TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
AVRUPA BİRLİĞİ VE ULUSLARARASI EKONOMİK İLİŞKİLER ANABİLİM DALI
AB HUKUKU BİLİM DALI

AVRUPA BİRLİĞİ'NDE CEZAİ KONULARDA KOLLUK VE ADLİ İŞBİRLİĞİ ÇERÇEVESİNDE KİŞİSEL VERİLERİN KORUNMASI REJİMİNİN EVRİMİ

Yüksek Lisans Tezi

Ersin ALTUNBAŞ

Ankara, 2025

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
AVRUPA BİRLİĞİ VE ULUSLARARASI EKONOMİK İLİŞKİLER ANABİLİM DALI
AB HUKUKU BİLİM DALI

AVRUPA BİRLİĞİ'NDE CEZAİ KONULARDA KOLLUK VE ADLİ İŞBİRLİĞİ ÇERÇEVESİNDE KİŞİSEL VERİLERİN KORUNMASI REJİMİNİN EVRİMİ

Yüksek Lisans Tezi

Ersin ALTUNBAŞ

Tez Danışmanı

Prof. Dr. İlke GÖÇMEN

Ankara, 2025

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
AVRUPA BİRLİĞİ VE ULUSLARARASI EKONOMİK İLİŞKİLER ANABİLİM DALI
AB HUKUKU BİLİM DALI

AVRUPA BİRLİĞİ'NDE CEZAİ KONULARDA KOLLUK VE ADLİ İŞBİRLİĞİ ÇERÇEVESİNDE KİŞİSEL VERİLERİN KORUNMASI REJİMİNİN EVRİMİ

Yüksek Lisans Tezi

Tez Danışmanı

Prof. Dr. İlke GÖÇMEN

TEZ JÜRİSİ ÜYELERİ

1- Prof.Dr. İlke GÖÇMEN

2- Prof.Dr. Sanem BAYKAL

3- Dr.Öğr.Üyesi Esra DEMİR

Tez Savunma Tarihi

10/07/2025

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü'ne

Prof. Dr. İlke GÖÇMEN danışmanlığında hazırladığım "Avrupa Birliği'nde Cezai Konularda Kolluk ve Adli İşbirliği Çerçevesinde Kişisel Verilerin Korunması Rejiminin Evrimi (Ankara.2025)" adlı yüksek lisans tezimdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallarına uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul edeceğimi beyan ederim.

10.07.2025
Ersin ALTUNBAŞ

İÇİNDEKİLER

KISALTMALAR

AAET : Avrupa Atom Enerjisi Topluluğu

AB : Avrupa Birliği

ABA : Avrupa Birliği Antlaşması

ABAD : Avrupa Birliği Adalet Divanı

ABTHŞ : Avrupa Birliği Temel Haklar Şartı

AET : Avrupa Ekonomik Topluluğu

AİHM : Avrupa İnsan Hakları Mahkemesi

AİHS : Avrupa İnsan Hakları Sözleşmesi

Aİİ : Adalet ve İçişlerinde İşbirliği

AKÇT : Avrupa Kömür ve Çelik Topluluğu

AP : Avrupa Parlamentosu

AT : Avrupa Topluluğu

ATA : Avrupa Topluluğu Antlaşması

AVKD : Avrupa Veri Koruma Denetmeni

bkz. : Bakınız

CKKAİ : Cezai Konularda Kolluk ve Adli İşbirliği

EUDPR : Kişisel verilerin Birlik kurumları, organları, ofisleri ve ajansları tarafından işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu tür verilerin serbest dolaşımına ilişkin ve 45/2001/EC sayılı Tüzük ile 1247/2002/EC sayılı Kararı yürürlükten kaldıran 23 Ekim 2018 tarihli ve (AB) 2018/1725 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü

EUROPOL : Avrupa Polis Ofisi

GDPR : Genel Veri Koruma Tüzüğü

MDG : Organize Suçlar Multidisipliner Grubu

ODGP : Ortak Dış ve Güvenlik Politikası

ÖGAA : Özgürlük, Güvenlik ve Adalet Alanı

Para : Paragraph(s) / Paragraf(lar)

s. : Sayfa(lar)

VKED: : Veri Koruma Etki Değerlendirmesi

GİRİŞ

Modern toplumların giderek dijitalleşmesi sadece ekonomik ve sosyal hayatı değil, aynı zamanda kamu kurumlarının, özellikle de kolluk kuvvetleri ile adli makamların işleyişini de derinden etkilemiştir. Gelişen teknoloji ile birlikte otomatik veri tabanlarından yüz tanıma sistemlerine ve sınır ötesi bilgi aktarım platformlarına kadar yeni teknolojilerin geliştirilmesi ve uygulanması, kişisel verilerin kolluk kuvvetleri tarafından toplanma, işlenme ve paylaşılma şeklini temelden değiştirmiştir. Bu teknolojik ilerlemeler şüphesiz kolluk kuvvetleri ve adli makamların verimliliğini ve kabiliyetlerini artırmıştır. Ancak aynı zamanda, başta mahremiyet ve kişisel verilerin korunması hakları olmak üzere temel hakların korunmasına ilişkin zorlukları da beraberinde getirmiştir. Bu zorluklara yanıt olarak Avrupa Birliği (AB), kamu güvenliğinin zorunlulukları ile başta özel hayatın gizliliği ve kişisel verilerin korunması hakkı olmak üzere temel hakların korunmasını uzlaştırmayı amaçlayan yasal bir çerçeve geliştirmiştir.

Bu tez, AB'de cezai konularda kolluk ve adli işbirliği (CKKAİ) alanında kişisel verilerin korunmasının evrimini inceleyerek, AB hukukunun bu alanını şekillendiren tarihsel, maddi ve kurumsal değişiklikleri ele almaktadır. AB hukuk düzeninin temel hakların merkeziliğini yeniden teyit ederken değişen teknolojik gelişmelere nasıl uyum sağladığını göstermek için yasal metinlerden, uluslararası belgelerden, içtihat hukukundan ve akademik literatürden yararlanmaktadır. Özellikle kolluk kuvvetleri tarafından kamu güvenliğinin sağlanması dahil olmak üzere suçların önlenmesi ve soruşturulması için kişisel verilere daha fazla ihtiyaç duyulurken, bireyler için yeterli güvenceler sağlamanın zorluklarını vurgulamaktadır. Tez çalışması, iki ana bölüm şekilde, iki farklı döneme odaklanmaktadır: CKKAİ'nin AB'nin "Üçüncü Sütunu" altında hükümetlerarası mekanizmalar tarafından

yönetildiği Lizbon öncesi dönem ve bu alanın AB hukukunun ulusüstü anayasal çerçevesine dâhil edildiği Lizbon sonrası dönem.

İlk bölüm, 2009 yılında Lizbon Antlaşması'nın yürürlüğe girmesinden önce AB'nin sütunlu yapısının oluşmasına ve CKKAİ alanında veri korumaya ilişkin yasal ve tarihsel sürece genel bir bakış sunmaktadır. Veri korumaya ilişkin ilk bağlayıcı uluslararası anlaşma olan "28 Ocak 1981 tarihli Kişisel Verilerin Otomatik Olarak İşlenmesine İlişkin Olarak Bireylerin Korunmasına Yönelik 108 sayılı Avrupa Konseyi Sözleşmesi (108 sayılı Sözleşme)"[1] ve kişisel verilerin kolluk sektöründe kullanımını özel olarak ele alan "Avrupa Konseyi Bakanlar Komitesi'nin kolluk sektöründe kişisel verilerin kullanımına ilişkin 17 Eylül 1987 tarihli ve R (87) 15 sayılı Tavsiye Kararı (R (87) 15 sayılı Tavsiye Kararı)"[2] ile başlayarak, uluslararası ve AB belgeleri kapsamında kişisel verilerin korunması incelenmektedir.

Kişisel verilerin korunmasına yönelik genel bir AB çerçevesi oluşturan Veri Koruma Direktifi'nin[3] kabul edilmesine rağmen, kolluk faaliyetleri açıkça kapsam dışında bırakılmıştır. Bu mevzuat boşluğunu doldurmak için AB tarafından CKKAİ bağlamında işlenen kişisel verilerin korunmasını uyumlu hale getirmeyi amaçlayan "Cezai konularda kolluk ve adli işbirliği çerçevesinde işlenen kişisel verilerin korunmasına ilişkin 27 Kasım 2008 tarih ve 2008/977 sayılı Konsey Çerçeve Kararı (2008/977 sayılı Çerçeve Karar)"[4]

[1] Council of Europe. "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data." *Council of Europe Treaty Series 108*, Council of Europe, 1981.
[2] Recommendation No R(87)15 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector, adopted on 17 September 1987.
[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, s.31–50.
[4] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, s.60–71.

kabul edilmiştir. Bununla birlikte, bu Çerçeve Karar'ın hükümetlerarası niteliği, sınırlı uygulama mekanizmaları ve genel veri koruma ilkeleri ile tutarlı olmaması, uygulamada büyük ölçüde etkisiz kalmasına neden olmuştur.

İkinci bölüm, AB'nin CKKAİ alanının ulusüstü anayasal çerçevesine dahil edildiği Lizbon Antlaşması sonrası dönemi analiz etmektedir. Lizbon Antlaşması sadece sütun yapısını kaldırmakla kalmamış, aynı zamanda "Avrupa Birliği Temel Haklar Şartı"nı[5] (ABTHŞ) yasal olarak bağlayıcı hale getirerek[6] ABTHŞ'nin 8'inci maddesi kapsamında "kişisel verilerin korunması" hakkının anayasal statüsünü güçlendirmiştir. Bu kurumsal reformlar, AB'nin kolluk kuvvetlerinin veri işlemesinin özelliklerini de ele alan kapsamlı ve uyumlaştırılmış bir veri koruma çerçevesi benimsemesini sağlamıştır.

Bu yeni çerçevenin merkezinde, Genel Veri Koruma Tüzüğü (GDPR)[7] ile birlikte kabul edilen "kişisel verilerin suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezai yaptırımların infazı amacıyla yetkili makamlar tarafından işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu tür verilerin serbest dolaşımına ilişkin" Direktif (Kolluk Direktifi)[8] yer almaktadır. GDPR genel olarak özel ve kamu sektörleri için geçerli olsa da Kolluk Direktifi yetkili makamlar tarafından kişisel verilerin işlenmesine yönelik hedeflenmiş bir dizi kural sunmaktadır. Kolluk Direktifi, sadece geleneksel kolluk kayıtlarını değil, aynı zamanda otomatik karar verme, biyometrik

[5] Charter of Fundamental Rights of the European Union [2000] OJ C364/1.
[6] Lizbon Antlaşması ile değişik Avrupa Birliği Antlaşması madde 6.
[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.
[8] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

tanımlama gibi büyük ölçekli veri paylaşım sistemlerini içeren teknolojik olarak gelişmiş veri işleme biçimlerini düzenleme ihtiyacını yansıtmaktadır.

Bu açıklamalar ışığında tezin ilk bölümünde, AB'nin sütunlu yapısının ortaya çıkışı ve gelişimi, anayasal çerçevede Üçüncü Sütun, Lizbon Antlaşması öncesi dönemde genel olarak kişisel verilerin korunması ortaya konulmakta ve son olarak 2008/977 sayılı Çerçeve Karar'ın ayrıntılı analizi yapılmaktadır. Tezin ikinci bölümünde, Lizbon Antlaşması ile sütunlu yapının ortadan kaldırılması, anayasal çerçevede ÖGAA, Lizbon Antlaşması sonrası genel olarak kişisel verilerin korunması incelenmekte ve son olarak Kolluk Direktifi ayrıntılı olarak analiz edilmektedir.

BİRİNCİ BÖLÜM: LİZBON ANTLAŞMASI ÖNCESİ CEZAİ KONULARDA KOLLUK VE ADLİ İŞBİRLİĞİ ÇERÇEVESİNDE KİŞİSEL VERİLERİN KORUNMASI

Tezin birinci bölümü Lizbon Antlaşması öncesi dönemde AB'de CKKAİ çerçevesinde kişisel verilerin nasıl korunduğuna ilişkin ayrıntılı bir inceleme sunmaktadır. Lizbon Antlaşması öncesi dönemde CKKAİ çerçevesinde kişisel verilerin korunmasını anlayabilmek için ilk olarak AB'nin sütunlu yapısını ve anayasal çerçevede Üçüncü Sütunu ortaya koymak gerekmektedir. Bu dönemde 2008/977 sayılı Çerçeve Kararına kadar olan süreçte kolluk ve ceza adaleti alanında kişisel verilerin korunmasının nasıl sağlandığı ve bu açıdan önemli rol oynayan uluslararası belgelerin incelenmesi önem arz etmektedir. Son olarak da Lizbon Antlaşması öncesi AB'de CKKAİ çerçevesinde kişisel verilerin korunmasının temel yasal aracı olan 2008/977 sayılı Konsey Çerçeve Kararı ayrıntılı olarak incelenecektir.

1. ÜÇ SÜTUNLU YAPININ ORTAYA ÇIKIŞI

1.1 Maastricht Antlaşması Öncesi Durum

Avrupa'nın bütünleşmesi süreci ilk konuşulmaya başladığında, Avrupa'nın kurucu babalarının zihninde, yaşanan iki dünya savaşının ekonomik sebeplerle olduğu ve bu nedenle Avrupa'nın ekonomik olarak bir birlik olması düşüncesi hakimdi.[9] Avrupa entegrasyonu 1950'lerin başında, İkinci Dünya Savaşı felaketinin ardından savaş hammaddelerini Topluluk kontrolü altına almak için tasarlanan Avrupa Kömür ve Çelik Topluluğu'nun (AKÇT) 1952'de kurulmasıyla hayat bulmuştur. Bu düşünceler ışığında ete kemiğe bürünen iş birliği arzusu, 1957 yılında Roma Antlaşması ile kurulan Avrupa Atom Enerjisi Topluluğu

[9] BİLGİN, AHMET BURAK, *Avrupa Birliği'nde İnsan Haklarının Gelişimi ve Korunması*, Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2015, s.20.

(AAET) ve bilhassa Avrupa Ekonomik Topluluğu (AET) ile ekonomik bir birliğe doğru yol almaya başlamıştır. Böylece günümüzdeki AB'nin temelleri atılmıştır.

1950'lerin Kurucu Antlaşmaları, ekonomik bir birliktelik kurma hedefi ile kaleme alındığından 1970'lerden itibaren Topluluk düzeyinde ortaya çıkan CKKAİ ihtiyacını karşılayabilecek herhangi bir hüküm öngörmemiştir. 1970'lerdeki terör olayları dalgası, üye devletler arasında cezai konularda karşılıklı yardımlaşmanın hızlanması ve sonucunda bir "Avrupa yargı alanı" inşası konusunu gündeme getirmiştir. [10] 1980'lerin ortalarından itibaren Schengen Anlaşması[11] ile birlikte serbest dolaşıma açılan ortak bir alanın elde edilmesi, daha sonra cezai boyuta özellikle kolluk ve adli işbirliğine yönelik yansımaları genişletmiştir.[12]

Maastricht Antlaşması öncesinde Avrupa Topluluğu (AT) kurumlarının CKKAİ açısından hiçbir rolü bulunmuyordu.[13] Bu alandaki işbirliğine ilişkin tüm müzakereler üye devletler arasındaki "hükümetlerarası" bir perspektifte yürütülen görüşmeler olarak değerlendirilmiş ve sonuçta ortaya çıkan her türlü eylem AT hukuku değil, tüm anlaşmalara oybirliğiyle varılması gereken uluslararası kamu hukuku olarak sınıflandırılmıştır.[14] Hükümetlerarası bir perspektifte yürütülen bu görüşmelerde Avrupa Komisyonu gözlemci konumunda bulunmaktan öteye geçememiş, Avrupa Parlamentosu (AP) ise zaman zaman görüşü sorulan bir yer olarak kalmıştır.[15] Böylece CKKAİ, hükümetlerarası bir yapıda oluşturulmaya çalışılmış ve bu kapsamda daha sonra "Avrupa Polis Ofisi (Europol)"nin

[10] LABAYLE, HENRI, "The institutional framework", MITSILEGAS, VALSAMIS et.al. (Eds.), *Research Handbook on EU Criminal Law,* Edward Elgar Publishing Limited, Cheltenham, 2016, s.29.
[11] The Schengen acquis- Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, 14 Haziran 1985.
[12] LABAYLE, HENRI, (2016), s.29.
[13] KÖKTAŞ, ARİF, "Özgürlük, Güvenlik ve Adalet Alanı", AKÇAY, BELGİN ve GÖÇMEN, İLKE (Eds.), *Avrupa Birliği Tarihçe, Teoriler, Kurumlar ve Politikalar*, 3.Baskı, Seçkin Yayıncılık, Ankara, 2016, s.501.
[14] PEERS, STEVE, *EU Justice and Home Affairs Law Volume II: EU Criminal Law, Policing, and Civil Law*, 5th Edition, Oxford University Press, Oxford, 2023, s.9.
[15] KÖKTAŞ, ARİF, (2016), s.502.

ortaya çıkışına öncülük edecek TREVI (Fransızca "terörizm, radikalizm, esktremizm ve uluslararası şiddet" kelimelerinin ilk harflerinden oluşmaktadır.) Grubu[16] gibi Topluluk dışı girişimler ve işbirliği türleri ile bu ihtiyaç giderilmeye çalışılmıştır.[17]

1.2 Maastricht Antlaşması ve "Üç Sütunlu" Yapı

1980'li yılların başında Konsey ve Komisyon bünyesinde, sadece Topluluk içinde tek bir iç ekonomik pazar oluşturmak için değil, aynı zamanda, bu pazarın tamamlayıcısı olarak, AB'yi oluşturmak için formüle edilen öneriler, sınır ötesi kolluk ve adli işbirliğinin geliştirilmesine ilişkin siyasi tartışmalara önemli bir ivme kazandırmıştır.[18] Üye devletlerin sınırlarında, başka bir deyişle kurulmak istenen AB'nin iç sınırlarında, kişiler, mallar, hizmetler ve sermaye üzerindeki her türlü kontrolün kaldırılması gerektiği fikri bu tartışmada özellikle önemli bir rol oynamıştır. Bu fikir, başta Almanya ve Fransa olmak üzere, daha sonra Benelüks ülkeleri[19] tarafından ulusal ve ortak güvenlik açısından öylesine ciddi bir risk olarak görülmüştür ki, bu riski en aza indirmek için telafi edici önlemler alınması gerektiği düşünülmüştür.[20] Bu kapsamda önemli bir gelişme de AT'nin yasal çerçevesinin dışında, Benelüks ülkeleri, Fransa ve Almanya arasında 1985 yılında imzalanan Schengen Anlaşması'dır. Schengen Anlaşması'nın uygulanmasına yönelik 1990 yılında kabul edilen

[16] AB içinde adalet ve içişleri alanında işbirliğinin ilk adımları 1975 yılında üye devletlerin Adalet ve İçişleri Bakanlarından oluşan TREVI grubunun kurulmasıyla atılmıştır. TREVI, 1-2 Aralık 1975'te Roma'da yapılan Avrupa Konseyi toplantısı sırasında önerilen, Avrupa Topluluğu çerçevesi dışında, Adalet ve İçişleri Bakanlıklarından ulusal yetkililerin oluşturduğu hükümetler arası bir ağ ya da forumdu. TREVI Grubu Avrupa Konseyi İçişleri Bakanları toplantısında 29 Haziran 1976'da Lüksemburg'da resmileştirildi. Maastricht Antlaşması'nın 1993 yılında yürürlüğe girmesiyle Avrupa Birliği'nin (AB) Adalet ve İçişlerinde İşbirliği (Aİİ) olarak adlandırılan sütununa entegre edildiğinde varlığı sona ermiştir. BLASI CASAGRAN, CRISTINA, *Global Data Protection in the Field of Law Enforcement: An EU Perspective*, Routledge Taylor & Francis Group, London, 2018, s.10; Ayrıca TREVI Grubu ile ilgili ayrıntılı bilgi için bkz. FIJNAUT, CYRILLE, *A Peaceful Revolution: The Development of Police and Judicial Cooperation in the European Union*, Cambridge: Intersentia, 2019.

[17] BACHE, IAN, GEORGE, STEPHAN ve BULMER, SIMON, *Politics in the European Unıon*, 3th Edition, Oxford University Press, Oxford, 2011, s.467.

[18] FIJNAUT, CYRILLE, 2019. s.145.

[19] Hollanda, Belçika ve Lüksemburg.

[20] FIJNAUT, CYRILLE, 2019. s.146.

Schengen Uygulama Sözleşmesi[21], Schengen Bilgi Sisteminin kurulması da dahil olmak üzere göç, iltica, sınır kontrolleri ve kolluk işbirliği konularında geniş kapsamlı hükümler içermekteydi. Topluluk çerçevesi dışında bir dizi üye devlet arasında daha yakın entegrasyon modeli olan Schengen Anlaşması, o dönemde öncü bir adımdı ve AT içinde bu tür yakın entegrasyonun genişletilmesine yönelik bir ivme ile sonuçlandı.[22]

CKKAİ'ye ilişkin hükümetlerarası sürdürülen girişimler devam ederken, 1987 yılında yürürlüğe giren "Avrupa Tek Senedi" Avrupa'nın bütünleşmesinin nihai hedefi olan ortak bir iç pazar temelinde AB'ye giden yolu iyice hızlandırmış ve sonucunda "Avrupa halkları arasında, kararların vatandaşlara mümkün olduğunca yakın bir şekilde alındığı, giderek daha yakın bir birlik oluşturma sürecinde yeni bir aşama"[23] şeklinde tarif edilen AB'yi kuran Avrupa Birliği Antlaşması (ABA) veya diğer adıyla Maastricht Antlaşması 1992'de imzalanarak, 1993 yılında yürürlük kazanmıştır.[24] Maastricht Antlaşması AB'yi salt ekonomik bir bütünleşme sürecinden siyasi bir bütünleşmeye geçiren ilk kurucu antlaşma özelliğini taşıdığından Avrupa entegrasyonunun dönüm noktası olmuştur.[25]

Maastricht Antlaşması, Roma Antlaşması'nda hem kurumsal hem de maddi anlamda önemli değişiklikler yapmıştır. Maastricht Antlaşması, AB çatısı altında Steve Peers'ın tabiriyle "Yunan Tapınağı" benzeri "üç sütunlu" bir yapıyı ortaya koyduğu için genel yasal mimari açısından da önemliydi.[26] Avrupa Toplulukları (AKÇT, AAET, AET) bu sütunlardan

[21] Convention Implementing the Schengen Agreement of 14 June 1985 between theGovernments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic, on the Gradual Abolition of Checks at their Common Borders ('Schengen Implementation Agreement'), 19 Haziran 1990.
[22] MITSILEGAS, VALSAMIS, *EU Criminal Law*, 2th Edition, Hart Publishing, Oxford, 2022, s.3.
[23] Avrupa Birliği Antlaşması madde A.
[24] BAYKAL, SANEM ve GÖÇMEN, İLKE, *Avrupa Birliği Kurumsal Hukuku*, 1.Baskı, Seçkin Yayıncılık, Ankara, 2016, s.111.
[25] RIPOLL SERVENT, ARIADNA, "The European Parliament in justice and home affairs: becoming more realistic at the expense of human rights?", RIPOLL SERVENT, ARIADNA ve TRAUNER, FLORIAN (Eds.), *The Routledge Handbook of Justice and Home Affairs Research*, 1st Edition, Routledge Taylor & Francis Group, London, 2018, s.386.
[26] PEERS, STEVE, 2023, s.6.

ilkini oluşturuyordu ve AET Antlaşması resmi olarak Avrupa Topluluğu Antlaşması (ATA) olarak yeniden adlandırılmıştı. Üç sütunlu yapının ikinci sütunu "Ortak Dış ve Güvenlik Politikası (ODGP)" ile ilgiliydi ve "Avrupa Siyasi İşbirliği" için daha önceki mekanizmalar üzerine kurulmuştu. Üç sütunlu yapının son sütunu yani Üçüncü Sütunu "Adalet ve İçişlerinde İşbirliği (Aİİ)" ile ilgiliydi ve bu alandaki daha önceki girişimler üzerine inşa edilmişti.[27]

ABA ile AB'ye ODGP ve Aİİ ile ilgili yeni sorumluluklar verilmiştir. Bu nedenle kilit mesele, bu yeni yetkilerin neden daha önceki Antlaşma değişikliklerinde yapıldığı gibi mevcut olanlara eklenmediğidir. ODGP ve Aİİ için ayrı sütunlar oluşturulmasının temel gerekçesi ise şu şekilde açıklanabilir. Üye Devletler ODGP ve Aİİ ile ilgili olarak iş birliği yapabilecekleri bir kurumsal yapı oluşturma niyetindeydi, ancak bu kurumsal yapının eksikliği her yeni sorunu görüşmek üzere sürekli toplantılar düzenlenmesini gerektirmekteydi. Bu süreç zaman alıcı ve külfetli bir işti.[28] Üye devletler bir taraftan söz konusu alanlarda 1970'lerden beridir devam eden süreci kurumsal bir yapı altında sürdürmeyi istemiş, diğer taraftan İkinci ve Üçüncü Sütunlar ulusal egemenliğin merkezinde yer aldığı düşünülen hassas politika alanlarıyla ilgili olduğundan ve AP, Avrupa Komisyonu ve Avrupa Birliği Adalet Divanı'nın (ABAD) "Topluluk Sütunu" kapsamında sahip oldukları yetkilerine bu alanda sahip olmasını istemediklerinden bu alanları Topluluk Sütununu karakterize eden normal ulusüstü karar alma yöntemlerine tabi tutmak istememişlerdir.[29]

---

[27] ABA toplam yedi başlıktan oluşmaktaydı. Başlık I, ABA'nın temel hedeflerini ortaya koyan "ortak hükümleri" içeriyordu. Başlık II, III ve IV, sırasıyla AET, AKÇT ve Euratom Antlaşmalarında yapılan Birinci Sütun değişikliklerini kapsamaktaydı. Başlık V ODGP'yı yani Antlaşmanın İkinci Sütununu, Başlık VI Aİİ'yi yani Antlaşmanın Üçüncü Sütununu ve Başlık VII ise nihai hükümleri düzenliyordu.

[28] CRAIG PAUL ve DE BÚRCA GRAINNE, *Eu Law: Text. Cases, and Materials*, 7th Edition, Oxford University Press, Oxford, 2020, s.17.

[29] ARAT, TUĞRUL *et.al.*, "Avrupa Bütünleşmesi: 1957 – 1993 Arası", AKÇAY, BELGİN ve GÖÇMEN, İLKE (Eds.), *Avrupa Birliği: Tarihçe, Teoriler, Kurumlar ve Politikalar*, 3.Baskı, Seçkin Yayıncılık, Ankara, 2016, s.75.

Dolayısıyla, İkinci ve Üçüncü Sütunlar kapsamında karar alma süreci daha çok hükümetlerarası bir nitelik taşımış, Konsey ve AB Zirvesi'ndeki üye devletler birincil güç dizginlerini ellerinde tutmuşlardır.[30] Maastricht Antlaşması öncesi başlayan hükümetlerarası yaklaşım, Aİİ işbirliği için etkin bir şekilde "resmi hükümetlerarası" bir sistem kuran Maastricht Antlaşması ile sağlamlaştırılmıştır.[31]

Maastricht Antlaşması'nın Üçüncü Sütunun açılış hükmü olan K Maddesi, Adalet ve İçişleri konusunda Birinci Sütunda olduğu gibi ortak bir politikaya veya İkinci Sütun girişimlerine değil, "Adalet ve İçişleri alanlarında işbirliğine" atıfta bulunmaktadır.[32] K.1 maddesinde Üye Devletlerin "ortak çıkar" olarak gördükleri[33] "özellikle kişilerin serbest dolaşımı başta olmak üzere Birliğin hedeflerine ulaşılması amacıyla ve Avrupa Topluluğunun yetkilerine halel getirmeksizin"[34], "iltica politikası", "Üye Devletlerin dış sınırlarının kişiler tarafından geçilmesini ve bu sınırlar üzerindeki kontrollerin uygulanmasını düzenleyen kurallar", "göçmen politikası ve üçüncü ülke vatandaşlarına ilişkin politika", "uyuşturucu bağımlılığı ile mücadele", "uluslararası ölçekte dolandırıcılıkla mücadele", "medeni hukuk alanında adli işbirliği", "ceza hukuku alanında işbirliği", "gümrük işbirliği", "Avrupa Polis Ofisi (Europol) bünyesinde bilgi aktarımına yönelik AB çapında bir sistemin düzenlenmesiyle bağlantılı olarak, gerektiğinde gümrük işbirliğinin belirli yönleri de dahil olmak üzere, terörizm, yasadışı uyuşturucu kaçakçılığı ve diğer ciddi uluslararası suç türlerinin önlenmesi ve bunlarla mücadele edilmesi amacıyla kolluk işbirliği" konuları yer almaktadır.

[30] CRAIG PAUL ve DE BÚRCA GRAINNE, 2020, s.17.
[31] PEERS, STEVE, 2023, s.10.
[32] MITSILEGAS, VALSAMIS, 2022, s.6
[33] KÖKTAŞ, ARİF, (2016), s.501.
[34] ABA madde K.

