.4.2. Rregullat e Detyrueshme të Korporatave

Shumë shpesh, rregullat shumëpalëshe të detyrueshme të korporatave (BCR-të) përfshijnë njëkohësisht disa autoritete evropiane të mbrojtjes së të dhënave.[235] Në mënyrë që BCR-të të miratohen, drafti i tyre i duhet dërguar autoritetit drejtues, së bashku me formularët e standardizuar të aplikimit.[236] Autoriteti drejtues identifikohet në formularin e standardizuar të aplikimit. Ky autoritet informon më pas të gjithë autoritetet mbikëqyrëse të vendeve anëtare të EEA-së, në të cilat janë vendosur filialet e grupit, edhe pse pjesëmarrja e tyre në procesin e shqyrtimit të BCR-ve është vullnetare. Megjithëse nuk është e detyrueshme, të gjitha autoritetet e mbrojtjes së të dhënave të përfshira, duhet ta përfshijnë rezultatin e shqyrtimit në procedurat e tyre zyrtare të autorizimit.

---

[232] Grupi I përfshihet në Aneksin e Vendimit të Komisionit 2001/497/EC, Komisioni Evropian (2001), i datës 15 qershor 2001 mbi klauzolat kontraktuese standarde për transferimin e të dhënave personale drejt vendeve të treta, sipas Direktivës 95/46/EC. JO 2001 L 181; Grupi II përfshihet në Aneksin e Vendimit të Komisionit 2004/915/EC, Komisioni Evropian (2004), i datës 27 dhjetor 2004 që ndryshon Vendimin 2001/497/EC për sa i takon miratimit të një grupi alternativ klauzolash kontraktuese standarde për transferimin e të dhënave personale drejt vendeve të treta, JO 2004 L 385.

[233] Komisioni Evropian (2010), Vendimi i Komisionit 2010/87, i datës 5 shkurt 2010 në lidhje me klauzolat kontraktuese standarde për transferimin e të dhënave personale drejt përpunuesve të vendosur në vende të treta, sipas Direktivës 95/46/EC të Parlamentit Evropian dhe Këshillit, JO 2010 L 39.

[234] KiE, Komiteti Konsultativ i Konventës 108 (2002), *Udhëzues për hartimin e klauzolave kontraktuese për që rregullojnë mbrojtjen e të dhënave gjatë transferimit të të dhënave personale drejt palëve të treta, të cilat nuk kanë nivel të mjaftueshëm të mbrojtjes së të dhënave.*

[235] Përmbajtja dhe struktura e rregullave të përshtatshme të detyrueshme të korporatave shpjegohen në *Dokumentin e punës që përcakton një kuadër ligjor strukturën e Rregullave të Detyrueshme të Korporatave* të Grupit të Punës së Nenit 29 (2008), WP 154, Bruksel, 24 qershor 2008, dhe në *Dokumentin e punës që përcakton tabelën e elementeve dhe parimeve të Rregullave të Detyrueshme të Korporatave* të Grupit të Punës së Nenit 29 (2008), WP 153, Bruksel, 24 qershor 2008.

[236] Grupi i Punës së Nenit 29 (2007), *Rekomandimi 1/2007 në lidhje me standardet e aplikimit për miratimin e rregullave të detyrueshme të korporatave për transferimin e të dhënave personale,* WP 133, Bruksel, 10 janar 2007.

6.4.3. Marrëveshjet ndërkombëtare speciale

BE-ja ka lidhur marrëveshje speciale për dy lloje transferimesh të të dhënave:

Të Dhënat e Pasagjerëve

Të Dhënat e Pasagjerëve (PNR) mblidhen nga shoqëritë e fluturimit gjatë procesit të rezervimit dhe përfshijnë emrat, adresat, të dhënat e kartës së kreditit dhe numrat e ndenjëseve të pasagjerëve. Sipas legjislacionit të Shteteve të Bashkuara, shoqëritë e fluturimit janë të detyruara t'ia vënë në dispozicion këto të dhëna Departamentit të Sigurisë Kombëtare përpara nisjes së pasagjerëve, qoftë kur ikin apo kur mbërrijnë në SHBA.

Për të siguruar mbrojtje të mjaftueshme të të dhënave të PNR-ve, në përputhje me dispozitat e Direktivës 95/46/EC, u miratua në 2004-ën një "paketë e PNR-ve",[237] e cila parashikonte nivel të mjaftueshëm të mbrojtjes së përpunimit të të dhënave që kryhet nga Departamenti i Sigurisë Kombëtare të SHBA-ve (U.S Department of Homeland Security DHS).

Pas anulimit nga ana e GjDBE-së së paketës së PNR-ve,[238] BE-ja dhe Shtetet e Bashkuara nënshkruan dy marrëveshje të veçanta, të cilat kishin si objekti së pari të ofronin një kuadër ligjor për transferimin e të dhënave të PNR-ve drejt autoriteteve të SHBA-ve dhe së dyti, të siguronin mbrojtje të mjaftueshme të të dhënave në vendin marrës.

Marrëveshja e parë mbi mënyrën se si vendet e BE-së dhe Shtetet e Bashkuara shkëmbejnë e menaxhojnë të dhënat, e nënshkruar në 2012-ën, kishte disa të meta dhe u zëvendësua po atë vit me një tjetër marrëveshje, për të garantuar më shumë siguri ligjore.[239] Marrëveshja e re ofron përmirësime të rëndësishme. Ajo kufizon dhe qartëson qëllimet për të cilat mund të përdoret informacioni, sikurse të krimeve të rënda trans-nacionale dhe terrorizmit dhe përcakton afatin kohor për mbajtjen e të dhënave: pas gjashtë muajsh, të dhënat duhet të depersonalizohen dhe maskohen. Çdo personi që i keqpërdoren të dhënat, ka të drejtën e ankimit administrativ dhe gjyqësor në përputhje me legjislacionin e SHBA-ve. Çdo person ka gjithashtu të drejtën e aksesit në të dhënat PNR në lidhje me të dhe të kërkojë korrigjimin e tyre nga ana e Departamentit të Sigurisë Kombëtare të SHBA-ve, përfshirë edhe mundësinë e fshirjes, nëse informacioni është i pasaktë.

Marrëveshja e cila hyri në fuqi në datën 1 korrik 2012, do të mbetet në fuqi për shtatë vite, deri në vitin 2019.

---

[237] Vendimi i Këshillit 2004/496/EC i 17 majit 2004 mbi lidhjen e një Marrëveshjeje midis Komunitetit Evropian dhe Shteteve të Bashkuara të Amerikës, në lidhje me përpunimin dhe transferimin e të dhënave të PNR-ve nga Shoqëritë e Fluturimit drejt Departamentit të Sigurisë Kombëtare të Shteteve të Bashkuara, Byrosë së Doganave dhe Mbrojtjes së Kufirit, JO 2004 L 183, fq. 83 dhe Vendimi i Komisionit 2004/535/EC i 14 majit 2004 mbi mbrojtjen e mjaftueshme të të dhënave personale të Të Dhënave të Pasagjerëve që transferohen në Byronë e Doganave dhe Mbrojtjes të Kufirit të Shteteve të Bashkuara, JO 2004 L 235, fp. 11-22.

[238] GjDBE, Çështje të bashkuara C-317/04 dhe C-318/04, *Parlamenti Evropian kundër Këshillit të Bashkimit Evropian*, 30 maj 2006, parag. 57, 58 dhe 59, ku Gjykata vendosi se si vendimi për nivelin e mjaftueshëm të mbrojtjes së të dhënave ashtu edhe marrëveshja në lidhje me përpunimin e të dhënave, janë jashtë objektit të Direktivës.

[239] Vendimi 2012/472/UE i Këshillit i 26 prillit 2012 mbi lidhjen e Marrëveshjes midis Shteteve të Bashkuara të Amerikës dhe Bashkimit Evropian për përdorimin dhe transferimin e të dhënave të pasagjerëve tek Departamenti i Sigurisë Kombëtare të Shteteve të Bashkuara, JO 2012 L215/4/ Teksti i Marrëveshjes gjendet bashkëlidhur me Vendimin, JO 2012 L 215, fq. 5-14.

Në dhjetor të 2011-ës, Këshilli i Bashkimit Evropian miratoi lidhjen e Marrëveshje të përditësuar midis BE-së dhe Australisë, në lidhje me përpunimin dhe transferimin e të dhënave të PNR-ve.[240] Marrëveshja midis BE-së dhe Australisë në lidhje me të dhënat e PNR-ve është një hap përpara në agjendën e BE-së, e cila parashikon një qasje gjithëpërfshirëse në lidhje me PNR-të,[241] ngritjen e një sistemi PNR të BE-së[242] dhe negocimin e marrëveshjeve me vendet e treta.[243]

Të dhënat e komunikimeve financiare

Shoqata Botërore e Telekomunikimit Financiar Ndër-bankar (SWIFT) me seli në Belgjikë, e cila përpunon pjesën më të madhe të transfertave globale të parave nga bankat evropiane, operonte me një qendër binjake të vendosur në SHBA. Kjo e fundit mori një kërkesë për komunikim të dhënash nga ana e Departamentit të Thesarit të SHBA-ve për qëllime të hetimit të terrorizmit.[244]

Nga këndvështrimi i BE-së, nuk ekzistonte baza e nevojshme ligjore për komunikimin e këtyre të dhënave evropiane të rëndësishme, të cilat ishin të aksesueshme në Shtetet e Bashkuara vetëm për shkak se qendrat e shërbimit të përpunimit të të dhënave të SWIFT-it ishin të vendosura atje.

Një marrëveshje speciale midis BE-së dhe Shteteve të Bashkuar, që njihet si "Marrëveshja SWIFT", u nënshkrua në 2010-ën, me qëllim që të sigurohej kuadri i nevojshëm ligjor dhe të garantohej mbrojtja e të dhënave.[245]

---

[240] Vendim i Këshillit 2012/381/EU i 13 dhjetorit 2011 mbi lidhjen e Marrëveshjes midis Bashkimit Evropian dhe Australisë në lidhje me përpunimin dhe transferimin e Të Dhënave të Pasagjerëve (PNR) nga shoqëritë fluturimit drejt Shërbimit Doganor dhe të Mbrojtjes së Kufijve të Australisë, JO 2012 L 186/3. Teksti i Marrëveshjes, i cili zëvendëson një marrëveshje të mëparshme të 2008-ës, gjendet bashkëlidhur me Vendimin, JO 2012 L 186, fq. 4-16.

[241] Shih veçanërisht Komunikatën e Komisionit datë 21 shtator 2010 mbi qasjen gjithëpërfshirëse për transferimet e Të Dhënave të Pasagjerëve (PNR) drejt vendeve të treta, COM(2010) 492 përfundimtar, Bruksel, 21 shtator 2010. Shih gjithashtu Grupi i Punës së Nenit 29 (2010), *Opinioni 7/2010 në lidhje me Komunikatën e Komisionit Evropian mbi qasjen gjithëpërfshirëse për transferimet e Të Dhënave të Pasagjerëve (PNR) drejt vendeve të treta*, WP 178, Bruksel, 12 nëntor 2010.

[242] Propozim për një Direktivë të Parlamentit Evropian dhe Këshillit në lidhje me përdorimin e të dhënave të PNR-ve për qëllime të parandalimit, zbulimit, hetimit dhe gjykimit penal të krimeve të rënda dhe terrorizmit, COM(2011) 32 përfundimtar, Bruksel, 2 shkurt 2011. Në prill të 2011-ës, Parlamenti Evropian i kërkoi FRA-së të jepte opinion në lidhje me këtë Propozim dhe përputhshmërinë e tij me Kartën e të Drejtave Themelore të Bashkimi Evropian. Shih: FRA (2011), *Opinion 1/2011 – Të dhënat e Pasagjerëve*, Vjenë, 14 qershor 2011.

[243] BE-ja po negocion një marrëveshje PNR me Kanadanë, e cila do të zëvendësojë marrëveshjen e 2006-ës e cila është ende në fuqi.

[244] Shih në këtë kontekst, Grupi i Punës së Nenit 29 (2011), *Opinioni 14/2011 mbi çështjet e mbrojtjes së të dhënave në lidhje me parandalimin e pastrimit të parave dhe financimit të terrorizmit*, WP186, Bruksel, 13 qershor 2011; 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; Komisioneri Belg për Mbrojtjen e Privatësisë (*Commission de la protection de la vie privée*) (2008), (*kontrolli dhe procedura e rekomandimit të iniciuar në lidhje me shoqërinë SWIFT scrl*", Vendim, 9 dhjetor 2008.

[245] Vendimi i Këshillit 2010/412/EU datë 13 korrik 2010 mbi lidhjen e Marrëveshjes midis Bashkimit Evropian dhe Shteteve të Bashkuara të Amerikës për përpunimin dhe transferimin e të Dhënave të Komunikimeve Financiare nga Bashkimi Evropian drejt Shteteve të Bashkuara, për qëllime të Programit të Survejimit të Financimit të Terrorizmit, JO 2010 L 195, fq. 3 dhe 4. Teksti i Marrëveshjes gjenden i bashkëlidhur me këtë Vendim, JO 2010 L 195, fq. 5-14.

Sipas kësaj marrëveshjeje, të dhënat financiare të ruajtura nga SWIFT-i vazhdojnë t'i vihen në dispozicion Departamentit të Thesarit të SHBA-ve, për qëllime të parandalimit, hetimit, zbulimit ose gjykimit penal të terrorizmit apo financimit të terrorizmit. Departamenti i Thesarit të SHBA-ve mund të kërkojë të dhëna financiare nga SWIFT-i me kusht që kërkesa:

- Të identifikojë sa më qartë të jetë e mundur të dhënat financiare;
- Të vërtetojë në mënyrë të qartë domosdoshmërinë e këtyre të dhënave;
- Të jetë përshtatur në mënyrën më restriktive të mundshme, me qëllim që të minimizohet sasia e të dhënave të kërkuara;
- Të mos synojë të marrë të dhëna në lidhje me Zonën e Unifikuar të Pagesave në Euro (SEPA).

Europol-i duhet të ketë një kopje për secilën kërkesë të Departamentit amerikan të Thesarit dhe të verifikojë nëse janë respektuar parimet e Marrëveshjes SWIFT.[246] Nëse po, SWIFT-i duhet t'ia vërë në dispozicion të dhënat financiare drejtpërdrejt Departamentit amerikan të Thesarit. Ky i fundit duhet t'i mbajë të dhënat financiare në një ambient fizik të sigurt, ku të aksesohen vetëm nga analistët, të cilët hetojnë terrorizmin apo financimin e tij dhe të dhënat financiare nuk duhet të ndërlidhen me asnjë bazë tjetër të dhënash. Në përgjithësi, të dhënat financiare të marra nga SWIFT-i duhet të fshihen, pas një periudhe maksimale prej pesë vitesh nga marrja e tyre. Të dhënat financiare të cilat janë të rëndësishme për hetime apo gjykime penale të veçanta, mund të mbahen për aq kohë sa të dhënat janë të nevojshme për këto hetime apo gjykime penale.

Departamenti amerikan i Thesarit mund të transferojë informacion nga të dhënat e marra prej SWIFT-it, tek autoritete të caktuara të zbatimit të ligjit, sigurisë publike ose kundër-terrorizmit, brenda apo jashtë Shteteve të Bashkuara, vetëm për qëllime të hetimit, zbulimit, parandalimit apo gjykimit penal të terrorizmit dhe financimit të tij. Nëse transferimi i mëtejshëm i të dhënave financiare përfshin një qytetar apo një person me banim në një Shtet Anëtar të BE-së, çdo shkëmbim të dhënash me autoritetet e një vendi të tretë, duhet të marrë pëlqimin paraprak nga autoritetet kompetente të Shtetit Anëtar përkatës. Përjashtim bëhet kur shkëmbimi i të dhënave është thelbësor për parandalimin e një kërcënimi të menjëhershëm dhe të rëndë ndaj sigurisë publike.

Kontrolluesit e pavarur, përfshirë edhe një person të ngarkuar nga Komisioni Evropian, monitorojnë respektimin e parimeve të Marrëveshjes SWIFT.

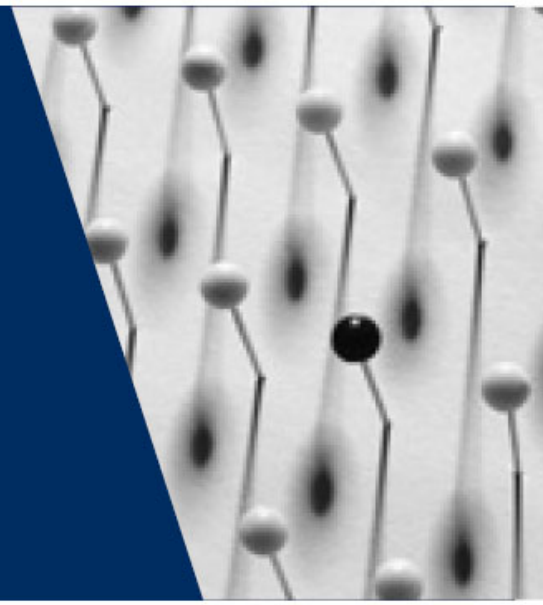
Subjektet e të dhënave kanë të drejtën të marrin konfirmim nga autoriteti kompetent i mbrojtjes së të dhënave të BE-së, se të drejtat e tyre për mbrojtje të të dhënave personale, janë respektuar. Subjektet e të dhënave kanë gjithashtu të drejtën e korrigjimit, fshirjes apo bllokimit të të dhënave të tyre, të mbledhura dhe të ruajtura nga Departamenti amerikan i Thesarit bazuar në marrëveshjen SWIFT. Gjithsesi, të drejtat e subjekteve të të dhënave për akses, mund të pësojnë disa kufizime ligjore. Kur aksesi refuzohet, subjektet e të dhënave duhet të informohen me shkrim për refuzimin si dhe në lidhje me të drejtën e tyre për ankim administrativ apo gjyqësor në Shtetet e Bashkuara.

Marrëveshja SWIFT është e vlefshme për pesë vite, deri në gusht të 2015-ës. Ajo zgjatet automatikisht për periudhat pasuese me një vit, përveçse kur një nga palët njofton tjetrën të paktën gjashtë muaj përpara, në lidhje me qëllimin e saj për të mos e zgjatur marrëveshjen.

[246] Organi i Përbashkët Mbikëqyrës i Europol-it ka kryer auditime në lidhje me aktivitetet e Europol-it në këtë fushë, rezultatet e së cilave gjenden në adresën: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

7

Mbrojtja e të dhënave në kontekstin e policisë dhe drejtësisë penale



BE	Çështje të trajtuara	KiE
	Në përgjithësi	**Konventa 108**
	Policia	Rekomandimi për Policinë
		GjEDNj, *B.B. kundër Francës*, nr. 5335/06, 17 dhjetor 2009 GjEDNj, *S. dhe Marper kundër Mbretërisë së Bashkuar*, nr. 30562/04 dhe 30566/04, 4 dhjetor 2008 GjEDNj, *Vetter kundër Francës*, nr. 59842/00, 31 maj 2005
	Krimi kibernetik	Konventa e Krimit Kibernetik
Mbrojtja e të dhënave në kontekstin e bashkëpunimit ndërkufitar të autoriteteve policore dhe gjyqësore		
Vendimi Kuadër për Mbrojtjen e të Dhënave	**Në përgjithësi**	Konventa 108 Rekomandimi për Policinë
Vendimi Prüm	**Për të dhëna të veçanta: gjurmë gishtash, ADN, vandalizëm etj.**	Konventa 108 Rekomandimi për Policinë
Vendimi mbi Europol-in Vendimi mbi Eurojust-in Rregullorja e Frontex-it	**Nga agjencitë speciale**	Konventa 108 Rekomandimi për Policinë
Vendimi mbi Schengen II Rregullorja e VIS-it	**Nga sisteme të përbashkëta speciale të informacionit**	Konventa 108 Rekomandimi për Policinë
Rregullorja e Eurodac-ut Vendimi mbi CIS-in		GjEDNj, *Dalea kundër Francës, nr. 964/07*, 2 shkurt 2010

KiE-ja dhe BE-ja kanë miratuar instrumente ligjore specifike, me qëllim që të ekuilibrohen interesat e individit për mbrojtje të të dhënave dhe interesat e shoqërisë për mbledhjen e të dhënave, për të luftuar krimin dhe për të garantuar siguri kombëtare dhe publike.

7.1. E drejta e KiE-së në lidhje me mbrojtjen e të dhënave në fushën e policisë dhe drejtësisë penale

Pikat kryesore

- Konventa 108 dhe Rekomandimi për Policinë i KiE-së përfshin mbrojtjen e të dhënave në të gjitha fushat e punës së policisë.
- Konventa mbi Krimin Kibernetik (*Konventa e Budapestit)* është një instrument ligjor ndërkombëtar i detyrueshëm, i cili trajton krimet e kryera ndaj dhe me anët të rrjeteve elektronike

Në nivel evropian, Konventa 108 përfshin të gjitha fushat e përpunimit të të dhënave personale dhe dispozitat e saj synojnë të rregullojnë përpunimin e të dhënave personale në përgjithësi. Për rrjedhojë, Konventa 108 zbatohet për mbrojtjen e të dhënave në fushën e policisë dhe drejtësisë penale, megjithëse Palët Kontraktuese mund të kufizojnë zbatimin e saj.

Detyrat ligjore të autoriteteve të policisë dhe drejtësisë penale kërkojnë shpesh përpunime të të dhënave personale, të cilat mund të kenë pasoja të rënda për individët e përfshirë. Rekomandimi për të Dhënat e Policisë miratuar nga KiE-ja në 1987-ën, udhëzon Palët Kontraktuese mbi mënyrën se si të zbatojnë parimet e Konventës 108, në kontekstin e përpunimit të të dhënave personale nga autoritetet policore.[247]

7.1.1. Rekomandimi për policinë

Sipas jurisprudencës së qëndrueshme të GjEDNj-së, regjistrimi dhe ruajtja e të dhënave personale nga autoritetet e policisë apo sigurisë kombëtare, përbën ndërhyrje në nenin 8 (1) të KEDNj-së. Shumë vendime të GjEDNj-së kanë të bëjnë me justifikimin e këtyre ndërhyrjeve.[248]

Shembull: tek çështja *B.B. kundër Francës,*[249] GjEDNj-ja vendosi se përfshirja e të dhënave të një të dënuari për krim seksual në një bazë të dhënash gjyqësore kombëtare, përfshihej në qëllimin e nenit 8 të KEDNj-së. Gjithsesi, meqenëse ishin zbatuar masa të mjaftueshme për mbrojtjen e të dhënave personale, sikurse e drejta e subjektit të të dhënave për të kërkuar fshirjen e të dhënave, afati i kufizuar i mbajtjes së të dhënave dhe aksesi i kufizuar në këto të dhëna, ishte vendosur ekuilibër i drejtë midis interesave private dhe atyre publike. Gjykata vendosi se nuk kishte pasur shkelje të nenit 8 të KEDNj-së.

Shembull: tek çështja *S. dhe Marper kundër Mbretërisë së Bashkuar,*[250] të dy ankuesit ishin akuzuar, por jo dënuar, për vepra penale. Gjithsesi, gjurmët e gishtave, profilet e ADN-së dhe mostrat e tyre biologjike ishin regjistruar dhe mbaheshin nga policia.

[247] KiE, Komiteti i Ministrave (1987), Rekomandimi Rec(87) 15 për shtetet anëtare që rregullon përdorimin e të dhënave personale në sektorin e policisë, 17 shtator 1987.
[248] Shih, për shembull GjEDNj, *Leander kundër Suedisë,* nr. 9248/81, 26 mars 1987; GjEDNj, *M.M. kundër Mbretërisë së Bashkuar*, nr. 24029/07, 13 nëntor 2012; GjEDNj, *M.K. kundër Francës,* nr. 19522/09, 18 prill 2013.
[249] GjEDNj-, *B.B. kundër Francës,* nr. 5335/06, 17 dhjetor 2009.
[250] GjEDNj, *S. dhe Marper kundër Mbretërisë së Bashkuar*, nr. 30562/04 dhe 30566/04, 4 dhjetor 2008, parag. 119 dhe 125

Mbajtja e pakufizuar në kohë e të dhënave biometrike parashikohej nga ligji, në rastin kur një person ishte i dyshuar për një vepër penale, edhe nëse personi më vonë lirohej ose shpallej i pafajshëm. GjEDNj-ja vendosi se mbajtja në mënyrë të përgjithshme dhe pa dallim e të dhënave personale, pa afate kohore dhe kur individët e liruar kishin mundësi të kufizuar të kërkonin fshirjen e tyre, përbënte një cënim jo proporcional të të drejtës së ankuesit për respektim të jetës private. Gjykata doli në përfundimin se ishte shkelur neni 8 i KEDNj-së.

Shumë çështje të tjera të gjykuara nga KEDNj-ja kanë të bëjnë me justifikimin e ndërhyrjes së survejimit tek e drejta për mbrojtje të të dhënave.

Shembull: tek çështja *Allan kundër Mbretërisë së Bashkuar,*[251] bisedat private të një të burgosuri me një mikun e tij në ambientin e vizitave të burgut dhe me një shok qelie, ishin regjistruar në mënyrë të fshehtë nga autoritetet. Në qëndrimin e saj GjEDNj-ja u shpreh se përdorimi i pajisjeve regjistruese audio-video në qelinë e ankuesit, në ambientin e vizitave dhe për të dënuarin tjetër, përbënte ndërhyrje tek e drejta e ankuesit për jetë private. Meqenëse nuk atë kohë nuk ekzistonte asnjë kuadër ligjor për të rregulluar përdorimin e pajisjeve të fshehta të regjistrimit nga ana e policisë, ndërhyrja nuk ishte e parashikuar në ligj. GjEDNj-ja vendosi se kishte pasur shkelje të nenit 8 të KEDNj-së.

Shembull: tek çështja *Klass dhe të Tjerët kundër Gjermanisë,*[252] ankuesit pretendonin se disa akte ligjore gjermane, të cilat lejonin survejimin në mënyrë të fshehtë të postës, postës elektronike dhe telekomunikimeve, përbënin shkelje të nenit 8 të KEDNj-së, veçanërisht për shkak se personi i përfshirë nuk vihej në dijeni për masat e survejimit dhe në përfundim të këtyre masave, nuk mund t'i drejtohej gjykatës. GjEDNj-ja në qëndrimin e saj vuri në dukje se rreziku i survejimit përbënte domosdoshmërish cënim të lirisë së komunikimit, për përdoruesit e shërbimeve postare dhe të telekomunikacioneve. Nga ana tjetër, gjykata theksoi se ishin marrë masat e përshtatshme të sigurisë kundër abuzimeve. Ligjvënësi gjerman kishte pasur të drejtë në vlerësimin e këtyre masave, si të nevojshme në një shoqëri demokratike, në interes të sigurisë kombëtare dhe për ruajtjen e rendit dhe parandalimin e krimit. GjEDNj-ja vendosi se nuk kishte pasur shkelje të nenit 8 të KEDNj-së.

Meqenëse përpunimi i të dhënave nga ana e autoriteteve policore mund të ketë ndikim të rëndësishëm tek subjektet e përfshira, është tepër i nevojshëm përcaktimi i rregullave të hollësishme për mbrojtjen e të dhënave, për sa i takon mbajtjes së bazave të të dhënave në këtë fushë. Rekomandimi për Policinë i KiE-së synoi të zgjidhte këtë problematikë, duke ofruar udhëzim në lidhje me mënyrën se si të dhënat duhet të mblidhen për kryerjen e punës policore; si duhet të mbahen skedarët e të dhënave në këtë fushë, kush duhet të lejohet të ketë akses në këto skedarë, përfshirë edhe kushtet për transferimin e të dhënave drejt autoriteteve policore të huaja; në çfarë mënyre duhet të kenë mundësi subjektet e të dhënave të ushtrojnë të drejtat e tyre për mbrojtje të të dhënave dhe si duhet zhvilluar kontrolli nga ana e autoriteteve të pavarura. Merret në konsideratë gjithashtu edhe detyrimi për të garantuar siguri të mjaftueshme të të dhënave.

[251] GjEDNj, *Allan kundër Mbretërisë së Bashkuar*, nr. 48539/99, 5 nëntor 2002.
[252] GjEDNj, *Klass dhe të Tjerët kundër Gjermanisë*, nr. 5029/71, 6 shtator 1978.

Rekomandimi nuk parashikon mbledhje pa kufi dhe pa dallim të të dhënave nga ana e autoriteteve policore. Ai kufizon mbledhjen e të dhënave personale nga autoritetet policore tek ato të dhëna të cilat janë të nevojshme për parandalimin e një rreziku konkret apo për të luftuar një vepër penale të caktuar. Çdo mbledhje shtesë të dhënash duhet të mbështetet në legjislacionin specifik kombëtar. Përpunimi i të dhënave sensitive duhet të kufizohet vetëm në atë çka është absolutisht e domosdoshme në kuadër të një hetimit të veçantë.

Kur të dhënat mblidhen pa dijeninë e subjektit të të dhënave, ky i fundit duhet të informohet në lidhje me mbledhjen e të dhënave menjëherë, sapo që komunikimi i këtij informacioni nuk pengon më hetimet. Mbledhja e të dhënave me anë të survejimit teknik, ose me anë të mjeteve të tjera të automatizuara, duhet gjithashtu të mbështetet në dispozita ligjore specifike.

Shembull: tek çështja *Vetter kundër Francës,*[253] dëshmitarë anonimë kishin akuzuar ankuesin për vrasje. Meqenëse ankuesi shkonte rregullisht në banesën e një miku, policia kishte montuar pajisje dëgjimi në të, pa autorizimin e gjyqtarit hetues. Bazuar në bisedat e regjistruara, ankuesi ishte arrestuar dhe ndjekur penalisht me akuzën e vrasjes. Ai kërkoi që regjistrimet të shpalleshin si prova të pavlefshme, duke pretenduar në mënyrë të veçantë se nuk ishin kryer në mënyrë të ligjshme. Për GjEDNj-në, çështja qëndronte në faktin nëse pajisjet përgjuese ishin "në përputhje me ligjin". Vendosja e aparateve përgjuese në ambientet private ishte qartazi jashtë qëllimit të neneve nga 100-ta e në vijim, të Kodit të Procedurës Penale, meqenëse ato dispozita kishin të bënin me përgjimin e linjave telefonike. Neni 81 i Kodit nuk e shpreh qartësisht masën apo mënyrën e ushtrimit të kompetencës së autoriteteve, për autorizimin e kontrollit të bisedimeve private. Për rrjedhojë, ankuesi nuk kishte përfituar nivelin minimal të mbrojtjes, që u garantohet qytetarëve nga shteti i së drejtës në një shoqëri demokratike. Gjykata vendosi se kishte pasur shkelje të nenit 8 të KEDNj-së.

Rekomandimi del në përfundimin se kur regjistrohen të dhëna personale, duhet të bëhen dallime të qarta ndërmjet: të dhënave administrative dhe të dhënave të policisë; llojeve të ndryshme të subjekteve të të dhënave, sikurse të dyshuar, viktima dhe dëshmitarë; dhe të dhënave të konsideruara si të mbështetura në fakte, nga ato të mbështetura në dyshime apo supozime.

Të dhënat policore duhet të jenë të kufizuara rreptësisht, gjë që ka pasoja sa i takon komunikimit të të dhënave të policisë tek palët e treta: transferimi apo komunikimi i këtyre të dhënave brenda sektorit të policisë, duhet të varet nga ekzistenca e interesit 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. Transferimi apo komunikimi ndërkombëtar duhet të kufizohet vetëm tek ai i kryer drejt autoriteteve policore të huaja dhe të mbështetet në dispozita ligjore të veçanta, mundësisht në marrëveshje ndërkombëtare, përveçse kur është e nevojshme për parandalimin e një kërcënimi të rëndë dhe të menjëhershëm.

[253] GjEDNj, *Vetter kundër Francës*, nr. 59842/00, 31 maj 2005.

Përpunimi i të dhënave nga policia duhet të jetë subjekt monitorimi të pavarur, për të garantuar respektim të legjislacionit kombëtar në fushën e mbrojtjes së të dhënave. Subjektet e të dhënave duhet të gëzojnë të gjitha të drejtat për akses, të parashikuara në Konventën 108. Kur të drejtat për akses të subjekteve të të dhënave kufizohen në përputhje me nenin 9 të Konventës 108, për nevoja të hetimeve policore të efektshme, subjektet e të dhënave duhet të kenë të drejtën, parashikuar në legjislacionin kombëtar, të ankohen pranë autoritetit kombëtar mbikëqyrës të mbrojtjes së të dhënave ose pranë një organi tjetër të pavarur.

7.1.2. Konventa e Budapestit mbi Krimin Kibernetik

Duke qenë se aktivitetet kriminale po përdorin e prekin gjithnjë e më tepër sistemet elektronike të përpunimit të të dhënave, nevojiten dispozita ligjore penale të reja, për t'u përballur më këtë sfidë. Për rrjedhojë, KiE-ja ka miratuar një instrument ligjor ndërkombëtar, Konventën e Krimit Kibernetik – e njohur gjithashtu si Konventa e Budapestit – për të trajtuar problematikën e krimeve që kryhen ndaj dhe me anë të rrjeteve elektronike.[254] Kjo konventë është e hapur për aderim edhe nga shtetet të cilat nuk janë anëtare të KiE-së dhe deri në gjysmën e 2013-ës, katër shtete jashtë KiE-së – Australia, Republika Dominikane, Japonia dhe Shtetet e Bashkuara - janë bërë palë të konventës dhe 12 shtete të tjera jo anëtare e kanë nënshkruar ose janë ftuar të aderojnë.

Konventa e Krimit Kibernetik mbetet traktati më i rëndësishëm ndërkombëtar, që trajton shkeljet e ligjit të kryera në internet ose rrjete të tjera informatike. Ajo i detyron palët të përditësojnë dhe harmonizojnë legjislacionet e tyre penale, kundër piraterisë dhe thyerjeve të tjera të sigurisë, përfshirë shkeljen e të drejtave të autorit, mashtrimin kompjuterik, pedo-pornografinë dhe aktivitete të tjera kibernetike të paligjshme. Konventa parashikon gjithashtu kompetenca procedurale, që përfshijnë kontrollin e rrjeteve kompjuterike dhe përgjimin e komunikimeve në kuadër të luftës kundër krimit kibernetik. Së fundi, ajo mundëson bashkëpunim ndërkombëtar të efektshëm. Protokolli shtesë i konventës trajton inkriminimin e propagandës me natyrë raciste dhe ksenofobe në rrjetet kompjuterike.

Meqenëse konventa nuk është në fakt një instrument për nxitjen e mbrojtjes së të dhënave, ajo i konsideron si kriminale aktivitetet të cilat kanë gjasa të shkelin të drejtën e subjektit për mbrojtjen e të dhënave të tij apo të saj. Konventa detyron gjithashtu Palët Kontraktuese që gjatë zbatimit të saj, të parashikojnë mbrojtje të mjaftueshme të së drejtave dhe lirive të njeriut, përfshirë edhe të drejtat e garantuara nga KEDNj-ja, sikundër të drejtën për mbrojtje të të dhënave.[255]

[254] Këshilli i Evropës, Komiteti i Ministrave (2001), Konventa e Krimit Kibernetik, CETS nr. 185, Budapest, 23 nëntor 2001, hyrë në fuqi në datë 1 korrik 2004.
[255] Po aty, neni 15 (1).

7.2. E drejta e BE-së në lidhje me mbrojtjen e të dhënave në fushën e policisë dhe drejtësisë penale

Pikat kryesore

- Në nivel BE-je, mbrojtja e të dhënave në sektorin e policisë dhe drejtësisë penale rregullohet vetëm në kontekstin e bashkëpunimit ndërkufitar të autoriteteve të policisë dhe drejtësisë.
- Ekzistojnë regjime specifike të mbrojtjes së të dhënave për Zyrën e Policisë Evropiane (Europol) dhe Njësinë e Bashkëpunimit Gjyqësor të BE-së (Eurojust), të cilat janë organe të BE-së të cilat asistojnë dhe përkrahin bashkëpunimin ndërkufitar për zbatimin e ligjit.
- Ekzistojnë po ashtu regjime specifike të mbrojtjes së të dhënave për sistemet e përbashkëta të informacionit, të cilat funksionojnë në nivel BE-je, për shkëmbime ndërkufitare informacioni ndërmjet autoriteteve kompetente policore dhe gjyqësore. Shembuj të rëndësishëm janë Schengen II, Sistemi i Informacionit të Vizave (VIS) dhe Eurodac-u, i cili është një sistem i përqendruar i të dhënave të gjurmëve të gishtave të vendeve të treta, të cilët aplikojnë për azil në në Shtet Anëtar të BE-së.

Direktiva e Mbrojtjes së të Dhënave nuk gjen zbatim në fushën e policisë dhe drejtësisë penale. Paragrafi 7.2.1. përshkruan instrumentet ligjore më të rëndësishme në këtë fushë.

7.2.1. Vendimi Kuadër për Mbrojtjen e të Dhënave

Vendimi Kuadër i Këshillit 2008/977/JHA për mbrojtjen e të dhënave personale që përpunohen në kuadër të bashkëpunimit policor dhe gjyqësor për çështje penale (*Vendimi Kuadër për Mbrojtjen e të Dhënave*)[256] synon të garantojë mbrojtjen e të dhënave personale të personave fizikë, kur të dhënat e tyre personale përpunohen për qëllime të parandalimit, hetimit, zbulimit ose gjykimit të një vepre penale apo ekzekutimit të një vendimi penal. Autoritetet kompetente që punojnë në fushën e policisë dhe drejtësisë penale veprojnë për llogari të Shteteve Anëtare apo BE-së. Këto autoritete janë agjenci apo organe të BE-së, ashtu si edhe autoritete të Shteteve Anëtare.[257] Zbatueshmëria e vendimit kuadër kufizohet vetëm në garantimin e mbrojtjes së të dhënave, në bashkëpunimin ndërkufitar ndërmjet atyre autoriteteve dhe nuk shtrihet tek siguria kombëtare.

Vendimi Kuadër për Mbrojtjen e të Dhënave mbështetet në një pjesë të madhe të tij mbi parimet dhe përkufizimet e Konventës 108 dhe Direktivës së Mbrojtjes së të Dhënave.