Fijnaut'un iyi bir şekilde özetlediği üzere: ABA'da CKKAİ'nin düzenlenmesine ilişkin tartışma, bu işbirliğinin düzenlenmesinin, üye devletlerin böyle bir antlaşmada birbirleriyle kurmaya istekli oldukları anayasal ilişkilere ne kadar bağlı olduğuna dair bir izlenim vermektedir. Bu tür bir antlaşma temelinde örgütlenen bir ittifaka katılan devletler, güç kullanma tekellerini paylaşmaya, hatta teslim etmeye bile yanaşmıyorlarsa, bu işbirliğinin de ezici bir çoğunlukla devletlerarası ya da hükümetlerarası bir temelde örgütlenmesi gerekir. Bu sonuç, AB'ye Üye Devletlerin bu işbirliği biçimlerinin düzenlenmesini antlaşmaya dahil etme konusundaki istekliliğinin, kolluk ve adli işbirliği tarihinde "küçük bir devrim" oluşturduğu gerçeğini ortadan kaldırmaz. Bu açıdan bakıldığında, bu karmaşık ilişkilerin bir antlaşmayla neticelenmesi de önemli bir adımı oluşturmaktadır.[35]

1.3 Amsterdam Antlaşması ve "Modifiye Edilen Üçüncü Sütun"

Maastricht Antlaşması'nın yürürlüğü girmesinden sadece altı yıl sonra AB'ye üye devlet sayısının artması ve aslen soğuk savaş döneminin bitmesi ile birlikte AB'nin daha da genişlemesi ve derinleşmesi yönündeki gelişmeler 1997 yılında imzalanan ve 1999 yılında yürürlüğe giren Amsterdam Antlaşması ile sonuçlanmıştır.[36] Amsterdam Antlaşması ABA'da birçok değişiklik yapmasına karşın üç sütunlu yapıyı korumuştur. Amsterdam Antlaşması'nın müzakereleri sırasında, ABA'nın Aİİ hükümlerinde yapılmak istenen değişiklikler, Aİİ kapsamındaki işbirliği hedeflerinin net olmaması, AB kurumlarının rollerinin iyi bir şekilde ortaya konulmamış olması, işbirliğini gerçekleştirmek için

[35] FIJNAUT, CYRILLE, 2019. s.202.
[36] BAYKAL, SANEM ve GÖÇMEN, İLKE, 2016, s.117.

kullanılacak araçların yasal etkisinin belirsiz olması ve Üçüncü Sütün ile Birinci Sütun sınır çizgisinin zaman zaman belirsiz olması gerekçeleri ile kilit bir konu haline gelmiştir.[37]

Amsterdam Antlaşması ile Üçüncü Sütun "Cezai Konularda Kolluk ve Adli İşbirliği" adını almıştır.[38] Amsterdam Antlaşması ile Üçüncü Sütunda yer alan "vize", "iltica", "göç" ve "kişilerin serbest dolaşımının diğer yönleriyle ilgili kısımlar" eski karar alma kurallarının (istişare ve oybirliği) uygulanacağı beş yıllık bir geçiş dönemine tabi tutularak[39] Birinci Sütuna yani Topluluk Sütununa alınmış[40], CKKAİ Üçüncü Sütundaki yerini korumuştur.[41] Amsterdam Antlaşması'nın dibacesinde "Bu Antlaşma hükümlerine uygun olarak bir özgürlük, güvenlik ve adalet alanı oluşturarak, halklarının emniyet ve güvenliğini sağlarken, kişilerin serbest dolaşımını kolaylaştırmaya"[42] ve Amsterdam Antlaşması ile değiştirilen ABA'nın 29'uncu maddesinde "Avrupa Topluluğu'nun yetkilerine halel getirmeksizin, AB'nin amacı, CKKAİ alanlarında Üye Devletler arasında ortak eylem geliştirerek ve ırkçılık ve yabancı düşmanlığını önleyerek ve bunlarla mücadele ederek, özgürlük, güvenlik ve adalet alanı içerisinde vatandaşlara yüksek düzeyde güvenlik sağlamaktır" denilerek özgürlük, güvenlik ve adalet alanı (ÖGAA) ilk kez kurucu antlaşma düzeyinde ifade edilmiştir.

---

[37] PEERS, STEVE, 2023, s.15.
[38] Amsterdam Antlaşması madde 1(11) ile değiştirilen ABA madde 29 – 42.
[39] RIPOLL SERVENT, ARIADNA, *The European Parliament*, 1st Edition, Palgrave and Macmillan, London, 2018, s.17.
[40] Amsterdam Antlaşmanın yürürlüğe girmesinden sonraki ilk beş yıl boyunca Konsey, Komisyon veya bir Üye Devlet tarafından sunulan teklifler üzerine oybirliğiyle karar alacaktır. Herhangi bir karar almadan önce Konsey, Avrupa Parlamentosu'na danışmak zorundadır. Bu süreden sonra Konsey, sadece Komisyon'dan gelen teklifler üzerine karar alacaktır. Bununla birlikte Komisyon, bir Üye Devlet tarafından Konsey'e sunulmak üzere yapılan herhangi bir teklif talebini değerlendirmek zorunda olacaktır. Avrupa Parlamentosu'na danıştıktan sonra Konsey, Başlık IV kapsamındaki tedbirleri kabul ederken ve Avrupa Toplulukları Adalet Divanı'na ilişkin hükümleri değiştirirken ortak karar usulünü ve nitelikli çoğunluk oylamasını uygulamaya oybirliğiyle karar vermek zorunda olacaktır. European Commission, *The Amsterdam Treaty: A Comprehensive Guide*, 1999, s.20.
[41] BAYKAL, SANEM ve GÖÇMEN, İLKE, 2016, s.119.
[42] Amsterdam Antlaşması Dibace paragraf 10

Amsterdam Antlaşması bir ÖGAA oluşturarak Adalet ve İçişleri alanındaki işbirliğini yeniden şekillendirmiştir. Hedefler daha geniş ve daha spesifik, yöntemler daha etkili ve demokratik olurken AB kurumlarına da daha dengeli bir rol verilmiştir. Ayrıca Schengen müktesebatı, Amsterdam Anlaşması'na ek "Avrupa Birliği Yasal Çerçevesine Schengen Müktesebatının Dâhil Edilmesine İlişkin Protokol" ile tekrar müzakere edilmeksizin kabul edilerek AB'nin ikincil hukuk kuralları haline gelmiş, AB kurumsal ve hukuki düzeninin bir parçası olmuştur.[43] AB'de CKKAİ açısından ve bu çerçevede kişisel verilerin korunması yönünden Schengen Müktesebatı önemli düzenlemeler içermektedir.

Amsterdam Antlaşması, ABA'nın VI. başlığını yürürlükten kaldırmamıştır. Ancak "CKKAİ ilişkin hükümler" şeklindeki yeni başlık, Konsey ile Komisyon arasında müzakereler sürecinde yaşanan tartışma ışığında çok şey ifade etmektedir. Sonuçta bu, Komisyon'un Adalet ve İçişleri konularının kısmen Topluluk çerçevesine, diğer bir deyişle Birinci Sütuna aktarılması yönündeki tavsiyesine uyulduğu anlamına gelmektedir.[44] Görüldüğü üzere Maastricht Antlaşması ile Üçüncü Sütun kapsamında olan birçok konu "ulusüstü" AB kurumlarının yetkisinin olduğu Birinci Sütuna taşınmış ancak "kolluk ve adli işbirliği" Üçüncü Sütun içerisinde "hükümetlerarası" statüde kalmaya devam etmiştir.

2001 yılında imzalanan ve 2003 yılında yürürlüğe giren Nice Antlaşması, AB'yi daha sonra 2004 ve 2007 yıllarında gerçekleşen önemli genişlemeye hazırlamak için gerekli olduğuna inanılan Antlaşmalardaki diğer değişikliklere odaklandığından, Üçüncü Sütun konuları ile ilgili konularda mütevazı değişiklikler[45] yapmıştır.[46]

---

[43] ÖZCAN, MEHMET, *Avrupa Birliği Sığınma Hukuku - Ortak Bir Sığınma Hukukunun Ortaya Çıkışı*, 1.Baskı, USAK Yayınları, İstanbul, 2005, s.139.
[44] FIJNAUT, CYRILLE, 2019. s.209.
[45] Üçüncü sütun kapsamında Nice Antlaşması, ABA'nın 29. maddesini değiştirmiş, ABA'nın 31(2) maddesine yeni bir madde eklemiş ve güçlendirilmiş işbirliğine ilişkin kuralları gözden geçirmiştir (ABA 40. maddesinin yerini 40, 40a ve 40b maddeleri almıştır). PEERS, STEVE, 2023, s.15.
[46] PEERS, STEVE, 2023, s.7.

AB entegrasyonunun ilk günlerinden bu yana, Adalet ve İçişleri alanının AB düzeyinde koordine edilmesinin ardındaki fikir, serbest dolaşımın kolaylaştırılması nedeniyle sınır ötesi suç faaliyetlerinin artan tehdidine ve özellikle Soğuk Savaş'ın sona ermesi ve SSCB'nin dağılması ile birlikte Doğu Avrupa'dan AB alanına suçluların girme riskinin oluşturduğu hassas duruma tepki vermek olmuştur. Adalet ve İçişleri alanının uyumlaştırılması ihtiyacına rağmen, Avrupa'nın bu konulardaki entegrasyonu yukarıda kurucu antlaşma hükümleri de göz önüne alındığında "yavaş ve doğrusal olmayan" bir şekilde gerçekleşmiştir.[47]

Sonuç olarak, Avrupa Tek Senedi'nin devamı olarak ATA'nıın değiştirilmesine yönelik müzakerelerde Aİİ giderek daha önemli hale gelmiş ve bu müzakerelerde, Topluluk yetkisinin Adalet ve İçişleri konularını kapsayıp kapsamayacağı hususu son derece tartışmalı olmuştur.[48] Nihai uzlaşma, AB için üç sütunlu bir yapı getiren Maastricht Antlaşması'nın kabul edilmesiyle gelmiştir. Bu yapının temel işlevi, bir yandan dış ve güvenlik politikası ile Adalet ve İçişleri gibi tartışmalı alanları AB'nin yetki alanına dahil etmek, diğer yandan da AB'nin egemenlik açısından hassas olan bu alanlardaki eylemlerinin birinci sütunun ulusüstü unsurları altında değil, hükümetlerarası bir yasal çerçeveye tabi olmasını sağlamaktır.[49] Bu sütun yapısı Lizbon Antlaşması'nın yürürlüğe girmesine kadar korunmuş, AB'nin CKKAİ'ye ilişkin eylemleri büyük ölçüde Üçüncü Sütunla sınırlı kalmıştır.

[47] MÖLLER, CAROLIN, *The Evolution of Data Protection and Privacy in the Public Security Context-An Institutional Analysis of Three EU Data Retention and Access Regimes*, Yayımlanmamış Doktora Tezi, Queen Mary University of London, London, 2017, s.95.
[48] MITSILEGAS, VALSAMIS, 2022. s.5.
[49] MITSILEGAS, VALSAMIS, 2022. s.6.

2. ANAYASAL ÇERÇEVEDE ÜÇÜNCÜ SÜTUN

2.1 Maastricht Antlaşması: "Üye Devletlerin ve Konseyin Hükümranlığı"

Aİİ'ye ilişkin hükümler Maastricht Antlaşmasının VI. bölümünde (K) maddesi altında K.1-K.9 maddeleri arasında düzenlenmiştir. Üçüncü Sütun kapsamında giren konular K.1 maddesi ile düzenlenmekte olup bunlar yukarıda dile getirilmiştir.

K.2 maddesi ile Aİİ'nin Avrupa İnsan Hakları Sözleşmesi'nde (AİHS) sağlanan korumaya "uygun olarak ele alınması" gerektiğini belirtmiş ve ABA'nın "hukuk ve düzenin sağlanması ve iç güvenliğin korunmasına ilişkin olarak Üye Devletlere düşen sorumlulukların yerine getirilmesini" etkileyemeyeceği ileri sürülmüştür.

K.3.1 maddesinde "Madde K.1'de atıfta bulunulan alanlarda, Üye Devletler, eylemlerini koordine etmek amacıyla Konsey bünyesinde birbirlerini bilgilendirir ve birbirlerine danışırlar" denilerek Konsey'in ve dolayısıyla Üye Devletlerin Üçüncü Sütundaki baskın rolü açıkça ortaya konulmuştur. K.3.2 maddesinde, Üçüncü Sütun kapsamında "herhangi bir üye devletin veya Komisyon'un girişimiyle, Madde K.1(1) ila (6)'da atıfta bulunulan alanlarda" ve "herhangi bir üye devletin girişimiyle Madde K1(7) ila (9)'da atıfta bulunulan alanlarda" işbirliğinin Konsey tarafından kabul edilecek "ortak tutum", "ortak eylem" veya "sözleşme" vasıtasıyla sağlanacağı düzenlenmektedir.

Bu düzenlemeden de anlaşılacağı üzere ABA'nın K.1 maddesinde belirtilen "ortak çıkar" alanlarında yasal olarak bağlayıcı adımlar atma yetkisi hem sınırlı hem de belirsizdi. Söz konusu işbirliği metotlarından yasal olarak bağlayıcı tek işbirliği metodu, Birleşmiş Milletler ve Avrupa Konseyi gibi uluslararası hukuk forumları altında hükümetlerarası işbirliğini açıkça yansıtan "sözleşmeler"di. Konsey ayrıca görünüşte yasal bağlayıcılığı olmayan "ortak tutum" ve "ortak eylem"ler de kabul edebilirdi ki bunların yasal bağlayıcılığı belirsizdi ve tartışmalıydı. Açıkçası Maastricht Antlaşması'nın Üçüncü Sütunu ilke olarak

AB'ye CKKAİ de dahil olmak üzere Aİİ alanında bir dereceye kadar yetki tanımış olsa da, AB'ye bu yetkiyi kullanması için tanınan araçlar önemli ölçüde sınırlı ve belirsiz kalmıştır.[50] Bu belirsizliklerin bir sonucu olarak Maastricht sonrası dönemde Konsey tarafından alınan 127 resmi kararın sadece dörtte biri "ortak eylemler" veya "ortak pozisyonlar" şeklinde olmuştur.[51]

K.6 maddesinin ikinci paragrafındaki "Başkanlık, bu Başlıkta atıfta bulunulan alanlardaki faaliyetlerin temel yönleri hakkında AP'ye danışır ve AP'nin görüşlerinin gerektiği şekilde dikkate alınmasını sağlar" ibaresi ile AP'ye Üçüncü Sütun kapsamındaki konularda karar alma süreçlerine dahil edilmeyen ve sadece bağlayıcı olmayan görüşler bildiren bir danışma organı rolü biçilmektedir. Görüldüğü üzere üye devletlerin bu bağlamdaki hakim konumu, sadece üye devletlerin Konsey bünyesinde "kolluk, adli ve gümrük işbirliği" alanında işbirliğini düzenlemeye yönelik araçlardan herhangi birini kabul etmek için girişimde bulunabileceğini öngören K.3.2 ve K.6 maddesi ile daha da açık bir şekilde ortaya konmaktadır.[52] Maastricht Antlaşması Komisyon'a Konsey'deki karar alma masasında en azından "hoşgörülü" bir yer verirken, AP, Konsey'in yeni Aİİ politika oluşturma alanındaki "faaliyetlerin temel yönleri hakkında kendisine danışması" ve "görüşlerinin gerektiği gibi dikkate alınmasını sağlaması" için muğlak bir şekilde ifade edilmiş bir yükümlülükle yetinmek zorunda kalmıştır.[53]

K.4.1 maddesi ile üst düzey yetkililerden oluşan bir Koordinasyon Komitesi (K4 Komitesi olarak anılacaktır) kurulmuştur. K.4.3 maddesinde "Konsey, usule ilişkin konular

[50] MITSILEGAS, VALSAMIS, 2022. s.6.
[51] MONAR, JÖRG, "Justice and Home Affairs: The Treaty of Maastricht as a Decisive Intergovernmental Gate Opener", Journal of European Integration, Cilt:34, Sayı:7, 2012, s.727.
[52] FIJNAUT, CYRILLE, 2019. s.163.
[53] MONAR, JÖRG, s.730.

ve K.3 maddesinin açıkça başka oylama kuralları öngördüğü durumlar haricinde, oybirliğiyle hareket eder" denilerek Üçüncü Sütun kapsamında kararların üye devletlerin hepsinin mutabakatı ile alınacağını net bir şekilde düzenlenmiştir. Bu husus Üçüncü Sütun'un hükümetlerarası yapısının açık bir sonucudur. K.3.2(b) maddesinde sadece ortak eylemlerin nitelikli çoğunluk ve K.3.2(c) maddesinin ikinci paragrafında uygulama tedbiri niteliğindeki sözleşmelerin üçte iki çoğunluk ile kabul edilebileceğinin düzenlenmesi oybirliği kuralının istisnasını oluşturmaktadır.

Üçüncü Sütun kapsamında ABAD'ın genel bir yargı yetkisi bulunmamakla birlikte K.3.2 (c) maddesinin son paragrafında, işbirliği türlerinden olan sözleşmelerde öngörülmesi halinde ABAD'ın sözleşme hükümlerini yorumlayabileceği ve sözleşmeden doğan ihtilaflar üzerine karar verebileceği ifade edilmektedir. Bu durum, Konsey'in diğer tüm Üçüncü Sütun tasarruflarını ABAD'ın yargısal denetiminden muaf tutmakla kalmamış, aynı zamanda Konsey'de ABAD'ın yargı yetkisinin Üçüncü Sütun sözleşmelerinde ne ölçüde uygulanacağı hususunda başlangıçta bir uzlaşma sağlanamamasına neden olmuştur.[54]

Üçüncü Sütunun yapılandırılma şekli, AB kurumlarına Üçüncü Sütun kapsamında AB tasarruflarının kabulü ve uygulanmasında sadece küçük bir rol vermiş ve Üye Devletlerin kararları üzerinde herhangi bir kontrol uygulama imkanı tanımamıştır.[55] Sonuç olarak Maastricht Antlaşması ile ortaya çıkan Üçüncü Sütun kapsamında; ABAD, sözleşmelerde bunu açıkça öngören bir madde varsa sözleşmeleri yorumlama yetkisine sahipti; AP'ye Konsey tarafından danışılabilirdi, ancak çoğu zaman sadece bilgilendirilirdi; Avrupa

[54] MONAR, JÖRG, s.731.
[55] PEERS, STEVE, "The European Union and substantive criminal law: reinventing the wheel?", Netherlands Yearbook of International Law, Volume 33, 2002, s.49.

Komisyonu'nun inisiyatif hakkı belirli alanlarla sınırlıydı ve Üye Devletlerle paylaşılıyordu; Konsey, her kararın oybirliği ile alınması zorunluluğu nedeniyle sık sık felç oluyordu.[56]

2.2 Amsterdam Antlaşması: "Avrupa Birliği Kurumlarının Sınırlı Yetkisi Altında Hükümetlerarası Yapının Korunması"

Amsterdam Antlaşması'nın yürürlüğe girmesiyle genel olarak "ulusüstü" AB kurumlarının (Komisyon, AP ve ABAD) Üçüncü Sütundaki rolü artmıştır. Bununla birlikte, Üye Devletler, Adalet ve İçişleri entegrasyonunun tüm yönleri üzerinde AB çerçevesindeki ekonomik entegrasyona kıyasla daha fazla kontrole sahip olmaya devam etmişlerdir.[57]

Üçüncü Sütuna ilişkin hükümler Amsterdam Antlaşması'nın VI. bölümünde "Cezai Konularda Kolluk ve Adli İşbirliğine İlişkin Hükümler" başlıklı 29-42'inci maddeler arasında düzenlenmiştir. Bunlar içerisinde temel kurumsal hükümler madde 34 (Konsey, Komisyon, yasal araçlar ve yasal etki), madde 35 (ABAD) ve madde 39 (AP)'dur.

Amsterdam Antlaşması ile değişik ABA madde 29 ile işbirliği alanları "üye devletlerdeki kolluk güçleri, gümrük makamları ve diğer yetkili makamlar arasında daha yakın işbirliği", "üye devletlerin adli ve diğer yetkili makamları arasında daha yakın işbirliği" ve "üye devletlerde cezai konulara ilişkin kuralların yakınlaştırılması" şeklinde düzenlenmiştir. Amsterdam Antlaşması ile değişik ABA madde 30 "kolluk işbirliği alanındaki ortak eylemleri" ve madde 31 "cezai konularda adli işbirliğine ilişkin ortak eylemleri" belirlemektedir.

Amsterdam Antlaşması ile değişik ABA madde 32 ile Konsey'in, 30 ve 31'inci maddelerde atıfta bulunulan makamların, özellikle de Europol'ün, başka bir üye devletin

[56] European Commission, *The Amsterdam Treaty: A Comprehensive Guide*, 1999, s.19.
[57] PEERS, STEVE, 2023, s.7.

topraklarında faaliyet göstermesine izin verecek koşulları ve kısıtlamaları, bu devletin makamlarına danışarak ve onların rızasını alarak belirleyeceği düzenlemektedir.

Amsterdam Antlaşması ile değişik ABA madde 33 "Bu Başlık, hukuk ve düzenin korunması ve iç güvenliğin sağlanması ile ilgili olarak Üye Devletlere düşen sorumlulukların yerine getirilmesini etkilemez" hükmü ile Maastricht Antlaşması'nın K.2.2 maddesi aynen tekrar edilmiş ve AB'nin cezai konulara erişiminin kontrol edilmesi konusunda bir güvence daha elde edilmiştir.[58]

Amsterdam Antlaşması ile değişik ABA madde 34'ün ilk paragrafı, bir yandan 30 ve 31'inci maddeler ile diğer yandan 34(2) maddesi arasındaki geçişe işaret etmektedir.[59] Amsterdam Antlaşması ile değişik madde 34(1) Üye Devletleri, eylemlerini koordine etmek ve yetkili makamları arasında işbirliği tesis etmek amacıyla Üçüncü Sütun çerçevesinde belirtilen alanlarda Konsey bünyesinde birbirlerini bilgilendirmek ve birbirlerine danışmakla yükümlü kılmıştır. Amsterdam Antlaşması ile değişik madde 34(2)'nin ilk cümlesi ile Konsey, AB'nin hedeflerinin gerçekleştirilmesine katkıda bulunacak tedbirleri almak ve işbirliğini teşvik etmek ile görevlendirilmiştir. Bu amaçla, Konsey, her bir üye devletin veya Komisyon'un girişimi üzerine, oybirliğiyle "ortak tutumlar"[60] benimseyebilir, "çerçeve kararlar"[61] ile "kararlar"[62] kabul edebilir ve "sözleşmeler"[63] oluşturabilirdi.[64] Amsterdam Antlaşması ile Komisyon, Üçüncü Sütundaki işbirliği alanları için üye devletlerle ortak bir inisiyatif kazanarak gücünü arttırmıştır.[65] Amsterdam Antlaşması ile değişik madde 39'daki

[58] MITSILEGAS, VALSAMIS, 2022. s.5.
[59] FIJNAUT, CYRILLE, 2019. s.215.
[60] Amsterdam Antlaşması ile değişik ABA madde 34(2)(a)
[61] Amsterdam Antlaşması ile değişik ABA madde 34(2)(b)
[62] Amsterdam Antlaşması ile değişik ABA madde 34(2)(c)
[63] Amsterdam Antlaşması ile değişik ABA madde 34(2)(d)
[64] Amsterdam Antlaşması ile değişik ABA madde 34(2)
[65] PEERS, STEVE, 2023, s.15.

düzenlemeyle AP, Maastricht Antlaşması dönemindeki yetkilerini korumuş, ilave olarak Konsey'in belirlediği ve üç aydan az olmamak koşuluyla bir zaman sınırı dahilinde Üçüncü Sütun yasal düzenlemelerinin kabul edilmesinden önce kendisine danışılması zorunluluğu hakkını elde etmiştir.[66] Ancak, beklenebileceği gibi, AP'nin görüşlerinin Konsey'in Üçüncü Sütun tedbirleri üzerinde sınırlı bir etkisi olmuştur.[67]

Amsterdam Antlaşması ile karar alma düzenlemeleri özünde hükümetlerarası olmaya devam etse de Amsterdam Antlaşması Üçüncü Sütun kapsamındaki yasal araçları önemli ölçüde güçlendirmiştir.[68] Üçüncü Sütun kapsamında Maastricht Antlaşması ile getirilen sözleşmeler, Amsterdam Antlaşması sonrası yürürlüğe girmelerindeki gecikmelerden dolayı kullanımları asgari düzeyde olmasına rağmen, mevcudiyetini korumuştur.[69] Amsterdam Antlaşması Üçüncü Sütun için yukarıda isimleri zikredilen bir dizi yeni araç ortaya koymuştur. Bu araçlardan ilki bağlayıcılığı tartışmalı olan "Birliğin belirli bir konuya yaklaşımını tanımlayan" ortak tutumdur. Ortak tutumlar özellikle AB'nin dış eylemleri bağlamında önemliydi ve üye devletlerin bunları uluslararası örgütlerde ve uluslararası konferanslarda savunması gerektiğini belirtiyordu.[70]

Amsterdam Antlaşma'nın açıkça yasal bağlayıcılık getirdiği Üçüncü Sütun tedbirleri, mevzuatın yakınlaştırılması dışında kalan ve doğrudan etki doğurmayan "kararlar"[71] ve mevzuatın yakınlaştırılmasını amaçlayan ve doğrudan etki doğurmayan "çerçeve kararlar"[72]dır. Amsterdam Antlaşması sonrası Üçüncü Sütun yasa yapımının ana şeklini oluşturan çerçeve kararların yürürlüğe girmesi, Üçüncü Sütun hukukunu önemli ölçüde

[66] Amsterdam Antlaşması ile değişik ABA madde 39(1)
[67] PEERS, STEVE, 2023, s.16.
[68] MITSILEGAS, VALSAMIS, 2022. s.10.
[69] PEERS, STEVE, 2002, s.52.
[70] Amsterdam Antlaşması ile değişik ABA madde 37
[71] Amsterdam Antlaşması ile değişik ABA madde 34(2)(c)
[72] Amsterdam Antlaşması ile değişik ABA madde 34(2)(b)

güçlendirmiştir.[73] Çerçeve kararlar AB'nin Üçüncü Sütun kapsamındaki mevzuatı uyumlaştırılmak için kullandığı tek yöntem haline gelmiştir. Çerçeve kararların, sözleşmelere göre daha cazip olmasının temel nedeni yürürlüğe girebilmeleri için üye devletlerin onayına ihtiyaç duymamasıdır.[74]

Bu tezin konusu açısından da çerçeve kararlar üzerinde özel olarak durulacaktır. Çerçeve kararlar, Birinci Sütun "direktifleri"[75] gibi elde edilecek sonuç bakımından üye devletleri bağlamakta ancak şekil ve yöntem seçimini ulusal makamlara bırakmaktadırlar. Çerçeve kararların, direktiflerden temel farkı, doğrudan etki doğurmamalarıydı.[76] Ancak, bu durum ABAD'ı, çerçeve kararların yasal etkilerini açıklığa kavuşturduğu ve ABAD'ın Üçüncü Sütun kapsamında verdiği en önemli kararlardan biri olan *Pupino* kararında[77] Üçüncü Sütun çerçeve kararlarının uygun yorum ilkesi çerçevesinde dolaylı etkisi olduğunu[78] vurgulamaktan ve üye devletlerde uygulanmasına yönelik çabaları artırmaktan alıkoymamıştır.[79] *Pupino* davasındaki ufuk açıcı kararında ABAD, Üçüncü Sütun hukukunun uygulanabilirliğini ve bağlayıcılığını artırmak amacıyla çerçeve kararlara dolaylı etki ilkesinin uygulanabilirliğini teyit etmiştir.[80] Ayrıca *Melloni* kararında[81] ABAD, AB

[73] MITSILEGAS, VALSAMIS, 2022. s.11.
[74] PEERS, STEVE, 2002, s.52.
[75] Amsterdam Antlaşması ile değişik Avrupa Topluluğu Antlaşması madde 249(3).
[76] Amsterdam Antlaşması ile değişik ABA madde 34(2)(c).
[77] Case C-105/03, *Maria Pupino v. Italy*, [2005], ECR I-5285, Pupino kararı ve bu kararın AB hukukuna etkisi ile ilgili ayrıntılı bilgi için bakınız. FLETCHER, MARIA, "Impact of the Pupino Decision on Eu Law" MITSILEGAS, VALSAMIS *et.al.*(Eds.), *The Court of Justice and European Criminal Law: Leading Cases in a Contextual Analysis*, Hart Publishing, 2019, s.67-82.
[78] Case C-105/03, [2005], para 43 "*Yukarıda belirtilen tüm hususlar ışığında Divan, Avrupa Birliği Antlaşması'nın VI. başlığı bağlamında kabul edilen çerçeve kararlarla ilgili olarak uygun yorum ilkesinin bağlayıcı olduğu sonucuna varmıştır. Ulusal hukuku uygularken, bu hukuku yorumlamakla yükümlü olan ulusal mahkeme, bunu mümkün olduğunca çerçeve kararın lafzı ve amacı ışığında yapmalı ve böylece ABA'nın 34(2)(b) maddesine uygun bir sonuç elde etmelidir.*"
[79] MITSILEGAS, VALSAMIS, 2022. s.11.
[80] MITSILEGAS, VALSAMIS, *Eu Criminal Law After Lisbon: Rights, Trust and the Transformation of Justice In Europe*, Hart Publishing, Oxford, 2016, s.8.
[81] Case C-399/11, *Melloni v Ministerio Fiscal*, [2013], ECLI:EU:C:2013:107.

hukukunun önceliği ilkesinin Üçüncü Sütun hukukuna, yani 2009 Çerçeve Kararı ile değiştirilen Avrupa Tutuklama Emrine ilişkin Çerçeve Kararı'na, ulusal anayasa hukuku karşısında gıyabi kararların uygulanmasını teyit etmiştir.[82]

ABAD'ın yargı yetkisi Amsterdam Antlaşması'nın son hükümlerinde[83], ABAD'ın yetkilerine ilişkin ATA hükümlerinin "madde 35'te öngörülen koşullar altında Başlık VI hükümlerine"[84] uygulanacağını öngören Amsterdam Antlaşması ile değişik madde 46'da yer almaktadır.[85] Bu hüküm Amsterdam Antlaşması ile eklenmiş ve ABAD'ın Üçüncü Sütun üzerindeki yargı yetkisini önemli ölçüde genişletmiştir.[86]

ABAD, esas olarak, Amsterdam Antlaşması'nda öngörülen bazı durumlarda ön karar prosedürü işletebilmektedir. Öncelikle ABAD, madde 35'te belirtilen koşullara tabi olarak, çerçeve kararların ve kararların geçerliliği ve yorumlanması, Üçüncü Sütun altında oluşturulan sözleşmelerin yorumlanması ve bunları uygulayan tedbirlerin geçerliliği ve yorumlanması hakkında ön kararlar verme yetkisine sahiptir.[87] Ancak ABAD'ın bu yetkisi, bir üye devletin bu tür bir yargı yetkisini kabul ettiğine dair beyanına tabidir.[88] Üye devletler böyle bir beyanda bulunduklarında, tüm mahkeme ve yargı mercilerinin mi yoksa sadece nihai mahkeme veya yargı mercilerinin mi ABAD'a ön karar başvurusunda bulunabileceğine karar vermelidirler.[89] Tüm üye devletler, ulusal mahkemelerden gelen başvurulara ilişkin olarak ABAD'ın yargı yetkisini kabul etmemiş olsalar dahi, ABAD önünde olan bir ön karar

[82] MITSILEGAS, VALSAMIS, 2016, s.8.
[83] Amsterdam Antlaşması ile değişik madde 46-53.
[84] Amsterdam Antlaşması ile değişik madde 46(1)(b).
[85] PEERS, STEVE, "Salvation Outside The Church: Judicial Protection In The Third Pillar After The *Pupino* And *Segi* Judgments", Common Market Law Review, Cilt:44, Sayı:4, 2007, s.885.
[86] PEERS, STEVE, 2007, s.886.
[87] Amsterdam Antlaşması ile değişik madde 35(1).
[88] Amsterdam Antlaşması ile değişik madde 35(2).
[89] Amsterdam Antlaşması ile değişik madde 35(3).

beklenirken beyan veya gözlemlerini sunabilirler.[90] ABAD, bir üye devletin kolluk kuvvetleri tarafından yürütülen operasyonların geçerliliğini veya orantılılığını ya da hukuk ve düzenin sağlanması ve iç güvenliğin korunmasıyla ilgili olarak üye devletlere düşen sorumlulukların yerine getirilmesini inceleme yetkisine sahip değildir.[91]

ABAD, ayrıca, birtakım başka durumlarda da yargı yetkisi verilmiştir. ABAD'a, bir üye devlet veya Komisyon tarafından yetkisizlik, usule ilişkin temel bir gerekliliğin ihlali, ABA'nın veya uygulanmasına ilişkin herhangi bir hukuk kuralının ihlali veya yetkilerin kötüye kullanılması gerekçeleriyle açılan davalardaki çerçeve kararların ve kararların hukuka uygunluğunu inceleme yetkisine verilmiştir.[92] Son olarak ABAD, bir anlaşmazlığın bir Üye Devlet tarafından Konsey'e havale edilmesinden itibaren altı ay içerisinde Konsey'de çözüme kavuşturulamaması halinde, ABA madde 34'te atıfta bulunulan tedbirlerden (ortak tutumlar, kararlar, çerçeve kararlar ve sözleşmeler) herhangi birinin yorumlanması veya uygulanmasına ilişkin olarak üye devletler arasındaki anlaşmazlıklar ile sözleşmelerin yorumlanması veya uygulanmasına ilişkin olarak üye devletler ile Komisyon arasındaki anlaşmazlıklar üzerinde yargı yetkisine sahiptir.[93]

ABAD'ın, Birinci Sütunun aksine, Üçüncü Sütun konuları üzerindeki yargı yetkisi üye devletlerin gönüllü beyanlarına dayandığı için ABAD bu alanı denetlemekten büyük ölçüde muaf tutulmuş[94] ve ABAD'ın yetkisi genellikle kısıtlanmış bir yargı yetkisi olarak

[90] Amsterdam Antlaşması ile değişik madde 35(4).
[91] Amsterdam Antlaşması ile değişik madde 35(5).
[92] Amsterdam Antlaşması ile değişik madde 35(6).
[93] Amsterdam Antlaşması ile değişik madde 35(7).
[94] HERLIN-KARNEL, ESTER, "The European Court of Justice as a game-changer: fiduciary obligations in the area of freedom, security and justice", RIPOLL SERVENT, ARIADNA ve TRAUNER, FLORIAN (Eds.), *The Routledge Handbook of Justice and Home Affairs Research*, 1st Edition, Routledge Taylor & Francis Group, London, 2018, s.396.

görülmüştür.[95] Yine de Maastricht Antlaşması ile kıyaslandığında Amsterdam Antlaşması'nın yürürlüğe girmesi ile birlikte ABAD Üçüncü Sütun için iyileştirilmiş bir yargısal güce kavuşabilmiştir.