Të dhënat duhet të përdoren vetëm nga një autoritet kompetent dhe vetëm për qëllimin për të cilin ato janë transmetuar apo vënë në dispozicion. Shteti Anëtar marrës duhet të respektojë çdo kufizim ndaj shkëmbimit të të dhënave përcaktuar në legjislacionin e Shtetit Anëtar. Përdorimi i të dhënave nga shteti marrës për një qëllim tjetër është gjithsesi i lejuar me disa kushte të caktuara. Regjistrimi dhe dokumentimi i transmetimeve është detyrë specifike e autoriteteve kompetente, me qëllim që të bëhet i mundur qartësimi i përgjegjësive në rastet e ankesave.

[256] Këshilli i Bashkimit Evropian (2008), Vendimi Kuadër i Këshillit 2008/977/JHA i datës 27 nëntor 2008 në lidhje me mbrojtjen e të dhënave personale të përpunuara në kuadër të bashkëpunimit policor dhe gjyqësor për çështje penale (Vendimi Kuadër për Mbrojtjen e të Dhënave), JO 2008 L 350.
[257] Po aty, neni 2 (h).

Transferimi i mëtejshëm i të dhënave drejt palëve të treta, të përftuara në sajë të bashkëpunimit ndërkufitar, nevojit pëlqimin e Shtetit Anëtar nga të i cili janë marrë të dhënat, megjithëse bëhen përjashtime në raste urgjente.

Autoritetet kompetente duhet të marrin masat e nevojshme të sigurisë, për të mbrojtur të dhënat personale ndaj çdo formë të paligjshme përpunimi.

Secili Shtet Anëtar duhet të garantojë që një apo më shumë autoritete kombëtare mbikëqyrëse të pavarura, të kenë përgjegjësinë për udhëzimin dhe monitorimin e zbatimit të dispozitave të miratuara në përputhje me Vendimin Kuadër për Mbrojtjen e të Dhënave. Gjithashtu ato duhet të trajtojnë ankesat e depozituara nga çdo person, që kanë të bëjnë me mbrojtjen e të drejtave dhe lirive të tij apo të saj, në lidhje me përpunimin e të dhënave personale nga autoritetet kompetente.
Subjekti i të dhënave ka të drejtë të informohet në lidhje me përpunimin e të dhënave personale të tij apo të saj dhe ka të drejtën e aksesit, korrigjimit, fshirjes apo bllokimit. Kur ushtrimi i këtyre të drejtave refuzohet për arsye bindëse, subjekti i të dhënave duhet të ketë të drejtën të ankohet pranë autoritetit kompetent mbikëqyrës të vendit të tij dhe/ose në një gjykatë. Nëse një person pëson dëmtim për shkak të shkeljeve të legjislacionit kombëtar i cili zbaton Vendimin Kuadër për Mbrojtjen e të Dhënave, ky person gëzon të drejtën e kompensimit nga ana e kontrolluesit.[258] Përgjithësisht, subjektet e të dhënave duhet të kenë akses në një procedim gjyqësor, për çdo shkelje të të drejtave të tyre, të cilat garantohen nga legjislacioni kombëtar i cili zbaton Vendimin Kuadër për Mbrojtjen e të Dhënave.[259]

Komisioni Evropian propozoi një reformë, e cila konsiston në një Rregullore të Përgjithshme të Mbrojtjes së të Dhënave[260] dhe në një Direktivë të Përgjithshme të Mbrojtjes së të Dhënave.[261] Kjo Direktivë e re do të zëvendësojë Vendimin aktual Kuadër për Mbrojtjen e të Dhënave dhe do të aplikojë parimet dhe rregullat e përgjithshme për bashkëpunimin policor dhe gjyqësor për çështjet penale.

7.2.2. Instrumente ligjore më specifike në fushën e mbrojtjes së të dhënave në kuadër të bashkëpunimit ndërkufitar të policisë dhe autoriteteve ligj-zbatuese

Përveç Vendimit Kuadër për Mbrojtjen e të Dhënave, shkëmbimi i informacionit që mbahet nga Shtetet Anëtare në fusha të caktuara, rregullohet edhe me anë të disa instrumenteve ligjore, sikurse Vendimi Kuadër i Këshillit 2009/315/JHA mbi organizimin dhe përmbajtjen e shkëmbimit të informacionit të nxjerrë nga dosjet penale ndërmjet Shteteve Anëtare dhe Vendimi i Këshillit në lidhje me modalitetet e bashkëpunimit ndërmjet njësive informative financiare të Shteteve Anëtare për sa i takon shkëmbimit të informacionit.[262]

[258] Po aty, neni 19.
[259] Po aty, neni 20.
[260] Komisioni Evropian (2012), *Propozim për një Rregullore të Parlamentit Evropian dhe Këshillit në lidhje me mbrojtjen e individëve nga përpunimi i të dhënave personale dhe mbi lëvizjen e lirë të këtyre të dhënave (Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave),* COM(2012) 11 përfundimtar, Bruksel, 25 janar 2012.
[261] Komisioni Evropian (2012), *propozim për një Direktivë të Parlamentit Evropian dhe Këshillit në lidhje me mbrojtjen e individëv nga përpunimi i të dhënave personale nga ana e autoriteteve kompetente për qëllime të parandalimit, hetimit, zbulimit dhe gjykimit të veprave penale ose ekzekutimin e dënimeve penale dhe mbi lëvizjen e lirë të këtyre të dhënave (Direktiva e Përgjithshme e Mbrojtjes së të Dhënave),* COM(2012) 10 përfundimtar, Bruksel, 25 janar 2012.
[262] Këshilli i Bashkimit Evropian (2009), Vendimi Kuadër i Këshillit 2009/315/JHA i datës 26 shkurt 2009 mbi organizimin dhe përmbajtjen e shkëmbimit të informacionit të nxjerrë nga dosjet penale ndërmjet Shteteve Anëtare, JO 2009 L 93; Këshilli i Bashkimit Evropian (2000), Vendimi i Këshillit 2000/642/JHA i 17 tetorit 2000 në lidhje me modalitetet e bashkëpunimit ndërmjet njësive informative financiare të Shteteve Anëtare për sa i takon shkëmbimit të informacionit, JO 2000 L 271.

Është e rëndësishme të nënvizohet se bashkëpunimi ndërkufitar[263] ndërmjet autoriteteve kompetente, përfshin gjithnjë e më tepër shkëmbim të dhënash në lidhje me emigracionin.

Kjo sferë e së drejtës nuk hyn në sektorin e policisë dhe drejtësisë penale, por është në shumë aspekte e rëndësishme për punën e organeve të policisë dhe të drejtësisë. E njëjta gjë vlen edhe për të dhënat në lidhje me mallrat e importuara apo eksportuara nga BE-ja. Heqja e kufijve të brendshëm të kontrollit në BE ka rritur rrezikun e mashtrimit, duke e bërë të nevojshëm intensifikimin e bashkëpunimit të Shteteve Anëtare, veçanërisht duke përmirësuar shkëmbimet ndërkufitare të informacioneve, për të zbuluar e ndjekur me më tepër efikasitet shkeljet e legjislacionit doganor kombëtar dhe të BE-së.

Vendimi Prüm

Shembull i rëndësishëm i bashkëpunimit ndërkufitar të institucionalizuar, me anë të shkëmbimit të të dhënave të ruajtura në nivel kombëtar, është Vendimi i Këshillit 2008/615/JHA mbi forcimin e bashkëpunimit ndërkufitar, veçanërisht në luftën kundër terrorizmit dhe kriminalitetit ndërkufitar *(Vendimi Prüm)*, i cili transpozoi Traktatin Prüm në ligj të BE-së në 2008-ën.[264] Traktati Prüm ishte një marrëveshje ndërkombëtare e bashkëpunimit policor, e nënshkruar në 2005-ën nga Austria, Belgjika, Franca, Gjermania, Luksemburgu, Vendet e Ulëta dhe Spanja.[265]

Qëllimi i Vendimit Prüm ishte të ndihmonte Shtetet Anëtare të përmirësojnë shkëmbimin e informacionit, për qëllime të parandalimit dhe luftës kundër krimit në tre fusha: terrorizmi, kriminaliteti ndërkufitar dhe emigracioni i paligjshëm. Për këtë qëllim, vendimi përcakton disa dispozita në lidhje me:

- Aksesin e automatizuar në profilet e ADN-së, të dhënave të gjurmëve të gishtave dhe në disa të dhëna kombëtare të regjistrimit të automjeteve;
- Transmetimin e të dhënave në lidhje me ngjarje të rënda, të dimensionit ndërkufitar;
- Transmetimin e informacionit me qëllim parandalimin e akteve terroriste;
- Masa të tjera për forcimin e bashkëpunimit policor ndërkufitar.

Bazat e të dhënave të vëna në dispozicion në kuadër të Vendimit Prüm, rregullohen tërësisht nga legjislacioni i brendshëm, por nga ana tjetër, shkëmbimi i të dhënave rregullohet nga Vendimi dhe së fundmi, nga Vendimi Kuadër për Mbrojtjen e të Dhënave. Organet kompetente për monitorimin e këtyre qarkullimeve të të dhënave janë autoritetet kombëtare mbikëqyrëse të mbrojtjes së të dhënave.

---

[263] Komisioni Evropian (2012), Komunikatë e Komisionit drejtuar Parlamentit Evropian dhe Këshillit – Përforcimi i bashkëpunimit në fushën e zbatimit të ligjit në BE: Modeli Evropian i Shkëmbimit të Informacionit (EIXM), COM(2012) 735 përfundimtar, 7 dhjetor 2012.

[264] Këshilli i Bashkimit Evropian (2008), Vendimi i Këshillit 2008/615/JHA, datë 23 qershor 2008 në lidhje me forcimin e bashkëpunimit ndërkufitar, veçanërisht për luftën kundër terrorizmit dhe kriminalitetit ndërkufitar, JO 2008 L 210.

[265] 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 në lidhje me forcimin e bashkëpunimit ndërkufitar, veçanërisht për luftën kundër terrorizmit, kriminalitetit ndërkufitar dhe emigracionit të paligjshëm, i disponueshëm tek: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

7.2.3. Mbrojtja e të Dhënave në Europol dhe Eurojust

Europol-i

Europol-i, agjencia policore e BE-së, e ka selinë në Hagë dhe ka Njësi Kombëtare Europol-i (ENU-të) në secilin Shtet Anëtar. Europol-i u themelua në 1998-ën; statusi ligjor i tij aktual si institucion i BE-së, mbështetet në Vendimin e Këshillit që themelon Zyrën Policore Evropiane (*Vendimi për Europol*-in).[266] Objektivi i Europol-it është të asistojë në parandalimin dhe hetimin e krimit të organizuar, terrorizmit dhe formave të tjera të krimeve të rënda, sikurse renditen në Shtojcën e Vendimit për Europol-in, të cilat cënojnë dy apo më shumë Shtete Anëtare.

Me qëllim që të përmbushë misionin e tij, Europol-i ka ngritur Sistemin e Informacionit të Europol-it, i cili vë në dispozicion të Shteteve Anëtare një bazë të dhënash, për shkëmbimin e të dhënave dhe informacioneve në lidhje me veprat penale, nëpërmjet ENU-ve të tyre. Sistemi i Informacionit të Europol-it mund të përdoret për të vënë në dispozicion të dhëna që kanë të bëjnë me: persona të cilët janë të dyshuar ose kanë qenë të dënuar për vepra penale, të cilët janë subjekt i kompetencave të Europol-it; ose persona ndaj të cilëve ekzistojnë prova të besueshme se do të kryejnë vepra të tilla penale. Europol-i dhe ENU-të mund të regjistrojnë të dhëna drejtpërdrejt në Sistemin e Informacionit të Europol-it dhe të marrin të dhëna prej tij. Vetëm pala e cila ka hedhur të dhëna në sistem, mund të modifikojë, korrigjojë apo t'i fshijë ato.

Kur është e nevojshme për ushtrimin e kompetencave të tij, Europol-i mund të mbajë, modifikojë apo përdorë të dhëna në lidhje me veprat penale në arkivat e punës, për qëllime analizimi. Këto arkiva janë në dispozicion për qëllime të mbledhjes, përpunimit apo përdorimit të të dhënave, me synimin për të mbështetur hetime penale konkrete, të cilat zhvillohen nga Europol-i së bashku me Shtetet Anëtare të BE-së.

Për t'iu përgjigjur zhvillimeve të reja, u themelua më 1 janar 2013 Qendra Evropiane e Luftës Kundër Krimit Kibernetik.[267] Qendra i shërben BE-së si një platformë informacioni në lidhje me krimin kibernetik, duke ndihmuar për reagim të shpejtë në rastet e krimeve në internet, duke zhvilluar dhe zgjeruar kapacitetet digjitale të kriminalistikës dhe duke reflektuar praktikat më të mira në fushën e hetimeve të veprave penale kibernetike. Qendra fokusohet në krimin kibernetik i cili:

- Kryhet nga grupe të organizuara, për të gjeneruar përfitime të mëdha të paligjshme, sikurse mashtrimi në internet;
- I shkakton viktimës dëmtim të rëndë, sikurse shfrytëzimi seksual i fëmijëve në internet;
- Cënon infrastrukturën e rëndësisë së veçantë dhe sistemet e informacionit të BE-së.

[266] Këshilli i Bashkimit Evropian (2009), Vendimi i Këshillit, datë 6 prill 2009 për themelimin e Zyrës Policore Evropiane, JO 2009 L 121 (Europol). Shih gjithashtu propozimin e Komisionit për një rregullore, e cila parashikon një kuadër ligjor për një Europol të ri, i cili pason dhe zëvendëson Europol-in e ngritur me Vendimin e Këshillit 2009/371/JHA, datë 6 prill 2009 që themelon Zyrën Policore Evropiane (Europol) dhe CEPOL-in, të themeluar me Vendimin e Këshillit 2005/681/JHA që themelon Akademinë Policore Evropiane (CEPOL), COM(2013) 173 përfundimtar.

[267] Shih gjithashtu EDPS (2012), *Opinion i Mbikëqyrësit të Mbrojtjes së të Dhënave në lidhje me Komunikatën e Komisionit Evropian drejtuar Këshillit dhe Parlamentit Evropian mbi themelimin e Qendrës Evropiane të Luftës Kundër Krimit Kibernetik*, Bruksel, 29 qershor 2012.

Sistemi i mbrojtjes së të dhënave që rregullon aktivitetet e Europol-it, është përmirësuar. Vendimi për Europol-in, parashikon në nenin 27 të tij, se gjejnë zbatim parimet e përcaktuara në Konventën 108 dhe në Rekomandimin e të Dhënave të Policisë, në lidhje me përpunimin automatik ose jo automatik të të dhënave. Transmetimi i të dhënave ndërmjet Europol-it dhe Shteteve Anëtare duhet të respektojë gjithashtu rregullat e përcaktuara në Vendimin Kuadër për Mbrojtjen e të Dhënave.

Për të garantuar respektimin e legjislacionit të fushës së mbrojtjes së të dhënave dhe sidomos që përpunimi i të dhënave personale të mos shkelë të drejtat e individëve, Organi i Përbashkët i Mbikëqyrjes së Europol-it (JSB) shqyrton dhe kontrollon aktivitetet e Europol-it.[268] Çdo individ ka të drejtën e aksesit tek të gjitha të dhënat personale në lidhje me të, të cilat mbahen nga Europol-i, përveç të drejtës për të kërkuar verifikimin e këtyre të dhënave personale, korrigjimin apo fshirjen e tyre. Në rast se një person është i pakënaqur me vendimin e Europol-it në lidhje me ushtrimin e këtyre të drejtave, ai apo ajo mund të ankohet në Komitetin e Apelit të JSB-së.

Në rast të një shkeljeje si rezultat i gabimeve ligjore apo të fakteve, i të dhënave që mbahen apo përpunohen nga Europol-i, pala e dëmtuar mund të ankohet vetëm në gjykatën kompetente të Shtetit Anëtar, në të cilin ka ndodhur shkelja.[269] Europol-i do të zhdëmtojë Shtetin Anëtar, nëse shkelja ka ardhur si rezultat i mosrespektimit të detyrimeve ligjore të Europol-it.

Eurojust-i

Eurojust-i, organi i BE-së i themeluar në 2012-ën, me seli në Hagë, mbështet bashkëpunimin gjyqësor për hetime dhe gjykime që kanë të bëjnë me krime të rënda, që prekin të paktën dy Shtete Anëtare.[270] Eurojust-i është kompetent për:

- Nxitjen dhe përmirësimin e koordinimit të hetimeve dhe ndjekjeve penale, ndërmjet autoriteteve kompetente të disa Shteteve Anëtare;
- Lehtësimin e ekzekutimit të kërkesave dhe vendimeve, në lidhje me bashkëpunimin gjyqësor.

Funksionet e Eurojust-it kryhen nga funksionarë kombëtarë. Secili Shtet Anëtar delegon një gjyqtar ose prokuror tek Eurojust-i, statusi i të cilit i nënshtrohet së drejtës kombëtare dhe i cili gëzon kompetencat e duhura për kryerjen e detyrave të nevojshme, për nxitjen dhe përmirësimin e bashkëpunimit gjyqësor. Gjithashtu, funksionarët kombëtarë veprojnë bashkërisht, në formën e një kolegji, për të ushtruar detyrat e veçanta të Eurojust-it.

[268] Vendimi për Europol-in, neni 34.
[269] Po aty, neni 52.
[270] Këshilli i Bashkimi Evropian (2002), Vendimi i Këshillit 2002/187/JHA, datë 28 shkurt 2002 që themelon Eurojust-in me qëllim përforcimin e luftës kundër krimeve të rënda, JO 2002 L 63; Këshilli i Bashkimit Evropian (2003), Vendimi i Këshillit 2003/659/JHA, datë 18 qershor 2003, që ndryshon Vendimin 2002/187/JHA që themelon Eurojust-in me qëllim përforcimin e luftës kundër krimeve të rënda, JO 2003 L 44; Këshilli i Bashkimit Evropian (2009), Vendimi i Këshillit 2009/426/JHA, datë 16 dhjetor 2008 në lidhje me përforcimin e Eurojust-it dhe që ndryshon Vendimin 2002/187/JHA që themelon Eurojust-in, me qëllim përforcimin e luftës kundër krimeve të rënda, JO 2009 L 138 (*Vendimet për Eurojust*-in).

Eurojust-i mund të përpunojë të dhëna personale për aq sa është e nevojshme për plotësimin e objektivave të tij. Gjithsesi, ky përpunim kufizohet vetëm në informacionin që ka të bëjë me persona të cilët janë të dyshuar se kanë kryer, ose kanë marrë pjesë, ose janë dënuar, për një vepër penale, e cila është subjekt i kompetencave të Eurojust-it. Eurojust-i mund të përpunojë gjithashtu disa lloj informacionesh, në lidhje me dëshmitarë ose viktima të veprave penale, të cilat janë subjekt i kompetencave të Eurojust-it.[271] Në raste të veçanta, Eurojust-i mund të përpunojë për një periudhë të kufizuar kohore, një sasi më të madhe të dhënash personale, që lidhen me rrethanat e një vepre penale, kur këto të dhëna janë urgjentisht të nevojshme për një hetim në kryerje e sipër. Në kuadër të kompetencave të 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 shkëmbejë gjithashtu të dhëna personale me vende dhe organizata të treta.

Për sa i përket mbrojtjes së të dhënave, Eurojust-i duhet të garantojë nivel mbrojtje të paktën të barasvlershëm me parimet e Konventës 108 të Këshillit të Evropës dhe ndryshimeve të mëvonshme të saj. Në rastet e shkëmbimeve të të dhënave, duhen respektuar rregulla dhe kufizime specifike, të cilat përcaktohen qoftë në marrëveshjet e bashkëpunimit,ashtu edhe në ato të punës, në përputhje me Vendimet e Këshillit për Eurojust-in dhe me Rregulloren e Mbrojtjes së të Dhënave të Eurojust-it.[272]

Një JSB e pavarur është ngritur pranë Eurojust-it, e cila ka për detyrë të kontrollojë përpunimin e të dhënave personale që zhvillon Eurojust-i. Individët mund të ankohen pranë kësaj JSB-je, nëse janë të pakënaqur me përgjigjen e Eurojust-it ndaj kërkesës së tyre për akses, korrigjim, bllokim apo fshirje të të dhënave personale. Në rast se Eurojust-i përpunon të dhëna personale në mënyrë të paligjshme, Eurojust-i është përgjegjës para legjislacionit kombëtar të Shtetit Anëtar tek i cili e ka selinë ai, në Vendet e Ulëta, për çdo shkelje ndaj subjektit të të dhënave.

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

Përveç shkëmbimit të të dhënave ndërmjet Shteteve Anëtare dhe krijimit të autoriteteve të specializuara të BE-së, për të luftuar kriminalitetin ndërkufitar, janë ngritur disa sistemeve të përbashkëta informacioni, për të shërbyer si platformë për shkëmbim të dhënash ndërmjet autoriteteve kombëtare dhe të BE-së, për qëllime specifike të zbatimit të ligjit, përfshirë legjislacionin për emigracionin dhe doganat. Disa nga këto sisteme janë krijuar nga marrëveshjet shumëpalëshe, të cilat më pas janë plotësuar nga akte dhe sisteme ligjore të BE-së, sikurse Sistemi i Informacionit Schengen, Sistemi i Informacionit të Vizave, Eurodac-u, Eurosur-i apo Sistemi Doganor i Informacionit.

[271] Varianti i konsoliduar i Vendimit të Këshillit 2002/187/JHA i ndryshuar me Vendimin e Këshillit 2003/659/JHA dhe me Vendimin e Këshillit 2009/426/JHA, neni 15 (2).
[272] Rregullore e Procedurave të Përpunimit dhe Mbrojtjes së të Dhënave Personale nga Eurojust-i, JO 2005 C 68/01, 19 mars 2005, fq. 1.

Agjencia Evropiane për Menaxhimin e Sistemeve IT në Shkallë të Gjerë (eu-LISA),[273] krijuar në 2012-ën, është përgjegjëse për menaxhimin operacional afatgjatë të Sistemit të Informacionit Schnegen të gjeneratës së dytë (SIS II), Sistemin e Informacionit të Vizave dhe Eurodac-un. Detyrat thelbësore të eu-LISA-s janë shfrytëzimi i efektshëm, i sigurt dhe i vazhdueshëm i 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 Schengen

Në vitin 1985, disa Shtete Anëtare dhe ish Komuniteti Evropian, nënshkruan një Marrëveshje midis shteteve të Bashkimit Ekonomik të Beneluksit, Gjermanisë dhe Francës, për eliminimin e përshkallëzuar të kontrolleve në kufijtë e tyre të përbashkët (Marrëveshja Schengen), me synimin për të krijuar një zonë të lëvizjes së lirë të personave, pa u penguar nga kontrollet kufitare brenda territorit të Schengen-it.[274] Me qëllim që të kundërpeshohej kërcënimi ndaj sigurisë publike, që mund të shfaqet për shkak të kufijve të hapur, u vendosën kontrolle të përforcuara në kufijtë e jashtëm të zonës së Schengen-it, ashtu si edhe bashkëpunim i ngushtë midis autoriteteve kombëtare të policisë dhe drejtësisë.

Si pasojë e aderimit të shteteve të tjera në Marrëveshjen e Schengen-it, sistemi Schengen u integrua përfundimisht në kuadrin ligjor të BE-së me anë të Traktatit të Amsterdamit.[275] Zbatimi i këtij vendimi nisi në 1999-ën. Varianti më i ri i Sistemit të Informacionit Schengen, i ashtuquajturi SIS II, nisi funksionimin e tij më 9 prill 2013. Ai i shërben tashmë të gjitha Shteteve Anëtare të BE-së si edhe Islandës, Lihtenshtejnit, Norvegjisë dhe Zvicrës.[276] Edhe Europol-i, edhe Eurojust-i kanë akses në 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 lloje të dhënash të regjistruara nga Shtetet Anëtare në lidhje me persona dhe objekte. C-SIS-i përdoret nga autoritetet kombëtare të kontrollit kufitar, policisë, doganave, drejtësisë anembanë Zonës Schengen. Secili Shtet Anëtar shfrytëzon një kopje kombëtare të C-SIS-it, e cila njihet si Sistemi Kombëtar i Informacionit Schengen (N-SIS), i cili përditësohen në mënyrë konstante, duke përditësuar rrjedhimisht C-SIS-in. N-SIS-kontrollohet dhe sinjalizon kur:

[273] Rregullore (EU) nr. 1077/2011 e Parlamentit Evropian dhe Këshillit, datë 25 tetor 2011 që themelon një Agjenci Evropiane për menaxhimin operacional të Sistemeve IT në shkallë të gjerë në fushën e lirisë, sigurisë dhe drejtësisë, JO 2011 L 286.

[274] Marrëveshje ndërmjet Qeverive të Shteteve të Bashkimit Ekonomik të Beneluksit, Republikës Federale të Gjermanisë dhe Republikës Franceze mbi eliminimin e përshkallëzuar të kontrolleve në kufijtë e tyre të përbashkët, JO 2000 L 239.

[275] Komuniteti Evropian (1997), Traktati i Amsterdamit që ndryshon Traktatin e Bashkimit Evropian, Traktatet që themelojnë Komunitetin Evropian dhe disa aspekte në lidhje me të, JO 1997 C 340.

[276] Rregullorja (EC) nr. 1987/2006 e Parlamentit Evropian dhe Këshillit, datë 20 dhjetor 2006 mbi ngritjen, funksionimin dhe përdorimin e Sistemit të Informacionit Schengen të gjeneratës së dytë, JO 2006 L 381 (*SIS II)* dhe Këshillit të Bashkimit Evropian (2007), Vendimi i Këshillit 2007/533/JHA, datë 12 qershor 2007 mbi ngritjen, funksionimin dhe përdorimin e Sistemit të Informacionit Schengen të gjeneratës së dytë (*SIS II*), JO 2007 L 205.

- Personi nuk ka të drejtë të hyjë apo të qëndrojë në territorin Schengen; ose
- Personi apo sendi kërkohet nga autoritetet gjyqësore apo të zbatimit të ligjit; ose
- Personi është denoncuar se ka humbur; ose
- Mallra, sikurse bankënota, automjete, kamionë, armë zjarri dhe dokumente identiteti, janë denoncuar si të vjedhura apo të humbura.

Në rastin e një sinjalizimi, veprimet në vijim duhet të iniciohen nëpërmjet Sistemeve Kombëtare të Informacionit Schengen.

SIS II ka funksione të reja, sikurse mundësia për të regjistruar: të dhëna biometrike, si gjurmë gishtash dhe fotografi; ose kategori të reja sinjalizimesh, si mjete lundrimi, avionë, kontenierë apo mjete pagese të vjedhura; dhe sinjalizime të përmirësuara për persona dhe sende; kopje të Mandat-Arresteve Evropiane (EAW-të) për persona të kërkuar për t'u arrestuar, dorëzuar apo ekstraduar.

Vendimi i Këshillit 2007/533/JHA në lidhje me ngritjen, funksionimin dhe përdorimin e Sistemit të Informacionit Schengen të gjeneratës së dytë (Vendimi Schengen II) integron Konventën 108: "Të dhënat personale të përpunuar në zbatim të këtij vendimi, do të mbrohen në përputhje me Konventën 108 të Këshillit të Evropës".[277] Kur përpunimi i të dhënave personale nga ana e autoriteteve policore kombëtare bëhet në zbatim të Vendimit Schengen II, dispozitat e Konventës 108, ashtu si edhe Rekomandimi i të Dhënave të Policisë, duhet të transpozohen në legjislacionin kombëtar.

Autoriteti kompetent mbikëqyrës kombëtar në secilin Shtet Anëtar, monitoron N-SIS-in vendas. Në mënyrë të veçantë, ai duhet të kontrollojë cilësinë e të dhënave që regjistrojnë Shtetet Anëtare në C-SIS nëpërmjet N-SIS-it. Autoriteti kombëtar mbikëqyrës duhet të garantojë që auditimi i përpunimeve të të dhënave tek N-SIS vendas, të kryhet të paktën një herë në katër vite. Autoritetet kombëtare mbikëqyrëse dhe EDPS-ja bashkëpunojnë dhe garantojnë mbikëqyrje të koordinuar të SIS-it, ndërsa EDPS-ja është përgjegjëse për mbikëqyrjen e C-SIS-it. Për motive transparence, i duhet dërguar Parlamentit Evropian, Këshillit dhe eu-LISA-s një raport i përbashkët i aktiviteteve çdo dy vjet.

Të drejtat e individëve për akses në lidhje me SIS II mund të ushtrohen në çdo Shtet Anëtar, meqenëse N-SIS-i është një kopje ekzakte e C-SIS-it.

Shembull: tek çështja *Dalea kundër Francës*,[278] ankuesit iu refuzua viza franceze, meqenëse autoritetet franceze kishin sinjalizuar në Sistemin e Informacionit Schengen se atij duhet t'i refuzohej hyrja. Ankuesi u mundua, por nuk arriti të përfitonte akses dhe korrigjim të të dhënave nga Komisioni Francez i Mbrojtjes së të Dhënave dhe në instancën e fundit, nga Këshilli i Shtetit. GjEDNj-ja vendosi se sinjalizimi i ankuesit në Sistemin e Informacionit Schengen parashikohej në ligj dhe ishte bërë për qëllimin legjitim të mbrojtjes së sigurisë kombëtare.

[277] Këshilli i Bashkimit Evropian (2007), Vendimi i Këshillit 2007/533/JHA, datë 12 qershor 2007 në lidhje me ngritjen, funksionimin dhe përdorimin e Sistemit të Informacionit Schengen, JO 2007 L 205, neni 57.
[278] GjEDNj, *Dalea kundër Francës* (dec.), nr. 964/07, 2 shkurt 2010.

Meqenëse ankuesi nuk kishte vërtetuar se çfarë pasojash kishte pasur për shkak të refuzimit të hyrjes në zonën Schengen dhe duke qenë se ekzistonin masat e duhura për ta mbrojtur atë nga vendimet arbitrare, ndërhyrja në të drejtën e tij për respektim të jetës private, kishte qenë proporcionale. Ankesa e tij referuar nenit 8 ishte shpallur e papranueshme.

Sistemi i Informacionit të Vizave

Sistemi i Informacionit të Vizave (VIS), i cili shfrytëzohet gjithashtu nga eu-LISA, u ngrit për të mbështetur zbatimin e politikave të përbashkëta të BE-së ne lidhje me vizat.[279] Sistemi VIS u mundëson shteteve të Schengen-it të shkëmbejnë të dhëna në lidhje me vizat, nëpërmjet një sistemi i cili ndërlidh konsullatat e shteteve të Schengen-it, të vendosura në shtetet jo anëtare të BE-së, me pikat kufitare të jashtme të të gjitha shteteve të Schengen-it. Sistemi VIS përpunon të dhëna në lidhje me aplikimet për viza me afat të shkurtër qëndrimi, për të vizituar apo udhëtuar tranzit në zonën Schengen. Sistemi VIS i mundëson autoriteteve kufitare të verifikojnë, me ndihmën e të dhënave biometrike, nëse një person që paraqet një vizë, është vërtet personi i autorizuar për këtë vizë dhe për të identifikuar personat pa dokumente ose me dokumente të falsifikuara.

Sipas Rregullores (EC) nr. 767/2008 të Parlamentit Evropian dhe Këshillit në lodhje me Sistemin e Informacionit të Vizave (VIS) dhe shkëmbimit të të dhënave ndërmjet Shteteve Anëtare në lidhje me vizat me afat të shkurtër qëndrimi (Rregullorja VIS), vetëm të dhënat në lidhje me aplikuesin, vizat e tij apo të saj, fotografitë, gjurmët e gishtave, lidhjet me aplikimet e mëparshme dhe skedarët e aplikimit të personave që e shoqërojnë atë, mund të regjistrohen në Sistemin VIS.[280] Aksesi në Sistemin VIS me qëllim regjistrimin, ndryshimin apo fshirjen e të dhënave, është i mundur vetëm për autoritetet e vizave të Shteteve Anëtare, ndërsa aksesi për të këqyrur të dhënat, i jepet autoriteteve të vizave dhe autoriteteve kompetente për kontrollet e pikave të jashtme të kalimit kufitar, kontrollit të emigracionit dhe azilit. Me disa kushte të caktuara, autoritetet kompetente kombëtare të policisë dhe Europol-it mund të kërkojnë akses në të dhënat e regjistruara në Sistemin VIS për qëllime të parandalimit, zbulimit dhe hetimit të veprave për qëllime terroriste dhe veprave të tjera penale.[281]

[279] Këshilli i Bashkimit Evropian (2004), Vendimi i Këshillit datë 8 qershor 2004 që themelomn Sistemin e Informacionit të Vizave (VIS), JO 2004 L 213; Rregullorja (EC) nr. 767/2008 e Parlamentit Evropian dhe e Këshillit, datë 9 qershor 2008 në lidhje me Sistemin e Informacionit të Vizave (VIS) dhe shkëmbimin e të dhënave ndërmjet Shteteve Anëtare për vizat me afat të shkurtër qëndrimi, JO 2008 L 218 (*Rregullorja VIS)*; Këshilli i Bashkimit Evropian (2008), Vendimi i Këshillit 2008/633/JHA, datë 23 qershor 2008 në lidhje me aksesin për këqyrje të Sistemit të Informacionit të Vizave (VIS) nga autoritetet e përcaktuara të Shteteve Anëtare dhe Europol-i, për qëllime të parandalimit, zbulimit dhe hetimit të veprave terroriste dhe veprave të tjera penale të rënda, JO 2008 L 218.

[280] Neni 5 i Rregullores (EC) nr. 767/2008 e Parlamentit Evropian dhe e Këshillit, datë 9 korrik 2008, në lidhje me Sistemin e Informacionit të Vizave (VIS) dhe shkëmbimin e të dhënave ndërmjet Shteteve Anëtare për vizat me afat të shkurtër qëndrimi (Rregullorja VIS), JO 2008 L 218.

[281] Këshilli i Bashkimit Evropian (2008), Vendimi i Këshillit 2008/633/JHA, datë 23 qershor 2008, në lidhje me aksesin për këqyrje të Sistemit të Informacionit të Vizave (VIS) nga ana e autoriteteve të përcaktuara të Shteteve Anëtare dhe Europol-it, për qëllime të parandalimit, zbulimit dhe hetimit të veprave terroriste dhe veprave të tjera penale të rënda, JO 2008 L 218.

Eurodac-u

Emërtesa Eurodac i referohet daktilogrameve apo gjurmëve të gishtave. Ai është një sistem i përqendruar, që përmban të dhënat daktiloskopike të shtetasve të vendeve të treta, të cilët aplikojnë për azil në një Shtet Anëtar të BE-së.[282] Sistemi është në punë që prej janarit të 2003-shit dhe qëllimi i tij është të ndihmojë në përcaktimin se cili Shtet Anëtar duhet të jetë përgjegjës për shqyrtimin e një aplikimi të caktuar për azil, sipas Rregullores së Këshillit (EC) nr. 343/2003, e cila përcakton kriteret dhe mekanizmat për përcaktimin e Shtetit Anëtar përgjegjës për shqyrtimin e një aplikimi për azil të depozituar në një Shtet Anëtar, nga ana e një shtetasi të një vendi të tretë (*Rregullorja Dublin II).*[283] Të dhënat personale që përmban Eurodac-u mund të përdoren vetëm për qëllime të lehtësimit të zbatimit të Rregullores Dublin II; çdo përdorim për qëllime të tjera është subjekt sanksioni.

Eurodac-u përbëhet nga një njësi qendrore, e cila shfrytëzohet nga eu-LISA, për regjistrimin dhe krahasimin e gjurmëve të gishtave dhe nga një sistem transmetimi elektronik të të dhënave ndërmjet Shteteve anëtare dhe nga baza qendrore e të dhënave. Shtetet Anëtare marrin dhe transmetojnë gjurmët e gishtave të çdo shtetasi të vendeve të treta apo pa shtetësi, që është të paktën 14 vjeç, i cili kërkon azil në territorin e tyre, ose i cili është kapur për kalim të paligjshëm të kufirit të tyre të jashtëm. Shtetet Anëtare mund të marrin dhe transmetojnë gjithashtu gjurmët e gishtave të secilit shtetas nga vende të treta apo pa shtetësi, që qëndrojnë në territorin e tyre pa leje.

Të dhënat e gjurmëve të gishtave mbahen në bazën e të dhënave të Eurodac-ut vetëm në formë të pseudonimizuar. Në rast përputhshmërie, pseudonimi së bashku me emrin e Shtetit të parë Anëtar i cili ka transmetuar të dhënat e gjurmëve të gishtave, i komunikohen Shtetit të dytë Anëtar. Ky Shtet i dytë Anëtar do t'i drejtohet më pas Shtetit të parë Anëtar, për shkak se sipas Rregullores Dublin II, Shtetit i parë Anëtar është përgjegjës për përpunimin e aplikimit për azil.

Të dhënat personale që ruhen në Eurodac, të cilat lidhen me azilkërkuesit, mbahen për 10 vite, duke nisur nga data e marrjes së gjurmëve të gishtave, përveç rastit kur subjekti i të dhënave merr shtetësinë e një Shteti Anëtar të BE-së. Në këtë rast, të dhënat duhet të fshihen menjëherë. Të dhënat në lidhje me shtetasit e juaj, të cilët janë kapur për kalim të paligjshëm të kufirit të jashtëm, ruhen për dy vite. Këto të dhëna duhet të fshihen menjëherë sapo subjekti i të dhënave merr një leje qëndrimi, largohet nga territori i BE-së apo përfiton shtetësinë e një Shteti Anëtar.

Përveç Shteteve Anëtare të BE-së, edhe Islanda, Norvegjia, Lihtenshtejni dhe Zvicra përdorin Eurodac-un, mbështetur në marrëveshjet ndërkombëtare.

---

[282] Rregullorja e Këshillit (EC) nr. 2725, datë 11 dhjetor 2000 në lidhje me ngritjen e Eurodac-ut për krahasimin e gjurmëve të gishtave, për zbatimin me efektshmëri të Konventës së Dublinit, JO 2000 L 316; Rregullorja e Këshillit (EC) nr. 407/2002, datë 28 shkurt 2002 që përcakton disa rregulla për zbatimin e Rregullores (EC) nr. 2725/2000 në lidhje me ngritjen e Eurodac-ut, për krahasimin e gjurmëve të gishtave, për zbatimin me efektshmëri të Konventës së Dublinit, JO 2002 L 62 (*Rregulloret Eurodac*).