Sonuç olarak Maastricht Antlaşması ile Amsterdam Antlaşması dönemi karşılaştırılırsa şu tespitler yapılabilir. Maastricht Antlaşması ile kurulan üç sütunlu yapıda hükümetlerarası yapıda bulunan Üçüncü Sütunda yer alan CKKAİ hususunda Maastricht Antlaşması döneminde Konsey her anlamda başat aktör olmuştur. Bu dönemde Komisyon CKKAİ alanında herhangi girişimde bulunamazken, AP ihtiyari bir danışma organı olarak kalmış, ABAD ise neredeyse yok sayılmıştır. Amsterdam Antlaşması'nın yürürlüğe girmesi ile birlikte Üçüncü Sütun her ne kadar hükümetlerarası yapısını korusa da esaslı denilebilecek değişiklikler geçirmiştir. Öncelikle belirtmek gerekir ki kararlar halen Konsey tarafından oybirliği ile alınıyor olsa da CKKAİ alanında Komisyon insiyatif elde etmiş ve Konsey'e bu anlamda ortak olmuştur. AP danışma organı olarak korumu korumuş ancak kendisine danışılması zorunlu hale gelmiştir. ABAD Birinci Sütun yetkilerine sahip olamasa da önem arz eden yetkilere kavuşmuştur. Özellikle ABAD, Üçüncü Sütun başlığı altında kalan konuların "topluluklaştırma"sında tam anlamıyla bir "oyun değiştirici" rol oynamıştır.[96]

3. LİZBON ANTLAŞMASI ÖNCESİ KİŞİSEL VERİLERİN KORUNMASI

3.1 Kişisel Verilerin Korunmasında Sütunsal Sorunlar

Lizbon Antlaşması öncesi AB veri korumasına ilişkin olarak belirtilmesi gereken ilk husus, Birinci Sütun olarak adlandırılan sütun kapsamındaki kişisel verilerin işlenmesi ile Üçüncü Sütun kapsamındaki kişisel verilerin işlenmesi arasındaki temel farkın ortaya

[95] ABAD'ın Üçüncü Sütun kapsamındaki rolü ile ilgili ayrıntılı bilgi için bakınız. GRIGORIEV, IVAN, "Role of the European Court of Justice in the Third Pillar: Does Not it Grow Too Fast?", Higher School of Economics Research Paper No. WP BRP 11/IR/2014, 2014.
[96] HERLIN-KARNEL, ESTER, 2018, s.397.

konmasıdır. Maastricht Antlaşması ile oluşturulan sütun yapısını takiben, Birinci Sütun kapsamındaki kişisel verilerin işlenmesi esasen tüm ticari işlemleri, yani normalde özel tarafların kendi işleri sırasında gerçekleştirdikleri işlemleri kapsamaktadır. Üçüncü Sütun kapsamındaki kişisel verilerin işlenmesi ise, kolluk ve adli makamlar tarafından kendi yetki ve görevlerini yerine getirirken gerçekleştirilen tüm işlemleri ifade etmektedir.[97]

Lizbon Antlaşması öncesi dönemde Birinci Sütunda kişisel verilerin işlenmesi ve korunması temel olarak; kişisel verilerin işlenmesine ilişkin olarak bireylerin korunması ve bu tür verilerin serbest dolaşımına ilişkin kapsamlı hükümler içeren ve bu alanı düzenleyen ana belge olan Veri Koruma Direktifi ile sağlanmaktadır. Ayrıca bir nevi kişisel verilerin korunmasında Veri Koruma Direktifi'nin tamamlayıcısı niteliğinde olan ve verileri AT kurum ve kuruluşları tarafından işlenirken "veri sahiplerine" veri koruması sağlamak amacıyla yürürlüğe konulan[98] "Topluluk kurum ve kuruluşları tarafından kişisel verilerin işlenmesine ilişkin olarak bireylerin korunması ve bu tür verilerin serbest dolaşımına ilişkin 18 Aralık 2000 tarihli ve 45/2001/EC sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (45/2001 sayılı Tüzük)"[99] bulunmaktadır. Üçüncü Sütun kapsamında ve özellikle CKKAİ alanında ise kişisel verilerin korunmasına ilişkin, 2008/977 sayılı Çerçeve Karar 2008 yılında yürürlüğe girene kadar, AB düzeyinde herhangi bir düzenleme bulunmamakla birlikte bu alanda veri koruma rejiminin yasal çerçeveleri Üçüncü Sütunun kurumları özelinde sektör

[97] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, "The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for", Computer Law & Security Review, Cilt:25, Sayı:5, 2009, s.404.
[98] O'NEILL, MARIA, "The Issue of Data Protection and Data Security in the (Pre-Lisbon) EU Third Pillar", Journal of Contemporary European Research, Cilt:6, Sayı:2, 2010, s.217.
[99] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, s. 1–22

odaklı (Schengen müktesebatı, Europol[100] ve Eurojust[101]) oldukça parçalı görünmektedir.[102] Hepsi de kendi metinlerinde detaylı veri koruma prosedürlerine yer vermiş ve kurumlar oluşturmuştur. Aslında olan şey De Hert ve Papakonstantınou'nun ifade ettiği gibi, ne zaman güvenlikle ilgili veri koruma mevzuatına ihtiyaç duyulsa, bunun, Veri Koruma Direktifi'nde ortaya konan temel ilke ve usuller kullanılarak, geçici olarak çözülmesiydi. Ancak bu şekilde normal yasa yapma akışı tersine dönmüş, Birinci Sütunda olduğu gibi, önce standart belirleyici metin ve ardından sektöre özel metinlerin yayınlanması yerine, Üçüncü Sütunda sektöre özel metinler standart belirleyici metinden önce gelmiştir.[103] Buradan da anlaşılacağı üzere kolluk ve adli makamlar tarafından herhangi bir veri işlemeyi içeren tüm Avrupa girişimleri, özel veri koruma kuralları öngörmüş ve bu da parçalanmış bir düzenlemeler bütünü ile sonuçlanmıştır.[104]

Yukarıda da belirtildiği üzere Birinci Sütun kapsamında veri koruması Veri Koruma Direktifi tarafından sağlanmaktadır. 24 Ekim 1995 tarihinde yürürlüğe giren ve 24 Ekim 1998'e kadar Üye Devletlerin ulusal hukuk sistemlerine aktarılması öngörülen Veri Koruma Direktifi AB'de kişisel verilerin korunmasına yönelik ilk düzenlemedir. Bu Direktif, hukuki dayanağını AB'nin kurucu antlaşmasında yer alan ve iç pazarın kurulması ile işleyişini sağlamak amacıyla üye devletlerin hukuk sistemlerini uyumlaştırmaya yönelik tedbirler almasını öngören Maastricht Antlaşması ile değişik ATA madde 100a'dan almaktadır.[105]

---

[100] Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), OJ C 316, 27.11.1995, s. 2–32

[101] 2002/187/JHA: Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 63, 6.3.2002, s. 1–13

[102] O'NEILL, MARIA, 2010, s.214.

[103] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2009), s.405.

[104] DE HERT, PAUL, *et.al.*, "Data protection in the third pillar: Cautious pessimism", MARTIN, MAIK (Ed.), *Crime, Rights and the EU: The Future of Police and Judicial Cooperation*, Justice, London, 2007, s.122.

[105] GÖÇMEN, İLKE ve ŞEKER, EMRİYE ÖZLEM, "Kişisel Verilerin Korunması Tüzüğü'ne İlişkin Avrupa Birliği Adalet Divanının İlk Kararları", ŞENOCAK, KEMAL, *Muhtelif Yönleriyle Kişisel Verilerin Korunması Hukuku*, Yetkin Yayıncılık, Ankara, 2022, s.241.

Veri Koruma Direktifi'nin dibacesinde, teknolojik gelişmeler nedeniyle kişisel verilerin üye devletler arasında kolayca dolaşabildiği, ancak üye devletlerin bu konuda farklı ulusal düzenlemelere sahip olmasının iç pazarın işleyişini engellediği vurgulanmıştır.[106] Bu engellerin ortadan kaldırılması ve kişisel verilerin korunmasına ilişkin ulusal düzenlemelerin uyumlaştırılması ihtiyacı, Veri Koruma Direktifi'nin kabul edilmesinin temel nedenleri arasında gösterilmiştir.[107] Dolayısıyla, kişisel verilerin korunması ve serbest dolaşımı, iç pazarın işleyişiyle bağlantılı bir AB yetkisi kapsamında bu Direktif ile düzenlenmiştir.[108] AB hukukunda düzenleyici araçlardan biri olan direktifler, Üye Devletler için ulaşılması gerekli hedefler açısından bağlayıcıdır; ancak bu hedeflere ulaşmak için izlenecek yöntemin ve şeklin belirlenmesinde Üye Devletlere esneklik tanır. Bu çerçevede, her üye devlet, belirli bir süre içinde ilgili direktifi ulusal mevzuatına aktarmakla yükümlüdür.[109]

Verilerin korunmasına ilişkin Veri Koruma Direktifi kişisel verilerin işlenmesi ve serbest dolaşımı konusunu düzenleyerek uyulması gereken genel ilkeleri ortaya koymuştur. Komisyon tarafından da vurgulandığı üzere, direktifte yer alan uyumlaştırılmış kurallar dizisi "AB genelinde kişisel veriler için yüksek standartta bir koruma sağlamakta ve vatandaşlar, işletmeler ve yetkililer için önemli faydalar getirmektedir".[110] Bununla birlikte, CKKAİ çerçevesinde kişisel verilerin işlenmesi Avrupa düzeyinde düzenlenmemiştir. Veri Koruma Direktifinin 3(2) maddesinde "Bu direktif, Avrupa Birliği Antlaşması'nın V. ve VI. Başlıklarında öngörülenler gibi Topluluk hukuku kapsamı dışında kalan bir faaliyet sırasında ve her halükarda kamu güvenliği, savunma, devlet güvenliği (işleme faaliyetinin devlet

[106] Veri Koruma Direktifi, Dibace paras 3-7.
[107] Veri Koruma Direktifi, Dibace para 8.
[108] GÖÇMEN, İLKE ve ŞEKER, EMRİYE ÖZLEM, 2022, s.242.
[109] GÖÇMEN, İLKE ve ŞEKER, EMRİYE ÖZLEM, 2022, s.242.
[110] Communication from the European Commission to the European Parliament and Council on the follow-up of the Work Programme for better implementation of the data protection directive, COM(2007) 87 final, 7 March 2007, s.2.

güvenliği konularıyla ilgili olması halinde devletin ekonomik refahı da dahil olmak üzere) ve devletin ceza hukuku alanlarındaki faaliyetleri ile ilgili işleme faaliyetlerine uygulanmaz" denilerek bu Veri Koruma Direktifi'nin İkinci Sütun (ODGP) ve Üçüncü Sütun (Aİİ) ile ilgili faaliyetler bakımından geçerli olmadığına açıkça yer verilmiştir.[111]

Görüldüğü üzere Veri Koruma Direktifi, Üçüncü Sütun ile ilgili kişisel verilerin korunması açısından herhangi bir koruma sağlamayacağını net bir şekilde ortaya koymuştur. Peki, 2008/977 sayılı Çerçeve Karar yürürlüğe konulana kadar Üçüncü Sütun kapsamındaki CKKAİ çerçevesinde işlenen kişisel verilerin herhangi bir koruması yok muydu? Bunun cevabını verebilmek için bu alandaki kişisel verilerinin korunmasının tarihsel gelişimine ve bu alandaki uluslararası düzenlemelere bakmak gerekir. Bir sonraki başlık altında bu konu üzerinde durulacaktır.

3.2 Üçüncü Sütunda 2008/977 sayılı Çerçeve Karar'a Kadar Olan Süreçte Kişisel Verilerin Korunması

Veri Koruma Direktifi'nin hâkim olduğu Birinci Sütunda yaşananların aksine, güvenlikle ilgili Üçüncü Sütunda işleme için 2008/977 sayılı Çerçeve Karar'ın yayınlanmasına kadar hiçbir standart belirleyici AB yasal metni mevcut değildi. Üçüncü Sütun kapsamında, CKKAİ çerçevesinde kişisel verilerin koruması konusu Veri Koruma Direktifi kapsamında olmasa da, tamamen korumasız değildi.[112] Bu alanda kişisel verilerin korunması AB dışındaki aktörler tarafından ortaya konan düzenlemeler ile sağlanıyordu.

Öncelikle, doğrudan kişisel verilerin korunmasından bahsetmese de, 1950 yılından beri uluslararası hukukta var olan ve imzacı devletler (tüm AB Üye Devletleri Avrupa

[111] KOSTA, ELENI, *et.al*, "Data Protection in the Third Pillar: In the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive", International Review of Law, Computers & Technology, Cilt:2, Sayı:3, 2007, s.348.
[112] KOSTA, ELENI, *et.al*, 2007, s.348.

Konseyi üyesidir) için bağlayıcılığı bulunan Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) "özel hayata saygı hakkı" başlıklı 8'inci maddesi ve bu maddeyi yorumlayarak kişisel verilerin korunmasını da bu hakkın bir parçası olarak kabul eden Avrupa İnsan Hakları Mahkemesi (AİHM) içtihat hukuku bu alanda koruma sağlamaktaydı. AİHM, kişisel veri ihlalleri söz konusu olduğunda AİHS'nin 8'inci maddesindeki "özel hayata saygı hakkına" atıfta bulunmaktadır. Kişisel veriler bu madde tarafından açıkça korunmasa bile, AİHM "kişisel verilerin korunmasının" bir kişinin özel ve aile yaşamına saygı hakkından yararlanması için "temel öneme" sahip olduğunda ısrar etmektedir.[113] Belirli bir duruma uyarlanmış içtihatlardan genel uygulama ilkeleri çıkarmak zor gibi görünse de AİHM yine de bu özel alanda oldukça kapsamlı bir veri koruma çerçevesi geliştirmeyi başarmıştır.[114]

İkinci olarak, AB'ye üye devletler ile sınırlı olmamak üzere, CKKAİ alanında kişisel verilerin korunmasını da kapsayan, uluslararası bağlayıcılığı olan ilk belge özelliğine sahip, "108 sayılı Sözleşme" ile "R (87) 15 sayılı Tavsiye Kararı" Üçüncü Sütun çerçevesinde AB'de gerekli kişisel verilerin korunması için geçerli olan ve AB'nin Üçüncü Sütunun tamamı için geçerli olmayan sektör odaklı AB belgelerinde[115] en çok atıf yaptığı

[113] AİHM'in kişisel verilerin korunmasına ilişkin bazı kararları: Application No. 27798/95, Case of *Amann v. Switzerland*, Application No. 30562/04, Case of *S. and Marper v. the United Kingdom*.

[114] BOEHM, FRANZISKA, "Information Sharing in the Area of Freedom, Security and Justice—Towards a Common Standard for Data Exchange Between Agencies and EU Information Systems", GUTWİRTH, SERGE, *et.al.*, *European data protection: in good health?*, Springer Science & Business Media, 2012, s.147.

[115] Bu konuda en iyi örnek 1995 yılında hazırlanan ve 1999 yılında yürürlüğe giren "Europol Sözleşmesi"nin "Veri koruma standardı" başlıklı 14'üncü maddesidir.

"1. Bu Sözleşme'nin en geç yürürlüğe girdiği tarihte, her Üye Devlet, ulusal mevzuatı çerçevesinde, bu Sözleşme çerçevesinde veri dosyalarındaki kişisel verilerin işlenmesiyle ilgili olarak, en azından 28 Ocak 1981 tarihli Avrupa Konseyi Sözleşmesi'nin ilkelerinin uygulanmasından kaynaklanan standarda karşılık gelen bir veri koruma standardı sağlamak için gerekli önlemleri alacak ve bunu yaparken, Avrupa Konseyi Bakanlar Komitesi'nin kolluk sektöründe kişisel verilerin kullanımına ilişkin 17 Eylül 1987 tarihli ve R (87) 15 sayılı Tavsiye Kararı'nı dikkate alacaktır.

2. Bu Sözleşmede öngörülen kişisel verilerin iletimi, yukarıdaki 1. paragrafta belirtilen veri koruma kuralları, söz konusu iletişime dahil olan Üye Devletlerin her birinin topraklarında yürürlüğe girene kadar başlayamaz.

3. Europol, kişisel verilerin toplanması, işlenmesi ve kullanılmasında 28 Ocak 1981 tarihli Avrupa Konseyi Sözleşmesi ve Avrupa Konseyi Bakanlar Komitesi'nin 17 Eylül 1987 tarihli ve R (87) 15 sayılı Tavsiye Kararı ilkelerini dikkate alacaktır.

düzenlemelerdi. Genel olarak, Lizbon Antlaşması öncesi dönemde kabul edilen Üçüncü Sütun belgeleri, R (87)15 sayılı Tavsiye Kararı da dikkate alınarak, kendi bağlamlarında işlenen verilere erişimi, üye devletler tarafından kişisel verilerin en azından 108 sayılı Sözleşme'nin ilkelerinden kaynaklanan koruma düzeyine eşit bir düzeyde koruması şartına bağlamıştır.[116] Üçüncü Sütun kapsamında kişisel verilerin korunması hususunun tam anlaşılabilmesi için bu korumayı sağlayan ve yukarıda adları zikredilen belgelere[117] yakından bakmak gerekmektedir.

3.2.1 108 sayılı Sözleşme ve Ek Protokolleri

1981 yılında, Avrupa çapında ilk ortak "model yasa" olan 108 sayılı Sözleşme, onaylayan üyeler için 1 Ekim 1985 tarihinde yürürlüğe girmiştir. Sözleşme, veri koruma konusunda uluslararası bağlayıcılığı olan ilk belgedir ve sonraki tüm ulusal veri koruma yasaları için önemli bir yönlendirme noktası oluşturmuştur.[118]

108 sayılı Sözleşme, her bireyin "kendisiyle ilgili kişisel verilerin otomatik olarak işlenmesi ("verilerin koruması") ile ilgili olarak haklarına ve temel özgürlüklerine ve özellikle de özel hayata saygı gösterilmesini" güvence altına almayı amaçlamıştır.[119] 108 sayılı Sözleşme'de "kişisel veri", kimliği belirli veya belirlenebilir bir kişiye ("veri sahibi") ilişkin her türlü bilgi, "otomatik işleme" ise tamamen veya kısmen otomatik araçlarla, verilerin depolanması, bu veriler üzerinde mantıksal ve/veya aritmetiksel işlemlerin

Europol, veri dosyaları şeklinde tutulan otomatik olmayan verilerle, yani belirli kriterlere uygun olarak erişilebilen herhangi bir yapılandırılmış kişisel veri setiyle ilgili olarak da bu ilkeleri gözetecektir."

[116] FUSTER, GLORIA GONZÁLEZ, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer Science & Business, 2014, s.146.

[117] AİHS'nin 8'inci maddesi, 108 sayılı Sözleşme ve R (87)15 sayılı Tavsiye Kararı ile ilgili ayrıntılı bilgi için bakınız. BOEHM, FRANZISKA, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Springer Science & Business Media, Heidelberg, 2012, s.22-106.

[118] DE HERT, PAUL, *et.al.*, 2007, s.124.

[119] 108 sayılı Sözleşme, madde 1.

gerçekleştirilmesi, değiştirilmesi, silinmesi, geri alınması veya yayılması olarak tanımlanmaktadır.[120] Devlet müdahalesine karşı bireyin korunmasıyla ilgili olan AİHS'nin aksine, 108 sayılı Sözleşme hem özel hem de kamu sektörünü kapsamaktadır.[121]

108 sayılı Sözleşme kapsamında otomatik işleme tabi tutulan kişisel veriler; adil ve hukuka uygun olarak elde edilmeli ve işlenmeli, belirli ve meşru amaçlar için saklanmalı ve bu amaçlarla bağdaşmayacak şekilde kullanılmamalı, saklandıkları amaçlara ilişkin olarak yeterli ve ilgili olmalı ancak aşırı olmamalı ve son olarak doğru bir şekilde tutulmalı ve gerektiğinde güncellenmelidir.[122] 108 sayılı Sözleşme, ırksal köken, siyasi görüşler, dini veya diğer inançlar, sağlık ve cinsel yaşamla ilgili veriler ve cezai mahkumiyetleri ortaya koyan özel veri kategorilerine özellikle dikkat etmiş ve ulusal mevzuat uygun güvenceler sağlamadığı sürece bunların işlenmesinin otomatik olarak yapılmasını yasaklamıştır.[123]

108 sayılı Sözleşme, bireyler için bilgi edinme, erişim, düzeltme ve verilerin silinmesine yönelik maddi haklar tesis etmiştir.[124] Ayrıca, tesis edilen bu hakların kullanılmasının ihlaline yönelik genel çözüm yolları ve yaptırımlara[125] ek olarak, maddi haklara işlerlik kazandıran usuli bir çözüm hakkı da düzenlenmiştir.[126]

108 sayılı Sözleşme'de genel kural Sözleşme ile getirilen hükümlere sınırlama getirilemeyeceği şekilde belirtilirken, bu duruma iki istisna getirilmiştir: (1) Devlet güvenliğinin, kamu güvenliğinin, Devletin parasal çıkarlarının korunması veya suçların bastırılması. (2) veri sahibinin veya başkalarının hak ve özgürlüklerinin korunması.[127] 108

[120] 108 sayılı Sözleşme, madde 2 (a) ve (c).
[121] 108 sayılı Sözleşme, madde 3(1).
[122] 108 sayılı Sözleşme, madde 5.
[123] 108 sayılı Sözleşme, madde 6.
[124] 108 sayılı Sözleşme, madde 8 (a), (b) ve (c).
[125] 108 sayılı Sözleşme, madde 8 (d).
[126] 108 sayılı Sözleşme, madde 10.
[127] 108 sayılı Sözleşme, madde 9.

sayılı Sözleşme, sınır ötesi veri akışlarını, yalnızca otomatik veri dosyalarına veya belirli kategorilere ait verilere ilişkin ulusal yasalar olması halinde kısıtlamalar getirerek ve verilerin 108 sayılı Sözleşme'ye bağlı olmayan bir ülke üzerinden yeniden yönlendirilmesi yoluyla yasağının delinmesini önlemek için izin verici bir şekilde düzenlemiştir.[128]

108 sayılı Sözleşme verilerin üçüncü devletlere aktarımını düzenlemediğinden, Avrupa Konseyi Kasım 2001'de denetim makamları ve sınır ötesi veri akışlarına ilişkin 108 sayılı Sözleşmeyi tadil eden ek bir protokol kabul etmiştir.[129] Ek protokol ile 108 sayılı Sözleşme ve ek protokollerinde belirtilen ilkelere yürürlük kazandıran iç hukuk tedbirlerine uyulmasını sağlamaktan sorumlu bir veya birden fazla "bağımsız" denetim makamı öngörülmüştür.[130] Bu protokole göre, üçüncü taraflara aktarıma genellikle üçüncü tarafın amaçlanan aktarım için yeterli düzeyde koruma sağlaması koşuluyla izin verilmektedir.[131] Yeterlilik mekanizması her bir aktarım için koruma düzeyini değerlendirirken dikkate alınması gereken belirli kriterler sunmaktadır. Aktarımın koşullarının, özellikle de veri türünün incelenmesine ek olarak, verilerin aktarıldığı amaçlar ve işleme süresi, menşe ülke ve nihai varış ülkesi, söz konusu devlet veya kuruluşta geçerli olan genel ve sektörel hukuk kuralları ve orada yürürlükte olan mesleki ve güvenlik kuralları dikkate alınmalıdır.[132] Bununla birlikte, taraf devletler, iç hukukun öngörmesi halinde, veri sahibinin özel menfaati veya meşru üstün menfaat (özellikle önemli kamu menfaati) nedeniyle veya aktarımdan sorumlu kontrolör tarafından yeterli güvencelerin sağlanması halinde bu hükme istisna getirebilirler.[133]

---

[128] 108 sayılı Sözleşme, madde 12.
[129] Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin Sözleşme'nin denetim makamları ve sınır ötesi veri akışlarına ilişkin Ek Protokolü (Ek Protokol), 8 Kasım 2001.
[130] Ek Protokol, madde 1.
[131] Ek Protokol, madde 2(1).
[132] Ek Protokol'ün Açıklayıcı Raporu, madde 27.
[133] Ek Protokol, madde 2(2).

108 sayılı Sözleşme'nin önemi sadece içeriğinde, ilkelerinde veya "veri koruma" teriminin ilk kez bağlayıcı bir belgede kullanılmış olmasında değil, başta Avrupa ülkeleri olmak üzere dünya çapında veri koruma yasalarının gelişiminde oynadığı rolden gelmektedir.[134]

3.2.2 R (87)15 sayılı Tavsiye Kararı

R (87)15 sayılı Tavsiye Kararı özellikle Üçüncü Sütun kapsamında kolluk ve adli makamlar tarafından işlenen kişisel verilerin korunması açısından Lizbon Antlaşması öncesi dönem için önem arz etmektedir. Tavsiye kararları, bağlayıcı olmamakla birlikte Avrupa Konseyi üye devletlerine yön gösterici nitelikte metinlerdir. R (87) 15 sayılı Tavsiye Kararı da bu çerçevede, kolluk sektöründe kişisel verilerin işlenmesine ilişkin ilkelerini belirlemekte ve üye devletlerin ulusal mevzuatlarını bu doğrultuda şekillendirmelerini teşvik etmektedir. Yukarıda da bahsedildiği üzere Lizbon Antlaşması öncesi Üçüncü Sütun AB kurumlarının belgelerinde söz konusu Tavsiye Kararına birçok kez atıfta bulunulmuştur.[135]

R (87) 15 sayılı Tavsiye Kararı'nın "kontrol ve bildirim" başlıklı ilk ilkesi, bu Tavsiye Kararda yer verilen ilkelere uygunluğu denetleyecek, kolluk sektörü dışında oluşturulması gereken, "bağımsız bir denetim makamına" atıfta bulunmaktadır.[136] Kolluk birimleri tarafından veri işlemeye yönelik yeni teknik araçların uygulamaya konulabilmesi için R (87) 15 sayılı Tavsiye Kararında iki gerekliliğin yerine getirilmesi düzenlemektedir: sorumlu ulusal denetim makamına uygulamaya konulmadan önce danışılması ve bu araçların kullanımının mevcut veri koruma mevzuatının ruhuna uygun olmasını sağlamak için tüm

[134] KAMARA, IRENE, *Data protection standardisation: The role and limits of technical standards in the EU data protection law*, Doktora Tezi, TILT, Vrije Universiteit Brussel – LSTS, 2021, s.45.
[135] BOEHM, FRANZISKA, 2012, s.96.
[136] R (87) 15 sayılı Tavsiye Kararı, İlke 1.1.

makul tedbirlerin alınması.[137] R (87) 15 sayılı Tavsiye Kararı'nın açıklayıcı notunda bağımsız denetim makamının rolünün danışma organı niteliğinde bir rolle sınırlı tutulsa da, bu organa önceden danışılmasının, yeni teknolojiler uygulamaya konulmadan önce bu uygulamaların kamuoyunda tartışılmasının önünü açacağı vurgulanmaktadır.[138] Ayrıca, denetim makamına kalıcı olarak otomatikleştirilmiş dosyalara ilişkin yapılan bildirimin, beyan edilen her dosyanın niteliğini, işlenmesinden sorumlu organı, amaçlarını, dosyada yer alan veri türünü ve verilerin iletildiği kişileri içermesi gerekmektedir.[139]

R (87) 15 sayılı Tavsiye Kararı'nın "verilerin toplanması" başlıklı ikinci ilkesi, verilerin kullanımına ilişkin sert sayılabilecek bir sınırlama ile başlamaktadır. Bu ilke kapsamında "kişisel verilerin kolluk amaçları doğrultusunda toplanması, gerçek bir tehlikenin önlenmesi veya belirli bir suçun bastırılması için gerekli olanlarla sınırlı olmalıdır". Ancak bu sert ifade, bir sonraki cümlede, bu hükme getirilecek herhangi bir istisnanın özel ulusal mevzuata tabi olacağı belirtilerek sınırlandırılmıştır.[140] R (87) 15 sayılı Tavsiye Kararı'nın açıklayıcı notunda, bu kuralın kolluk tarafından açık uçlu ve gelişigüzel veri toplanmasını yasaklayarak 108 sayılı Sözleşme'nin 5 (c) maddesinde yer alan ve kişisel verilerin saklanma amacına göre yeterli ve ilgili olması ve aşırı olmaması gerektiğini belirten ifadeye niteliksel ve niceliksel bir yaklaşımı ifade ettiği belirtilmektedir.[141] Açıklayıcı notta ayrıca R (87) 15 sayılı Tavsiye Kararı'nın ikinci ilkesinin, 108 sayılı Sözleşme'nin 9(2)(a) maddesinde öngörülen ve "cezai suçların bastırılması" ile ilgili olarak kişisel verilerin saklanma amacına göre yeterli ve ilgili olması ve aşırı olmaması gerektiği ilkesinden

[137] R (87) 15 sayılı Tavsiye Kararı, İlke 1.2 ve 1.3.
[138] R (87) 15 sayılı Tavsiye Kararının açıklayıcı notu madde 31-35. BOEHM, FRANZISKA, 2012, s.97.
[139] R (87) 15 sayılı Tavsiye Kararı, İlke 1.4.
[140] R (87) 15 sayılı Tavsiye Kararı, İlke 2.1.
[141] R (87) 15 sayılı Tavsiye Kararının açıklayıcı notu madde 43.

sapmaya izin veren istisnanın, mevzuat bilgi toplamak için daha geniş kolluk yetkilerine açıkça izin vermediği sürece, gerçek bir tehlikenin önlenmesi veya belirli bir suçun bastırılması için gerekli olan verilerin toplanmasıyla sınırlı olması gerektiği belirtilmektedir. Açıklayıcı notta gerçek tehlike, "belirli bir suç veya suçlu ile sınırlı olmayıp, desteklenmeyen spekülatif olasılıklar hariç olmak üzere, ciddi suçların işlendiğine veya işlenebileceğine dair makul şüphenin bulunduğu her türlü durumu kapsar" şeklinde tanımlanmaktadır.[142] AİHM'nin *Leander*[143] kararını dikkate alarak, ikinci ilke ayrıca, kolluk faaliyetlerinin amacı artık tehlikeye girmeyeceği anda, ilgili kişinin bilgisi dışında hakkında veri toplandığında ve saklandığında kendisine bildirimde bulunulmasını gerektirmektedir.[144]

R (87) 15 sayılı Tavsiye Kararı'nın "verilerin depolanması" başlıklı üçüncü ilkesi, depolanan verilerin doğru olması ve ulusal ve uluslararası hukuk çerçevesinde kolluğun görevlerini yerine getirmesi için gerekli olması sınırlamasına ek olarak, idari amaçlarla toplanan veriler ile kolluk amaçları için toplanan veriler arasında ayrım yapılması gerektiğini vurgulamaktadır. Her iki kategorinin de ayrı dosyalarda tutulması ve idari verilerin kolluk verilerine uygulanan kurallara tabi olmaması gerektiğini dile getirilmektedir.[145] Ayrıca depolanan farklı veri kategorilerinin, doğru ve güvenilir olma dereceleri göz önünde bulundurularak tasnif edilmesi ve özellikle gerçeklere dayanan veriler ile kişisel görüş ve değerlendirmeler içeren verilerin açıkça ayrı tutulması gerektiği belirtilmektedir.[146] R (87) 15 sayılı Tavsiye Kararı'nın üçüncü ilkesi, kolluk tarafından toplanan veriler ile idari

[142] R (87) 15 sayılı Tavsiye Kararının açıklayıcı notu madde 43. Ayrıca aynı madde gerçek tehlike kavramını açıklığa kavuşturmak için bir örnek vermektedir; "tanımlanamayan özel yatlar tarafından bir liman üzerinden ülkeye yasadışı yollardan uyuşturucu sokulduğuna dair makul şüphe, o limanı kullanan tüm yatlar, sahipleri ve yolcuları hakkında veri toplanmasını haklı kılacaktır, ancak o ülkedeki her limanı kullanan tüm yatlar, sahipleri ve yolcuları hakkında değil."
[143] Application No. 9248/81, Case of *Leander v. Sweden*
[144] R (87) 15 sayılı Tavsiye Kararı, İlke 2.2 ve R (87) 15 sayılı Tavsiye Kararının açıklayıcı notu madde 45.
[145] R (87) 15 sayılı Tavsiye Kararı, İlke 3.1 ve 3.3.
[146] R (87) 15 sayılı Tavsiye Kararı, İlke 3.2.

amaçlarla toplanan veriler arasındaki önemli ayrımı kabul etmektedir. Birinci Sütun aktörleri ile Üçüncü Sütun aktörleri (özellikle kolluk teşkilatları) arasında artan veri aktarımı sonucu bir zamanlar idari veya ekonomik bağlamda toplanan veriler için geçerli olan veri koruma kuralları, verilerin kolluk birimlerine aktarıldığı anda değişmektedir. Çoğu durumda, kişiler kolluk birimlerine yapılan bu aktarımdan veya kişisel verilerin korunması çerçevesinde uygulanan kurallarda gerçekleşen değişimden haberdar olamayacaktır.[147]

R (87) 15 sayılı Tavsiye Kararı'nın "verilerin kolluk tarafından kullanımı" başlıklı dördüncü ilkesi, kolluk tarafından toplanan ve saklanan verilerin sadece kolluk amaçları için, yani suçların önlenmesi ve bastırılması veya kamu düzeninin korunması için kullanılmasını düzenlemektedir. Ancak bu ilkenin mutlak niteliği, verilerin iletilmesi ile ilgili beşinci ilke ile kısmen değiştirilebilir.[148]

R (87) 15 sayılı Tavsiye Kararı'nın "verilerin aktarılması" başlıklı beşinci ilkesine göre, verilerin kamu makamlarına aktarılması, yukarıda belirtilen esaslara uygun olarak meşru bir menfaat temelinde gerçekleştirilmelidir. Böyle bir aktarım, veri sahibinin menfaatine açıkça hizmet ettiği, rıza gösterdiği veya rıza gösterdiğine dair güçlü bir karine bulunduğu veya ciddi ve yakın bir tehlikenin önlenmesi için gerekli olduğu durumlarda mümkündür.[149] Beşinci ilke çeşitli veri aktarım yöntemlerini düzenlerken, aynı zamanda tüm veri aktarım süreçleri için geçerli olan genel ilkeleri de içermektedir. Verilerin özel taraflara aktarımı için yalnızca daha katı istisnalar öngörülmüştür.[150] Verilerin yabancı makamlara aktarımı esas olarak kolluk teşkilatlarıyla sınırlı tutulmuş ve yalnızca ulusal veya uluslararası hukukta açık bir yasal dayanak varsa gerçekleştirileceği hüküm altına alınmıştır. Böyle bir

[147] BOEHM, FRANZISKA, 2012, s.99.
[148] R (87) 15 sayılı Tavsiye Kararı, İlke 4 ve R (87) 15 sayılı Tavsiye Kararının açıklayıcı notu madde 55.
[149] R (87) 15 sayılı Tavsiye Kararı, İlke 5.2.i.–5.3.ii.
[150] R (87) 15 sayılı Tavsiye Kararı, İlke 5.3.i.–5.3.ii.

yasal dayanağın bulunmaması halinde, veri aktarımı sadece ciddi ve yakın bir tehlikenin önlenmesi veya ciddi bir suçun soruşturulması için kesinlikle gerekli olması halinde mümkün olacaktır.[151] Yabancı kolluk makamlarına aktarılan veriler yalnızca talep edildiği amaç için kullanılacak ve farklı bir amaç için kullanımı ilgili taraflarla önceden varılan bir anlaşmaya dayandırılacaktır.[152] Ayrıca, dosyaların farklı amaçlarla tutulan dosyalarla birbirine bağlanması ya denetim makamının iznine tabi ya da açık bir yasal hükme uygun olmalıdır.[153]

R (87) 15 sayılı Tavsiye Kararı'nın "Tanıtım, kolluk dosyalarına erişim hakkı, düzeltme hakkı ve itiraz hakkı" başlıklı altıncı ilkesine göre, bireylere kollukta bulunan kendine ait verilere ilişkin erişim, düzeltme ve silme hakkı vermektedir.[154] Ancak veri sahibinin tanımlanan bu haklarına, kolluğun yasal görevini yerine getirmesi için kaçınılmaz veya veri sahibinin ya da başkalarının hak ve özgürlüklerinin korunması için gerekli olduğunda kısıtlamalar getirilebileceği düzenlenmektedir.[155] Bireylerin erişim talebinin reddedilmesi halinde, bireyin denetim makamına veya bağımsız bir organa itiraz etme imkânı olmalıdır.[156]

R (87) 15 sayılı Tavsiye Kararı'nın "Depolama süresi ve verilerin güncellenmesi" başlıklı yedinci ilkesine göre verilerin saklanması ve saklandıkları amaçlar için artık gerekli olmamaları halinde silinmeleri için gerekli tedbirlerin alınması gerekmektedir. Söz konusu tedbirler belirlenirken belirli bir davaya ilişkin bir soruşturmanın sonuçlanması, nihai bir yargı kararı, özellikle beraat, rehabilitasyon, geçmiş mahkumiyetler, aflar, veri sahibinin yaşı ve belirli veri kategorileri ışığında verilerin saklanması ihtiyacı göz önünde

[151] R (87) 15 sayılı Tavsiye Kararı, İlke 5.4.
[152] R (87) 15 sayılı Tavsiye Kararı, İlke 5.5.iii.
[153] R (87) 15 sayılı Tavsiye Kararı, İlke 5.6.
[154] R (87) 15 sayılı Tavsiye Kararı, İlke 6.1-6.3.
[155] R (87) 15 sayılı Tavsiye Kararı, İlke 6.4.
[156] R (87) 15 sayılı Tavsiye Kararı, İlke 6.6.

bulundurulmalıdır.[157] Verilerin kalitesine ilişkin düzenli kontrollere ek olarak, R (87) 15 sayılı Tavsiye Kararı'nın "veri güvenliği" başlıklı sekizinci ilkesi verilerin uygun fiziksel ve mantıksal güvenliğinin sağlanması ve yetkisiz erişim, iletişim veya değişikliğin önlenmesi için gerekli tedbirlerin genel olarak alınmasını öngörmektedir.[158] Sonuç olarak, R (87) 15 sayılı Tavsiye Kararı kolluk sektörü için önemli ve temel veri koruma ilkelerini içermektedir. Her ne kadar R (87) 15 Tavsiye Kararı bağlayıcı olmasa da AB'de CKKAİ alanında kişisel verilerin korunmasına ilişkin politikaların şekillenmesinde temel bir rol oynamıştır.

4. 2008/977 SAYILI KONSEY ÇERÇEVE KARARI

4.1 Kolluk ve Adli İşbirliğindeki Gelişmeler ve Lahey Programı

Bir ÖGAA'nın oluşturulması, ekonomik bir birliktelik kurulması amacıyla çıkılan yolda Avrupa entegrasyonunun iddialı bir projesi olmuştur. Amsterdam Antlaşması ile ortaya konan bu projenin bir ayağını da Üçüncü Sütun altında düzenlenen CKKAİ oluşturmaktaydı. Daha önceki bölümlerde de dile getirildiği üzere 1970'lerde başlayan bu alandaki girişimler daha sonra her ne kadar hükümetlerarası yapıyı muhafaza etse de kurucu antlaşmalar ile AB yapısı içine aktarılmış ve kurumsal bir yapıya kavuşturulmuştur.

İtalya'nın girişimiyle Üçüncü Sütunda kişisel verilerin korunması konusu 1998 yılında tartışılmaya başlanmıştır. O dönemde Adalet ve İçişleri Konseyi, Viyana Eylem Planı olarak adlandırılan planı kabul etmiştir.[159] Bu plan, CKKAİ bağlamındaki yatay sorunlarla ilgili olarak, Amsterdam Antlaşması'nın yürürlüğe girmesinden itibaren iki yıl içinde veri

[157] R (87) 15 sayılı Tavsiye Kararı, İlke 7.1.
[158] R (87) 15 sayılı Tavsiye Kararı, İlke 7.2 ve 8.
[159] Action Plan of the Council and the Commission on how best to implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice - Text adopted by the Justice and Home Affairs Council of 3 December 1998, OJ C 19, 23.1.1999, s.1–15.

korumaya ilişkin uyumlaştırılmış kurallara yönelik olasılıkların incelenmesini öngörmektedir.[160]

Ancak iki yıl içerisinde AB'nin Üçüncü Sütunu kapsamındaki araçlarda kişisel verilerin korunması kurallarına ilişkin bir karar taslağı kabul edilememiştir.[161] Haziran 2003'te Yunanistan Dönem Başkanlığı Üçüncü Sütunda kişisel verilerin korunmasına ilişkin olarak Veri Koruma Direktifi'nden esinlenen bir dizi genel ilke önermiştir.[162] AP tarafından da Üçüncü Sütun araçlarında kişisel verilerin korunmasına ilişkin mevcut kuralların uyumlaştırılması ve bunların Birinci Sütunda öngörülenle aynı düzeyde veri korumasını garanti eden tek bir araçta bir araya getirilmesini tavsiye edilmiştir.[163] Ayrıca 2005 yılında, Avrupa Birliği Üye Devletlerinin Veri Koruma Otoriteleri ve Avrupa Veri Koruma Denetmeni (AVKD) tarafından Üçüncü Sütunda kişisel verilerin korunmasına yönelik yeni bir yasal araç için güçlü bir destek verilmiş ve bu destek şu şekilde ifade edilmiştir:[164]

> "*Amsterdam Antlaşması'nın üye devletlere ÖGAA yaratma taahhüdünde bulunmasından bu yana, kolluk kuvvetleri arasındaki işbirliğini geliştirmeyi amaçlayan girişimler olmuştur. AB çapındaki bu girişimler genellikle kişisel veri aktarımı içerdiğinden, bu belge, mevcut yasal belgelerde yer alan temel haklar dikkate alınarak, yüksek standartta veri korumasını güvence altına alacak uygun tedbirlerin alınmasını sağlamak amacıyla hazırlanmıştır.*"

[160] Commission, Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, (COM(2005) 475 final), 4.10.2005, s.3.
[161] Council Working Document 6316/2/01 REV 2 JAI 13.
[162] 2514th Council Meeting, Justice and Home Affairs, Luxembourg, 5-6 June 2003, Council Document 9845/03 (Presse 150), s.32.
[163] No. 1 h of European Parliament recommendation to the European Council and the Council on the exchange of information and cooperation concerning terrorist offences (2005/2046(INI)), adopted on 7 Mayıs 2005.
[164] Declaration and Position paper on law enforcement and information exchange in the EU, adopted by the Spring Conference of European Data Protection Authorities, Krakow, 25-26 Nisan 2005.

AB'de CKKAİ alanındaki ilerleme açısından dönüm noktasını 11 Eylül 2001 New York'taki terör saldırı oluşturmuştur. Söz konusu saldırılar dünyada olduğu gibi AB üye devletlerinde de güvenlik endişelerinin artmasına neden olmuş, 2004 ve 2005'teki Madrid ve Londra saldırıları da bu güvenlik endişelerini en üst düzeye çıkartmıştır. Bu durum AB Zirvesi tarafından 4 Kasım 2004 tarihinde kabul edilen AB'de özgürlük, güvenlik ve adaletin güçlendirilmesine ilişkin Lahey Programı'nda aşağıdaki şekilde ifade edilmiştir:[165]

> "*Avrupa Birliği ve Üye Devletlerinin güvenliği, özellikle 11 Eylül 2001 tarihinde Amerika Birleşik Devletleri'nde ve 11 Mart 2004 tarihinde Madrid'de meydana gelen terörist saldırılar ışığında yeni bir aciliyet kazanmıştır. Avrupa vatandaşları haklı olarak Avrupa Birliği'nin, temel hak ve özgürlüklere saygıyı garanti altına alırken, yasadışı göç, insan ticareti ve kaçakçılığı, terörizm ve örgütlü suçlar gibi sınır ötesi sorunlara ve bunların önlenmesine yönelik daha etkin ve ortak bir yaklaşım benimsemesini beklemektedir. Özellikle güvenlik alanında, iç ve dış boyut arasındaki koordinasyon ve uyumun önemi giderek artmaktadır ve bu konunun güçlü bir şekilde takip edilmeye devam edilmesi gerekmektedir.*"[166]

Ayrıca Lahey Programı'nda "bilginin erişilebilirliği ilkesi" kabul edilerek, CKKAİ çerçevesinde kişisel veri alışverişinin, yetkili makamlar arasında karşılıklı güveni arttıran ve ilgili bilgilerin üye devletler arasında bu tür bir işbirliğine ilişkin herhangi bir ayrımcılığı dışlayacak ve bireylerin temel haklarına tam olarak saygı gösterecek şekilde korunmasını sağlayan açık kurallarla desteklenmesi gerektiği vurgulanmaktadır.[167] Bu husus AB'de özgürlük, güvenlik ve adaletin güçlendirilmesine ilişkin Lahey Programı'nı uygulayan

[165] The Hague Programme: strengthening freedom, security and justice in the European Union, OJ C 53, 3.3.2005, s.1–14. (Lahey Programı)
[166] Lahey Programı, s.1.
[167] Lahey Programı, s.8.

Konsey ve Komisyon Eylem Planı'nda[168] da yerini almış, veri koruma alanındaki temel koşullara sıkı sıkıya bağlı kalınarak kolluk kuvvetlerinin sınır ötesi bilgi alışverişine yönelik yenilikçi bir yaklaşımın gerekliliğini ifade edilerek, Komisyon en geç 2005 yılı sonuna kadar "CKKAİ amacıyla kişisel verilerin aktarılmasına yönelik yeterli güvenceler ve etkili hukuki yollara ilişkin" teklif sunmaya davet edilmiştir.[169]

4.2 Taslak Çerçeve Kararları ve 2008/977 sayılı Çerçeve Karar'ın Kabulüne Giden Çetin Yol

2008/977 sayılı Çerçeve Karar yürürlüğe girene kadar[170] Üçüncü Sütun konularında veri işleme, uzun bir süre boyunca yalnızca Avrupa Konseyi'nin yukarıda belirtilen uluslararası kamu hukuku belgeleri (108 sayılı Sözleşme, R (87) 15 sayılı Tavsiye Kararı ve AİHS) tarafından yönetilmiştir.[171] 2005 yılına gelindiğinde Komisyon tarafından sunulan ilk teklif[172] kapsamında Çerçeve Karar taslağının Veri Koruma Direktifi doğrultusunda hazırlandığı görülmektedir.[173] Bu husus taslağın açıklayıcı not kısmında "Çerçeve Karar, CKKAİ'nin özel ihtiyaçlarını göz önünde bulundurarak ve orantılılık ilkesi ışığında Veri Koruma Direktifi'nin ruhunu ve yapısını mümkün olduğunca takip etmelidir" şeklinde dile getirilmiştir.[174] Veri koruma alanında AB düzeyinde sağlam bir mevzuatın zaten mevcut olması, ilkelerin ve ulusal mevzuatın bu doğrultuda uyumlaştırılmış olması ve denetim

[168] Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union, OJ C 198, 12.8.2005, s.1–22.(Eylem Planı)
[169] Eylem Planı, s.10.
[170] 2008/977 sayılı Konsey Çerçeve Kararının kabul edilmesine kadar geçen süreç ile ilgili ayrıntılı bilgi için bakınız. DE HERT, PAUL, *et.al.*, 2007, s.162-175.
[171] BOEHM, FRANZISKA, 2012, s.115.
[172] Commission, Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, (COM(2005) 475 final), 4.10.2005.
[173] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2009), s.406.
[174] Commission, Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, (COM(2005) 475 final), 4.10.2005, s.6.

mimarisinin zaten kurulmuş olması dikkate alındığında, teklif edilen çerçeve kararın Veri Koruma Direktifi'nden feyz alması kadar doğal bir sonuç olamazdı.[175]

İlk taslakta, dikkat çekici olan ilk şey ve belki de en kritik düzenleme "Bu Çerçeve Karar, kişisel verilerin tamamen veya kısmen otomatik yollarla işlenmesine ve bir dosyalama sisteminin parçasını oluşturan veya suçların önlenmesi, soruşturulması, tespiti ve kovuşturulması amacıyla yetkili bir makam tarafından bir dosyalama sisteminin parçasını oluşturması amaçlanan kişisel verilerin otomatik yollar dışında işlenmesine uygulanır" şeklinde ifade edilen "kapsam" maddesidir.[176] Bu maddeden de anlaşılacağı üzere teklif edilen Çerçeve Karar ile kişisel verilerin hem ulusal düzeyde hem de üye devletler arasında işlenmesinin düzenlenmesi amaçlanmaktaydı. Bazı üye devletler bu tek tip uygulamaya itiraz ederek, yürürlüğe konulmak istenen Çerçeve Karar hükümlerinin sadece üye devletler arası veri aktarımları için uygulanması gerektiğini öne sürmüşlerdir.[177] Çerçeve Kararın kabul edilen ve yürürlüğe giren versiyonunda, kişisel verilerin hem ulusal düzeyde hem de üye devletler arasında işlenmesinin düzenlenmesi fikirden vazgeçildiği görülmektedir.

Sonuç olarak, teklif edilen Çerçeve Karar hem yapısı hem de konuya yaklaşımı Veri Koruma Direktifi'nden etkilenmiştir. Bölüm I'de kapsam ve tanımlar, Bölüm II'de genel veri koruma ilkeleri, Bölüm III'de özel işleme türlerini ve veri aktarımları (kullanılabilirlik ilkesi), Bölüm IV, V ve VI'da veri öznesinin (bireylerin) hakları, Bölüm VII'de bir Denetim Makamı ve bir Çalışma Grubu kurulması düzenlenmektedir. Sadece özel işleme türlerini ve

[175] DE HERT, PAUL, *et.al.*, 2007, s.164.
[176] Commission, Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, (COM(2005) 475 final), 4.10.2005, Madde 3(1).
[177] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2009), s.407.

veri aktarımlarını (kullanılabilirlik ilkesi) tanımlayan Bölüm III Veri Koruma Direktifi'nden ayrılan tamamen emsalsiz bir düzenlemedir.[178]

Tam da bu süre zarfında, Kasım 2005 ile Kasım 2006 arasında, Konsey'in Organize Suçlar Multidisipliner Grubu (MDG), taslak hazırlama faaliyetlerini Komisyon'dan devralmış ve Komisyon teklifini önemli ölçüde değiştirmiştir. Kolluk ve adalet birimlerinin yetkililerinden oluşan ve doğası gereği veri koruma konusuna pek de ilgi göstermeyen bir grup olan MDG, yeniden taslak hazırlama sürecine herhangi bir veri koruma uzmanının katılımını reddetmiştir.[179] Taslak Çerçeve Karar'a MDG'nin müdahaleleri ve yapmış olduğu değişiklikler sonucu ortaya çıkan Çerçeve Karar'ın Kasım 2006'daki taslağı, AVKD ve AP tarafından başta kendi görüşlerinin dikkate alınmaması olmak üzere bireylerin korunmasının kolluk kuvvetlerinin çıkarları lehine önemli ölçüde kötüleştirebildiği gerekçesiyle olumsuz karşılanmıştır. Kasım 2006 tarihli Çerçeve Karar Taslağı, ilk teklife sadece şekil olarak benzemekte, aslında her bir temel veri koruma ilkesini, uygulamada kontrol edilemez hale getiren istisnalara bağlanmaktadır.[180] Netice itibariyle taraflar arasındaki bu görüş ayrılıkları ve çatışmalar yaklaşık iki yıl daha sürmüş ve sonucunda 2008/977 sayılı Çerçeve Karar genel görünüm itibari ile Konsey'in ve dolayısıyla üye devletlerin istediği doğrultuda kabul edilmiş, sınırlı bir kapsam ve veri koruma ilkeleri ile bireylerin haklarına getirilen birçok istisna ile hayata girmiştir.

4.3 2008/977 sayılı Çerçeve Karar

Bir önceki bölümde ifade edilen sancılı bir sürecin ve yıllar süren tartışmaların ardından, hukuki dayanağı Amsterdam Antlaşması ile değişik ABA madde 30, 31 ve 34(2)(b)

[178] DE HERT, PAUL, *et.al.*, 2007, s.164.
[179] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2009), s.407.
[180] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2009), s.408.

olan 2008/977 sayılı Çerçeve Karar nihayet Kasım 2008'de Üçüncü Sütun konularında veri işlemeyi de kapsayacak şekilde kabul edilmiştir. 2008/977 sayılı Çerçeve Karar hükümlerinin 27 Kasım 2010 tarihine kadar ulusal hukuka aktarılması gerekmektedir.[181] Bu Çerçeve Karar, Üçüncü Sütunda genel uygulamaya sahip bir yasal çerçeveye yönelik ilk adım olarak nitelendirilebilir. Ancak çeşitli eksiklikler nedeniyle Birinci Sütunda böyle bir yasal çerçeve sağlayan Veri Koruma Direktifi'ne eşdeğer olarak görülemez.[182] 2008/977 sayılı Çerçeve Karar'da, kendisinden önceki veri korumaya ilişkin düzenlemelerin mevcut yapısına benzer bir şekilde, ilk olarak düzenlemenin amaç ve kapsamını ortaya koyulmakta, tanımların ardından verilerin işlenmesine ilişkin temel ilkeler belirlenmekte, hassas verilerin nasıl işleneceği ele alınmakta, veri sahiplerinin hakları ortaya konulmakla birlikte bunlara getirilebilecek istisnalar düzenlenmekte ve bir denetim makamı oluşturulmaktadır. Bu çalışma kapsamında bu başlıklar altında 2008/977 sayılı Çerçeve Karar incelenecektir.

4.3.1 Amaç ve Kapsam

2008/977 sayılı Çerçeve Karar'ın "ABA Başlık VI'da öngörülen CKKAİ çerçevesinde kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin temel hak ve özgürlüklerinin ve özellikle de mahremiyet haklarının yüksek düzeyde korunmasını ve aynı zamanda yüksek düzeyde kamu güvenliğinin garanti altına alınmasını" amaçladığı görülmektedir.[183]

2008/977 sayılı Çerçeve Karar'ın kapsamını; "Üye devletler arasında iletilen veya kullanıma sunulan", "üye devletler tarafından yetkili makamlara veya ABA'nın VI.

[181] 2008/977 sayılı Konsey Çerçeve Karar, madde 29(1)
[182] HIJMANS, HIELKE ve SCIROCCO, ALFONSO, "Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to help?", Common Market Law Review, Cilt:46, Sayı:5, 2009, s.1494.
[183] 2008/977 sayılı Konsey Çerçeve Karar, madde 1(1)

Bölümüne dayalı olarak kurulan bilgi sistemlerine iletilen veya sağlanan" ve "ABA veya ATA temelinde kurulan makamlar veya bilgi sistemleri tarafından üye devletlerin yetkili makamlarına iletilen veya iletilmiş olan" kişisel veriler oluşturmaktadır.[184] Bu durum, verilerin belirli bir üye devletin sınırları dahilinde elde edilmiş olması halinde kişisel verilerin işlenmesini kapsamamaktadır. Başka bir deyişle, 2008/977 sayılı Çerçeve Karar yalnızca kişisel verilerin sınır ötesi aktarımlarına uygulanmaktadır.[185] Ayrıca 2008/977 sayılı Çerçeve Karar'ın "Europol, Eurojust, Schengen Bilgi Sistemi ve Gümrük Bilgi Sistemi'nin işleyişini düzenleyen ve Üye Devletlerin makamlarının diğer Üye Devletlerin belirli veri sistemlerine doğrudan erişimini sağlayan bu düzenlemelerin ilgili veri koruma hükümleri ile özellikle terörizm ve sınır ötesi suçlarla mücadelede sınır ötesi işbirliğinin artırılmasına ilişkin 23 Haziran 2008 tarihli ve 2008/615/JHA sayılı Konsey Kararı uyarınca DNA profillerinin, daktiloskopik verilerin ve ulusal araç kayıt verilerinin Üye Devletler arasında otomatik olarak aktarılmasını düzenleyen veri koruma hükümleri için"[186] geçerli olmadığını belirtmek gerekir.

Bu kapsam sınırlamalarının, bireylerin 2008/977 sayılı Çerçeve Karar tarafından her koşulda korunmadığı yönünde bir etkisi olduğu açıktır.[187] Dolayısıyla, 2008/977 sayılı Çerçeve Karar'ın kapsamının çok sınırlı olduğu ve CKKAİ çerçevesinde kişisel verilerin işlenmesi için tutarlı bir veri koruma yasal çerçevesine ulaşma amacını gerçekleştirmekten uzak olduğu ortaya çıkmaktadır. Bu sistem, Üçüncü Sütun genelinde veri korumasına ilişkin olarak önemli ölçüde parçalanmaya ve şeffaflık eksikliğine yol açmakla kalmamakta, aynı

[184] 2008/977 sayılı Konsey Çerçeve Karar, madde 1(2)(a)(b)(c).
[185] VIOLA DE AZEVEDO CUNHA, MARIO, "Privacy, Security and the Council Framework Decision 2008/977/JHA", Law Technology, Cilt:43, Sayı:4, 2010, s.12.
[186] 2008/977 sayılı Konsey Çerçeve Kararı, Dibace para 39.
[187] HIJMANS, HIELKE ve SCIROCCO, ALFONSO, 2009, s.1494.

zamanda bu parçalı yaklaşım, AB veri tabanlarının çoğalması ve erişimleri ışığında gerekli olan AB ve ulusal düzeyde gerekli gizlilik standardına ilişkin anlamlı bir tartışmayı da pratikte ortadan kaldırmaktadır.[188]

Üye devletler kendi içlerinde "ulusal düzeyde toplanan veya işlenen kişisel verilerin korunması için bu Çerçeve Kararında belirlenenden daha yüksek güvenceler" sağlayabilir.[189] Ayrıca 2008/977 sayılı Çerçeve Karar'ın, "temel ulusal güvenlik çıkarlarına ve ulusal güvenlik alanındaki özel istihbarat faaliyetlerine halel getirmeyeceği" ifade edilmektedir.[190]

2008/977 sayılı Çerçeve Karar'ın yalnızca "Üye devletler arasında iletilen veya kullanıma sunulan kişisel veriler" için geçerli olacağını yukarıda açıklamıştık. Bu sınırlama temel bir sınırlamadır, çünkü AB üye devletlerinin kişisel verileri kolluk alanında ulusal seviyede işlemesini dışarıda bırakmaktadır. Başka bir deyişle, üye devletlerdeki kolluk kuvvetleri 2008/977 sayılı Çerçeve Karar'ın ilkelerine sadece başka bir üye devlete aktardıkları ya da başka bir üye devlet tarafından kendilerine aktarılan bu kişisel veri setleri için uyacaklardır. Üye devletler yetki alanları dahilindeki verilerin işlenmesi söz konusu olduğunda, Avrupa Konseyi'nin bu alandaki müktesebatına uygun olarak istediklerini yapmakta serbesttirler.[191]

Üçüncü Sütunda karar alınabilmesi için oybirliğinin gerekli olduğu unutulmamalıdır. 2008/977 sayılı Çerçeve Karar'ın kapsamının genişletilmesine itiraz eden üye devletler, belki azınlıkta olsalar da aksini isteyen çoğunluk tarafından göz ardı edilemezdi. İtirazlarının dikkate alınması ve bir şekilde uzlaşmaya varılması gerekiyordu. Böylece, daha fazla Avrupa

[188] MITSILEGAS, VALSAMIS, "The Third Wave of Third Pillar Law: Which Direction for EU Criminal Justice?", Queen Mary School of Law Legal Studies Research Paper No. 33/2009, European Law Review, Cilt:34, Say:4, 2009, s.559.
[189] 2008/977 sayılı Konsey Çerçeve Kararı, madde 1(5) ve Dibace para 8.
[190] 2008/977 sayılı Konsey Çerçeve Kararı, madde 1(4).
[191] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2009), s.410.

entegrasyonu isteyenlerle daha azını isteyenler arasındaki savaş, tartışmalı bir şekilde, birincilerin yenilgisiyle sonuçlanmıştır.[192]

Kapsamın bu derece sınırlı olması, AVKD tarafından Çerçeve Karar ile ilgili vermiş olduğu üçüncü görüşünde açık bir şekilde eleştirilmiştir. Buna göre:[193]

> "*Dolayısıyla, mevcut taslak, kişisel verilerin yurt içinde işlenmesinde tek tip veri koruma ilkelerinin uygulanmasını Üye Devletlerin takdirine bırakmakta ve Üye Devletleri, iç sınırların kaldırılması gereken kolluk ve adli işbirliği alanında aynı ortak veri koruma standartlarını uygulama konusunda bağlamamaktadır. Bu çerçevede AVKD, üçüncü sütun kapsamında farklı Üye Devletlerde farklı veri koruma seviyelerine sahip olma ihtimalinin altını bir kez daha çizmektedir.*"[194]

2008/977 sayılı Çerçeve Karar'ın üye devletlerin üçüncü devletler ile yaptıkları ve 2008/977 sayılı Çerçeve Karar'ın kabul edildiği tarihte yürürlükte olan kişisel verilerin aktarılmasına ilişkin ikili anlaşmalara halel getirmeyeceğini[195] de belirtmek gerekmektedir. Bu durum 2008/977 sayılı Çerçeve Karar'ın kapsamı açısından önem arz etmektedir.