[283] Rregullorja e Këshillit (EC) nr. 343/2003, datë 18 shkurt 2003 që përcakton kriteret dhe mekanizmat për përcaktimin e Shtetit Anëtar përgjegjës për shqyrtimin e një aplikimi për azil, të depozituar në një Shtet Anëtar nga ana e një shtetasi të një vendi të treta, JO 2003 L 50 (*Rregullorja Dublin II*).

Eurosur-i

Sistemi Evropian i Kontrollit të Kufijve (*Eurosur-i)*[284] është konceptuar për të përmirësuar kontrollin e kufijve të jashtëm të Schengen-it, nëpërmjet zbulimit, parandalimit dhe luftës kundër emigracionit të paligjshëm dhe kriminalitetit ndërkufitar. Ai shërben për të përmirësuar shkëmbimin e informacionit dhe bashkëpunimin praktik ndërmjet qendrave kombëtare të koordinimit dhe Frontex-it, agjencisë së BE-së përgjegjëse për zhvillimin e zbatimin e konceptit të ri të menaxhimit të integruar të kufijve.[285] Objektivat kryesorë të tij janë:

- Reduktimi i numrit të vdekjeve të emigrantëve të paligjshëm, duke shpëtuar jetën e tyre në det;
- Rritjen e sigurisë së brendshme të BE-së në tërësi, duke kontribuuar në parandalimin e kriminalitetit ndërkufitar.[286]

Sistemi nisi punën më 2 dhjetor 2013 në të gjitha Shtetet Anëtare me kufij të jashtëm, ndërsa do të nisë punën tek të tjerët që nga 1 dhjetori 2014 dhe do të zbatohet për kontrollin e kufijve tokësorë, detarë dhe ajrorë të Shteteve Anëtare.

Sistemi i Doganor i Informacionit

Një sistem tjetër i përbashkër informacioni me rëndësi, i ngritur në nivel BE-je, është Sistemi Doganor i Informacionit (CIS).[287] Në kuadër të krijimit të tregut të brendshëm, të gjitha kontrollet dhe të gjitha formalitetet në lidhje me mallrat që qarkullojnë në territorin e BE-së u shfuqizuan, duke sjellë kështu në një shtim të riskut të mashtrimit. Ky risk u kundërpeshua me anë të intensifikimit të bashkëpunimit ndërmjet administratave doganore të Shteteve Anëtare. Qëllimi i CIS-it është të ndihmojë Shtetet Anëtare të parandalojnë, hetojnë dhe ndjekin penalisht shkeljet e rënda të legjislacionit kombëtar dhe të BE-së në fushën e doganave dhe të bujqësisë.

[284] Rregullorja (EU) nr. 1052/2013 e Parlamentit Evropian dhe e Këshillit, datë 22 tetor 2013 që krijon Sistemin Evropian të Kontrollit të Kufijve (Eurosur), Jo 2013 L 295.

[285] Rregullorja (EU) nr. 1168/2011 e Parlamentit Evropian dhe e Këshillit, datë 25 tetor 2011, që ndryshon Rregulloren e Këshillit (EC) nr. 2007/2004 për krijimin e Agjencisë Evropiane të Menaxhimit të Bashkëpunimit Operacional në Kufijtë e Jashtëm të Shteteve Anëtare të Bashkimit Evropian, JO 2011 L 394 (*Rregullorja e Frontex-it*).

[286] Shih gjithashtu: Komisioni Evropian (2008), Komunikatë e Komisionit drejtuar Parlamentit Evropian, Këshillit, Komitetit Ekonomik dhe Shoqëror Evropian dhe Komitetit të Rajoneve: Vlerësimi i krijimit të një Sistemi Evropian të Kontrollit të Kufijve (Eurosur), COM(2008) 68, përfundimtar, Bruksel, 13 shkurt 2008; Komisioni Evropian (2011), Vlerësimi i Ndikimit që shoqëron Propozimin për një Rregullore të Parlamentit Evropian dhe Këshillit për krijimin e Sistemit Evropian të Kontrollit të Kufijve (Eurosur), dokumenti i punës së shërbimeve të Komisionit, SEC(2011) 1536 përfundimtar, Bruksel, 12 dhjetor 2011, fq. 18.

[287] Këshilli i Bashkimit Evropian (1995), Akti i Këshillit, datë 26 korrik 1995 që harton Konventën për përdorimin e teknologjisë së informacionit në fushën e doganave, JO 1995 C 316, ndryshuar nga Këshilli i Bashkimit Evropian (2009), Rregullorja nr. 515/97, datë 13 mars 1997 mbi mbështetjen reciproke ndërmjet autoriteteve administrative të Shteteve Anëtare dhe bashkëpunimin ndërmjet këtyre të fundit dhe Komisionit, për të garantuar zbatimin e duhur të legjislacionit në fushën e doganave dhe bujqësisë, Vendimi i Këshillit 2009/917/JHA, datë 30 nëntor 2009 në lidhje me përdorimin e teknologjisë së informacionit në fushën e doganave, JO 2009 L 323 (*Vendimi për CIS-in*).

Informacioni që përmban CIS-i përfshin të dhëna personale që kanë të bëjnë me produkte, mjete transporti, biznese, persona, mallra dhe parà të bllokuara, të sekuestruara dhe të konfiskuara. Ky informacion mund të përdoret vetëm për qëllime të identifikimit, raportimit apo kryerjes së inspektimeve të caktuara ose për analiza strategjike ose operative në lidhje me persona të dyshuar për shkelje të dispozitave doganore.

Aksesi në CIS autorizohet për autoritetet kombëtare, doganore, të tatimeve, të bujqësisë, shëndetit publik dhe të policisë, ashtu si edhe të Europol-it dhe Eurojust-it.

Përpunimi i të dhënave personale duhet të respektojë rregullat specifike të përcaktuara në Rregulloren nr. 515/97 dhe Konventën e CIS-it,[288] ashtu si edhe dispozitat e Direktivës së Mbrojtjes së të Dhënave, Rregulloren e Mbrojtjes së të Dhënave të Institucioneve të BE-së, Konventës 108 dhe Rekomandimit të të Dhënave të Policisë. EDPS-ja është përgjegjëse për mbikëqyrjen e respektimit të Rregullores nr. 45/2001 nga ana e CIS-it dhe zhvillon takime, të paktën një herë në dy vjet, me autoritetet kombëtare mbikëqyrëse të mbrojtjes së të dhënave, të cilat janë kompetente për monitorimin e CIS-it.

[288] Po aty.

8

Ligje të tjera evropiane specifike për fushën e mbrojtjes së të dhënave

BE	Çështje të trajtuara	KiE
Direktiva e Mbrojtjes së të dhënave Direktiva mbi privatësinë dhe komunikimet elektronike	**Komunikimet elektronike**	Konventa 108 Rekomandimi për Shërbimet e Telekomunikacioneve
Direktiva e Mbrojtjes së të Dhënave, neni 8 (2) (b)	**Marrëdhëniet e punësimit**	Konventa 108 Rekomandimi i Punësimit
		GjEDNj, *Copland kundër Mbretërisë së Bashkuar*, nr. 62617/00, 3 prilll 2007
Direktiva e Mbrojtjes së të Dhënave, neni 8 (3)	**Të dhënat mjekësore**	Konventa 108 Rekomandimi i të Dhënave Mjekësore
		GjEDNj, *Z. Kundër Finlandës*, nr. 22009/93, 25 shkurt 1997
Direktiva në lidhje me provat klinike	**Provat klinike**	
Direktiva në lidhje me mbrojtjen e të dhënave, neni 6 (1) (b) dhe (e), neni 13 (2)	**Statistikat**	Konventa 108 Rekomandimi për të Dhënat Statistikore
Rregullorja (EC) nr. 223/2009 e statistikave evropiane GjDBE, C-524/06, *Huber kundër Gjermanisë*, 16 dhjetor 2008	**Statistikat zyrtare**	Konventa 108 Rekomandimi për të Dhënat Statistikore
Direktiva 2004/39/EC në lidhje me tregjet e instrumenteve financiare Rregullorja (EU) nr. 648/2012 e instrumenteve financiare derivate OTC, palëve qendrore dhe	**Të dhënat financiare**	Konventa 108 Rekomandimi 90(19) për mbrojtjen e të dhënave personale të përdorura për pagesa dhe operacionet e tjera në lidhje me to

regjistrave qendrorë të transaksioneve Rregullorja (EC) nr. 1060/2009 mbi agjencitë e vlerësimit të kredisë Direktiva 2007/64/EC mbi shërbimet e pagesave në tregun e brendshëm		GjEDNj, *Michaud kundër Francës, nr. 12323/11, 6 dhjetor 2012*

Në rrethana të ndryshme, janë miratuar akte ligjore specifike në nivel evropian, të cilat zbatojnë në mënyrë më të detajuar normat e përgjithshme të Konventës 108 apo të Direktivës së Mbrojtjes së të Dhënave.

8.1. Komunikimet elektronike

Pikat kryesore

- Rekomandimi i KiE-së i 1995-ës përmban rregulla specifike në lidhje me mbrojtjen e të dhënave në sektorin e telekomunikacioneve, me vëmendje të veçantë në shërbimet telefonike.
- Përpunimi i të dhënave personale në lidhje me ofrimin e shërbimeve të komunikimit në nivel BE-je, rregullohet me anë të Direktivës së privatësisë dhe komunikimeve elektronike.
- Konfidencialiteti i komunikimeve elektronike ka të bëjë jo vetëm me përmbajtjen e komunikimit, por edhe me të dhënat e trafikut, sikurse informacioni mbi atë se kush komunikoi me kë, kur dhe për sa kohë dhe të dhënat e vendndodhjes, si për shembull vendi nga i cili u komunikuan të dhënat.

Rrjetet e komunikimit kanë potencial të madh ndërhyrjeje të pajustifikuar në sferën personale të përdoruesit, duke qenë se ofrojnë mjetet teknike për të dëgjuar dhe kontrolluar komunikimet e kryera në këto rrjete. Për rrjedhojë, është vlerësuar si i nevojshëm miratimi i rregulloreve speciale të mbrojtjes së të dhënave, me qëllimin përballimin e risqeve specifike ndaj përdoruesve të shërbimeve të komunikimit.

Në 1995-ën, KiE-ja publikoi një Rekomandim për mbrojtjen e të dhënave në fushën e telekomunikacioneve, me vëmendje të veçantë tek shërbimet telefonike.[289] Sipas këtij rekomandimi, qëllimet e mbledhjes dhe përpunimit të të dhënave personale në kontekstin e telekomunikacioneve, duhet të kufizohen tek: lidhja e përdoruesit me rrjetin, vënia në dispozicion e shërbimit të caktuar të telekomunikimit, faturimit, verifikimit të pagesës, garantimit të funksionimit teknik optimal dhe zhvillimit të rrjetit dhe të shërbimit.

Një vëmendje e veçantë iu dha gjithashtu përdorimit të rrjeteve të komunikimit për dërgimin e mesazheve të marketingut të drejtpërdrejtë. Si rregull i përgjithshëm, mesazhet e marketingut të drejtpërdrejtë nuk mund t'i dërgohen abonentëve, të cilët kanë kërkuar të përjashtohen nga marrja e mesazheve reklamuese.

[289] KiE, Komiteti i Ministrave (1995), Rekomandimi Rec(95)4 drejtuar shteteve anëtare për mbrojtjen e të dhënave personale në fushën e shërbimeve të telekomunikacionit, me vëmendje të veçantë në shërbimet telefonike, 7 shkurt 1995.

Telefonatat automatike, për transmetimin e mesazheve reklamuese të regjistruara më parë, mund të përdoren vetëm nëse abonenti ka dhënë pëlqimin e tij të qartë. Legjislacioni kombëtar duhet të përcaktojë rregulla të hollësishme në këtë fushë.

Sa i takon **kuadrit ligjor të BE-së**, pas një përpjekjeje të parë në 1997-ën, Direktiva në lidhje me privatësinë dhe komunikimet elektronike u miratua në 2002-shin dhe u ndryshua në 2009-ën, me qëllim kompletimin dhe saktësimin e dispozitave të Direktivës së Mbrojtjes së të Dhënave për sektorin e telekomunikacioneve.[290] Zbatimi i Direktivës në lidhje me privatësinë dhe komunikimet elektronike, kufizohet vetëm në shërbimet e komunikimit në rrjetet elektronike publike.

Direktiva në lidhje me privatësinë dhe komunikimet elektronike bën dallimin e tre kategorive kryesore të të dhënave, të gjeneruara nga një komunikim:

- Të dhëna që përbëjnë përmbajtjen e mesazheve, të dërguara gjatë komunikimit; këto të dhëna janë rreptësishtë konfidenciale;
- Të dhëna të nevojshme për vendosjen dhe ruajtjen e komunikimit, të ashtuquajturat të dhënat e trafikut, për shembull informacioni në lidhje me partnerët e komunikimit, koha dhe kohëzgjatja e komunikimit;
- Brenda të dhënave të trafikut, ka të dhëna që kanë të bëjnë veçanërisht me vendndodhjen e pajisjes së komunikimit, të ashtuquajturat të dhënat e vendndodhjes; këto të dhëna kanë të bëjnë njëkohësisht me vendndodhjen e *përdoruesve* të pajisjeve të komunikimit dhe kanë rëndësi të veçantë për përdoruesit e pajisjeve të lëvizshme të komunikimit.

Të dhënat e trafikut mund të përdoren nga operatori i shërbimit vetëm për qëllime të faturimit dhe për operimin teknik të shërbimit. Gjithsesi, me pëlqimin e subjektit të të dhënave, këto të dhëna mund të përhapen tek kontrollues të tjerë, të cilët ofrojnë shërbime me vlerë të shtuar, sikurse dhënia e informacionit në lidhje me vendndodhjen e përdoruesit sa i takon stacionit më të afërt të metrosë apo farmacisë ose parashikimit të motit për atë vendndodhje.

Lloje të tjera aksesi në të dhënat në lidhje me komunikimet në rrjetet elektronike, sikundër aksesi për qëllime të hetimit të krimeve, në përputhje me nenit 15 të Direktivës së e-Privatësisë, duhet të plotësojnë disa norma për ndërhyrje të justifikuar në të drejtën për mbrojtje të të dhënave, sikurse sanksionohet në nenin 8 (2) të KEDNj-së dhe konfirmohet në nenet 8 dhe 52 të Kartës.

Ndryshimet e bëra në Direktivën e privatësisë dhe komunikimeve elektronike[291] që nga 2009-ta sollën elementet në vijim:

---

[290] Direktiva 2002/58/EC e Parlamentit Evropian dhe e Këshillit, datë 12 korrik 2002, në lidhje me përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike, JO 2002 L 201 (*Direktiva e privatësisë dhe komunikimeve elektronike)*, ndryshuar me Direktivën 2009/136/EC të Parlamentit Evropian dhe Këshillit, datë 25 nëntor 2009, që ndryshon Direktivën 2002/22/EC mbi shërbimet universale dhe të drejtat e përdoruesve në lidhje me rrjetet dhe shërmbimet e komunikimeve elektronike, Direktiva 2002/58/EC në lidhje me përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike dhe Rregulloren (EC) nr. 2006/2004 mbi bashkëpunimin ndërmjet autoriteteve kombëtare përgjegjëse për zbatimin e legjislacionit të mbrojtjes së konsumatorëve, JO 2009 L 337.

[291] Direktiva 2009/136/EC e Parlamentit Evropian dhe e Këshillit e 25 nëntorit 2009, që ndryshon Direktivën 2002/22/EC mbi shërbimet universale dhe të drejtat e përdoruesve në lidhje me rrjetet dhe shërbimet e komunikimeve elektronike, Direktivën 2002/58/EC në lidhje me përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike dhe Rregulloren (EC) nr. 2006/2004 mbi bashkëpunimin ndërmjet autoriteteve kombëtare përgjegjëse për zbatimin e legjislacionit për mbrojtjen e konsumatorëve, JO 2009 L 337.

- Kufizimet e dërgimit të postës elektronike për qëllime të marketingut të drejtpërdrejtës, u shtrinë edhe tek shërbimet e mesazheve të shkurtra telefonike, shërbimet e mesazheve multimediale dhe në aplikacione të ngjashme të llojeve të ndryshme; posta elektronike për qëllime marketingu është e ndaluar, përveçse kur është marrë pëlqimi paraprak. Pa një pëlqim të tillë, vetëm klientët e mëparshëm mund të kontaktohen me postë elektronike reklamuese, nëse këta kanë komunikuar adresat e tyre elektronike dhe nuk kanë kundërshtuar.
- Është caktuar një detyrim për Shtetet Anëtare që të parashikojnë procedim gjyqësor kundër shkeljeve të ndalimit të komunikimeve të padëshiruara.[292]
- Instalimi i shënjuesve (*cookies)*, program kompjuterik i cili monitoron dhe regjistron veprimet e përdoruesit të kompjuterit, nuk lejohet më pa pëlqimin e përdoruesit të kompjuterit. Legjislacioni kombëtar duhet të rregullojë më me hollësi mënyrën se si duhet të shprehet dhe merret pëlqimi, me qëllim që të ofrohet mbrojtje e mjaftueshme.[293]

Kur ndodh një shkelje të dhënash, për shkak të aksesit të paautorizuar, me humbje apo shkatërrim të të dhënave, autoriteti mbikëqyrës kompetent, duhet të vihet në dijeni menjëherë. Abonentët duhet të informohen kur ekziston mundësia që t'u shkaktohen dëme si rrjedhojë e shkeljes së të dhënave.[294]

Direktiva e Ruajtjes së të Dhënave[295] (shfuqizuar më 8 prill 2014, shih për shembull rastin e mëposhtëm) detyronte operatorët e shërbimeve të komunikimit, që të ruanin të dhënat e trafikut, sidomos për qëllime të luftës kundër krimeve të rënda, për një periudhë prej të paktën gjashtë muajsh, po jo më shumë se 24 muaj, pavarësisht nëse operatorit i nevojiteshin më ato të dhëna për qëllime faturimi ose jo, apo për operimin teknik të shërbimit.

Shtetet Anëtare të BE-së duhet të përcaktojnë autoritetet publike të pavarura, të cilat janë përgjegjëse për monitorimin e sigurisë së të dhënave të ruajtura.

Ruajtja e të dhënave të telekomunikacioneve, cënon qartësisht të drejtën për mbrojtje të të dhënave.[296] Nëse kjo ndërhyrje është e justifikuar ose jo, diçka e tillë ka qenë objekt i disa çështjeve gjyqësore në Shtetet Anëtare të BE-së.[297]

Shembull: tek çështja *Digital Rights Ireland dhe Seitlinger dhe të Tjerët,*[298] GjDBE-ja e shpalli Direktivën e Ruajtjes së të Dhënave të pavlefshme. Sipas Gjykatës, "ndërhyrja në shkallë të gjerë dhe mjaft serioze e Direktivës tek të drejtat themelore, nuk është e kufizuar sa duhet për të garantuar që kjo ndërhyrje të kufizohet vetëm tek ajo çka është e domosdoshme."