4.3.2 Veri Koruma İlkeleri

Avrupa'da 1960'lardan bu yana ulusal ve uluslararası alanda oluşturulan temel veri koruma ilkeleri, 2008/977 sayılı Çerçeve Karar'da, geniş istisna hükümlerine maruz kalsa da kendisine yer bulmaktadır.[196] 2008/977 sayılı Çerçeve Karar çerçevesinde "Kişisel veriler yetkili makamlar tarafından görevleri çerçevesinde yalnızca belirli, açık ve meşru amaçlar için toplanabilir ve yalnızca verilerin toplandığı amaçla aynı amaç için işlenebilir. Verilerin

[192] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2009), s.410.
[193] KOSTA, ELENI, *et.al*, 2007, s.352.
[194] Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, 2007/C 139/01, para 18.
[195] 2008/977 sayılı Konsey Çerçeve Kararı, madde 26.
[196] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2009), s.409.

işlenmesi hukuka uygun ve yeterli olmalı, ilgili olmalı ve toplandıkları amaçlarla bağlantılı olarak aşırı olmamalıdır".[197] Söz konusu düzenlemede her ne kadar temel ilke olarak kişisel verilerin yalnızca toplandıkları amaçla aynı amaç için işlenebileceği belirlenmiş olsa da hemen devamı düzenleme ile toplandıkları amacın dışında başka bir amaç için daha fazla işlemeye izin veren şu istisnalar bulunmaktadır: "verilerin toplanma amaçlarıyla uyumsuz olmaması", "yetkili makamların geçerli yasal hükümler uyarınca söz konusu verileri başka bir amaçla işleme yetkisine sahip olması" ve "işlemenin söz konusu diğer amaç için gerekli ve orantılı olması".[198]

2008/977 sayılı Çerçeve Karar'a göre "kişisel veriler yanlışsa düzeltilecek ve bunun mümkün ve gerekli olduğu durumlarda tamamlanacak veya güncellenecektir"[199], bununla birlikte, söz konusu hüküm veri sahiplerinin haklarını tam anlamıyla güvence altına almamakla birlikte "mümkün ve gerekli"nin ne olduğunu tanımlamamakta ve farklı yorumlara açık kapı bırakmaktadır. Bu hüküm 2008/977 sayılı Çerçeve Karar'ın temel sorunlarından birini teşkil etmektedir; çünkü bireysel hakların kullanılmasını objektif olmayan bir kritere tabi tutmakta ve veri koruma sütunlarından biri olan veri kalitesi ilkesinin gözetilmemesi riskini yaratmaktadır.[200] Ayrıca "kişisel veriler, yasal olarak toplandıkları amaçlar için artık gerekli olmadıklarında veya yasal olarak daha fazla işlendiklerinde silinecek veya anonim hale getirilecektir. Bu verilerin ulusal yasalar uyarınca uygun bir süre için ayrı bir veri setinde arşivlenmesi bu hükümden etkilenmeyecektir."[201] Bu durum 2008/977 sayılı Çerçeve Karar'ın dibacesinde şu şekilde ifade edilmektedir:[202]

[197] 2008/977 sayılı Konsey Çerçeve Kararı, madde 3(1).
[198] 2008/977 sayılı Konsey Çerçeve Kararı, madde 3(2).
[199] 2008/977 sayılı Konsey Çerçeve Kararı, madde 4(1).
[200] VIOLA DE AZEVEDO CUNHA, MARIO, 2010, s.13.
[201] 2008/977 sayılı Konsey Çerçeve Kararı, madde 4(2).
[202] 2008/977 sayılı Konsey Çerçeve Kararı, Dibace para 13.

"*Ayrı bir veri setinde arşivlemeye ancak verilerin suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infazı için artık gerekli olmaması ve kullanılmaması halinde izin verilmelidir. Ayrı bir veri setinde arşivlemeye, arşivlenen verilerin suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezai yaptırımların infazı için artık kullanılamayacak şekilde diğer verilerle birlikte bir veri tabanında saklanması halinde de izin verilmelidir. Arşivleme süresinin uygunluğu arşivleme amaçlarına ve veri sahiplerinin meşru menfaatlerine bağlı olmalıdır. Tarihsel amaçlarla arşivleme durumunda çok uzun bir süre öngörülebilir.*"

Her ne kadar kişisel verilerin toplandıkları amaçlar için artık gerekli olmadıklarında silinmesi esas ilke olarak ortaya konmuş olsa da uygulamada, kişisel veriler hiçbir zaman silinmeyecek, sadece veri tabanlarını değiştireceklerdir. 2008/977 sayılı Çerçeve Karar kapsamında "kişisel verilerin silinmesi veya verilerin saklanması ihtiyacının periyodik olarak gözden geçirilmesi için uygun zaman sınırları belirlenecektir."[203] Özel veri kategorilerinin işlenmesi ise yalnızca kesinlikle gerekli olduğunda ve üye devletlerin ulusal hukukları yeterli güvenlik önlemleri sağladığında izin verilecektir.[204] Veri Koruma Direktifi'nde özel veri kategorilerinin işlenmesi ilke olarak yasaklanmış ancak bazı istisnai durumlarda işlenmesine izin verilmişken[205] 2008/977 sayılı Çerçeve Karar'da bu tür veriler, CKKAİ çerçevesinde ana bilgi kaynaklarından biri olduğundan, işlenmesinin bir istisna olarak değerlendirilmemesi makul ve orantılı olarak görülebilecektir.[206] Aynı durum, yalnızca veri

[203] 2008/977 sayılı Konsey Çerçeve Kararı, madde 5.
[204] 2008/977 sayılı Konsey Çerçeve Kararı, madde 6.
[205] Veri Koruma Direktifi, madde 8.
[206] VIOLA DE AZEVEDO CUNHA, MARIO, 2010, s.18.

sahiplerinin meşru menfaatlerini garanti altına alan bir yasayla yetkilendirilebilecek olan otomatik bireysel kararlar için de geçerlidir.[207]

2008/977 sayılı Çerçeve Karar'da, yetkili makamlar, kişisel verilerin iletilmeden veya paylaşılmadan önce mümkün olduğunca doğruluğunu, eksiksizliğini ve güncelliğini kontrol etmekle yükümlüdür. Ayrıca, veri iletimi sırasında, alıcı üye devletin verilerin doğruluk, eksiksizlik, güncellik ve güvenilirlik derecesini değerlendirmesine olanak tanıyan bilgiler eklenmelidir. Talep olmaksızın iletilen kişisel verilerin, iletilme amacına uygun olup olmadığı alıcı makam tarafından gecikmeksizin kontrol edilmelidir.[208] Yanlış verilerin iletilmesi veya verilerin hukuka aykırı şekilde paylaşılması durumunda, alıcı taraf derhal bilgilendirilmelidir. Ayrıca, bu tür veriler, Çerçeve Karar'ın 4'üncü maddesi uyarınca gecikmeksizin düzeltilmeli, silinmeli veya bloke edilmelidir.[209]

2008/977 sayılı Çerçeve Karar kapsamında bir üye devletin yetkili makamları kişisel verileri doğal olarak iletildikleri veya kullanıma sunuldukları amaçlar doğrultusunda işleyebilirler. Bununla birlikte, bir dizi istisna kapsamında, söz konusu yetkili makamların yukarıda iletilen veya kullanıma sunulan verileri "daha fazla işlemesine" izin verilmektedir.[210] Ancak istisnaların listesi o kadar geniş kapsamlıdır ki, pratikte her durumda veriler, orijinal olarak iletildikleri veya kullanıma sunuldukları amaçlarla tamamen ilgisiz amaçlar için kullanabilecektir.[211] Bu geniş istisna listesi AVKD tarafından da, "kişisel verilerin daha fazla işlenmesine ilişkin mevcut hükümlerin temel amaç sınırlaması ilkesini ihlal ettiğine ve hatta 108 sayılı Sözleşme tarafından belirlenen mevcut standardın altına

[207] 2008/977 sayılı Konsey Çerçeve Kararı, madde 7.
[208] 2008/977 sayılı Konsey Çerçeve Kararı, madde 8(1).
[209] 2008/977 sayılı Konsey Çerçeve Kararı, madde 8(2).
[210] 2008/977 sayılı Konsey Çerçeve Kararı, madde 11.
[211] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2009), s.412.

düştüğüne inanmaktadır" denilerek eleştirilmiştir.[212] Sonuç olarak, 2008/977 sayılı Çerçeve Karar tarafından veri koruma ilkeleri ortaya konulmakla birlikte bu ilkelere getirilen istisna düzenlemeleri, temel veri koruma ilkelerinin içini boşaltılmış ve neredeyse uygulanmaz hale gelmesine neden olmuştur.

4.3.3 Üçüncü Taraflara Aktarım

2008/977 sayılı Çerçeve Karar kapsamında, üye devletler tarafından başka bir üye devletin yetkili makamı tarafından iletilen veya kullanıma sunulan kişisel verilerin "suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezai yaptırımların infazı için gerekli olması"; "üçüncü devletteki alıcı makamın veya alıcı uluslararası kuruluşun cezai suçların önlenmesi, soruşturulması, tespiti veya kovuşturulmasından veya cezai yaptırımların infazından sorumlu olması"; "verilerin elde edildiği üye devletin kendi ulusal hukukuna uygun olarak aktarıma rıza göstermiş olması" ve "ilgili üçüncü devletin veya uluslararası kuruluşun amaçlanan veri işleme faaliyeti için yeterli düzeyde koruma sağlaması" durumunda üçüncü devletlerdeki yetkili makamlara veya uluslararası kuruluşlara aktarımı mümkündür.[213] Üçüncü devletlere veya uluslararası kuruluşlara aktarımın, "bir üye devletin veya üçüncü bir devletin kamu güvenliğine veya bir üye devletin temel çıkarlarına yönelik acil ve ciddi bir tehdidin önlenmesi için gerekli olması ve önceden rızanın zamanında alınamaması" halinde, verilerin elde edildiği üye devletin "önceden rızası" olmaksızın gerçekleştirilebileceğini belirtmek gerekir.[214]

[212] Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, 2007/C 139/01, para 25.
[213] 2008/977 sayılı Konsey Çerçeve Kararı, madde 13(1).
[214] 2008/977 sayılı Konsey Çerçeve Kararı, madde 13(2).

2008/977 sayılı Çerçeve Karar'ın kapsamından sonra en tartışmalı hükmü, Çerçeve Karar kapsamında toplanan kişisel verilerin üye devletlerdeki özel taraflara aktarılmasına ilişkin hükmüdür. Ancak Çerçeve Karar bu tür işlemlere bazı sınırlamalar getirmektedir.[215] İlk olarak, "verilerin elde edildiği üye devletin yetkili makamının onay vermesi", ikinci olarak, "veri sahiplerinin meşru menfaatlerinin aktarımı engellememesi" ve üçüncü olarak, aktarımın, verileri özel bir tarafa aktaran yetkili makam için "(i) kendisine yasal olarak verilmiş bir görevin yerine getirilmesi; (ii) suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezai yaptırımların infazı; (iii) kamu güvenliğine yönelik acil ve ciddi bir tehdidin önlenmesi veya (iv) bireylerin haklarına ciddi zarar gelmesinin önlenmesi" için gerekli olması gerekmektedir.[216] Yetkili makam, verilerin münhasıran hangi amaçlarla kullanılabileceği hakkında özel tarafı bilgilendirmek zorundadır.[217] AVKD tarafından verilen son görüşte, özel taraflara ve yetkili olmayan makamlara kişisel verilerin iletilmesi veya onların kullanımına sunulmasının, R (87) 15 sayılı Tavsiye Kararı ilkelerine uymadığını belirtilerek, bu durumun ortaya çıkaracağı olumsuz durumlar üzerinde durulmuştur.[218]

4.3.4 Veri Sahibinin Hakları

2008/977 sayılı Çerçeve Karar doğrultusunda üye devletler veri sahibini kişisel verilerin toplanması veya işlenmesine ilişkin olarak bilgilendirecektir. Ancak üye devletler kişisel verileri ileten veya kullanıma sunan diğer üye devletin veri sahibini bilgilendirmemesini isteyebilir.[219]

---

[215] VIOLA DE AZEVEDO CUNHA, MARIO, 2010, s.15.
[216] 2008/977 sayılı Konsey Çerçeve Kararı, madde 14(1).
[217] 2008/977 sayılı Konsey Çerçeve Kararı, madde 14(2).
[218] Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, 2007/C 139/01, para 36.
[219] 2008/977 sayılı Konsey Çerçeve Kararı, madde 16.

Veri sahibi "en azından kontrolörden veya ulusal denetim makamından kendisi ile ilgili verilerin iletilip iletilmediğine veya kullanıma sunulup sunulmadığına ilişkin bir teyit ve verilerin iletildiği alıcılar veya alıcı kategorileri ve işlenmekte olan verilerin iletimi hakkında bilgi" alma hakkına sahip olmakla birlikte veri sahibine yapılacak "en azından ulusal denetim makamından gerekli tüm doğrulamaların yapıldığına dair bir teyit" de erişim hakkının kullanılması için yeterli sayılacaktır.[220] Ulusal denetim makamınca yapılacak teyit işlemi aslında söz konusu hakkın dolaylı olarak kullanımı olarak değerlendirilmekte ve veri sahiplerinin korunmasını zayıflattığı ve genel veri koruma standartlarına uymadığını dile getirilmektedir.[221] Ayrıca üye devletler "resmi veya yasal soruşturmaları, araştırmaları veya usulleri engellemekten kaçınmak", "cezai suçların önlenmesi, tespiti, soruşturulması ve kovuşturulmasına veya cezai yaptırımların infazına halel getirmekten kaçınmak", "kamu güvenliğini ve ulusal güvenliği korumak" ve "veri sahibini veya başkalarının hak ve özgürlüklerini korumak" için veri sahiplerinin bilgiye erişimini, ilgili kişinin meşru menfaatleri göz önünde bulundurularak ve gerekli ve orantılı olacak şekilde yasal tedbirler kabul ederek kısıtlayabilir.[222] Veri sahibinin erişim talebinin reddedilmesi veya kısıtlanması halinde kendisine, söz konusu ret veya kısıtlama kararının gerekçesini (gerekçenin bildirimi çoğu zaman zorunlu unsur değildir) ve yetkili ulusal denetim makamına, adli bir makama veya bir mahkemeye itirazda bulunabileceği bilgisini içerecek şekilde yazılı bildirimde bulunulur.[223]

AVKD tarafından verilen son görüşte, veri sahibinin, bilgilendirilme hakkının kontrolörün ve alıcıların kimliğine ilişkin bilgilerden bahsetmediği için eksik olduğu, erişim

[220] 2008/977 sayılı Konsey Çerçeve Kararı, madde 17(1).
[221] VIOLA DE AZEVEDO CUNHA, MARIO, 2010, s.20.
[222] 2008/977 sayılı Konsey Çerçeve Kararı, madde 17(2).
[223] 2008/977 sayılı Konsey Çerçeve Kararı, madde 17(3).

hakkının kısıtlanmasına ilişkin ortaya konan istisnaların ise çok geniş ve öngörülemez olduğu ifade edilmiştir.[224]

Veri sahibi kendisi ile ilgili 2008/977 sayılı Çerçeve Karar kapsamında işlenen kişisel verilerinin düzeltilmesi, silinmesi veya engellenmesi ilgili kontrolörden isteyebilmektedir. İlgili kontrolör tarafından söz konusu talepler, ulusal hukukta öngörülen şikâyette bulunma veya yargı yoluna başvurma imkânları da bildirilmek suretiyle, yazılı olarak reddedilebilir.[225] Ayrıca veri sahibi tarafından kendisi ile ilgili bir verinin doğruluğuna ilişkin yapılan itiraz sonucu söz konusu verinin doğruluğunun veya yanlışlığının kanıtlanamaması halinde itiraza konu verinin işlenmesine devam edilecektir.[226]

2008/977 sayılı Çerçeve Karar kapsamında veri sahiplerinin kendileri ile ilgili verilerin hukuka aykırı olarak işlemesi sonucu bir zarara uğramaları durumunda tazminat talep etme hakkı bulunmaktadır.[227] Ayrıca veri sahibi yürürlükteki ulusal hukuk tarafından kendisine garanti edilen haklarının herhangi bir ihlali için yargı yoluna başvurma hakkına sahip olacaktır.[228]

4.3.5 Ulusal Denetim Makamları

2008/977 sayılı Çerçeve Karar ile her üye devlet, bu Çerçeve Karar uyarınca kabul ettikleri hükümlerin kendi topraklarında uygulanmasını tavsiye etmek ve izlemekten sorumlu, bir veya birden fazla, kendilerine tevdi edilen işlevleri yerine getirirken tam bir

[224] Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, 2007/C 139/01, para 37.
[225] 2008/977 sayılı Konsey Çerçeve Kararı, madde 18(1).
[226] 2008/977 sayılı Konsey Çerçeve Kararı, madde 18(2).
[227] 2008/977 sayılı Konsey Çerçeve Kararı, madde 19.
[228] 2008/977 sayılı Konsey Çerçeve Kararı, madde 20.

bağımsızlıkla hareket eden, ulusal denetim makamlarının bulunmasını sağlamakla yükümlü kılınmıştır.[229]

2008/977 sayılı Çerçeve Karar kapsamında ulusal denetim makamları; "işleme faaliyetlerinin konusunu oluşturan verilere erişim yetkisi ve denetim görevlerinin yerine getirilmesi için gerekli tüm bilgileri toplama yetkisi gibi soruşturma yetkileri", "işleme faaliyetleri gerçekleştirilmeden önce görüş bildirme ve bu görüşlerin uygun şekilde yayınlanmasını sağlama, verilerin bloke edilmesi, silinmesi veya imha edilmesini emretme, işleme faaliyetine geçici veya kesin yasak getirme, kontrolörü uyarma veya ikaz etme veya konuyu ulusal parlamentolara veya diğer siyasi kurumlara havale etme gibi etkili müdahale yetkileri" ve "bu Çerçeve Karar uyarınca kabul edilen ulusal hükümlerin ihlal edildiği durumlarda yasal işlem başlatma veya bu ihlali adli makamların dikkatine sunma yetkisi" ile donatılmalıdır.[230] Ulusal denetim makamları, kişisel verilerin işlenmesi ile ilgili olarak hak ve özgürlüklerinin korunmasına ilişkin olarak herhangi bir kişi tarafından yapılan talepleri inceleyip ilgili kişiyi talebin sonucu hakkında bilgilendirmelidir.[231] Ayrıca 2008/977 sayılı Çerçeve Karar ile üye devletlere oluşturulacakları yeni bir dosyalama sisteminin bir parçasını teşkil edecek olan kişisel verilerin işlenmesinden önce ulusal denetim makamına danışılmasını zorunluluğu getirilmiştir.[232]

4.3.6 Sonuç

2008/977 sayılı Çerçeve Karar, veri koruma hakkı ile devlet güvenliği için artan ihtiyaç arasından bir denge kurmak zorunda kalmıştır. Taslağın hazırlandığı dönemdeki siyasi gündem özellikle 11 Eylül 2001 New York'taki terör saldırı ile 2004 ve 2005'teki

[229] 2008/977 sayılı Konsey Çerçeve Kararı, madde 25(1).
[230] 2008/977 sayılı Konsey Çerçeve Kararı, madde 25(2).
[231] 2008/977 sayılı Konsey Çerçeve Kararı, madde 25(3).
[232] 2008/977 sayılı Konsey Çerçeve Kararı, madde 23.

Madrid ve Londra saldırıları göz önünde bulundurulduğunda, şüphesiz ki Devlet güvenliğini ön plana çıkarmıştır. Bu durum sadece taslağın hazırlanmasından sorumlu kurumlar arasındaki dengeyi değil, aynı zamanda Avrupalıların ruh halini de yansıtıyordu. Avrupa başkentlerinin bombalandığı ya da tehdit edildiği bir dönemde sivil özgürlükler kaçınılmaz olarak kamuoyu gündeminde geri planda kalmıştır.[233] Siyasi koşullara ek olarak, 2008/977 sayılı Çerçeve Karar ile Veri Koruma Direktifi arasındaki temel farkı da göz ardı etmemek gerekir. Daha önce de belirtildiği üzere, Veri Koruma Direktifi, kişisel verilerin kâr amacıyla kullanıldığı iç pazar kapsamında ticari işlemeyi, 2008/977 sayılı Çerçeve Karar ise kişisel verilerin kolluk tarafından kullanımını düzenlemeyi amaçlamaktadır.[234]

2008/977 sayılı Çerçeve Karar'ın nihai metninde veri koruma ilkelerinden ödün verilmiştir. Bu ilkelerin neredeyse her biri, uygun gördükleri takdirde, kolluk tarafından ilkenin öngördüğünün aksini yapma kapısını açan bir muafiyetle birlikte gelmektedir. Tüm bu sorunlar 2008/977 sayılı Çerçeve Karar'ın öylesine zayıf bir yasal araç haline getirmektedir ki, "daha uyumlu bir dizi düzenlemeyi garanti altına almayı ve Avrupa'da sivil özgürlükleri güçlendirmeyi" başarması neredeyse imkânsız görünmektedir.[235] 2008/977 sayılı Çerçeve Karar'ın zayıf yönleri, mevcut Üçüncü Sütun konularında ortak bir veri koruma standardının eksikliğini açıkça göstermektedir.[236]

2008/977 sayılı Çerçeve Karar, 2008 yılında Komisyon tarafından büyük beklentilerle ortaya konan ancak daha sonra uzun müzakereler sonucunda neredeyse veri korumanın önemsiz olduğu bir noktaya kadar "sulandırılan" bir metne dönüşmüştür.[237] AB

[233] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2009), s.411.
[234] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2009), s.411.
[235] DE HERT, PAUL, *et.al.*, 2007, s.122.
[236] DE HERT, PAUL, *et.al.*, 2007, s.122.
[237] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, "The New Police and Criminal Justice Data Protection Directive: A First Analysis", New Journal of European Criminal Law, Cilt:7, Sayı:1, 2016, s.8.

üye devletlerinin başkentlerinde meydana gelen terör saldırılarının ardından yayımlanan çok sayıda AB kişisel veri koruma geçici belgesine veri koruma standardı getirmek amacıyla yayımlanan bir metin olan 2008/977 sayılı Çerçeve Karar, gerçekte kendisini bu rolden muaf tutmuştur.[238] Bu durum, istikrarlı veya yeknesak bir yasal yapı sunmayan ve hem önemli ölçüde yasal belirsizliğe hem de veri koruma kurallarının tutarsız bir şekilde uygulanmasına neden olan "veri koruma rejimlerinin yamalı bohçası" olarak nitelendirilmektedir.[239]

[238] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2016), s.8.
[239] MARQUENIE, THOMAS, "The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework", Computer Law & Security Review, Cilt:33, Sayı:3, 2017, s.325

İKİNCİ BÖLÜM: LİZBON ANTLAŞMASI SONRASINDA CEZAİ KONULARDA KOLLUK VE ADLİ İŞBİRLİĞİ ÇERÇEVESİNDE KİŞİSEL VERİLERİN KORUNMASI

Tezin ikinci bölümü Lizbon Antlaşması sonrası dönemde AB'de CKKAİ alanında kişisel verilerin nasıl korunduğuna ilişkin ayrıntılı bir inceleme sunmaktadır. Lizbon Antlaşması sonrası AB'nin sütunlu yapısı ortadan kaldırılmış ve AB ulusüstü bütünleşme çerçevesinde CKKAİ alanında kişisel verilerin korunmasına ilişkin yasal düzenleme yapma yetkisine kavuşmuştur. AB'nin bu alanda kişisel verilerin korunmasını ilişkin etkinliğini daha iyi anlayabilmek için sütunlu yapının ortadan kaldırılması ve özellikle anayasal çerçevede ÖGAA'nın ortaya konulması gerekmektedir. Ayrıca Lizbon Antlaşması sonrası ortaya çıkan veri koruma reform hareketi çerçevesinde AB'de kişisel verilerin genel anlamda nasıl korunduğunu da belirtmek gerekir. Son olarak ve en önemlisi CKKAİ alanında kişisel verilerin korunmasına ilişkin Kolluk Direktifi'nin ayrıntılı bir analizinin yapılması şarttır.

1. LİZBON ANTLAŞMASI VE ÜÇ SÜTUNLU YAPININ SONA ERMESİ

1.1 Anayasal Antlaşma'nın Başarısızlığı ve Lizbon Antlaşması'na Giden Yol

Nice Antlaşması'ndan Lizbon Antlaşması'na giden yol uzun ve engellerle dolu bir yol olmuştur.[240] 2007 yılında Lizbon Antlaşması'nın onaylanması, Aralık 2000'de Nice Zirvesi'nde imzalanan Nice Antlaşması'na ekli "Avrupa Birliği'nin Geleceği Hakkında Deklarasyon" ile başlayan ve yaklaşık on yıl süren AB'deki Antlaşma reformu girişimlerinin son noktasını oluşturmaktaydı.[241]

[240] Nice Antlaşmasından Lizbon Antlaşmasına giden süreç ile ilgli ayrıntılı bilgi için bkz. CRAIG, PAUL, *The Lisbon Treaty: Law, Politics, and Treaty Reform*, Oxford University Press, Oxford, 2013, s.1-25. PIRIS, JEAN-CLAUDE, *The Lisbon Treaty: A Legal and Political Analysis*, Cambridge University Press, Cambridge, 2010, s.7-49.

[241] BAYKAL, SANEM, "Reform Antlaşması ve Getirdikleri: Kurumsal Yapı Çerçevesinde Genel Bir Değerlendirme", Ankara Avrupa Çalışmaları Dergisi, Cilt:7, No:1, 2007, s.46.

Nice Antlaşması'na ekli "AB'nin Geleceği Hakkında Deklarasyon" Nice Antlaşması ile önemli reformların karara bağlandığı ve AB'nin genişlemesinin önündeki engellerin kaldırıldığı belirtilerek bir nevi kutlama havasıyla başlamaktadır.[242] Deklarasyon daha sonra "AB'nin geleceğine ilişkin daha derin ve daha geniş bir tartışma yapılması" çağrısında bulunmuştur.[243] Bu sürecin Aralık 2001'de Laeken Zirvesinde bir Deklarasyon ile ortaya konacak girişimler vasıtasıyla sürdürülmesi için bir takvim belirlenmiştir.[244] Laeken Deklarasyonu, diğer hususların yanı sıra, "yetkilerin sınırlandırılması", "ABTHŞ'nin statüsü", "Antlaşmaların sadeleştirilmesi" ve "ulusal Parlamentoların Avrupa mimarisindeki rolü" konularını ele alacaktır.[245] Bu hazırlık adımlarından sonra gerekli kurucu antlaşma değişikliklerinin yapılması görevi 2004 yılında toplanacak Hükümetlerarası Konferansa verilmiştir.[246]

Aralık 2001'de gerçekleştirilen Leaken Zirvesinde, dönemin Belçika Başbakanı Guy Verhofstadt'ın önerisi üzerine, "AB'nin Geleceğine İlişkin Deklarasyon" bilinen adıyla Laeken Deklarasyonu kabul edilmiştir.[247] Bu Deklarasyona göre, "Birliğin daha demokratik, daha şeffaf ve daha etkin hale gelmesi" gerekmektedir. Leaken Deklarasyonunda AB'nin "üç temel sorununun" çözüme kavuşturulması gerekliliği belirtilmiştir. Bunlar: "vatandaşların Avrupa tasarımına nasıl daha yakın hale getirileceği", "AB'nin nasıl organize edileceği" ve "genişlemiş bir AB içinde Avrupa siyasi alanı ve Birliğin yeni, çok kutuplu dünyada dengeleyici bir faktör ve model olarak nasıl geliştirileceği".[248] Ayrıca Deklarasyon, kurucu antlaşmaların nasıl basitleştirileceği ve yeniden düzenleneceği ve bunun "uzun vadede AB

[242] NA'ya ekli AB'nin Geleceği Hakkında Deklarasyon, madde 1-2. CRAIG, PAUL, 2013, s.2.
[243] NA'ya ekli AB'nin Geleceği Hakkında Deklarasyon, madde 3.
[244] NA'ya ekli AB'nin Geleceği Hakkında Deklarasyon, madde 4.
[245] NA'ya ekli AB'nin Geleceği Hakkında Deklarasyon, madde 5.
[246] NA'ya ekli AB'nin Geleceği Hakkında Deklarasyon, madde 7.
[247] Presidency Conclusions, Laeken, 14 and 15 December 2001, Ek 1.
[248] Presidency Conclusions, Laeken, 14 and 15 December 2001, Ek 1.

içinde anayasal bir metnin kabul edilmesine yol açıp açmayacağı" gibi soruların da yer aldığı çeşitli sorular ortaya koymuştur.[249]

Leaken Zirvesinde, bir sonraki Hükümetlerarası Konferansa mümkün olduğunca geniş ve açık bir şekilde zemin hazırlamak amacıyla, AB'nin geleceğine ilişkin tartışmalara katılan başlıca taraflardan oluşan bir Konvansiyon toplanmasına karar verilmiştir. Bu Konvansiyon'un sadece üye devletlerin devlet veya hükümet başkanları ile Avrupa Komisyonu'nun temsilcilerinden değil, aynı zamanda ve esas olarak ulusal parlamentoların ve AP'nin temsilcilerinden oluşmasına karar verilmiş olup, AB'ye aday devletler de temsil edilecek ve çalışmalara katılabilecektir.[250]

Konvansiyon, hem Nice Antlaşması'na ekli Deklarasyon'da yer alan konuları, hem de bu konuların Laeken Deklarasyonu'nda genişletilmesiyle meydana çıkan soruları çok taraflı ve şeffaf bir müzakere süreci içerisinde ele alarak 16 aylık hazırlık sürecinin sonunda 10 Haziran 2003 tarihinde tamamlanmış ve ilk başlarda küçük bir olasılık olarak görülen taslak "Avrupa için Anayasa Kuran Antlaşma" kabul edilerek 20 Haziran 2003 tarihinde Selanik Zirvesinde sunulmuştur.[251] Selanik Zirvesinde söz konusu taslağın bir Hükümetlerarası Konferans vasıtasıyla çalışılmasına karar verilmiştir.[252]

Ekim 2003'te başlayan Hükümetlerarası Konferans tarafından yürütülen çalışmalar sonucunda üzerinde anlaşmaya varılan "Avrupa için Anayasa Kuran Antlaşma" 2004'ün Haziran ayında Brüksel Zirvesinde onaylanmış ve 29 Ekim 2004 tarihinde Roma'da "Avrupa Birliği Anayasal Antlaşması" adıyla resmi olarak imza altına alınmıştır.[253] "Avrupa Birliği

[249] PIRIS, JEAN-CLAUDE, 2010, s.12.
[250] BAYKAL, SANEM ve GÖÇMEN, İLKE, "Avrupa Bütünleşmesi: 1993 Sonrası", AKÇAY, BELGİN ve GÖÇMEN, İLKE (Eds.), *Avrupa Birliği: Tarihçe, Teoriler, Kurumlar ve Politikalar*, 3.Baskı, Seçkin Yayıncılık, Ankara, 2016, s.94.
[251] BAYKAL, SANEM, 2007, s.48.
[252] Presidency Conclusions, Thessaloniki, 19 and 20 June 2003, para.5.
[253] PIRIS, JEAN-CLAUDE, 2010, s.19.

Anayasal Antlaşması", mevcut tüm Antlaşmaları yürürlükten kaldırmakta ve bunların yerine tek bir metin getirmekte, yasal araçları ve usulleri düzene sokmakta ve uzun süredir var olan ilke ve kuralları kodifiye etmekteydi.[254]

"Avrupa Birliği Anayasal Antlaşması"nın yürürlüğe girebilmesi için tüm üye devletler tarafından anayasal gerekliliklerine uygun olarak onaylanması gerekmekteydi. Bu süreç çok sancılı olmuş ve özellikle her ikisi de her zaman Avrupa entegrasyonunun merkezinde yer alan iki kurucu üye devlet olan Fransa ve Hollanda'daki referandumların sonuçlarının "hayır" ile neticelenmesi AB'de "siyasi bir deprem" olarak algılanmıştır.[255] Fransa ve Hollanda'nın referandumlarında Anayasal Antlaşmayı reddetmeleri, Anayasal Antlaşmanın onaylanma sürecinin aniden durmasına ve bu nedenle bazı üye devletlerin onay sürecini ertelemesine neden olmuştur. Bunun üzerine AB Zirvesi 2005 yılında Brüksel Zirvesinde bir "düşünme dönemi" geçirmenin en iyisi olacağına karar vermiştir.[256]

2006 yılında gerçekleştirilen Brüksel Zirvesinde söz konusu "düşünme dönemi"nin uzatılması gerekliliğine vurgu yapılmış ve 2007 yılının ilk yarısında Konsey Dönem Başkanlığını yürütecek olan Almanya'nın, Anayasal Antlaşma ile ilgili tartışmaların mevcut durumunun değerlendirildiği ve atılacak adımların neler olması gerektiğini araştıran bir rapor sunmasına[257] karar verilmiştir.[258] Gerçekte olan şudur ki Anayasal Antlaşma, Fransa ve Hollanda'daki olumsuz referandumların AB üzerinde yarattığı etkiden hiçbir zaman kurtulamamış ve yasalaşamamıştır.[259]

[254] PIRIS, JEAN-CLAUDE, 2010, s.20.
[255] BAYKAL, SANEM ve GÖÇMEN, İLKE, (2016), s.95.
[256] CRAIG PAUL ve DE BÚRCA GRAINNE, 2020, s.30.
[257] Presidency Conclusions, Brussels, 15 and 16 June 2006, para.45-47.
[258] BAYKAL, SANEM ve GÖÇMEN, İLKE, 2016, s.125.
[259] CRAIG PAUL ve DE BÚRCA GRAINNE, 2020, s.31.

Almanya Dönem Başkanlığı, 2007'de meseleleri ilerletme konusunda istekli bir süreç işletmiştir. Alman Hükümeti, gözden geçirilmiş bazı Antlaşma reformlarının kabul edilmesinin önünü açacak bir anlaşmanın üye devletler arasında sağlanıp sağlanamayacağını görmek maksadıyla iyi organize edilmiş ve zekice bir diplomasi yürüterek her bir üye devletten, o devletin değiştirilmiş bir belgeyi onaylaması için Anayasal Antlaşmada hangi hususların değiştirilmesi gerektiğini sormuştur.[260] Bu da Almanya'nın Haziran 2007'deki AB Zirvesinde, gözden geçirilmiş bir Antlaşmanın başarıyla sonuçlandırılabilmesi için Anayasal Antlaşmada yapılması gereken değişiklikleri ayrıntılı bir şekilde masaya getirmesini sağlamıştır.[261] Haziran 2007'de toplanan Brüksel Zirvesinde, Anayasal Antlaşma sürecinde yaşanan iki yıllık belirsizliğin ardından sorunların bir an önce çözüme kavuşturulması ve AB'nin yoluna devam etmesi zamanının geldiği sonucuna varılmıştır.[262] Bu kapsamda Almanya tarafından sunulan rapor memnuniyetle karşılanmış[263] ve kurucu antlaşma değişikliği çalışmalarını AB Zirvesi sonuçlarının ekinde yer alan ayrıntılı yetki çerçevesinde yürütecek ve müzakerelerini 2007 yılı sonuna kadar tamamlayacak olan bir Hükümetlerarası Konferansın toplanması kararlaştırılmıştır.[264]

Sonuç olarak oluşturulacak yeni antlaşmanın bir yandan Anayasal Antlaşmayı onaylayan on sekiz üye devlet[265] tarafından, diğer yandan da sadece halkları Anayasal Antlaşmayı reddeden Fransa ve Hollanda tarafından değil, aynı zamanda onay sürecini askıya alan yedi üye devlet[266] tarafından da kabul edilebilir olması gerekiyordu.[267] Bu

[260] CRAIG, PAUL, 2013, s.21.
[261] CRAIG, PAUL, 2013, s.22.
[262] Presidency Conclusions, Brussels, 21 and 22 June 2007, para.8.
[263] Presidency Conclusions, Brussels, 21 and 22 June 2007, para.9.
[264] Presidency Conclusions, Brussels, 21 and 22 June 2007, para.10-11.
[265] Almanya, Avusturya, Belçika, Bulgaristan, Estonya, Finlandiya, Güney Kıbrıs, İspanya, İtalya, Letonya, Litvanya, Lüksemburg, Macaristan, Malta, Romanya, Slovakya, Slovenya ve Yunanistan.
[266] Britanya, Polonya, Çek Cumhuriyeti, Danimarka, İsveç, İrlanda, Portekiz.
[267] PIRIS, JEAN-CLAUDE, 2010, s.30.

kapsamda yeni antlaşma hem Anayasal Antlaşmada ortaya konan mevcut hukuksal reformları, "Anayasa", "kanunlar", "bakan", "bayrak", "marş" gibi ifadeleri kullanmaksızın korumalı, hem de "Avrupa için Anayasa" anlayışını muhafaza etmeliydi. İşte bu yaklaşımın eseri olarak Hükümetlerarası Konferansın sonunda "Reform Antlaşması" olarak anılan Lizbon Antlaşması ortaya çıkmıştır.[268]

1.2 Lizbon Antlaşması ve Üç Sütunlu Yapının Sona Ermesi

13 Aralık 2007 tarihinde imzalanmış olan Lizbon Antlaşması'nın yürürlüğe girebilmesi için bütün üye devletler tarafından kendi anayasal prosedürlerine uygun olarak onaylanması gerekiyordu; ancak İrlanda'da yapılan referandumda "hayır" oyu çıktı. Bu engel, İrlanda'ya belirli konularda tavizler verilmesi sonucu Ekim 2009'da yapılan ikinci bir referandumda "evet" oyu çıkması ile aşılmıştır.[269] Lizbon Antlaşması'nın yürürlüğe girebilmesi için kalan son engel ise parlamentoda kabul edilmesine rağmen Çek Cumhurbaşkanı'nın Lizbon Antlaşması'nı onaylama konusundaki isteksizliğiydi. Ancak, Lizbon Antlaşması'na karşı yapılan anayasal itirazın Çek Anayasa Mahkemesi tarafından reddedilmesi ve diğer üye devletlerin daha sonraki bir tarihte Çek Cumhuriyeti'nin talep ettiği ABTHŞ ile ilgili Antlaşmalara bir Protokol eklemeyi kabul etmelerinin ardından Çek Cumhurbaşkanı "gönülsüzce" de parlamentoda kabul edilen Lizbon Antlaşması'nı onaylamıştır.[270] Böylece Lizbon Antlaşması 1 Aralık 2009 tarihinde yürürlüğe girmiştir.

Lizbon Antlaşması, "anayasa", "bayrak" ve "marş" da dahil olmak üzere anayasal sembollere yapılan tüm atıflar hariç olmak üzere Anayasal Antlaşmadaki düzenlemelerin birçoğunu muhafaza edecek şekilde AB'nin kurumsal yapısında birçok değişiklik

[268] BAYKAL, SANEM ve GÖÇMEN, İLKE, (2016), s.95.
[269] CRAIG PAUL ve DE BÚRCA GRAINNE, 2020, s.32.
[270] CRAIG PAUL ve DE BÚRCA GRAINNE, 2020, s.32.

yapmıştır.[271] Lizbon Antlaşması, Anayasal Antlaşma gibi yeni bir Antlaşma olmayıp, ABA ve ATA'yı kendisinden önceki kurucu antlaşmalar gibi tadil etmiştir. Lizbon Antlaşması öncesinde AB ve AT farklı tüzel kişiliklere haizken bu antlaşma ile AB AT'nin yerine geçtiğinden[272] ATA'nın adı "Avrupa Birliğinin İşleyişi Hakkında Antlaşma" (ABİHA) olarak değiştirilmiştir.[273] Lizbon Antlaşması ile ATA'nın adının değiştirilmesi haricinde, AB'nin temelini oluşturan bu antlaşmalarda köklü değişimler yapılmış, antlaşmalara eklenen hükümlerin yanında birçok madde numarası da değişikliğe uğramıştır.[274] Ayrıca Lizbon Antlaşması ile ABA ve ABİHA'nın "hukuki olarak aynı değere sahip olduğu"[275] ve AB'nin "tek bir tüzel kişiliğe sahip olduğu"[276] hüküm altına alınmaktadır.

Lizbon Antlaşması ile AB'nin "insan onuruna saygı, özgürlük, demokrasi, eşitlik, hukukun üstünlüğü ve azınlıklara mensup kişilerin hakları da dâhil olmak üzere insan haklarına saygı değerleri" üzerine kurulu olduğu belirtilmektedir.[277] Lizbon Antlaşması'nın 3'üncü maddesi ile AB'nin hedefleri ortaya konulmakta olup, AB'nin "vatandaşlarına, dış sınırların kontrolü, iltica, göç, suçun önlenmesi ve suçla mücadele konularında uygun tedbirler vasıtasıyla kişilerin serbest dolaşımının sağlandığı, iç sınırların olmadığı bir ÖGAA sunacağı"[278] vurgulanmaktadır. Lizbon Antlaşması'nın getirdiği önemli bir husus da 2000 yılında ilan edilen ancak yasal olarak bağlayıcılığı olmayan ABTHŞ'nin[279] AB'nin birincil

[271] LAURSEN, FINN, "The Lisbon Treaty: Overview of Institutional Choices and Beginning Implementation", LAURSEN, FINN (Ed.), *The EU's Lisbon Treaty: Institutional Choices and Implementation*, Ashgate Publishing, Farnham, 2012, s.4.
[272] Lizbon Antlaşması ile değişik ABA madde 1 para 3.
[273] GÜNEŞ, AHMET M, "Lizbon Antlaşması Sonrasında Avrupa Birliği", Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt:12, Sayı:1, 2008, s.743.
[274] GÜNEŞ, AHMET M, (2008), s.742.
[275] Lizbon Antlaşması ile değişik ABA madde 1 para 3, ABİHA madde 1(2).
[276] Lizbon Antlaşması ile değişik ABA madde 47.
[277] Lizbon Antlaşması ile değişik ABA madde 2.
[278] Lizbon Antlaşması ile değişik ABA madde 3(2).
[279] ABTHŞ ile ilgili ayrıntılı bilgi için bkz. BAYKAL, SANEM, "Temel Haklar", AKÇAY, BELGİN ve ÖZÇELİK, GÜLÜM BAYRAKTAROĞLU (Eds.), *Lizbon Antlaşması Sonrası Avrupa Birliği: Serbest Dolaşım ve Politikalar*, 2.Baskı, Seçkin Yayıncılık, Ankara, 2012, s.399-409, SPAVENTA, ELEANOR, "Fundamantel

hukuk statüsünde kabul edilmesi ve kurucu antlaşmalar ile aynı hukuki değere sahip olmasının sağlanmasıdır.[280] Ayrıca Lizbon Antlaşması'na AB'nin Avrupa İnsan Hakları Sözleşmesi'ne (AİHS) katılımı yönünde bağlayıcı bir hüküm eklenmiştir.[281]

Bununla birlikte Lizbon Antlaşması, ATA'nın yerine geçen ABİHA'nın mimarisinde iyileştirmeler yapmıştır. ABİHA yedi kısımdan oluşmaktadır. "İlkeler" başlıklı Birinci Kısım iki başlık içermektedir; bunlardan ilki "Birliğin Yetki Kategorileri ve Yetki Alanları" ile ilgilidir, ikincisi ise "Genel Uygulamaya Sahip Hükümleri" kapsamaktadır. İkinci Kısım, "Ayrımcılık Yapmama ve Birlik Vatandaşlığı" konularını ele almaktadır. "Birliğin Politikaları ve İç Eylemleri"ni kapsayan Üçüncü Kısım, yirmi dört başlık ile ABİHA'nın en büyük kısmıdır.[282] Bu açıdan en dikkat çekici değişiklik, eski ABA'nın Üçüncü Sütunu olan "CKKAİ ilişkin hükümlerin" yeni ABİHA'ya taşınmış olmasıdır.[283] ABİHA'nın Dördüncü Kısmı, daha önce olduğu gibi, "Denizaşırı Ülkeler ve Bölgeler Birliği"ni kapsamaktadır. Buna karşılık Beşinci Kısım yeni olup, dış boyutu olan bir dizi konuyu bir araya getirerek "Birliğin Dış Eylemleri"ni ele almaktadır. ABİHA'nın Altıncı Kısmı "Kurumsal ve Mali Hükümler" ile ilgiliyken, Yedinci Kısmı "Genel ve Nihai Hükümleri" içermektedir.

Rights in the European Union", BARNARD, CATHERINE ve PEERS, STEVE (Eds), *European Union Law*, Oxford University Press, Oxford, 2014, s.236-245. BİLGİN, AHMET BURAK, *Avrupa Birliği'nde İnsan Haklarının Gelişimi ve Korunması*, Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2015, s.307-334. VOGIATZOGLOU, PLIXAVRA ve VALCKE, PEGGY, "Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law", KOSTA, ELENI ve LEENES, RONALD, *Research Handbook On EU Data Protection Law*, Edward Elgar Publishing, Cheltenham, 2022, s.11-49.

[280] Lizbon Antlaşması ile değişik ABA madde 6(1). GÜNEŞ, AHMET M, (2008), s.750.

[281] Lizbon Antlaşması ile değişik ABA madde 6(2).

[282] Başlıklar aşağıdaki gibidir:I-İç Pazar; II-Malların Serbest Dolaşımı; III-Tarım ve Balıkçılık; IV-Kişilerin, Hizmetlerin ve Sermayenin Serbest Dolaşımı; Başlık V-Özgürlük, Güvenlik ve Adalet Alanı; VI-Ulaştırma; VII-Rekabet, Vergilendirme ve Yasaların Yakınlaştırılmasına ilişkin Ortak Kurallar; VIII-Ekonomik ve Parasal Politika; IX-İstihdam; X-Sosyal Politika; XI-Avrupa Sosyal Fonu; XII-Eğitim, Mesleki Eğitim, Gençlik ve Spor; XIII-Kültür; XIV-Kamu Sağlığı; XV-Tüketicinin Korunması; XVI-Trans-Avrupa Ağları; XVII-Sanayi; XVIII-Ekonomik, Sosyal ve Bölgesel Uyum; XIX-Araştırma ve Teknolojik Gelişim ve Uzay; XX-Çevre; XXI-Enerji; XXII-Turizm; XXIII-Sivil Koruma; XXIV-İdari İşbirliği.

[283] CRAIG, PAUL, 2013, s.26.

Lizbon Antlaşması ile getirilen ve bu çalışmanın konusu açısından da en önemli değişiklik ise Maastricht Antlaşması ile ortaya çıkan ve Lizbon Antlaşması'na kadar çeşitli değişiklikler ile korunan sütunlu yapının ortadan kaldırılmasıdır. Görüldüğü üzere Lizbon Antlaşması sütun sistemi üzerine inşa edilmemiş ve bu anlamda Maastricht Antlaşması'ndan bu yana hâkim olan üç sütunlu Antlaşma mimarisi sona ermiştir. Her ne kadar Lizbon Antlaşması ile sütunlu yapı sona ermiş olsa da ODGP'ye ilişkin düzenlemelerin eski hükümetlerarası yapısını koruduğu (oybirliği ile karar alma ve Komisyon, AP ve ABAD'ın sınırlı rolü) görülmektedir.[284] Eski Üçüncü Sütunun ise daha net belirtmek gerekirse Lizbon Antlaşması'nın yürürlüğe girmesiyle, 1993-99 yılları arasında neredeyse tüm Adalet ve İçişleri konularını, o tarihten bu yana da kolluk ve ceza hukuku konularını ilgilendiren AB'nin "Üçüncü Sütununun" 16 yıllık ömrü sona ermiştir.[285]

Lizbon Antlaşması ile, en azından ilk bakışta, Üçüncü Sütunun Birinci Sütuna aktarılması ve bu alanda, nitelikli çoğunluk oylaması ve olağan yasama usulü, ABAD için tam yargı yetkisi, olağan tasarruf türlerinin (Tüzük, Direktif ve Karar) kullanılması gibi Topluluk yönteminin çoğu unsurunun tam olarak uygulanmasıyla, eski Üçüncü Sütun konuları üzerinde Topluluk yönteminin "zafer kazandığı" söylenebilir.[286] Ancak, geçiş hükümlerini düzenleyen Lizbon Antlaşması'na ekli 36 nolu protokolün 9 ve 10'uncu maddeleri kapsamında, Topluluk yönteminin kolluk ve ceza hukukuna tam olarak uygulanması, Lizbon Antlaşması'nın yürürlüğe girmesinden önce kabul edilen Üçüncü Sütun

[284] Lizbon Antlaşması ile değişik ABA madde 24. YAKUT, BAHADIR, "Lizbon Sonrası AB'nin Yeni Kurumsal Yapısı ve Karar Alma Süreçlerinin Özgürlük, Güvenlik ve Adalet Alanındaki Yansımaları", Türkiye Adalet Akademisi Dergisi (TAAD), Yıl:1, Sayı:2, 2010, s.58.
[285] PEERS, Steve, *The 'Third Pillar acquis' after the Treaty of Lisbon enters into force*, Statewatch Analysis, 1 Aralık 2009, https://www.statewatch.org/media/documents/analyses/no-88-analysis-third%20pillar-ver2.pdf, Erisim Tarihi: 15/03/2025, s.1.
[286] PEERS, STEVE, "EU Criminal Law and Police Cooperation", CRAIG PAUL ve DE BÚRCA GRAINNE (Eds.), *The Evolution of the EU Law*, 3th Edition, Oxford University Press, Oxford, 2021, s.757.

tedbirleri üzerinde ABAD'ın yargı yetkisine ilişkin beş yıllık bir geçiş dönemi öngörülmesi sonucu bir süre ertelenmiştir.[287] Söz konusu hüküm, özellikle Komisyon'un bu geçiş dönemi boyunca önceden var olan tedbirlerin ihlali iddiasıyla ilgili olarak üye devletlere karşı ihlal davası açma yetkisine sahip olmayacağı ve hâlihazırda ABAD'ın ön karar prosedürüne ilişkin yetkisini kabul etmeyen üye devletlerin bu dönem boyunca bunu yapmaya devam edecekleri anlamına gelmekteydi.[288] Geçiş dönemi 1 Aralık 2014'te sonra erdiğinden bu konunun üzerinde daha fazla durulmayacaktır.

Maastricht Antlaşması'nda Üçüncü Sütun içerisinde yer alan ancak Amsterdam Antlaşması ile Birinci Sütuna aktarılan konular da dâhil olmak üzere eski Üçüncü Sütun konuları ABİHA'nın "Özgürlük, Güvenlik ve Adalet Alanı" adlı Başlık V altında toplanmıştır. Başlık V sırasıyla; genel hükümler[289], sınır kontrolleri, göç ve iltica ile ilgili politikalar[290], medeni hukuk alanında işbirliğine ilişkin bir madde[291], ceza hukuku alanında işbirliğine ilişkin beş madde[292] ve kolluk işbirliğine ilişkin üç madde[293] içermektedir.[294] ÖGAA başlığı altındaki düzenlemelerin Lizbon Antlaşması öncesi Üçüncü Sütunda olduğu gibi[295] "üye devletlerin, kamu düzeninin muhafaza edilmesi ve iç güvenliğin korunması konusundaki yetkilerine halel getirmeyeceği" belirtilmektedir.[296]

---

[287] GÖÇMEN, İLKE, "Avrupa Birliği Adalet Divanı", AKÇAY, BELGİN ve GÖÇMEN, İLKE (Eds.), *Avrupa Birliği Tarihçe, Teoriler, Kurumlar ve Politikalar*, 3. Baskı, Seçkin Yayıncılık, Ankara, 2016, s.272.
[288] PEERS, STEVE, "Finally 'Fit for Purpose'? The Treaty of Lisbon and the End of the Third Pillar Legal Order", Yearbook of European Law, Cilt:27, Sayı:1, 2008, s.53.
[289] ABİHA madde 67-76.
[290] ABİHA madde 77-80.
[291] ABİHA madde 81.
[292] ABİHA madde 82-86.
[293] ABİHA madde 87-89.
[294] ABİHA Başlık V altında yer alan düzenlemelere ilişkin genel bilgi için bkz. FIJNAUT, CYRILLE, 2019, s.446-453. CRAIG, PAUL, 2013, s.343-378.
[295] ABA madde K.2.2, Amsterdam Antlaşması ile değişik ABA madde 33.
[296] ABİHA madde 72.

Bu çalışmanın konusu açısından ÖGAA başlığı altında "Kolluk İşbirliği" başlıklı 5'inci Bölümde yer alan düzenlemelere kısaca değinmek faydalı olacaktır. İlk olarak AB'nin "suçların önlenmesi, tespiti ve soruşturulması ile ilgili olarak polis, gümrük ve diğer uzmanlaşmış kolluk hizmetleri de dâhil olmak üzere tüm üye devletlerin yetkili makamlarını arasında bir kolluk işbirliği tesis edileceği" hüküm altına alınmaktadır.[297] Daha sonra, AP ve Konsey'in olağan yasama usulü uyarınca hareket ederek; "gerekli bilgilerin toplanması, saklanması, işlenmesi, analizi ve değişimi", "personel eğitiminin desteklenmesi ve personel değişimi, teçhizat ve suç inceleme teknikleri konularında işbirliği yapılması", "ciddi nitelikteki örgütlü suç türlerinin ortaya çıkarılmasına ilişkin ortak soruşturma teknikleri" konularında tedbirler alabileceği düzenlenmektedir.[298] Ayrıca Konsey tarafından özel bir yasama usulü uyarınca hareket edilerek, oybirliğiyle ve AP'ye danıştıktan sonra, operasyonel işbirliğine ilişkin tedbirler kabul edilebileceği; Konsey'de oybirliği olmaması halinde, en az dokuz üye devletin güçlendirilmiş işbirliğine ilişkin hükümler çerçevesinde[299] işbirliğine devam edebileceği vurgulanmaktadır.[300] Bir sonraki maddede Europol'ün görevinin "iki veya daha fazla üye devleti ilgilendiren ciddi suçların, terörizmin ve AB politikalarından birinin kapsamına giren ortak bir çıkarı etkileyen suç türlerinin önlenmesi ve bunlarla mücadele edilmesi konusunda, üye devletlerin polis ve diğer kolluk kuvvetlerinin eylemlerini ve bu birimler arasında işbirliğini desteklemek ve güçlendirmek" olduğu ve Europol'ün yapısının, işleyişinin, faaliyet alanının ve görevlerinin olağan yasama usulüne uygun olarak kabul edilen tüzükler vasıtasıyla belirleyeceğini açık bir şekilde ifade edilmektedir.[301]

[297] ABİHA madde 87(1).
[298] ABİHA madde 87(2).
[299] Güçlendirilmiş işbirliğine ilişkin hükümler: Lizbon Antlaşması ile değişik ABA madde 20 ile ABİHA madde 326-334.
[300] ABİHA madde 87(3).
[301] ABİHA madde 88(1-2).

Sonuç olarak belirtmek gerekir ki Lizbon Antlaşması ile sütunlu yapının kaldırılmasının arkasındaki temel amacın, etkin bir karar alma sürecine ve AB tedbirlerinin üye devletler tarafından daha iyi uygulanmasına imkân tanıyarak, bunları uygun bir parlamento ve yargı denetimine tabi tutulması vasıtasıyla AB vatandaşlarının sahip olduğu hakların, güvenlik ve yargı yoluyla korunması arasındaki dengeyi iyileştirmek olduğu söylenebilir.[302]

2. ANAYASAL ÇERÇEVEDE ÖZGÜRLÜK, GÜVENLİK VE ADALET ALANI

Bir önceki bölümde ayrıntılı olarak bahsedildiği üzere Lizbon Antlaşması ile sütunlu yapı terk edilmiş ve eski Üçüncü Sütun Topluluk Sütunu içine aktarılarak, Topluluk yöntemlerinin CKKAİ alanına ilişkin düzenlemelere de uygulanabilir hale gelmesi sağlanmıştır. Lizbon Antlaşması ile ABİHA'nın ÖGAA başlığı altında, eski Üçüncü Sütun "topluluklaştırılmış" olmasına rağmen, Maastricht Antlaşması ile oluşturulan ve Amsterdam Antlaşması ile revize edilen Üçüncü Sütunda olduğu gibi bütün düzenlemeleri tek bir başlık altında bulunduran bir yapı mevcut değildir. Bu kapsamda ÖGAA'da AB'nin yetkisi, tasarruf türleri ve bunların hukuki etkileri ile karar alma usulleri ve bu alanda yargısal korumaya ilişkin hükümler Antlaşmaların genelinde ilgili maddelerinde düzenlenmiştir. Bu doğrultuda ilgili maddelerde yapılan düzenlemeler ışığında ÖGAA'nın anayasal çerçevesi incelenecektir.

[302] PIRIS, JEAN-CLAUDE, 2010, s.178.

2.1 Özgürlük, Güvenlik ve Adalet Alanı Kapsamında Avrupa Birliği'nin Yetkisi

AB'nin ÖGAA kapsamında sahip olduğu yetkiyi ortaya koyabilmek için öncelikle AB'nin Antlaşmalar ile belirlenen yetkisini kısaca açıklamak gerekmektedir.[303] Antlaşmalar kapsamında yetki AB ile üye devletler arasında bölünmüştür. Bu doğrultuda "yetkilendirme ilkesi" olarak adlandırılan ilke gereğince, esas olarak yetki üye devletlere ait olup, Antlaşmalarda açık bir şekilde kendisine yetki verildiği durumlarda AB yetkili olacaktır ki bu da AB'nin yetkisinin "sınırlı yetki" olduğu anlamına gelmektedir.[304] AB, yetkilendirme ilkesi kapsamında yetkilerini "katmanlı yetki"[305] ve "orantılılık"[306] ilkesi çerçevesinde kullanabilecektir.[307]

AB'nin "yetki kategorileri ve yetki alanları" ABİHA'nın Başlık I'i altında düzenlenmiştir. AB'nin yetkileri üçü temel ikisi özel olmak üzere beş kategori altında ifade edilmiştir. Bunlar "münhasır yetki", "paylaşılan yetki", "destekleyici, koordine edici ve tamamlayıcı yetki", "ekonomi ve istihdam politikalarının koordinesi" ve "ortak dış ve güvenlik politikası".[308] Bu sayılan beş kategori AB'nin genel olarak sahip olduğu yetki kategorilerini ifade etmekle birlikte AB'nin "yetkilerinin kapsamı ve bu yetkilerin kullanılmasına ilişkin kurallar, Antlaşmaların her bir alana ilişkin hükümleri uyarınca belirlenecektir".[309]

---

[303] AB'de yetki ile ilgili ayrıntılı bilgi için bkz. BAYKAL, SANEM ve GÖÇMEN, İLKE, 2016, s.249-282. CRAIG PAUL ve DE BÚRCA GRAINNE, 2020, s.177-237.
[304] Lizbon Antlaşması ile değişik ABA madde 4(1) ve madde 5(2).
[305] Lizbon Antlaşması ile değişik ABA madde 5(3). "*Katmanlı yetki ilkesi gereğince, Birlik, münhasır yetkisine girmeyen alanlarda, sadece, öngörülen eylemin amaçlarının üye devletler tarafından merkezi düzeyde veya bölgesel ve yerel düzeyde yeterli biçimde gerçekleştirilemeyeceği ve fakat söz konusu eylemin boyutu ya da etkileri itibarıyla Birlik düzeyinde daha iyi gerçekleştirilebileceği durumlarda harekete geçer*."
[306] Lizbon Antlaşması ile değişik ABA madde 5(4). "*Orantılılık ilkesi gereğince, Birlik eyleminin içeriği ve şekli, Antlaşmalar'ın amaçlarını gerçekleştirmek için gerekli olanı aşamaz.*"
[307] Lizbon Antlaşması ile değişik ABA madde 5(1).
[308] ABİHA madde 2(1-5). BAYKAL, SANEM ve GÖÇMEN, İLKE, 2016, s.263.
[309] ABİHA madde 2(6). YAKUT, BAHADIR, "Lizbon Sonrası Avrupa Birliğinin Cezai Meselelerde Yetkisinin Kapsamı", Ankara Avrupa Çalışmaları Dergisi, Cilt:9, No:2, 2010, s.173.