[292] Shih Direktivën e ndryshuar, neni 13.
[293] Po aty, neni 5; shih gjithashtu Grupi i Punës së Nenit 29 (2012), *Opinioni 04/2012 mbi përjashtimin për marrjen e pëlqimit në lidhje me disa lloj shënjuesish (cookies),* WP 194, Bruksel, 7 qershor 2012.
[294] Shih gjithashtu Grupin i Punës së Nenit 29 (2011), *Dokument Pune 01/2011 mbi kuadrin ligjor të BE-së në lidhje shkeljet e të dhënave personale dhe rekomandimet për veprimet për t'u ndërmarrë në të ardhmen,* WP 184, Bruksel, 5 prill 2011.
[295] Direktiva 2006/24/EC e Parlamentit Evropian dhe e Këshillit, datë 15 mars 2006 mbi ruajtjen e të dhënave të gjeneruara ose të përpunuara në lidhje me ofrimin e shërbimeve të komunikimeve elektronike, të disponueshme për publikun apo të rrjeteve publike të komunikimeve dhe që ndryshon Direktivën 2002/58/EC, JO 2006 L 105.
[296] EDPS (2011), *Opinion i datës 31 maj 2011 në lidhje me raportin e Vlerësimit të Komisionit drejtuar Këshillit dhe Parlamentit Evropian mbi Direktivën e Ruajtjes së të Dhënave (Direktiva 2006/24/EC),* 31 maj 2011.
[297] Gjermani, Gjykata Kushtetuese Federale (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 mars 2010; Rumani, Gjykata Kushtetuese (*Curtea Constituþionalã a României*), nr. 1258, 8 tetor 2009; Republika e Çekisë, Gjykata Kushtetuese (*Ústavní soud České republiky*), 94/2011 Coll., 22 mars 2011.
[298] GjDBE, Çështje të bashkuara C-293/12 dhe C-594/12, *Digital Rights Ireland dhe Seitlinger dhe të Tjerët,* 8 prill 2014, parag. 65.

Një çështje thelbësore në kontekstin e komunikimeve elektronike është ndërhyrja nga ana e autoriteteve publike. Pajisjet e survejimit dhe interceptimit të komunikimeve, si për shembull të pajisjeve të përgjimit, lejohen vetëm nëse parashikohet në ligj dhe nëse përbën një masë të domosdoshme në një shoqëri demokratike, në interes të: mbrojtjes së sigurisë shtetërore, rendit publik, interesave monetare të shtetit apo për luftën kundër krimit; ose për mbrojtjen e subjektit të të dhënave ose të të drejtave dhe lirive të të tjerëve.

Shembull: tek çështja *Malone kundër Mbretërisë së Bashkuar,*[299]ankuesi ishte akuzuar për një sërë veprash penale, në lidhje me tregtimin e mallrave të vjedhur. Gjatë gjykimit të tij u zbulua se një bisedë e ankuesit ishte përgjuar mbështetur në një mandat të lëshuar nga Sekretari i Shtetit për Departamentin e Brendshëm. Megjithëse mënyra sipas së cilës ishte përgjuar komunikimi i ankuesit, ishte e ligjshme sipas legjislacionit të brendshëm, GjEDNj-ja vlerësoi se nuk ekzistonte bazë ligjore në lidhje me shtrirjen dhe modalitet e ushtrimit të lirisë së veprimit që gëzonin autoritetet publike në këtë fushë dhe se për rrjedhojë ndërhyrja si rezultat i ekzistencës së praktikës në fjalë. nuk kishte qenë "në përputhje me ligjin". Gjykata vendosi se kishte pasur shkelje të nenit 8 të KEDNj-së.

8.2. Të dhënat e punësimit

Pikat kryesore

- Rekomandimi i KiE-së në lidhje me të dhënat e punësimit parashikon rregulla specifike për mbrojtjen e të dhënave në marrëdhëniet e punësimit.
- Tek Direktiva e Mbrojtjes së të Dhënave, marrëdhëniet e punësimit përmenden në mënyrë specifike në kontekstin e përpunimit të të dhënave sensitive.
- Vlefshmëria e pëlqimit, i cili duhet dhënë patjetër në mënyrë të lirë, si bazë ligjore për përpunimin e të dhënave të të punësuarve, mund të jetë i dyshimtë, për shkak të pabarazisë ekonomike midis punëdhënësit dhe punëmarrësit. Rrethanat e dhënies së pëlqimit duhen vlerësuar me kujdes.

Në BE nuk ekziston një kuadër ligjor specifik, i cili rregullon përpunimin e të dhënave në kontekstin e punësimit. Tek Direktiva e Mbrojtjes së të Dhënave, marrëdhëniet e punësimit përmenden në mënyrë specifike vetëm në nenin 8 (2) të Direktivës, i cili ka të bëjë me përpunimin e të dhënave sensitive. Për sa i përket KiE-së, Rekomandimi i të Dhënave të Punësimit është publikuar në 1989-ën dhe është aktualisht duke u përditësuar.[300]

Një studim në lidhje me problematikat më të zakonshme të mbrojtjes së të dhënave, specifike për kontekstin e punësimit, mund të gjendet në një dokument pune të Grupit të Punës së Nenit 29.[301] Grupi i Punës analizoi domethënien e pëlqimit, si një bazë ligjore për përpunimin e të dhënave të punësimit,[302]

[299] GjEDNj, *Malone kundër Mbretërisë së Bashkuar*, nr. 8691/79, 2 gusht 1984.
[300] Këshilli i Evropës, Komiteti i Ministrave (1989), Rekomandimi Rec(89)2 drejtuar shteteve anëtare në lidhje me mbrojtjen e të dhënave personale të përdorura për qëllime të punësimit, 18 janar 1989. Shih gjithashtu Komiteti Konsultativ i Konventës 108, Studim në lidhje me Rekomandimin nr. R (89) 2 mbi mbrojtjen e të dhënave personale të përdorura për qëllime të punësimit dhe për të propozuar rishikimin e Rekomandimit të sipërpërmendur, 9 shtator 2011.
[301] Grupi i Punës së Nenit 29 (2011), *Opinioni 8/2001 në lidhje me përpunimin e të dhënave personale në kontekstin e punësimit*, WP 48, Bruksel, 13 shtator 2001.
[302] Grupi i Punës së Nenit 29 (2005), *Dokument pune në lidhje me interpretimin e përbashkët të nenit 26(1) të Direktivës 95/46/EC të 24 tetorit 1995*, WP 114, Bruksel, 25 nëntor 2005.

Grupi i Punës konstatoi se pabarazia ekonomike midis punëdhënësit që kërkon pëlqimin dhe punëmarrësit që jep pëlqimin, do të ngrejë shpesh dyshime nëse pëlqimi është dhënë në mënyrë të lirë apo jo. Për këtë shkak, rrethanat në të cilat kërkohet pëlqimit, duhet të shqyrtohen me kujdes kur vlerësohet vlefshëmria e pëlqimit në kontekstin e punësimit.

Një problematikë e përhapur e mbrojtjes së të dhënave, në ambientin tipik aktual të punës, është shtrirja legjitime e monitorimit të komunikimeve elektronike të nëpunësve në vendin e punës. Shpesh pretendohet se ky problem mund të zgjidhet lehtësisht, nëpërmjet ndalimit të përdorimit të sistemeve të komunikimit të punës për çështje private. Por një ndalim i tillë i përgjithshëm mund të jetë gjithsesi jo proporcional dhe jo realist. Çështja gjyqësore në vijim e GjEDNj-së mund të jetë veçanërisht interesante në këtë kontekst:

Shembull: tek çështja *Copland kundër Mbretërisë së Bashkuar*,[303] përdorimi i telefonit, postës elektronike dhe internetit nga ana e nëpunësit të një kolegji, ishte kontrolluar në mënyrë të fshehtë, me qëllim që të përcaktohej nëse përdorte në mënyrë abuzive pajisjet e kolegjit për qëllime personale. GjEDNj-ja vlerësoi se telefonatat nga ambientet e punës përfshiheshin në nocionet e jetës private dhe korrespondencës. Për rrjedhojë, telefonatat dhe posta elektronike e dërguar nga puna, ashtu si edhe informacioni që buron nga monitorimi i përdorimit personal të internetit, mbroheshin nga neni 8 i KEDNj-së. Në rastin e ankuesit, nuk ekzistonin dispozita të cilat të rregullonin rrethanat, në të cilat punëdhënësit mund të monitoronimin përdorimin e telefonit, postës elektronike dhe internetit nga ana e nëpunësve. Për rrjedhojë, ndërhyrja nuk ishte në përputhje me ligjin. Gjykata doli në përfundimin se kishte pasur shkelje të nenit 8 të KEDNj-së.

Sipas Rekomandimit të Punësimit të KiE-së, të dhënat personale të mbledhura për qëllime të punësimit, duhet të merren drejtpërdrejt nga nëpunësi i përfshirë.

Të dhënat personale të mbledhura për qëllime të aplikimit për punësim, duhet të kufizohen vetëm në informacionin e domosdoshëm, për vlerësimin e përshtatshmërisë së kandidatëve dhe potencialit të tyre për karrierë.

Rekomandimi përmend gjithashtu në mënyrë eksplicite të dhënat e vlerësimit, që kanë të bëjnë me kryerjen e punës apo potencialin e punonjësve. Të dhënat e vlerësimit duhet të mbështeten në vlerësime të drejta dhe të ndershme dhe nuk duhet në asnjë mënyrë të jenë fyese. Kjo është ajo çka detyron parimi i përpunimit të drejtë të të dhënave dhe i saktësisë së të dhënave.

Një aspekt i veçantë i legjislacionit të mbrojtjes së të dhënave për marrëdhënien punëdhënës-punëmarrës, është roli i përfaqësuesve të nëpunësve. Këta përfaqësues mund të përftojnë të dhëna personale të nëpunësve, vetëm për aq sa është e domosdoshme që t'u mundësojë atyre të përfaqësojnë interesat e nëpunësve.

[303] GjEDNj, *Copland kundër Mbretërisë së Bashkuar*, nr. 62617/003, 3 prill 2007

Të dhënat personale sensitive, të mbledhura për qëllime të punësimit, mund të përpunohen vetëm në raste të veçanta dhe në përputhje me garancitë e përcaktuara nga legjislacioni i brendshëm. Punëdhënësit mund t'u kërkojnë punëmarrësve apo aplikantëve për punë, të dhëna në lidhje me gjendjen shëndetësore, apo mund t'i nënshtrojnë ata në një kontroll mjekësor vetëm kur është e nevojshme për të: përcaktuar nëse janë të përshtatshëm për vendin e punës; për plotësimin e kritereve të mjekësisë parandaluese; apo për të mundësuar përfitimin e sigurimeve shoqërore. Të dhënat në lidhje me shëndetin nuk duhet të mblidhen nga burime të tjera, të ndryshme nga ai i nëpunësit të përfshirë, përveç rastit kur është marrë pëlqimi në mënyrë të qartë dhe të informuar, ose kur e parashikon legjislacioni kombëtar.

Sipas Rekomandimit të Punësimit, nëpunësit duhet të informohen në lidhje me qëllimin e përpunimit të të dhënave të tyre personale, llojin e të dhënave personale të ruajtura, njësitë të cilave u komunikohen rregullisht të dhënat e tyre dhe qëllimin e bazën ligjore për këto lloj komunikimesh. Punëdhënësit duhet gjithashtu të informojnë nëpunësit e tyre paraprakisht në lidhje me futjen në përdorim apo përshtatjen e sistemeve të tyre automatike për përpunimin e të dhënave personale të nëpunësve ose për monitorimin e lëvizjeve apo për produktivitetin e nëpunësve.

Nëpunësit duhet të gëzojnë të drejtën e aksesit në të dhënat e tyre në lidhje me punësimin, ashtu si të drejtën për korrigjim apo fshirje. Nëse të dhënat e vlerësimit përpunohen, nëpunësit duhet gjithashtu të kenë të drejtën të kundërshtojnë vlerësimin. Sidoqoftë, këto të drejta mund të kufizohen për një periudhë të caktuar kohore, për shkaqe që lidhen me hetime të brendshme. Nëse një nëpunësi i refuzohet aksesi, korrigjimi apo fshirja e të dhënave personale të punësimit, legjislacioni kombëtar duhet të parashikojë procedura të përshtatshme për t'u ankuar në lidhje me këtë refuzim.

8.3. Të dhënat mjekësore

Pika kryesore

- Të dhënat mjekësore janë të dhëna sensitive dhe për rrjedhojë gëzojnë mbrojtje të veçantë.

Të dhënat personale në lidhje me gjendjen shëndetësore të subjektit të të dhënave, cilësohen si të dhëna sensitive në nenin 8 (1) të Direktivës së Mbrojtjes së të Dhënave dhe në nenin 6 të Konventës 108. E në këtë kuptim, të dhënat mjekësore janë subjekt i një regjimi më rigoroz të përpunimit të të dhënave, krahasuar me të dhënat jo sensitive.

Shembull: tek çështja *Z. Kundër Finlandës*,[304] ish bashkëshorti i ankueses, i cili ishte i infektuar me HIV, kishte kryer një sërë krimesh seksuale. Për rrjedhojë, ai u dënua për vrasje, bazuar në faktin se ai i kishte ekspozuar me paramendim viktimat ndaj riskut të infektimit me HIV. Gjykata kombëtare urdhëroi që proces-verbali i plotë i gjykimit dhe dokumentacioni i çështjes, të mbeten konfidenciale për 10 vite, pavarësisht kërkesave të ankueses për një periudhë më të gjatë konfidencialiteti. Këto kërkesa u refuzuan nga Gjykata e Apelit dhe vendimi gjyqësor i saj përmbante emrat e plotë të ankueses dhe të ish bashkëshortit të saj.

[304] GjEDNj, *Z. Kundër Finlandës*, nr. 22009/93, 25 shkurt 1997, parag. 94 dhe 112; shih gjithashtu GjEDNj, *M.S. kundër Suedisë*, nr. 20837/92, 27 gusht 1997; GjEDNj, *L.L.kundër Francës*, nr. 7508/02, 10 tetor 2006; GjEDNj, *I. kundër Finlandës*, nr. 20511/03, 17 korrik 2008; GjEDNj, *K.H. dhe të Tjerët kundër. Sllovakisë*, nr. 32881/04, 28 prill 2009; GjEDNj, *Szuluk kundër Mbretërisë së Bashkuar*, nr. 36936/05, 2 qershor 2009

GjEDNj-ja u shpreh se ndërhyrja nuk konsiderohet e rëndësishme në një shoqëri demokrative, për shkak se mbrojtja e të dhënave mjekësore kishte rëndësi thelbësore për ushtrimin e së drejtës për respektim të jetës private dhe familjare, sidomos kur bëhej fjalë për informacion në lidhje me infektimin me HIV, duke pasur parasysh stigmatizimin që i bëhet kësaj sëmundjeje në shumë shoqëri. Për rrjedhojë, Gjykata doli në përfundimin se autorizimi i aksesit në identitetin dhe gjendjen shëndetësore të ankueses, sikurse parashikohej në vendimin e Gjykatës së Apelit, pas një periudhe vetëm 10 vjeçare që nga marrja e vendimit, do të përbënte shkelje të nenit 8 të KEDNj-së.

Neni 8 (3) i Direktivës së Mbrojtjes së të Dhënave lejon përpunimin e të dhënave mjekësore, kur është i domosdoshëm për qëllime të mjekësisë parandaluese, diagnostikimit mjekësore, administrimit të kujdesit dhe trajtimit, apo për menaxhimin e shërbimeve të kujdesit shëndetësor. Gjithsesi, përpunimi është i lejuar vetëm kur kryhet nga stafi i shëndetësisë, i cili i nënshtrohet detyrimit të sekretit profesional, apo nga çdo person tjetër që është subjekt i një detyrimi të barasvlefshëm.[305]

Rekomandimi i KiE-së për të Dhënat Mjekësore të 1997—ës, zbaton në mënyrë më të detajuar parimet e Konventës 108 për përpunimin e të dhënave në fushën e mjekësisë.[306] Rregullat e propozuara në të, janë në përputhje me ato të Direktivës së Mbrojtjes së të Dhënave, për sa i takon qëllimeve legjitime të përpunimit të të dhënave mjekësore, detyrimeve të nevojshme për sekret profesional nga ana e personave të cilët përdorin të dhënat shëndetësore dhe të drejtave të subjekteve të të dhënave për transparencë dhe akses, korrigjim dhe fshirje. Gjithashtu, të dhënat mjekësore, të cilat përpunohen në mënyrë të ligjshme nga stafi i shërbimit shëndetësor, mund t'u transferohen autoriteteve të zbatimit të ligjit vetëm "kur ekzistojnë garancitë e mjaftueshme për të parandaluar çdo mundësi përhapjeje që bie ndesh me respektimin e [...] jetës private, të sanksionuar në nenin 8 të KEDNj-së".[307]

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 anonimizim 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 pikën 2.1.3.

[305] Shih gjithashtu, *Biriuk kundër Lituanisë*, nr. 23373/03, 25 nëntor 2008

[306] KiE, Komiteti i Ministrave (1997), Rekomandimi Rec(97)5 drejtuar shteteve anëtare në lidhje me mbrojtjen e të dhënave mjekësore, 13 shkurt 1997.

[307] GjEDNj, nr. 1585/09, *Avilkina dhe të Tjerët kundër Rusisë,* nr. 1585/09, 6 qershor 2013, parag. 53 (jo përfundimtar.

Janë zhvilluar diskutime të thella, në nivel kombëtar dhe evropian, sa i takon iniciativave që synojnë të regjistrojnë të dhëna në lidhje me trajtimin mjekësor të një pacienti në një kartelë shëndetësore elektronike.[308] Një aspekt i veçantë i ekzistencës së këtyre sistemeve mbarëkombëtare të kartelave shëndetësore elektronike është disponueshmëria e tyre përtej kufijve: çështje me interes të veçantë brenda BE-së, në kontekstin e kujdesit shëndetësor ndërkufitar.[309]

Një fushë tjetër e cila është duke u diskutuar me qëllim hartimin e dispozitave të reja, është ajo e testeve klinike, me fjalë të tjera testimi i ilaçeve të reja tek pacientët, në një ambient kërkimor të dokumentuar; edhe kjo fushë krijon problematika të mëdha për mbrojtjen e të dhënave. Testet klinike për produktet mjekësore për përdorim njerëzor, rregullohen me Direktivën 2001/20/EC të Parlamentit Evropian dhe Këshillit, datë 4 prill 2001, për përafrimin e legjislacionit, rregulloreve dhe dispozitave administrative të Shteteve Anëtare në lidhje me zbatimin e praktikave të mira klinike gjatë kryerjes së testeve klinike të medikamenteve për përdorim njerëzor (*Direktiva e Testeve Klinike*).[310] Në dhjetor 2012, Komisioni Evropian propozoi një rregullore për zëvendësimin e Direktivës së Testeve Klinike, me qëllimin që t'i bënte procedurat e testeve më të unifikuara dhe më të efektshme.[311]

Ekzistojnë shumë iniciativa ligjore dhe të tjera ende në proces vlerësimi në nivel BE-je, të cilat kanë të bëjnë të dhënat personale në sektorin shëndetësor.[312]

8.4. Përpunimi i të dhënave për qëllime statistikore

Pikat kryesore

- Të dhënat e mbledhura për qëllime statistikore nuk mund të përdoren për asnjë lloj qëllimi tjetër.