Lizbon Antlaşması ile AB'ye ÖGAA kapsamında münhasır bir yetki tanınmamış, bu alanda AB yetkisini önemli ölçüde genişletmiş olsa da özünde daha önceki Antlaşmalar'da olduğu gibi esas yetki üye devletlerde olmak üzere, AB'nin bu alandaki yetkisi paylaşılan yetki[310] içerisinde yer almıştır.[311] Paylaşılan yetki gereği AB ve üye devletler ÖGAA'ya ilişkin yasama faaliyetinde bulunabilecek ve hukuki bağlayıcılığı olan tasarruflar kabul edebilecektir. Ancak üye devletler bu yetkisini AB'nin kendisine tanınan yetkiyi kullanmadığı veya kullanmayı bırakmaya karar verdiği durumlarda kullanabilecektir.[312] Bu durum zorunlu olarak, en azından üye devletlerin bu alana ilişkin sorumluluklarının AB tedbirleriyle sınırlandırılacağı anlamına gelmekte olup, bu sınırlamanın niteliği ve derecesi, AB tarafından kabul edilen özel tedbire bağlı olacaktır.[313]

2.2 Özgürlük, Güvenlik ve Adalet Alanı Kapsamında Avrupa Birliği Kurumlarının Tasarrufları ve Hukuki Etkileri

Lizbon Antlaşması ÖGAA için, Amsterdam Antlaşması ile revize edilen Üçüncü Sütunda olduğu gibi ATA'da öngörülen tasarruf türlerinden bağımsız, ayrı bir tasarruf türü belirlememiştir.[314] Bu anlamda Lizbon Antlaşmasında belirlenen tasarruf türleri ÖGAA için de geçerli olacaktır. AB'nin kabul edebileceği tasarruf türleri ABİHA'nın 288'inci maddesinde "Kurumlar, Birliğin yetkilerinin kullanılması için tüzük, direktif, karar, tavsiye ve görüşler kabul eder" şeklinde düzenlenmiştir. Aynı maddede söz konusu tasarruf türlerinin hukuki etkileri de açıklanmıştır. Bu kapsamda; "Tüzükler genel uygulama alanına sahiptir.

[310] ABİHA madde 4(2)(j).
[311] ERDEM, MUSTAFA RUHAN, "Lizbon Antlaşması ve Avrupa Ceza Hukuku'nun Geleceği: Treaty of Lisbon and the Future of European Criminal Law", Yaşar Üniversitesi E-Dergisi, Cilt:8, Sayı: Özel, 2013, s.1036.
[312] ABİHA madde 2(2).
[313] CRAIG, PAUL, 2013, s.347.
[314] AB kurumlarının tasarrufları ve hukuki etkileri ile ilgili ayrıntılı bilgi için bkz. BAYKAL, SANEM ve GÖÇMEN, İLKE, 2016, s.336-370. CRAIG PAUL ve DE BÚRCA GRAİNNE, 2020, s.238-272.

Bütünüyle bağlayıcıdır ve tüm üye devletlerde doğrudan uygulanır."; "Direktifler, muhatap alınan her üye devleti, ulaşılması gerekli sonuçları itibarıyla bağlar, şekil ve yöntem seçimini ise ulusal otoritelere bırakır."; "Kararlar bütünüyle bağlayıcıdır. Muhatabı belirtilen bir karar, yalnızca muhatabı için bağlayıcıdır."; "Tavsiye ve görüşler bağlayıcı değildir."[315]

Antlaşmalarda söz konusu tasarruf türleri arasında herhangi bir hiyerarşi olduğuna dair bir hüküm bulunmamaktadır. Dolayısıyla bu tasarruf türleri arasında resmi bir hiyerarşi yoktur.[316] Bu durumu bir örnekle açıklamak gerekirse, tüzükler direktiflerin üst normu ya da direktifler kararların üst normu değildir. Hiçbir tasarruf türü diğer bir tasarruf türüne dayanılarak çıkarılmamaktadır. Tüzükler, direktifler ve kararlar, belirli bir alanda AB politikasının geliştirilmesinde genellikle birbirleriyle bağlantılı olacaktır.[317] Antlaşmalarda, bazı maddelerde söz konusu alanda bir düzenleme yapılması maksadıyla çıkarılacak tasarrufun türü belirlenmektedir. Bu durum istisnai bir durum olup, genellikle Antlaşmalarda hangi tasarruf türü kullanılacağı belirtilmemektedir. Bu durumda yani Antlaşmalarda kabul edilecek tasarruf türünün belirtilmediği hallerde, AB kurumlarının, "uygulanabilir usullere ve orantılılık ilkesine uygun olarak", duruma göre tasarruf türlerinden birini seçebileceği düzenlenmektedir.[318]

AB kurumlarınca çıkarılacak tasarruflar bazı şekil şartları tabi kılınmıştır. İlk olarak, söz konusu tasarruflar "kurucu antlaşmalarda öngörülen öneri, girişim, tavsiye, talep veya görüşlere atıfta bulunur."[319] Söz konusu atıfta bulunma zorunluluğu ilgili tasarrufun kabul

[315] ABİHA madde 288.
[316] BAYKAL, SANEM ve GÖÇMEN, İLKE, "Avrupa Birliği Hukukunun Kaynakları Bakımından Normlar Hiyerarşisi", *Prof Dr Erdal Onar'a Armağan*, Ankara Üniversitesi Basımevi, 2013, s.325.
[317] CRAIG PAUL ve DE BÚRCA GRAINNE, 2020, s.240.
[318] ABİHA madde 296, para 1. BAYKAL, SANEM ve GÖÇMEN, İLKE, (2013), s.325.
[319] ABİHA madde 296, para 2.

sürecinde ortaya konulan taslaklarına atıfta bulunulmasını ifade etmektedir.[320] İkinci olarak, söz konusu tasarruflarda "gerekçe" gösterilmesi zorunluluğu bulunmaktadır.[321]

Son olarak, ABİHA'nın 297'inci maddesinde söz konusu tasarrufların çıkarılmasında uygulanacak usule ilişkin kurallar belirlenmiştir. Öncelikle, bir tüzük, direktif veya karar; "olağan yasama usulü çerçevesinde kabul edilen yasama tasarrufu" şeklini aldığında, "AP ve Konsey Başkanı" tarafından imzalanacak; "özel yasama usulü uyarınca kabul edilen bir yasama tasarrufu" şeklini aldığında ise ilgili tasarrufu "kabul eden kurumun Başkanı" tarafından imzalanacaktır.[322] Bu süreç, söz konusu tasarrufun artık uygulanabilir olmasını ve mezkûr tasarrufların AB hukuk düzeni içerisinde yer almasını sağlamaktadır.[323] Kabul edilen tasarruflar AB Resmi Gazete'sinde yayımlanır ve burada belirtilen tarihte veya bunun olmaması halinde yayımlandıkları tarihi takip eden yirminci günde yürürlüğe girer.[324]

Bu çalışma açısından direktife ilişkin birkaç hususun daha açıklaması faydalı olacaktır.[325] Direktifler tüm üye devletlere hitap etmek zorunda değildirler ve elde edilecek sonuç bakımından bağlayıcı olmakla birlikte, şekil ve yöntem konusunda üye devletlere bazı seçenekler bırakırlar. Tüzüklerin yanı sıra direktifler yoluyla da hareket edebilme kabiliyeti AB'ye değerli bir esneklik kazandırmaktadır. Direktifler, özellikle belirli bir alandaki mevzuatın uyumlaştırılması veya karmaşık mevzuat değişikliklerinin gerçekleştirilmesi amaçlandığında faydalı olmaktadır. Çünkü üye devletler direktifin nasıl uygulanacağı konusunda takdir yetkisine sahiptir. Bununla birlikte, direktiflerin muğlak olduğu düşünülmemelidir. Direktifin içeriği ve belirtilen amaçlar genellikle çok ayrıntılı olacaktır ve

[320] BAYKAL, SANEM ve GÖÇMEN, İLKE, (2013), s.327.
[321] ABİHA madde 296, para 2.
[322] ABİHA madde 297(1), para 1-2.
[323] BAYKAL, SANEM ve GÖÇMEN, İLKE, (2013), s.328.
[324] ABİHA madde 297(1), para 3.
[325] Direktif ile ilgili ayrıntılı bilgi için bkz. GÖÇMEN, İLKE, *Avrupa Birliği Hukukunda Direktiflerin Bireyler Arasındaki İlişkilere Etkileri*, Yetkin Yayınevi, Ankara, 2008.

Üye Devletler, belirli bir direktifin verdiği yetkiler dışında, bu konuda takdir yetkisine sahip değildir.[326] Son olarak direktif, tüzük gibi doğrudan uygulanabilen bir tasarruf türü olmadığından, Üye Devletler tarafından iç hukuklarına aktarılması gereklidir.[327] ABAD tarafından *Van Duyn*[328] kararında, direktiflerin doğrudan etkiye sahip olduğuna ve bireylerin devlete karşı açacakları davalarda bu direktiflere dayanabileceklerine karar verilmiştir.[329]

2.3 Özgürlük, Güvenlik ve Adalet Alanı Kapsamında Karar Alma (Yasama) Usulü

Lizbon Antlaşması ile AB'nin iki türlü karar alma (yasama) usulü ile tasarruf çıkarabileceği düzenlenmektedir.[330] Bu usuller "olağan yasama usulü" ile "özel yasama usulü"dür. Bu yasama usullerinden hangisi kullanılarak çıkarılmak istenen tasarrufların kabul edileceği söz konusu tasarrufa dayanak teşkil edecek Antlaşma hükmünün içeriğinde hangi usule atıf yapıldığına göre belli olacaktır.[331]

ABİHA madde 298(1)'de "olağan yasama usulü", "Komisyon'un önerisi üzerine, AP ve Konsey tarafından bir tüzük, direktif veya kararın ortaklaşa kabulü" olarak ifade edilmekte ve bu usulün ABİHA'nın 294'üncü maddesinde[332] tanımlandığı belirtilmektedir. Yine ABİHA madde 289(2)'de "özel yasama usulü", "Antlaşmalarda öngörülen belirli durumlarda, bir tüzük, direktif veya kararın, Konsey'in katılımıyla AP tarafından veya AP'nin katılımıyla Konsey tarafından kabulü" olarak tanımlanmaktadır. Söz konusu yasama

[326] CRAIG PAUL ve DE BÚRCA GRAINNE, 2020, s.243-244.
[327] BAYKAL, SANEM ve GÖÇMEN, İLKE, 2016, s.348.
[328] Case 41/74 *Van Duyn v Home Office* [1974] ECR 1337, Case 148/78 *Pubblico Ministero v Tullio Ratti* [1979] ECR 1629.
[329] CRAIG PAUL ve DE BÚRCA GRAİNNE, 2020, s.243-244.
[330] AB'de yasama usullerine ilişkin ayrıntılı bilgi için bkz. TEZCAN, ERCÜMENT, "Avrupa Birliği'nde Politika Yapımı/Karar Alma", AKÇAY, BELGİN ve GÖÇMEN, İLKE (Eds.), *Avrupa Birliği Tarihçe, Teoriler, Kurumlar ve Politikalar*, 3. Baskı, Seçkin Yayıncılık, Ankara, 2016, s.345-381. BAYKAL, SANEM ve GÖÇMEN, İLKE, 2016, s.249-332. CRAIG PAUL ve DE BÚRCA GRAINNE, 2020, s.272-343.
[331] BAYKAL, SANEM ve GÖÇMEN, İLKE, 2016, s.288.
[332] ABİHA madde 294 olağan yasama usulünün aşamalarını ayrıntılı olarak açıklamakta olup bu çalışmanın konusu açısından ayrıca bahsedilmeyecektir.

usulleri kapsamında Konsey, "Antlaşmalarda aksi öngörülmedikçe nitelikli çoğunlukla[333] hareket edecektir."[334] ÖGAA kapsamında kabul edilecek tasarrufların büyük çoğunluğu bazı istisnalar hariç[335] olağan yasama usulü tabidir.

Söz konusu iki yasama usulünde de süreç Komisyon'un önerisi ile başlamaktadır. Bu durum Antlaşmalarda aksinin öngörülmemiş olması halinde genel uygulamadır.[336] Bu genel uygulama "cezai konularda adli işbirliği" ve "kolluk işbirliği" bölümleri hariç ÖGAA için de geçerlidir. Ancak "cezai konularda adli işbirliği" ve "kolluk işbirliği" bölümleri çerçevesinde kabul edilecek tasarruflar için, Komisyon'un önerisinin yanında üye devletlerin dörtte birinin de girişimiyle yasama süreci başlatılabilmesi bu genel uygulamanın istisnasını oluşturmaktadır.[337]

Bazı üye devletlerin ÖGAA içerisinde ceza hukuku ve kolluk faaliyetleri ile ilgili hayati alanlarda egemenlik kaybına ilişkin endişelerini gidermek amacıyla, biri "acil durum freni" olarak bilinen, diğeri ise "sözde veto" olarak adlandırılan iki özel karar alma kuralı içermektedir.[338] "Acil durum freni", ulusal ceza usulü ve maddi ceza hukuku ile ilgili kararlar için geçerli iken[339], "sözde veto", Avrupa Savcılığı Ofisi ve Schengen müktesebatına

[333] Lizbon Antlaşması ile değişik ABA madde 16(4): "Nitelikli çoğunluk, 1 Kasım 2014 tarihinden itibaren, Konsey üyelerinin en az onbeşinin dahil olduğu, Birlik nüfusunun en az % 65'ini oluşturan üye devletleri temsil eden Konsey üyelerinin en az % 55'i olarak tanımlanır."
[334] Lizbon Antlaşması ile değişik ABA madde 16(3).
[335] İstisnalar arasında, Konsey'de oybirliği ve Avrupa Parlamentosu'nun onayını gerektiren ABİHA Madde 86(1) kapsamında bir Avrupa Savcılığı kuran mevzuatın kabul edilmesi; Konsey'de oybirliği ve Avrupa Parlamentosu'na sadece danışılmasını gerektiren ABİHA Madde 87(3) kapsamında kolluk alanında operasyonel işbirliğine ilişkin tedbirlerin kabul edilmesi yer almaktadır; Konsey'de oybirliği ve Avrupa Parlamentosu'na danışılmasını gerektiren cezai konularda sınır ötesi kolluk ve adli işbirliği durumlarında başka bir Üye Devlet'teki ulusal makamların işleyişine ilişkin kuralların kabul edilmesi (ABİHA Madde 89); ve Antlaşma'da belirtilmeyen cezai usul alanlarında Konsey'de oybirliği ve Avrupa Parlamentosu'nun onayını gerektiren asgari AB kurallarının kabul edilmesi (Madde 82(2)(d)).
[336] Lizbon Antlaşması ile değişik madde 17(2).
[337] ABİHA madde 76.
[338] PEERS, STEVE, 2023, s.34.
[339] ABİHA madde 82(3) ve 83(3)

dayanan tedbirler hariç operasyonel kolluk işbirliği ile ilgili kararlar için geçerlidir.[340] Bu özel prosedürlerin her ikisi de bir taslak teklifin veya girişimin AB Zirvesi düzeyinde tartışılmasına yol açabilir ve her iki durumda da olası bir sonuç, bir grup üye devletin diğer üye devletlerin katılımı olmaksızın ilgili tedbiri kabul etmesi için "hızlı yol" onayıdır ve güçlendirilmiş işbirliğine izin verilmeden önce normalde geçerli olan maddi veya usule ilişkin gereklilikleri atlatır.[341] Ancak iki prosedür arasında farklılıklar vardır özellikle "sözde veto", "acil durum freni"nden farklıdır çünkü bir üye devletin veto kullanabileceği gerekçelere ilişkin herhangi bir sınırlama yokken "acil durum freni" sadece belirli gerekçelerle (kendi ceza hukuku sisteminin asli veçhelerini etkilediği kanaatini taşıması halinde) çekilebilir ve acil durum frenine itiraz edilebilse veya geçersiz kılınabilse bile vetoya itiraz edilemez.[342]

2.4 Özgürlük, Güvenlik ve Adalet Alanı Kapsamında Yargısal Koruma

ABAD'ın eski Üçüncü Sütun kapsamındaki yargı etkisi önceki bölümlerde ayrıntılı olarak açıklanmıştı.[343] Lizbon Antlaşması'na kadar olan süreci kısaca özetleyecek olursak; Maastricht Antlaşması ile getirilen Üçüncü Sütunda kendisine herhangi bir yargı yetkisi tanınmayan ABAD'a, Amsterdam Antlaşması ile üye devletlerin uygun görmesi halinde ön karar başvurusu yapılabileceği düzenlenmiştir. Aslında Maastricht Antlaşması ile Aİİ başlığı altında oluşturulan Üçüncü Sütunun konu kapsamı çok daha genişken, Amsterdam Antlaşması ile Üçüncü Sütunun kapsamı CKKAİ konuları ile sınırlandırılmış ve diğer konular Topluluk Sütununa aktarılarak ABAD'ın yargı yetkisi içerisine alınmıştır.

---

[340] ABİHA madde 86(1) ve 87(3).
[341] PIRIS, JEAN-CLAUDE, 2010, s.185.
[342] PEERS, STEVE, 2023, s.35.
[343] ABAD ve yargı yetkisi ile ilgili ayrıntılı bilgi için bkz. GÖÇMEN, İLKE, (2016), s.261-288. BAYKAL, SANEM ve GÖÇMEN, İLKE, 2016, s.377-527.

Lizbon Antlaşması ile sütunlu yapının ortadan kaldırılması ile ABAD'ın eski Üçüncü Sütundaki sınırlı yargı yetkisi de son bulmuştur. ABAD artık ÖGAA'da, kolluk kuvvetleriyle ilgili konularda yargı yetkisine ilişkin sınırlı bir kısıtlama hariç, tam yargı yetkisine haizdir.[344] Bu kısıtlama kapsamında, ABAD "bir üye devletin polis veya diğer kolluk kuvvetleri tarafından yürütülen operasyonların geçerliliğini veya orantılılığını veya üye devletlerin kamu düzenini koruma ve iç güvenliği sağlama konusundaki sorumluluklarını yerine getirmelerini denetleme yetkisine sahip değildir."[345]

3. LİZBON ANTLAŞMASI SONRASI KİŞİSEL VERİLERİN KORUNMASI

3.1. Lizbon Antlaşması: "Avrupa Birliği'nde Kişisel Verilerin Korunması Açısından Dönüm Noktası"

Lizbon Antlaşması, AB'de veri korumaya ilişkin yasal çerçeveye önemli değişiklikler getirmiştir. Özellikle ABA'nın 6(1) maddesi ile ABTHŞ'nin kurucu Antlaşmalar ile aynı hukuki değerde olduğu kabul ederek birincil hukuk statüsüne yükseltilmesi ve ABİHA'nın 16'ncı maddesinde veri koruma mevzuatı için açık bir yasal dayanak getirilmesi dikkate değerdir.[346] Ayrıca ABA madde 6(3), üye devletlerin ortak anayasal geleneklerinden kaynaklandığı söylenen ve AİHS tarafından tesis edilen temel hakların AB hukukunun genel ilkeleri olarak güvence altına alınacağını belirtmektedir. Dolayısıyla bu hüküm, ABAD'ın temel haklara ilişkin zaman içerisinde ortaya koyduğu yerleşik içtihat hukukunu, önceden olduğu gibi teyit etmektedir.[347] ABA madde 6(2), AB'nin AİHS'ye katılacağını ilan ederek, AB'nin AİHS'nin haklar dizisiyle olan bağlantısını güçlendirmektedir. Görüldüğü üzere

[344] PEERS, STEVE, (2021), s.757.
[345] ABİHA madde 276.
[346] LYNSKEY, ORLA, *The Foundations of EU Data Protection Law*, 1st Edition, Oxford University Press, Oxford, 2015, s.14.
[347] FUSTER, GLORIA GONZÁLEZ, 2014, s.230.

Lizbon Antlaşması AB'deki temel haklar mimarisini yeniden tanımlamakta ve kişisel verilerin korunmasına yönelik özel hükümler içermektedir.[348]

Lizbon Antlaşması'nın bağlayıcılık kazandırdığı ABTHŞ'nin 7'inci maddesindeki "özel hayata ve aile hayatına saygı" yani mahremiyet hakkına ek olarak 8'inci maddesi ile "kişisel verilerin korunması" hakkının ayrı bir temel hak olarak kabul edilmesi de kişisel verilerin korunması hakkı açısından önem arz etmektedir.[349] ABTHŞ kapsamında, AB kurumları ve organları ile AB hukukunu uygularken üye devletler, kişisel verilerin korunması hakkını güvence altına almalı ve bu hakka saygı göstermelidir. Veri Koruma Direktifi'nden birkaç yıl sonra formüle edilen ABTHŞ'nin 8'inci maddesi, önceden var olan AB veri koruma hukukunun somutlaştırılması olarak değerlendirilmektedir.[350]

ABTHŞ'nin 8'inci maddesiyle birlikte değerlendirildiğinde, ABİHA'nın 16'ncı maddesi, bireylerin temel hakları olarak kişisel verilerin korunmasına ilişkin AB'nin görevlerini ortaya koymaktadır. ABİHA madde 16(1) ve ABTHŞ madde 8(1)'de "Herkes, kendisiyle ilgili kişisel verilerin korunması hakkına sahiptir" denilerek, AB'nin nihai olarak ABAD'ın kontrolü altında garanti altına alması gereken veri koruma hakkını belirtmektedir. ABİHA madde 16(2), AB yasa koyucusuna "AB hukuku kapsamına giren faaliyetlerin yürütülmesinde, AB kurum, organ, ofis veya ajansları ile üye devletler tarafından kişisel verilerin işlenmesi sırasında bireylerin korunmasına ve bu bilgilerin serbest dolaşımına ilişkin olağan yasama usulü uyarınca" veri korumaya ilişkin kurallar koyma yetkisi vermektedir. Son olarak, ABİHA Madde 16(2)'nin son cümlesi ve ABTHŞ madde 8(3)

[348] FUSTER, GLORIA GONZÁLEZ, 2014, s.231.
[349] VOGIATZOGLOU, PLIXAVRA ve VALCKE, PEGGY, 2022. s.11.
[350] European Union Agency for Fundamental Rights (FRA), *Handbook on European Data Protection Law*, 2018 edition, Publications Office of the European Union, Luxembourg, 2018, s.28.

uyarınca kişisel verilerin korunmasına ilişkin konulan kuralların bağımsız makamlar tarafından denetiminin sağlanması gerektiği ifade edilmektedir.[351]

Lizbon Antlaşması ile sütunlu yapının ortadan kaldırılmasının önemli sonuçlarından biri de ABİHA'nın 16'ncı maddesinin, eski Üçüncü Sütun konuları olan CKKAİ alanı da dâhil olmak üzere, AB'nin yetki alanına giren tüm konuları kapsayan modern ve kapsamlı bir veri koruma yaklaşımı için AB'ye veri koruma konularında yasama yetkisi veren yeni bir yasal dayanak oluşturmasıdır.[352] Ancak ODGP ile ilgili olarak üye devletlerin ODGP kapsamına giren faaliyetleri yürütürken kişisel verilerin işlenmesi için farklı bir rejim tesis edebileceği düzenlenmiştir.[353] Bu konularla ilgili olarak Konsey, ODGP alanında kişisel verilerin işlenmesinin düzenlenmesine ilişkin bir karar kabul etme yetkisine sahiptir.[354] Bu düzenleme, kişisel verilerin işlenmesini düzenlerken sadece üye devletleri kapsadığından, AB'nin kurumları, organları, ofisleri ve ajansları tarafından ODGP alanında gerçekleştirilen bu tür işlemler ABİHA'nın 16'ncı maddesinin koruyucu kapsamı altında kalacaktır.[355]

3.2 Avrupa Veri Koruma Çerçevesinde Parçalı Yapının Sürdürülmesi

Lizbon Antlaşması öncesi dönemdeki sütunlu yapının bir sonucu olarak kişisel verilerin korunması farklı usullere göre kabul edilen farklı hukuki statülerde ve farklı kapsamları olan tasarruflar ile düzenlenmekteydi.[356] Lizbon Antlaşması sütunlu yapıyı ortadan kaldırmış ve AB'ye kişisel verilerin korunmasına ilişkin ABİHA madde 16(2) kapsamında kendi yetki alanına giren tüm konularda yasama yetkisi verilmiştir.

---

[351] HIJMANS HIELKE, *The European Union as Guardian of Internet Privacy; The Story of Art 16 TFEU*, Springer International Publishing, Switzerland, 2016, s.4.
[352] European Union Agency for Fundamental Rights (FRA), *Handbook on European Data Protection Law*, 2018 edition, Publications Office of the European Union, Luxembourg, 2018, s.29.
[353] Lizbon Antlaşması ile değişik ABA madde 16(2) son paragraf.
[354] Lizbon Antlaşması ile değişik ABA madde 39.
[355] HIJMANS, HIELKE ve SCIROCCO, ALFONSO, (2009), s.1515.
[356] Lizbon Antlaşması öncesi kişisel verilerin korunması ile ilgili bu çalışmanın birinci bölümüne bakınız.

Lizbon Antlaşması sonrası kişisel verilerin korunmasına değinmeden önce Lizbon Antlaşmasını kabul eden Hükümetlerarası Konferansın Nihai Senedine ekli "Cezai konularda adli işbirliği ve kolluk işbirliği alanlarında kişisel verilerin korunmasına ilişkin deklarasyon" başlıklı 21 no.lu deklarasyondan bahsetmek gerekmektedir. Söz konusu deklarasyonda "ABİHA'nın 16'ncı maddesine dayanan cezai konularda adli işbirliği ve kolluk işbirliği alanlarında kişisel verilerin korunması ve bu tür verilerin serbest dolaşımına ilişkin özel kuralların, bu alanların kendine özgü doğası nedeniyle gerekli olabileceği" kabul edilmiştir. Bu Deklarasyon, CKKAİ alanında kişisel verilerin korunması rejimi açısından bir dizi farklı kuralın uygulanmasına izin vermektedir.[357] Hijmans ve Scirocco'nun belirttiği gibi, "bu Deklarasyon'un anlamı tam olarak açık olmayabilir, ancak üye devletlerin görüşüne göre eski Üçüncü Sütunun veri korumasına ilişkin genel çerçevenin uygulandığı normal bir hukuk alanı olmayacağını açıklığa kavuşturmaktadır."[358]

Lizbon Antlaşması ile sütunlu yapının kaldırılması, getirilen kapsamlı değişiklikler ve ABİHA madde 16'nın oluşturulması, AB'de veri korumanın düzenlenmesi için yeni olanaklar sunmuş, ancak AB yasa koyucularını, ya iki ayrı yasal araçla (önceden var olan Direktif ve Çerçeve Karar yerine bir Tüzük ve bir Direktif) parçalanmış veri koruma rejimini korumak ya da kapsamlı bir yaklaşım izleyerek veri korumaya ilişkin konuları AB'nin bu iki yetki alanını kapsayacak tek bir yasal araçla düzenlemek ikilemiyle karşı karşıya bırakmıştır.[359]

[357] KOSTA, ELENI, "A divided European data protection framework: A critical reflection on the choices of the European legislator post-Lisbon", KOSTA, ELENI ve LEENES, RONALD (Eds.), *Research Handbook On EU Data Protection Law*, Edward Elgar Publishing, Cheltenham, 2022, s.74.
[358] HIJMANS, HIELKE ve SCIROCCO, ALFONSO, (2009), s.1516.
[359] KOSTA, ELENI, (2022), s.70.