- Të dhënat e mbledhura në mënyrë legjitime për çdo lloj qëllim tjetër, mund të përdoren më tej për qëllime statistikore, me kusht që legjislacioni kombëtar të parashikojë garanci të përshtatshme të cilat duhen respektuar nga përdoruesit. Për këtë qëllim, duhen parashikuar në mënyrë të veçantë anonimizimi ose pseudonimizimi i të dhënave, përpara transmetimit të tyre tek palët e treta.

---

[308] Grupi i Punës së Nenit 29 (2007), Dokument pune mbi përpunimin e të dhënave personale në lidhje me shëndetin në kartela shëndetësore elektronike (EHR), WP 131, Bruksel, 15 shkurt 2007.
[309] Direktiva 2011/24/EU e Parlamentit Evropian dhe e Këshillit, datë 9 mars 2011 në lidhje me zbatimin e të drejtave të pacientëve në fushën e kujdesit shëndetësor ndërkufitar, JO 2011 L 88.
[310] Direktiva 2001/20/EC e Parlamentit Evropian dhe e Këshillit, datë 4 prill 2001 në lidhje me përafrimin e legjislacionit, rregulloreve dhe dispozitave administrative të Shteteve Anëtare, në lidhje me zbatimin e praktikave të mira klinike gjatë kryerjes së testeve klinike të medikamenteve për përdorim njerëzor, JO 2001 L 121.
[311] Komisioni Evropian (2012), *Propozim për një Rregullore të Parlamentit Evropian dhe Këshillit në lidhje me testet klinike të medikamenteve për përdorim njerëzor, që shfuqizon Direktivën 2001/20/EC*, COM(2012) 369 përfundimtar, Bruksel, 17 korrik 2012.
[312] EDPS (2013), *Opinion i Mbikëqyrësit Evropian të Mbrojtjes së të Dhënave mbi Komunikatën e Komisionit në lidhje me "Planin e Veprimit eShëndeti 2012-2020 – Kujdesi Shëndetësor Inovativ për shekullin e 21-të", Bruksel, 27 mars 2013.*

Tek Direktiva e Mbrojtjes së të Dhënave, përpunimi i të dhënave për qëllime statistikore përmendet në kontekstin e përjashtimeve të mundshme nga parimet e mbrojtjes së të dhënave. Në nenin 6 (1) (b) të Direktivës, legjislacioni kombëtar mund të shmanget parimi i kufizimit të qëllimit për të lejuar përdorimin e mëtejshëm të të dhënave për qëllime statistikore, por legjislacioni i brendshëm duhet të përcaktojë gjithashtu edhe të gjitha garancitë e nevojshme. Neni 13 (2) i Direktivës lejon kufizimet e të drejtave për akses nga ana e legjislacionit kombëtar, nëse të dhënat përpunohen vetëm për qëllime statistikore; edhe këtu, legjislacioni kombëtar duhet të përcaktojë garancitë e përshtatshme. Në këtë kontekst, Direktiva e Mbrojtjes së të Dhënave përcakton një kriter specifik, sipas së cilit asnjë nga të dhënat e përftuara apo krijuara gjatë kërkimeve statistikore, nuk mund të përdoret për vendime konkrete në lidhje me subjektet e të dhënave.

Edhe pse të dhënat të cilat janë mbledhur në mënyrë të ligjshme nga një kontrollues për çfarëdo qëllimi, mund të përdoren sërish nga kontrolluesi për qëllimet e tij statistikore – të ashtuquajturat statistika sekondare – të dhënat duhet të anonimizohen ose pseudonimizohen, në varësi të kontekstit, përpara se t'i transmetohen një pale të tretë për qëllime statistikore, përveç rastit kur subjekti i të dhënave ka dhënë pëlqimin për të apo parashikohet në mënyrë specifike nga legjislacioni kombëtar. Diçka e tillë rrjedh nga kriteri për garanci të mjaftueshme të nenit 6 (1) (b) të Direktivës së Mbrojtjes së të Dhënave.

Rastet më të rëndësishme të përdorimit të të dhënave për qëllime statistikore janë statistikat zyrtare, që kryhen nga zyrat kombëtare të statistikave dhe të BE-së, mbështetur në legjislacionin kombëtar dhe evropian të statistikave zyrtare. Sipas këtyre dispozitave, qytetarët dhe bizneset janë zakonisht të detyruar t'u komunikojnë të dhëna autoriteteve të statistikave. Zyrtarët të cilët punojnë në zyrat e statistikave i nënshtrohen detyrimeve speciale të sekretit profesional, të cilat respektohen në mënyrë të kujdesshme, duke qenë se janë thelbësore për nivelin e besimit të qytetarëve, i cili është i domosdoshëm në mënyrë që të dhënat t'u vihen në dispozicion autoriteteve të statistikave.

Rregullorja (EC) nr. 223/2009 e Statistikave Evropiane (Rregullorja e Statistikave Evropiane) përmban rregullat thelbësore për mbrojtjen e të dhënave në statistikat zyrtare dhe për rrjedhojë, mund të konsiderohet e rëndësishme për dispozitat në lidhje me statistikat zyrtare në nivel kombëtar.[313] Rregullorja thekson parimin se të gjitha operacionet e statistikave zyrtare duhet të shoqërohen me një bazë ligjore mjaft të saktë.[314]

---

[313] Rregullorja (EC) nr. 223/2009 e Parlamentit Evropian dhe e Këshillit, datë 11 mars 2009 në lidhje me statistikat evropiane, që shfuqizon Rregulloren (EC, Euratom) nr. 1101/2008 të Parlamentit Evropian dhe Këshillit në lidhje me transmetimin tek Instituti i Statistikave të Komunitetit Evropian të të dhënave statistikore të mbrojtura nga sekreti, Rregulloren e Këshillit (EC) nr. 322/97 në lidhje me Statistikat e Komunitetit dhe Vendimin e Këshillit 89/382/EEC, Euratom, që themelon një Komitet të Programeve Statistikore të Komunitetit Evropian, JO 2009 L 87.

[314] Ky parim duhet detajuar më tej në Kodin e Sjelljes së Eurostat-it, i cili në përputhje, me nenin 11 të Rregullores së Statistikave Evropiane, duhet të udhëzojë në lidhje me mënyrën e realizimit të statistikave zyrtare, përfshirë përdorimin e kujdesshëm të të dhënave personale, i cili mund të gjendet tek: http://epp.eurostat.ec.europa.eu/ portal/page/portal/about_eurostat/introduction.

Shembull: tek çështja *Huber kundër Gjermanisë,*[315] GjDBE-ja u shpreh se mbledhja dhe ruajtja e të dhënave personale nga ana e një autoriteti, për qëllime statistikore, nuk ishte në vetvete një arsye e mjaftueshme që përpunimi të konsiderohet i ligjshëm. Legjislacioni i cili parashikon përpunimin e të dhënave personale, duhet gjithashtu të respektojë kriterin e domosdoshmërisë, çka nuk ishte rasti në kontekstin e dhënë.

Në kontekstin e KiE-së, Rekomandimi i të Dhënave Statistikore i cili është miratuar në 1997-ën, mbulon kryerjen e statistikave në sektorët privatë dhe publikë.[316] Ky rekomandim përfshin parimet të cilat përkojnë me normat kryesore të Direktivës së Mbrojtjes së të Dhënave të përshkruara më lart. Parashikohen norma më të detajuara për çështjet në vijim.

Ndërkohë që të dhënat të cilat janë mbledhur nga kontrolluesi për qëllime statistikore, nuk mund të përdoren për asnjë lloj qëllimi tjetër, të dhënat të cilat janë mbledhur për qëllime jo statistikore, duhet të jenë të disponueshme për përdorim të mëtejshëm për qëllime statistikore. Rekomandimi i të Dhënave Statistikore autorizon gjithashtu komunikimin e të dhënave drejt palëve të treta, nëse nevojitet, 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 të statistikave. Duke qenë se këto formalitete nuk mund të zëvendësojë pëlqimin e subjektit të të dhënave, në legjislacionin kombëtar duhen përcaktuar garanci shtesë të mjaftueshme, për të zvogëluar riskun e keqpërdorimit të të dhënave personale, si për shembull detyrimin për të anonimizuar apo pseudonimizuar të dhënat përpara transmetimit.

Profesionistët përgjegjës për hulumtimet statistikore, duhet t'i nënshtrohen kritereve speciale të sekretit profesional – sikundër funksionon për statistikat zyrtare – sipas legjislacionit kombëtar. Ky kriter duhet të shtrihet edhe tek intervistuesit, nëse ata janë punësuar për mbledhjen e të dhënave nga subjektet e të dhënave apo nga personat e 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 ose jo i të dhënave, është i detyrueshëm sipas legjislacioni kombëtar. Të dhënat sensitive nuk duhen mbledhur kurrë në mënyrë të tillë që ta bëjnë individin të identifikueshëm, përveç rastit kur është e parashikuar nga legjislacioni kombëtar.

Nëse një pyetësor statistikor nuk mund të kryhet me të dhëna të anonimizuara dhe të dhënat personale janë vërtet të domosdoshme, atëherë të dhënat e mbledhura për këtë qëllim, duhet të anonimizohen sa me shpejt të jetë e mundur. Rezultatet e pyetësorëve statistikorë, së paku nuk duhet të mundësojnë identifikimin e asnjë subjekti të dhënash, përveçse kur diçka e tillë qartazi nuk përbën asnjë rrezik.

[315] GjDBE, C-524/06, *Huber kundër Gjermanisë,* 16 dhjetor 2008; shih veçanërisht parag. 68.
[316] Këshilli i Evropës, Komiteti i Ministrave (1997), Rekomandimi Rec(97)18 drejtuar shteteve anëtare në lidhje me mbrojtjen e të dhënave personale të mbledhura dhe përpunuara për qëllime statistikore, 30 shtator 1997.

Pas kryerjes së analizës statistikore, të dhënat personale duhet ose të fshihen ose të anonimizohen. Në këtë rast, Rekomandimi i të Dhënave Statistikore sugjeron që të dhënat identifikuese të ruhen veçmas nga të dhënat e tjera personale. Kjo nënkupton, për shembull, se të dhënat duhen pseudonimizuar dhe si çelësi i enkriptimit, ashtu edhe lista me sinonimet identifikuese, duhet të ruhen në një vend të të ndryshëm nga ai i të dhënave të pseudonimizuara.

8.5. Të dhënat financiare

Pikat kryesore

- Megjithëse të dhënat financiare nuk janë të dhëna sensitive në kuptimin e Konventës 108, apo të Direktivës së Mbrojtjes së të Dhënave, për përpunimin e tyre duhen marrë masa të veçanta, me qëllim të të garantohet saktësi dhe siguri e të dhënave.
- Sistemet elektronike të pagesave kanë nevojë për mbrojtje të integruar të të dhënave, të ashtuquajturën "respektim të privatësisë që nga konceptimi" (*Privacy by design*).
- Në këtë fushë shfaqen problematika të veçanta të mbrojtjes së të dhënave, të cilat burojnë nga nevoja për të pasur mekanizma të përshtatshëm autentifikimi.

Shembull: tek çështja *Michaud kundër Francës*,[317] ankuesi, një avokat francez, kundërshtoi detyrimin që kishte sipas legjislacionit francez, që të sinjalizonte dyshimet në lidhje me aktivitetet e mundshme të pastrimit të parave nga klientët e tij. GjEDNj-ja vërejti se duke i kërkuar avokatëve të sinjalizonin tek autoritetet administrative, informacione në lidhje me një person tjetër, për të cilat vihen në dijeni nëpërmjet komunikimit me atë person, përbënte një cënim të së drejtës së avokatëve për respektim të korrespondencës dhe jetës së tyre private, sipas nenit 8 të KEDNj-së, duke qenë se ai koncept përfshinte aktivitetet me natyrë profesionale apo tregtare. Gjithsesi, ndërhyrja ishte në përputhje me ligjin dhe synonte përmbushjen e një qëllimi legjitim, konkretisht mbrojtjen e rendit dhe parandalimin e veprave penale. Meqenëse avokatët ishin subjekt i detyrimit për të raportuar dyshime vetëm në rrethana tepër të kufizuara, GjEDNj-ja vendosi se ky detyrim ishte proporcional dhe se nuk ishte shkelur neni 8.

Me anë të Rekomandimit Rec(90)19 të 1990-ës, KiE-ja propozoi zbatimin e kuadrit ligjor të përgjithshëm në fushën e mbrojtjes së të dhënave të Konventës 108 në kontekstin e pagesave.[318] 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 u propozon gjithashtu ligjvënësve të brendshëm rregullore të detajuara në lidhje me kufijtë e komunikimit të të dhënave të pagesave tek palët e treta, kufijtë kohorë për ruajtjen e të dhënave, transparencën, sigurinë e të dhënave dhe qarkullimet ndërkufitare të të dhënave dhe në fund edhe në lidhje me mbikëqyrjen dhe ankimin. Zgjidhjet e propozuara përkojnë me ato çka u përcaktuan më pas, në mënyrë të përgjithshme, në nivel BE-je, tek Direktiva e Mbrojtjes së të Dhënave.

---

[317] GjEDNj, *Michaud kundër Francës*, nr. 12323/11, 6 dhjetor 2012; shih gjithashtu GjEDNj, *Niemietz kundër Gjermanisë*, nr. 13710/88, 16 dhjetor 1992, parag. 29, dhe GjEDNj, *Halford kundër Mbretërisë së Bashkuar*, nr. 20605/92, 25 qershor 1997, parag. 42.

[318] KiE, Komiteti i Ministrave (1990), Rekomandimi nr. R(90)19 për mbrojtjen e të dhënave personale të përdorura për pagesa dhe operacione të tjera në lidhje me to, 13 shtator 1990.

Një sërë instrumentesh ligjore janë duke u hartuar, me qëllim rregullimin e tregjeve të instrumenteve financiare si dhe të aktiviteteve të institucioneve të kreditimit dhe ndërmarrjeve të investimeve,[319] ndërsa instrumente të tjera ligjore japin kontribut për aktivitetet e luftës kundër abuzimit me informacionin tregtar dhe manipulimit të tregut.[320] Problematikat më kritike në këto fusha, të cilat kanë ndikim në mbrojtjen e të dhënave janë:

- Ruajtja 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, Shteteve Anëtare dhe Autoritetit Evropian të Tregjeve Financiare (ESMA).

Ekzistojnë gjithashtu problematika të tjera në këto fusha, të cilat janë trajtuar në mënyrë të posaçme, përfshirë mbledhjen e të dhënave në lidhje me gjendjen financiare të subjekteve të të dhënave[321] apo pagesave ndërkufitare nëpërmjet transfertave bankare, të cilat pashmangshmërisht përfshijnë qarkullime të të dhënave personale.[322]

---

[319] Komisioni Evropian (2011), *Propozim për një Direktivë të Parlamentit Evropian dhe Këshillit për tregjet e instrumenteve financiare, që shfuqizon Direktivën 2004/39/EC të Parlamentit Evropian dhe Këshillit*, COM(2011) 656 përfundimtar, Bruksel, 20 tetor 2011; Komisioni Evropian (2011), *Propozim për një Rregullore të Parlamentit Evropian dhe Këshillit për tregjet e instrumenteve financiare, që ndryshon Rregulloren [EMIR] mbi instrumentet financiare derivate OTC, palëve qendrore dhe regjistrave qendrorë të transaksioneve*, COM(2011) 652 përfundimtar, Bruksel, 20 tetor 2011; Komisioni Evropian (2011), *Propozim për një Direktivë të Parlamentit Evropian dhe Këshillit në lidhje me aksesin në aktivitetin e institucioneve të kreditimit dhe mbikëqyrjes së kujdesshme të institucioneve të kreditimit dhe ndërmarrjeve të investimeve, që ndryshon Direktivën 2002/87/EC të Parlamentit Evropian dhe Këshillit në lidhje me mbikëqyrjen plotësuese të institucioneve të kreditimit, ndërmarrjeve të sigurimeve dhe ndërmarrjeve të investimeve në një konglomerat financiar*, COM(2011) 453 përfundimtar, Bruksel, 20 korrik 2011.

[320] Komisioni Evropian (2011), *Propozim për një Rregullore të Parlamentit Evropian dhe Këshillit në lidhje me abuzimin me informacionin tregtar dhe manipulimin e tregut (abuzimin me tregun)*, COM(2011) 651 përfundimtar, Bruksel, 20 tetor 2011; Komisioni Evropian (2011), *Propozim për një Direktivë të Parlamentit Evropian dhe Këshillit në lidhje me sanksionet penale për abuzimin me informacionin tregtar dhe manipulimin e tregut*, COM(2011) 654 përfundimtar, Bruksel, 20 tetor 2011.

[321] Rregullorja (EC) nr. 1060/2009 e Parlamentit Evropian dhe Këshillit, datë 16 shtator 2009 në lidhje me agjencitë e klasifikimit të kredive, JO 2009 L 302; Parlamenti Evropian, *Propozim për një Rregullore të Parlamentit Evropian dhe Këshillit për ndryshimin e Rregullores (EC) nr. 1060/2009 në lidhje me agjencitë e klasifikimit të kredive*, COM(2010) 289 përfundimtar, Bruksel, 2 qershor 2010.

[322] Direktiva 2007/64/EC e Parlamentit Evropian dhe Këshillit, datë 13 nëntor 2007 në lidhje me shërbimet e pagesave në tregun e brendshëm, që ndryshon Direktivat 97/7/EC, 2002/65/EC, 2005/60/EC dhe 2006/48/EC dhe shfuqizon Direktivën 97/5/EC, JO 2007 L 319.

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*, Vienna, Manzsche Verlags- und Universitätsbuchhandlung.

EDRi, *An introduction to data protection*, Brussels, www.edri.org/files/ paper06_datap.pdf.

Frowein, J. and 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. and Bates, E. (2009), Law of the European Convention on Human Rights, Oxford, Oxford University Press.

Jarass, H. (2010), Charta der Grundrechte der Europäischen Union, Munich, 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*, Oxford, 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*, Brussels, Emile Bruylant.

Simitis, S. (1997), 'Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?', *Neue Juristische Wochenschrift*, No. 5, pp. 281–288.

Warren, S. and Brandeis, L. (1890), 'The right to privacy', *Harvard Law Review*, Vol. 4, No. 5, pp. 193–220, http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. and Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Kapitulli 2

Carey, P. (2009), Data protection: *A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

Morgan, R. and Boardman, R. (2012*), Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell.

Ohm, P. (2010), 'Broken promises of privacy: Responding to the surprising failure of anonymization', *UCLA Law Review*, Vol. 57, No. 6, pp. 1701–1777.

Tinnefeld, M., Buchner, B. and Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Munich, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), Anonymisation: *managing data protection risk. Code of practice*, www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

Kapitujt nga 3 deri 5

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, Munich, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrucken, Éditions universitaires européennes.

Dammann, U. and Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (European Union Agency for Fundamental Rights) (2010), *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxembourg, 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), Vienna, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxembourg, Publications Office.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*, www.ico.org.uk/for_organisations/data_protection/topic_guides/ privacy_impact_assessment.

Kapitulli 6

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. and Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

Kapitulli 7

Europol (2012), *Data Protection at Europol*, Luxembourg, Publications Office, www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, The Hague, Eurojust.

Drewer, D. and Ellermann, J. (2012), *Europol's data protection framework as an asset in the fight against cybercrime*, ERA Forum, Vol. 13, No. 3, pp. 381–395.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, 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, No. 5, pp. 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 Working Papers 2013/2, www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

Kapitulli 8

Büllesbach, A., Gijrath, S., Poullet, Y. and Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

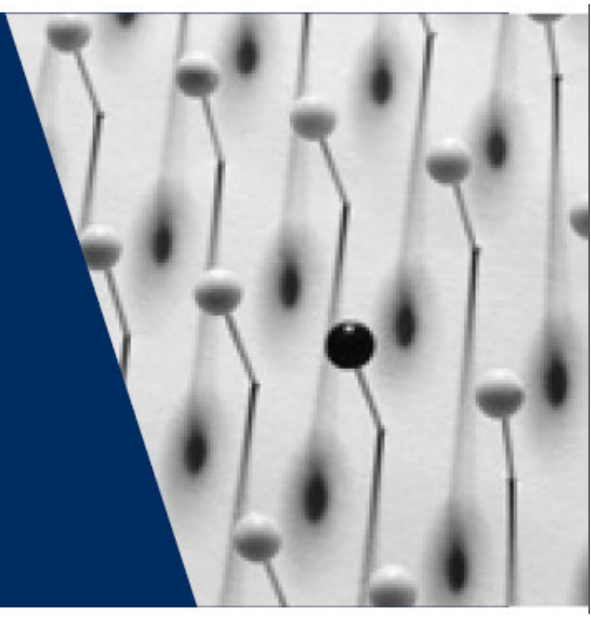
Gutwirth, S., Leenes, R., De Hert, P. and Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, 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, No. 5, pp. 722–776.

Rosemary, J. and Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.



Jurisprudenca

Jurisprudenca e Gjykatës Evropiane të të Drejtave të Njeriut

Aksesi në të dhënat personale

Gaskin kundër Mbretërisë së Bashkuar, nr. 10454/83, 7 korrik 1989
Godelli kundër Italisë, nr. 33783/09, 25 shtator 2012
K.H. dhe të Tjerët kundër Sllovakisë, nr. 32881/04, 28 prill 2009
Leander kundër Suedisë, nr. 9248/81, 26 mars 1987
Odièvre kundër Francës [GC], nr. 42326/98, 13 shkurt 2003

Ekuilibrimi i mbrojtjes së të dhënave me lirinë e shprehjes

Axel Springer AG kundër Gjermanisë [GC], nr. 39954/08, 7 shkurt 2012
Von Hannover kundër Gjermanisë, nr. 59320/00, 24 qershor 2004
Von Hannover kundër Gjermanisë (nr. 2) [GC], nr. 40660/08 dhe 60641/08, 7 shkurt 2012

Sfidat e mbrojtjes së të dhënave në internet

K.U. kundër Finlandës, nr. 2872/02, 2 dhjetor 2008.

Korrespondenca

Amann kundër Zvicrës [GC], nr. 27798/95, 16 shkurt 2000
Bernh Larsen Holding AS dhe të Tjerët kundër Norvegjisë, nr. 24117/08, 14 mars 2013
Cemalettin Canli kundër Turqisë, nr. 22427/04, 18 nëntor 2008
Dalea kundër Francës, nr. 964/07, 2 shkurt 2010
Gaskin kundër Mbretërisë së Bashkuar, nr. 10454/83, 7 korrik 1989
Haralambie kundër Rumanisë, nr. 21737/03, 27 tetor 2009
Khelili kundër Zvicrës, nr. 16188/07, 18 tetor 2011
Leander kundër Suedisë, nr. 9248/81, 26 mars 1987
Malone kundër Mbretërisë së Bashkuar, nr. 8691/79, 2 gusht 1984
McMichael kundër Mbretërisë së Bashkuar, nr. 16424/90, 24 shkurt 1995
M.G. kundër Mbretërisë së Bashkuar, nr. 39393/98, 24 shtator 2002
Rotaru kundër Rumanisë [GC], nr. 28341/95, 4 maj 2000
S. and Marper kundër Mbretërisë së Bashkuar, nr. 30562/04 dhe 30566/04, 4 dhjetor 2008
Shimovolos kundër Rusisë, nr. 30194/09, 21 qershor 2011

Turek kundër Sllovakisë, nr. 57986/00, 14 shkurt 2006

Bazat e të dhënave të dosjeve penale

B.B. kundër Francës, nr. 5335/06, 17 dhjetor 2009
M.M. kundër Mbretërisë së Bashkuar, nr. 24029/07, 13 nëntor 2012

Bazat e të dhënave të ADN-së

S. dhe Marper kundër Mbretërisë së Bashkuar, nr. 30562/04 dhe 30566/04, 4 dhjetor 2008.

Të dhënat e GPS-së

Uzun kundër Gjermanisë, nr. 35623/05, 2 shtator 2010

Të dhënat e shëndetit

Biriuk kundër Lituanisë, nr. 23373/03, 25 nëntor 2008
I. kundër Finlandës, nr. 20511/03, 17 korrik 2008
L.L. kundër Francës, nr. 7508/02, 10 tetor 2006
M.S. kundër Suedisë, nr. 20837/92, 27 gusht 1997
Szuluk kundër Mbretërisë së Bashkuar, nr. 36936/05, 2 qershor 2009
Z. kundër Finlandës, nr. 22009/93, 25 shkurt 1997

Identiteti

Ciubotaru kundër Moldavisë, nr. 27138/04, 27 prill 2010
Godelli kundër Italisë, nr. 33783/09, 25 shtator 2012
Odièvre kundër Francës [GC], nr. 42326/98, 13 shkurt 2003

Informacioni në lidhje me aktivitetet profesionale

Michaud kundër Francës, nr. 12323/11, 6 dhjetor 2012
Niemietz kundër Gjermanisë, nr. 13710/88, 16 dhjetor 1992

Interceptimi i komunikimeve

Amann kundër Zvicrës [GC], nr. 27798/95, 16 shkurt 2000
Copland kundër Mbretërisë së Bashkuar, nr. 62617/00, 3 prill 2007
Cotlet kundër Rumanisë, nr. 38565/97, 3 qershor 2003
Kruslin kundër Francës, nr. 11801/85, 24 prill 1990
Lambert kundër Francës, nr. 23618/94, 24 gusht 1998
Liberty dhe të Tjerët kundër Mbretërisë së Bashkuar, nr. 58243/00, 1 korrik 2008
Malone kundër Mbretërisë së Bashkuar, nr. 8691/79, 2 gusht 1984
Halford kundër Mbretërisë së Bashkuar, nr. 20605/92, 25 qershor 1997
Szuluk kundër Mbretërisë së Bashkuar, nr. 36936/05, 2 qershor 2009

Detyrimet e subjekteve të interesuara

B.B. kundër Francës, nr. 5335/06, 17 dhjetor 2009
I. kundër Finlandës, nr. 20511/03, 17 korrik 2008
Mosley kundër Mbretërisë së Bashkuar, nr. 48009/08, 10 maj 2011

Fotografitë

Sciacca kundër Italisë, nr. 50774/99, 11 janar 2005
Von Hannover kundër Gjermanisë, nr. 59320/00, 24 qershor 2004

E drejta për t'u harruar

Segerstedt-Wiberg dhe të Tjerët kundër Suedisë, nr. 62332/00, 6 qershor 2006

E drejta për të kundërshtuar

Leander kundër Suedisë, nr. 9248/81, 26 mars 1987
Mosley kundër Mbretërisë së Bashkuar, nr. 48009/08, 10 maj 2011
M.S. kundër Suedisë, nr. 20837/92, 27 gusht 1997
Rotaru kundër Rumanisë [GC], nr. 28341/95, 4 maj 2000

Kategoritë sensitive të të dhënave

I. kundër Finlandës, nr. 20511/03, 17 korrik 2008
Michaud kundër Francës, nr. 12323/11, 6 dhjetor 2012
S. dhe Marper kundër Mbretërisë së Bashkuar, nr. 30562/04 dhe 30566/04, 4 dhjetor 2008

Mbikëqyrja dhe zbatimi i ligjit (roli i aktorëve të ndryshëm, përfshirë autoritetet e mbrojtjes së të dhënave)

I. kundër Finlandës, nr. 20511/03, 17 korrik 2008
K.U. kundër Finlandës, nr. 2872/02, 2 dhjetor 2008
Von Hannover kundër Gjermanisë, nr. 59320/00, 24 qershor 2004
Von Hannover kundër Gjermanisë (nr. 2) [GC], nr. 40660/08 dhe 60641/08, 7 shkurt 2012

Metodat e survejimit

Allan kundër Mbretërisë së Bashkuar, nr. 48539/99, 5 nëntor 2002
Association "21 Décembre 1989" dhe të Tjerët kundër Rumanisë, nr. 33810/07 dhe 18817/08, 24 maj 2011
Bykov kundër Rusisë [GC], nr. 4378/02, 10 mars 2009
Kennedy kundër Mbretërisë së Bashkuar, nr. 26839/05, 18 maj 2010
Klass dhe të Tjerët kundër Gjermanisë, nr. 5029/71, 6 shtator 1978
Rotaru kundër Rumanisë [GC], nr. 28341/95, 4 maj 2000
Taylor-Sabori kundër Mbretërisë së Bashkuar, nr. 47114/99, 22 tetor 2002
Uzun kundër Gjermanisë, nr. 35623/05, 2 shtator 2010
Vetter kundër Francës, nr. 59842/00, 31 maj 2005

Video-survejimi

Köpke kundër Gjermanisë, nr. 420/07, 5 tetor 2010
Peck kundër Mbretërisë së Bashkuar, nr. 44647/98, 28 janar 2003

Kampionët vokalë

P.G. dhe J.H. kundër Mbretërisë së Bashkuar, nr. 44787/98, 25 shtator 2001
Wisse kundër Francës, nr. 71611/01, 20 dhjetor 2005

Jurisprudenca e Gjykatës së Drejtësisë së Bashkimit Evropian

Jurisprudenca në lidhje me Direktivën e Mbrojtjes së të Dhënave

C-73/07, *Tietosuojavaltuutettu kundër Satakunnan Markkinapörssi Oy dhe Satamedia Oy*, 16 dhjetor 2008
[Koncepti i 'aktiviteteve gazetareske' sipas kuptimit të nenit 9 të Direktivës së Mbrojtjes së të Dhënave]

Çështje të bashkuara C-92/09 dhe C-93/09, *Volker dhe Markus Schecke GbR dhe Hartmut Eifert kundër Land Hessen-it*, 9 nëntor 2010
[Proporcionaliteti i kriterit ligjor për të publikuar të dhëna personale në lidhje me përfituesit e disa fondeve bujqësore të BE-së]

C-101/01, *Bodil Lindqvist*, 6 nëntor 2003
[Legjitimiteti i publikimit të të dhënave nga një person privat në lidhje me jetën private të të tjerëve në internet]

C-131/12, *Google Spain, S.L., Google Inc. kundër Agencia Española de Protección de Datos, Mario Costeja González*, Referuar për vendim paraprak nga Audiencia Nacional (Spain) depozituar më 9 mars 2012, 25 maj 2012, në pritje për t'u shqyrtuar
[Detyrimet e operatorëve të motorrëve të kërkimit, që me kërkesë të subjektit të të dhënave, të mos shfaqin të dhëna personale në rezultatet e kërkimit]

C-270/11, *Komisioni Evropian kundër Mbretërisë së Suedisë*, 30 maj 2013
[Gjobë për moszbatimin e Direktivës]

C-275/06, *Productores de Música de España (Promusicae) kundër Telefónica de España SAU*, 29 janar 2008
[Detyrimi i operatorëve të aksesit në internet për të komunikuar identitetet e përdoruesve të programi të shkëmbimit të skedarëve elektronikë KaZaA, shoqatës për mbrojtjen e pronësisë intelektuale]

C-288/12, *Komisioni Evropian kundër Hungarisë*, 8 prill 2014
[Legjitimiteti i shkarkimit të komisionierit të autoritetit kombëtar mbikëqyrës për mbrojtjen e të dhënave]

C-291/12, *Michael Schwarz kundër Stadt Bochum*, Opinion i Avokatit të Përgjithshëm, 13 qershor 2013
[Shkelje e legjislacionit parësor të BE-së nga ana e Rregullores (EC) 2252/2004 e cila përcakton se gjurmët e gishtave duhen regjistruar në pasaporta]

Çështje të bashkuara C-293/12 dhe C-594/12, *Digital Rights Ireland dhe Seitling dhe të Tjerët kundër Irlandës*, 8 prill 2014
[Shkelje e legjislacionit parësor të BE-së nga ana e Direktivës së Ruajtjes së të Dhënave]

C-360/10, *SABAM kundër Netlog N.V.*, 16 shkurt 2012
[Detyrimi i operatorëve të rrjeteve sociale për të parandaluar shfrytëzim të paligjshëm të punimeve muzikore dhe audi-vizive nga përdoruesit e rrjeteve]

Çështje të bashkuara C-465/00, C-138/01 dhe C-139/01, *Rechnungshof kundër Österreichischer Rundfunk dhe të Tjerët dhe Neukomm dhe Lauermann kundër Österreichischer Rundfunk,* 20 maj 2003
[Proporcionaliteti i detyrimit ligjor për të publikuar të dhëna personale në lidhje me nëpunësit e disa kategorive të institucioneve të sektorit publik]

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) kundër Administración del Estado*, 24 nëntor 2011
[Zbatimi në mënyrën e duhur të nenit 7 (f) të Direktivës së Mbrojtjes së të Dhënave – "interesat legjitimë të të tjerëve" – në legjislacionin kombëtar]

C-518/07, *Komisioni Evropian kundër Republikës Federale të Gjermanisë*, 9 mars 2010
[Pavarësia e autoritetit mbikëqyrës kombëtar]

C-524/06, *Huber kundër Bundesrepublik Deutschland*, 16 dhjetor 2008
[Legjitimiteti i mbajtjes së të dhënave të shtetasve të huaj në një regjistër statistikor]

C-543/09, *Deutsche Telekom AG kundër Bundesrepublik Deutschland*, 5 maj 2011
[Domosdoshmëria e ripërtëritjes së pëlqimit]

C-553/07, *College van burgemeester en wethouders van Rotterdam kundër M.E.E. Rijkeboer*, 7 maj 2009
[E drejta e subjektit të të dhënave për akses]

C-614/10, *Komisioni Evropian kundër Republikës së Austrisë*, 16 tetor 2012
[Pavarësia e autoritetit mbikëqyrës kombëtar]

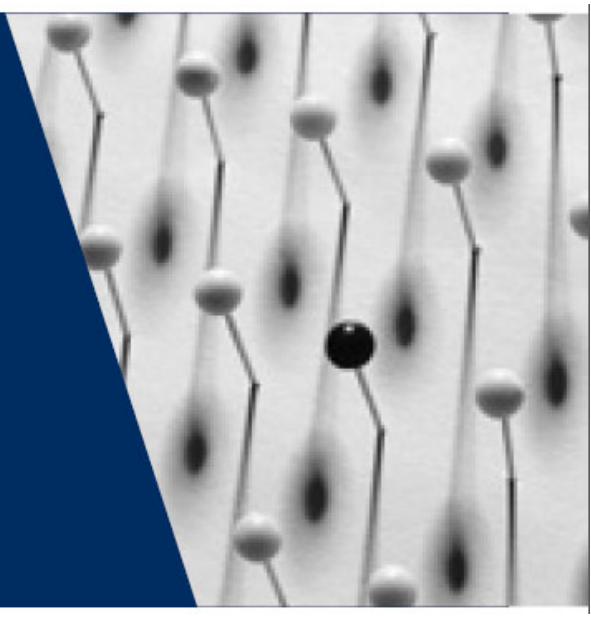
Jurisprudenca në lidhje me Rregulloren e Mbrojtjes së të Dhënave të Institucioneve të BE-së

C-28/08 P, *Komisioni Evropian kundër The Bavarian Lager Co. Ltd.*, 29 qershor 2010
[Aksesi në dokumente]

C-41/00 P, *Interporc Im- und Export GmbH kundër Komisionit të Komunitetit Evropian*, 6 mars 2003
[Aksesi në dokumente]

F-35/08, *Dimitrios Pachtitis kundër Komisionit Evropian*, 15 qershor 2010
[Përdorimi i të dhënave personale në kontekstin e punësimit në institucionet e BE-së]

F-46/09, *V kundër Parlamentit Evropian*, 5 korrik 2011
[Përdorimi i të dhënave personale në kontekstin e punësimit në institucionet e BE-së]



Indeksi

Jurisprudenca e Gjykatës së Drejtësisë së Bashkimit Evropian

Jurisprudenca e Gjykatës Evropiane të të Drejtave të Njeriut

Jurisprudenca e gjykatave kombëtare

Agjencia e Bashkimit Evropian për të Drejtat Themelore
Këshilli i Evropës – Gjykata Evropiane e të Drejtave të Njeriut

Manual i së Drejtës Evropiane në Fushën e Mbrojtjes së të Dhënave

2014 — 199 pp. — 14.8 × 21 cm

ISBN 978-92-871-9934-8 (CoE)
ISBN 978-92-9239-461-5 (FRA)
doi:10.2811/69915

Shumë informacione në lidhje me Agjencinë e Bashkimit Evropian për të Drejtat Themelore mund të gjendet në internet, nëpërmjet faqes zyrtare të FRA-së: fra.europa.eu.

Më shumë informacion në lidhje me Këshillin e Evropës mund të gjendet në internet në adresën hub.coe.int.

Informacion të mëtejshëm në lidhje me Gjykatën Evropiane të të Drejtave të Njeriut mund të gjendet në faqen zyrtare të Gjykatës: ecur.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.

10.2811/69915
TK-04-14-319-EN-C

Zhvillimi i shpejtë i teknologjive të informacionit dhe të komunikimit thekson nevojën në rritje për një mbrojtje solide 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). Zhvillimet teknologjike zgjerojnë kufijtë e survejimit, përgjimit të komunikimeve dhe ruajtjes së të dhënave; të gjitha këto përbëjnë sfida të mëdha për të drejtën për mbrojtje të të dhënave. Ky manual është konceptuar në mënyrë të tillë që juristët, të cilët nuk janë të specializuar në fushën e mbrojtjes së të dhënave, të informohen në lidhje me këtë fushë të së drejtës. Ai ofron një sintezë të kuadrit ligjor të zbatueshëm për BE-në dhe KiE-në. Ai shpjegon jurisprudencën më të rëndësishme, duke përmbledhur vendimet kryesore, si të Gjykatës Evropiane të të Drejtave të Njeriut (GjEDNj), ashtu edhe të Gjykatës së Drejtësisë së Bashkimit Evropian (GjDBE). Në rastet kur një jurisprudencë e tillë nuk ekziston, ai paraqet shembuj praktikë me skenarë hipotetikë. Thënë shkurt, ky manual synon të garantojë respektim të vendosur dhe të fuqishëm të së drejtës për mbrojtje të të dhënave.

AGJENCIA E BASHKIMIT EVROPIAN PËR TË DREJTAT THEMELORE
Schwarzenbergplatz 11 - 1040 Vienna - Austria
Tel. +43 (1) 580 30-60 - Fax +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

KËSHILLI I EVROPËS
GJYKATA EVROPIANE E TË DREJTAVE TË NJERIUT
67075 Strasbourg Cedex - France
Tel. +33 (0) 3 88 41 20 00 - Fax +33 (0) 3
http://echr.coe.int/ - publishing@echr.coe.int