Komisyon, 2010 yılında ÖGAA'nın geleceğine ilişkin bir Bildiri[360] sunmuş ve diğer hususların yanı sıra veri koruma hakkının tutarlı bir şekilde uygulanması ihtiyacını "AB'nin, kolluk kuvvetleri ve suçun önlenmesi de dâhil olmak üzere tüm AB politikaları bağlamında bireyin kişisel verilerini koruma konusundaki duruşunu güçlendirmesi gerektiği" şeklinde vurgulamıştır.[361] Söz konusu Bildiri'den sonra Kasım 2010'da Komisyon, "AB'de kişisel verilerin korunmasına ilişkin kapsamlı bir yaklaşım" konulu bir Bildiri daha yayınlamıştır.[362] Bildiri'de Komisyon, Lizbon Antlaşması'nın AB'nin önceki sütun yapısını ortadan kaldırdığını ve ABİHA madde 16 ile AB politikaları genelinde kişisel verilerin korunmasına yönelik yeni ve kapsamlı bir yasal temel getirdiğini kabul ederek, CKKAİ alanında geçerli olan veri koruma kurallarının gözden geçirilmesini öngörmüştür.[363] Komisyon, her ne kadar bu Bildiri'de "Birliğin tüm sektör ve politikalarındaki veri işleme faaliyetlerine uygulanacak kapsayıcı bir araca"[364] duyulan ihtiyacı vurgulamış olsa da nihai olarak Komisyon tarafından 2012 yılında önerilen veri koruma reform paketi bu tür kapsamlı bir araç içermemektedir. Bunun yerine, Komisyon'un reform veri koruma reform paketi, genel veri koruma kurallarını belirleyen ve Veri Koruma Direktifi'nin yerini alacak olan bir Tüzük[365] ve kolluk kuvvetleri

[360] European Commision, "Delivering an area of freedom, security and justice for Europe's citizens - Action Plan Implementing the Stockholm Programme", Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 20.04.2010, COM/2010/0171 final.
[361] "Delivering an area of freedom, security and justice for Europe's citizens - Action Plan Implementing the Stockholm Programme", s.3.
[362] European Commission, "A comprehensive approach on personal data protection in the European Union", Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 4.10.2010, COM/2010/0609.
[363] "A comprehensive approach on personal data protection in the European Union", s.14. GÖÇMEN, İLKE ve ŞEKER, EMRİYE ÖZLEM, 2022, s.243, QUINTEL, TERESA ve KOSTA, ELENI, "Background and evolution of the LED", KOSTA, ELENI ve BOEHM, FRANZISKA (Eds.), *The EU Law Enforcement Directive (LED): A commentary*, Oxford University Press, Oxford, 2024, s.5.
[364] "A comprehensive approach on personal data protection in the European Union", s.4.
[365] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", COM(2012) 11 final.

ve adli makamlar tarafından suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infazı amacıyla veri işlemeye uygulanacak ve 2008/977 sayılı Çerçeve Karar'ın yerini alacak bir Direktif[366] olacak şekilde iki yasama aracı önermiştir.[367] Komisyon'un ilk konseptini şekillendiren AB yaklaşımı, CKKAİ alanındaki kişisel verilerin işlenmesinin diğer tüm kişisel veri işlemelerinden ayrı olması gerektiğidir. Bu amaçla, AB'deki tüm kişisel veri işlemeyi kapsayan tek bir yasal araç yerine, biri genel diğeri kolluk kuvvetleri ve adli makamlar için özel olarak tasarlanmış iki araç getirilmiştir.[368]

Önerilen taslak Tüzük ve Direktif'in kabulü uzun ve meşakkatli bir süreç olmuştur.[369] Üç yıl süren müzakerelerin ardından 15 Aralık 2015 tarihinde Konsey ve AP hem GDPR hem de Kolluk Direktifi metni üzerinde anlaşmaya varmıştır. Hem GDPR hem de Kolluk Direktifi 27 Nisan 2016 tarihinde kabul edilmiş ve AB'de kişisel verilerin korunmasına yönelik yeni bir rejim oluşturmuştur.[370] GDPR, 24 Mayıs 2016 tarihinde yürürlüğe girmiş, ancak 25 Mayıs 2018'den itibaren uygulanmaya başlamıştır.[371] Kolluk Direktifi'nin ise (daha önceki bölümlerde belirtildiği üzere direktif, tüzük gibi doğrudan uygulanabilen bir tasarruf türü olmadığı için üye devletler tarafından iç hukuka aktarılması gerekmektedir) 6 Mayıs 2018 tarihine kadar üye devletler tarafından iç hukuklarına aktarılması gerekmektedir.[372] Bu sürelerin sonuna kadar Veri Koruma Direktifi ve 2008/977 sayılı Çerçeve Karar yürürlükte

[366] European Commission, "Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", COM(2012) 10 final.
[367] LYNSKEY, ORLA, 2015, s.19.
[368] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2016), s.8.
[369] Kolluk Direktifi'nin yasama süreci bir sonraki bölümde ayrıntılı olarak incelenecektir. GDPR'ın yasama süreci ile ilgili bkz. KUNER, CHRISTOPHER, *et.al.*, "Background and Evolution of the EU General Data Protection Regulation (GDPR)", KUNER, CHRISTOPHER, *et.al.* (Eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, s.3-10.
[370] KOSTA, ELENI, (2022), s.70.
[371] GDPR madde 99(2).
[372] Kolluk Direktifi madde 63(1). Bu sürenin istisnaları için bkz. Kolluk Direktifi madde 63(2) ve 63(3).

kalacaktır. Hem GDPR'nin hem de Kolluk Direktifi'nin kabul edildiği tarih ile uygulanmaya başladığı tarih arasındaki bu iki yıllık süre yeni yasal rejiminin getireceği önemli değişikliklere yeterince hazırlanmaları için üye devletlere gerekli zamanı tanımayı amaçlamıştır.[373] Ayrıca ABİHA madde 16(2) kapsamında kabul edilen üçüncü tasarruf olan, kişisel verilerin AB'nin kurum ve kuruluşları, ofisleri ve ajansları tarafından işlenmesini düzenleyen 45/2001 sayılı Tüzük'ün yerini alan 2018/1725 sayılı Tüzük'ü[374] de unutmamak gerekir. Böylece AB yasa koyucusu aşağıdaki şekilde özetlenebilecek parçalı bir yapıyı muhafaza etmeyi tercih etmiştir.[375]

Tablo 1: Lizbon Antlaşması sonrasında AB'nin veri koruma yasal çerçevesi

2016/679 sayılı Tüzük "GDPR"	2016/680 sayılı Direktif "Kolluk Direktifi"	2018/1725 sayılı Tüzük
* Üye Devletlerdeki ticari sektör * Kolluk ve ceza adaleti makamları hariç, Üye Devletlerdeki kamu sektörü	* Üye Devletlerdeki kolluk ve ceza adaleti makamları	* Avrupa Birliği kurumları, organları, ofisleri ve ajansları

Sonuç olarak; Lizbon Antlaşması, AB'de kişisel verilerin korunmasına ilişkin bir dönüm noktası olmuştur. İlk olarak, "kişisel verilerin korunması" hakkının özerk bir hak olarak tanındığı ilk belge olan ABTHŞ'nin birincil hukuk statüsüne çıkması ve bağlayıcılık kazanması temel hak açısından önem arz etmektedir. İkinci olarak Lizbon Antlaşması'nın

[373] MOORE, DOMINIQUE, "Article 99. Entry into force and application", KUNER, CHRISTOPHER, *et.al.* (Eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, s.1320.

[374] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21/11/2018, p. 39–98.

[375] DE HERT, PAUL ve SAJFERT, JURAJ, "The Role of the Data Protection Authorities in Supervising Police and Criminal Justice Authorities Processing Personal Data", BRIERE, CHLOE ve WEYEMBERGH, ANNE (Eds.), *The Needed Balances in EU Criminal Law: Past, Present and Future*, Hart Publishing, Oxford, 2018, s.246.

sütunlu yapıyı ortadan kaldırması ve ABİHA'nın 16'ncı maddesinin, hem kişisel verilerin korunması hakkını açık bir şekilde tanıması hem de AB'ye kişisel verilerin korunması için yasama yapma konusunda tam yetki vermesi, AB'nin yasa koyucularına ODGP alanı hariç tüm alanları kapsayacak şekilde kişisel verilerin korunmasına ilişkin gerekli adımları atmasına imkân vermiştir. Bu çerçeve kişisel verilerin korunmasına yönelik kabul edilen GDPR "lex generalis" yani genel düzenlemeyi, Kolluk Direktifi ise "lex specialis" yani özel düzenlemeyi oluşturmuştur.

4. 2016/680 SAYILI KOLLUK DİREKTİFİ

4.1 Genel Olarak

Lizbon Antlaşması'nın yürürlüğe girmesi ve özellikle ABİHA madde 16 ile kişisel verilerin korunmasına ilişkin yeni bir yasal dayanağın getirilmesi, CKKAİ alanının kendine özgü yapısına saygı gösterirken, bireylerin verileri için yüksek düzeyde koruma sağlayan kapsamlı bir veri koruma çerçevesinin oluşturulmasına izin vermiştir. Bu çerçevede AB tarafından kişisel verilerin korunmasına yönelik bir önceki başlık altında ayrıntıları ile açıklanan şekilde bir Tüzük ve bir Direktif kabul edilmiştir. CKKAİ alanında ayrı bir tasarruf türü tercihi söz konusu alanın kendi doğasından kaynaklanmaktadır.

Komisyon'un, CKKAİ alanında kişisel verilerin yüksek düzeyde korunmasını sağlamak ve üye devletlerin kolluk ve adli makamları arasında kişisel veri aktarımını kolaylaştırmak amacıyla ortaya koyduğu ilk konseptini şekillendiren AB yaklaşımı, Lizbon Antlaşması'nı kabul eden Hükümetlerarası Konferansın Nihai Senedine ekli "Cezai konularda adli işbirliği ve kolluk işbirliği alanlarında kişisel verilerin korunmasına ilişkin deklarasyon" başlıklı 21 no.lu deklarasyonda da açıkça vurgulandığı üzere, kolluk ve adli makamlar tarafından veri işlemenin diğer tüm kişisel veri işlemeden farklı olması gerektiği yönündedir. Bu amaçla, AB'deki tüm kişisel veri işlemeyi kapsayan tek bir yasal araç yerine,

biri genel diğeri kolluk kuvvetleri için özel olarak tasarlanmış iki araç getirilmiştir.[376] Ayrıca, genel anlamda kişisel verilerin korunması için, 1995 yılında beri uygulanan Veri Koruma Direktifi göz önüne alındığında, AB genelinde kişisel verilerin korunmasının bir Tüzük ile düzenlenmesi için yeterince olgunlaştığı kabul edilirken, kolluk ve adli makamlar tarafından işlenen kişisel verilerin korunması açısından tercih edilen araç, üye devletlere kendi ulusal yasalarına dâhil ederken belirli bir düzeyde esneklik sağlayan bir Direktif olmuştur.[377] Gerçekten de CKKAİ alanında kişisel veri işleme, genel veri işlemeden farklı olarak özel bir esneklik gerektirir. Güvenlikle ilgili veriler; söylentilere, gizli kaynaklara veya dolaylı bilgilere dayanabilir, bu nedenle "veri kalitesi" ve "amaç sınırlaması" gibi ilkelere sıkı şekilde uyulamayabilir. Ayrıca, kişilerin bilgi edinme ve erişim hakları tam anlamıyla tanındığında, gizli yürütülen soruşturma faaliyetleri tehlikeye girebilir. Bu sebeple veri koruma kuralları ile güvenlik politikaları arasında hassas bir denge kurulmalıdır.[378] Bu nedenlerle AB yasa koyucuları tarafından kişisel verilerin korunması adına bütüncül tek bir metin yerine, iki ayrı tasarruf türü kabul edilmiştir. Bu durum özellikle AVKD tarafından "Komisyon'un bu konuyu, önerilen Tüzük'e kıyasla çok daha yetersiz bir koruma düzeyi sağlayan ve kendi başına ayakta duran bir yasal araçla düzenlemeyi seçmiş olmasından" dolayı "hayal kırıklığı" olarak değerlendirilmiştir.[379]

Komisyon, Kolluk Direktifi'nin ilk teklifini hazırlarken eski Üçüncü Sütun, başta 2008/977 sayılı Çerçeve Karar olmak üzere, veri koruma çerçevesinin tutarsız ve parçalı

[376] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2016), s.8.
[377] CAN, NESLİHAN, *Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması*, Yayımlanmamış Tez, İstanbul Üniversitesi, İstanbul, 2020, s.25.
[378] BOSTANCI BOZBAYINDIR, GÜLŞAH, "Avrupa Birliği Ceza Hukuku'nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Sayı:2, 2018, s.71; DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2016), s.9.
[379] European Data Protection Supervisor, "Executive summary EDPS Opinion of 7 March 2012 on the data protection reform package", OJ C 192, 30.6.2012, s.7–15.

durumunun farkındaydı. Komisyon bu durumu, "Etki Değerlendirmesi Çalışma Belgesinde"[380] açıkça kabul etmiş ve bunları aktif bir şekilde ele alma arzusunu ortaya koymuştur.[381] Komisyon tarafından Kolluk Direktifi'ne ilişkin ilk taslak metin[382] 25 Ocak 2012 tarihinde sunulmuştur. Dört yıllık bir sürecin ardından[383], GDPR gibi, Kolluk Direktifi'de Mayıs 2016'da kabul edilmiş ve kolluk kuvvetleri alanında kişisel verilerin işlenmesine ilişkin kuralları belirleyen yasal olarak bağlayıcı ilk belge olarak kapsamlı bir AB veri koruma rejiminin kurulmasında önemli bir adım teşkil etmiştir.[384]

Kolluk Direktifi, gelişen teknolojinin de etkisiyle günümüz dijital çağında kişisel verileri işleyen kolluk kuvvetleri için tasarlanmış modern bir veri koruma aracıdır. Kolluk Direktifi, 6 Mayıs 2016 tarihinde yürürlüğe girmiş olup, üye devletlerin 6 Mayıs 2018 tarihine kadar Kolluk Direktifi'ni iç hukuklarına aktarmaları gerekmektedir.[385] Kolluk Direktifi'nin üye devletlerin iç hukuklarına aktarılması süreci kolay bir süreç olmamıştır. Komisyon, Temmuz 2018'de 19 üye devlet aleyhine, gerekli son tarihe kadar Kolluk Direktifi'ni iç hukuka aktaran mevzuat değişikliklerini kabul etmedikleri için ihlal prosedürleri başlatırken, Temmuz 2019'da başka bir üye devlete kısmi aktarmama için başka

---

[380] European Commission, "Commission Staff Working Paper – Impact Assessment accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", SEC(2012)72, Brussels, 25 Ocak 2012, s.31–35.

[381] MARQUENIE, THOMAS, (2017), s.328.

[382] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25.01.2012, COM/2012/010 final.

[383] Kolluk Direktifi'nin kabul sürecindeki ilgili kurumlara ait görüşlere Direktif'in ilgili bölümleri ayrıntılı olarak incelenirken yer verilecektir.

[384] SAJFERT, JURAJ ve QUINTEL, TERESA, "*Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities*", 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873, Erişim Tarihi:5.4.2025, s.3.

[385] Kolluk Direktifi madde 63(1).

bir prosedür başlatılmıştır.[386] İhlal prosedürleri 2020 yılına kadar kademeli olarak kapatılmıştır. 2021'de Komisyon, İspanya'ya karşı Kolluk Direktifi'ni iç hukuka aktarmadığı için açtığı ihlal davasını ABAD'a havale etmiş ve ABAD hem toplu para hem de ceza ödemesine hükmetmiştir.[387] Komisyon, Nisan 2022'de, Almanya, Yunanistan, Finlandiya ve İsveç'e karşı ihlal prosedürleri başlatmıştır.[388]

Kolluk Direktifi, 6 Mayıs 2018 tarihinden itibaren 2008/977 sayılı Çerçeve Karar'ını yürürlükten kaldırmış ve onun yerini almıştır.[389] Bu değişim, 2008/977 sayılı Çerçeve Karar'ın bu çalışmanın daha önceki bölümlerinde ayrıntılı olarak açıklandığı üzere kişisel verilerin korunmasına ilişkin yaşatmış olduğu "hayal kırıklığı" nedeniyle hiçbir veri koruma savunucusunun şikâyet etmeyeceği bir değişimdir.[390] Kolluk Direktifi, 2008/977 sayılı Çerçeve Karar'ın en büyük eksikliği olarak görülen kişisel verilerin sadece sınır ötesi işlenmesini düzenleyen dar kapsam sorununu ortadan kaldırmaktadır. Kolluk Direktifi, işlemenin ulusal sınırlar içerisinde veya ötesinde gerçekleşip gerçekleşmediğine bakılmaksızın, kolluk kuvvetleri ve adli makamlar tarafından gerçekleştirilen tüm kişisel verilerin işlenmesini kapsamayı amaçlamaktadır.[391] Bu şekilde 2008/977 sayılı Çerçeve Karar'ın en temel kısıtlaması nihai olarak kaldırılmış olup, AB içindeki başta kolluk

[386] European Commission, Communication from the Commission to the European Parliament and the Council, "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", COM(2022) 364 final, 25.7.2022, s.8.
[387] "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", s.8. Judgment of 25 February 2021, *European Commission v Kingdom of Spain*, C-658/19, EU:C:2017:548.
[388] Almanya'ya karşı açılan prosedür, Almanya'nın federal polisinin faaliyetleriyle ilgili olarak Kolluk Ditrktifi'nin iç hukuka aktarılmasındaki bir boşlukla ilgilidir. Yunanistan'a karşı açılan dava, Kolluk Direktifi'ne tabi aktörler ve Kolluk Direktifi'nin 5, 8 ve 11. maddelerinin iç hukuka aktarılması da dahil olmak üzere bir dizi hususla ilgilidir. Finlandiya ve İsveç'e karşı açılan davalar, ulusal kanunların veri sahiplerine bir mahkeme ya da yargı mercii önünde etkili bir hukuk yoluna erişim sağlamaması nedeniyle açılmıştır. "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", s.9.
[389] Kolluk Direktifi madde 58(1).
[390] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2016), s.7.
[391] Kolluk Direktifi madde 2(1).

kuvvetleri olmak üzere güvenlikle ilgili tüm yetkili makamlar Kolluk Direktifi'nin hükümlerini kişisel veri işleme süreçlerine uygulamak zorunda kalmıştır.[392]

AB genelinde CKKAİ alanındaki yetkili makamlar arasında uyumun sağlanması, özellikle bu alanın üye devletlerin egemenlik alanının önemli bir parçasını oluşturması ve ayrıca üye devletler arasındaki kolluk alanındaki teknolojik kapasite farkları ve kolluk faaliyetlerinde yeni teknolojilerin giderek daha fazla kullanılması nedeniyle oldukça zordur. Bu zorluklar, üye ülkeler arasında veri işleme uygulamalarında belirgin farklılıklara yol açmaktadır.[393] İşte bu nedenlerle Kolluk Direktifi'nin temel hedefi, bu tür farklılıkları en aza indirerek daha tutarlı bir veri koruma sistemi oluşturmaktır. Kolluk Direktifi'nin sadece kapsamı bile, 2008/977 sayılı Çerçeve Karar'ın kişisel verilerin korunması açısından yetersizliği karşısında veri koruma savunucularının kutlama yapması için yeterli bir neden oluşturmuştur.[394] Bununla birlikte, Kolluk Direktifi'nin asgari bir uyumlaştırma aracı teşkil ettiğini vurgulamak gerekir. Bir direktifin seçilmesi ve daha yüksek koruma standartları[395] da uygulayabilen üye devletlere genellikle geniş takdir yetkisi tanınması, ulusal düzeyde farklı uygulamaların devam etmesi riskini doğurmaktadır.[396]

Kolluk Direktifi, on bölümden oluşmaktadır. İlk bölümde Direktifin amacı, kapsamı ve tanımlar yer almaktadır. İkinci bölümde "kişisel verilerin işlenmesine ilişkin ilkeler", üçüncü bölümde "veri sahibinin hakları", dördüncü bölümde "veri sorumlusu ve veri

[392] BOSTANCI BOZBAYINDIR, GÜLŞAH, (2018), s.65.
[393] CAN, NESLİHAN, *Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması*, Yayımlanmamış Tez, İstanbul Üniversitesi, İstanbul, 2020, s.26.
[394] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2016), s.10.
[395] Kolluk Direktifi madde 1(3)'e göre; "Bu Direktif, Üye Devletlerin, yetkili makamlar tarafından kişisel verilerin işlenmesine ilişkin olarak veri sahibinin hak ve özgürlüklerinin korunması için bu Direktifte belirlenenden daha yüksek güvenceler sağlamasına engel teşkil etmez."
[396] CARUANA, MIREILLE M., "The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement", International Review of Law, Computers & Technology, Cilt:33, Sayı:3, 2017, s.3.

işleyenin yükümlülükleri", beşinci bölümde ise "kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılması" düzenlenmektedir. Altıncı bölümde "bağımsız denetim makamları", yedinci bölümde "işbirliği", sekizinci bölümde "hukuki yollar, sorumluluk ve yaptırımlar", dokuzuncu bölümde "uygulama tedbirleri" ve onuncu bölümde "son hükümler" ortaya konulmaktadır.

Üye devletlerin, CKKAİ alanında kişisel verileri nasıl işleyecekleri ve veri sahiplerinin haklarını nasıl koruyacakları hususlarını düzenlemek kadar ayrıntılı bir düzeyde uyumlaştırma çabası daha önce hiç denenmemiştir. AB üye devletlerinin tamamının CKKAİ amaçları doğrultusunda kişisel veri işlemesini ortak bir düzenleyici çerçeve altına alma başarısı, Kolluk Direktifi'nin veri koruma amaçlarına yönelik temel katkılarından birini oluşturmaktadır.[397] Genel olarak daha geniş kapsamlı ve daha genel uygulanabilir GDPR'nin gölgesinde kalmış olsa da, Kolluk Direktifi büyük önem taşımaya devam etmektedir ve önümüzdeki yıllarda kişisel verilerin adli makamlar ve kolluk kuvvetleri tarafından işlenmesini şekillendirmeye devam edecektir.[398]

4.2 Amaç ve Kapsam

Kolluk Direktifi, "kamu güvenliğine yönelik tehditlerin önlenmesi ve bunlara karşı koruma sağlanması da dâhil olmak üzere, suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezai yaptırımların infazı amacıyla kişisel verilerin yetkili makamlar tarafından işlenmesine ilişkin olarak gerçek kişilerin korunmasına yönelik kuralları ortaya koymaktadır."[399] Kolluk Direktifi'nin amacı "gerçek kişilerin temel hak ve özgürlüklerini ve özellikle kişisel verilerin korunması haklarını korumak" ve "AB veya üye devlet hukuku

[397] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2016), s.10.
[398] MARQUENIE, THOMAS, (2017), s.325.
[399] Kolluk Direktifi madde 1(1).

tarafından gerekli görüldüğü hallerde, AB içindeki yetkili makamlar tarafından kişisel veri alışverişinin, kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin korunmasıyla bağlantılı nedenlerle kısıtlanmamasını veya yasaklanmamasını sağlamak" şeklinde ifade edilmektedir.[400] Kolluk Direktifi, iki temel hedef belirlemektedir. Bu hedeflerden ilki, CKKAİ amaçları için yetkili makamlar arasında kişisel verilerin serbestçe akışının sağlanarak ÖGAA'nın gerçekleştirilmesine katkıda bulunulmasıdır. İkinci hedefi ise, Kolluk Direktifi kapsamında işlenen kişisel verilerin yüksek düzeyde korunmasını sağlamaktır.[401]

Görüldüğü üzere Kolluk Direktifi'nin amacı, üye devletler içerisinde veya arasında, kolluk kuvvetleriyle ilgili kişisel verilerin işlenmesinde yer alan kurumlar arasında bilgi akışını kısıtlamak değildir. Aksine Kolluk Direktifi, CKKAİ alanındaki yetkili makamlarca kişisel verilerin işlenmesinin nasıl yürütüleceğine ve bu kişisel verilerin nasıl değiş tokuş edileceğine ilişkin kapsamlı bir veri koruma yasal çerçevesi getirerek, bu tür veri akışlarını, veri sahiplerinin haklarını da koruyacak şekilde, kurumsallaştırmayı ve kolaylaştırmayı amaçlamaktadır. Başka bir deyişle, Kolluk Direkti'nin amacı, AB genelinde CKKAİ bağlamında kişisel verilerin işlenmesini yasaklamak değil, düzenleme yoluyla mümkün kılmaktır.[402]

Kolluk Direktifi, üye devletlerin, kişisel verilerin korunmasına ilişkin bu Direktif'te belirlenen koruma seviyesinden daha yüksek seviyede güvence sağlayan düzenlemeler kabul edebilmesine izin vermektedir.[403] Üye devletlerin, Kolluk Direktifi'nde öngörülen güvencelerin ötesine geçecek düzenlemeler kabul edebilecek olması kişisel verilerin

[400] Kolluk Direktifi madde 1(2).
[401] Kolluk Direktifi, Dibace (2) ve (4).
[402] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2016), s.11.; CAN, NESLİHAN, *Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması*, Yayımlanmamış Tez, İstanbul Üniversitesi, İstanbul, 2020, s.27.
[403] Kolluk Direktifi madde 1(3).

korunması açısından olumlu olmakla birlikte, böyle bir hüküm bir yanda mümkün olan en yüksek veri koruma düzeyini korumaya kararlı üye devletler ile diğer yanda asgari koruma düzeyinin üzerine çıkma konusunda isteksiz olan üye devletler arasında önemli farklılıklara yol açabilecektir.[404] Bu düzenleme, AVKD'nin Kolluk Direktifi'nin yasalaşma süresince vermiş olduğu görüşünde şu şekilde eleştirilmiştir.[405]

> "*Üye devletler arasında kolluk ve ceza adaleti alanında kişisel verilerin korunmasına ilişkin farklı standartların belirlenmesi, yetkili makamlar arasında serbest bilgi akışını engelleyecek ve dolayısıyla kolluk ve adli işbirliğinin etkinliğini olumsuz yönde etkileyecektir. Eğer üye devletler arasında standartlarda çok büyük farklılıklar varsa, bu aynı zamanda kendi veri koruma rejimi olan ve Direktif ile karşılaştırıldığında nispeten daha katı olan Europol ile bilgi alışverişini de zorlaştıracaktır: Üye devletler en düşük ortak payda temelinde ikili işbirliği yapmayı tercih edebilirler.*"

Kolluk Direktifi'nin kapsamını; "kişisel verilerin, kamu güvenliğine yönelik tehditlerin önlenmesi ve bunlara karşı koruma sağlanması da dâhil olmak üzere, suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezai yaptırımların infazı amacıyla yetkili makamlar tarafından işlenmesi" oluşturmaktadır.[406] Kolluk Direktifi'nin kapsamı, kişisel verilerin yetkili makamlar tarafından tamamen yurt içinde işlenmesini de kapsayacak şekilde, 2008/977 sayılı Çerçeve Karar tarafından belirlenen ve üye devletler

---

[404] MASEA, COSTANZA DI FRANCESCO, *Balance between security and fundamental rights protection: an analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name records (PNR)*, 2016, https://rivista.eurojus.it/balance-between-security-and-fundamental-rights-protection-an-analysis-of-the-directive-2016680-for-data-protection-in-the-police-and-justice-sectors-and-the-directive-2016681-on-the-use-of-passen/, Erişim Tarihi:10.04.2025, s.8.

[405] European Data Protection Supervisor (EDPS), "Opinion 6/2015 – a further step towards comprehensive EU data protection: EDPS recommendations on the Directive for data protection in the police and justice sectors", 28 October 2015. s.5.

[406] Kolluk Direktifi madde 1(1) ve 2(1).

arasında iletilen veya kullanıma sunulan kişisel verilerin işlenmesiyle ve dolayısıyla sadece verilerin sınır ötesi transferleriyle sınırlı olan önceki rejime kıyasla önemli ölçüde genişletilmiştir.[407]

Kolluk Direktifi'nin kapsamının tanımlayıcı çerçevesine daha derinlemesine bakıldığında, Kolluk Direktifi'nin uygulanmasını tanımlayan iki temel kavram, bir yandan "işleme amacı" (maddi kapsam) ve diğer yandan "yetkili makamlar" (kişisel kapsam) kavramıdır.[408] Bir kişisel veri işleme faaliyetine Kolluk Direktifi'nin uygulanabilmesi için hem kişisel hem de maddi kapsamının karşılanması gerekmektedir. Başka bir deyişle Kolluk Direktifi'nin uygulanabilmesi için, işleme faaliyetinin yetkili bir makam tarafından (kişisel kapsam), kamu güvenliğine yönelik tehditlerin önlenmesi ve bunlara karşı koruma sağlanması da dâhil olmak üzere, cezai suçların önlenmesi, soruşturulması, tespiti ve kovuşturulması veya cezai yaptırımların infazı amacıyla gerçekleştirilmesi gerekmektedir (maddi kapsam).[409] Kolluk Direktifi'nin kapsamının tam olarak anlaşılabilmesi için maddi kapsam ile kişisel kapsamın daha net ortaya konulması gerekmektedir.

Bir kişisel veri işleme faaliyetinin Kolluk Direktifi'nin maddi kapsamına girebilmesi için amacın ya "kamu güvenliğine yönelik tehditlere karşı koymayı amaçlayan önleme de dâhil olmak üzere önleme amacı" ya "cezai suçların önlenmesi, soruşturulması, tespiti ve kovuşturulması amacı" ya da "cezai suçların infazı" olmalıdır. Bu doğrultuda maddi kapsam açısından iki kavramın açıklığa kavuşturulması önem arz etmektedir. Bunlardan ilki "kamu güvenliği" diğeri de "cezai suç" kavramıdır.

---

[407] VOGIATZOGLOU, PLIXAVRA ve FANTIN, STEFANO, "National and Public Security Within and Beyond The Police Directive", VEDDER, ANTON *et.al.*(Eds.), *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, Intersentia, Cambridge, 2019, s.29.
[408] VOGIATZOGLOU, PLIXAVRA ve FANTIN, STEFANO, (2019), s.30.
[409] SAJFERT, JURAJ ve QUINTEL, TERESA, (2017), s.3.

Kolluk Direktifi'nin maddi kapsamı açısından ortaya konulması gereken ilk kavram "kamu güvenliği" kavramıdır. Kolluk Direktifi'nin ilk taslağında[410] yer almayan işleme amaçlarından biri olan "kamu güvenliğine yönelik tehditlerin önlenmesi ve bunlara karşı koruma sağlanması" ibaresi Konsey tarafından Kolluk Direktifi'ne eklenmiştir.[411] Konsey'in, Kolluk Direktifi'ne böyle bir ifade eklemesi, üye devletlerin, özel veri koruma rejiminin uygulanmasını gerektiren CKKAİ alanında, genel veri koruma kurallarına tabi olması gereken alanları kapsayacak şekilde daha da büyük bir hareket alanı yaratmada bir başka adım olarak görülmüştür.[412] Özellikle, hem AVKD[413] hem de Madde 29 Çalışma Grubu[414], kamu güvenliği kavramını çevreleyen ve genellikle geniş bir şekilde yorumlanan netlik eksikliğine dikkat çekerek, Kolluk Direktifi'nin kapsamının CKKAİ konularının ötesine genişleme riskine yol açacağını belirtmiştir.[415] Kolluk Direktifi'nin dibacesinin 12'nci paragrafında, kolluk kuvvetleri tarafından üstlenilen ilgili faaliyetlerin "kamu güvenliğine ve toplumun kanunla korunan temel menfaatlerine yönelik suç teşkil edebilecek

[410] European Commission, "Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", COM(2012) 10 final.
[411] Position (EU) No 5/2016 of the Council at first reading with a view to the adoption of a Directive of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA Adopted by the Council on 8 April 2016, OJ C 158, 3.5.2016, p. 1–45
[412] BREWCZYŃSKA, MAGDALENA, "A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation", KOSTA, ELENI ve LEENES, RONALD, *Research Handbook On EU Data Protection Law*, Edward Elgar Publishing, Cheltenham, 2022. s.112.
[413] European Data Protection Supervisor (EDPS), "Opinion 6/2015 – a further step towards comprehensive EU data protection: EDPS recommendations on the Directive for data protection in the police and justice sectors", 28 October 2015. s.5.
[414] Article 29 Data Protection Working Party, "Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", WP233, 01 Aralık 2015, s.5.
[415] VOGIATZOGLOU, PLIXAVRA ve FANTIN, STEFANO, (2019), s.31.

tehditlere karşı koruma sağlamak ve bunları önlemek için gerekli olduğu hallerde polis veya diğer kolluk kuvvetlerine verilen bir görev olarak kanun ve düzeni sağlamayı" kapsayabileceğini açıklamaktadır. Kamu güvenliği kavramının Kolluk Direktifi'nde açık bir şekilde ortaya konmamış olması söz konusu kavramın üye devletler tarafından farklı şekillerde yorumlanmasına neden olacaktır ki bu da kişisel veri işleme faaliyetinin üye devlet tarafından kamu güvenliği kavramı içerisinde değerlendirilmesi neticesinde GDPR yerine Kolluk Direktifi'nin uygulanmasına sebep olacaktır.

Kamu güvenliği kavramının Kolluk Direktifi'nin maddi kapsamı içerisinde yer almasına yönelik eleştirilerin bir sebebi de "kamu güvenliği" kavramı ile "ulusal güvenlik" kavramının üye devletlerce uygulamada iç içe geçmiş durumda olmasıdır.[416] Kişisel verilerin "AB hukuku kapsamı dışında kalan bir faaliyet sırasında" işlenmesi Kolluk Direktifi'nin kapsamı dışında bırakılmıştır.[417] ABA madde 4 ile "ulusal güvenlik" kavramı "her üye devletin kendi sorumluluğunda kalmaya devam eder" denilerek AB hukukunun dışında bırakılmıştır. Dolayısıyla "ulusal güvenlik" kavramı Kolluk Direktifi'nin kapsamı dışındadır. Aslında Kolluk Direktifi'nin ilk taslağında[418] "ulusal güvenlik" kavramı açıkça kapsam dışı bırakılmışken, daha sonra Kolluk Direktifi'nin dibacesine alınmıştır.[419] "Ulusal güvenlik" kavramı geleneksel olarak devlet egemenliği ile bağlantılıdır ve ABAD tarafından belirtildiği

[416] "Kamu güvenliği" ve "ulusal güvenlik" kavramlarının Kolluk Direktifi açısında değerlendirmesine ilişkin bkz. VOGIATZOGLOU, PLIXAVRA ve FANTIN, STEFANO, (2019), s.32-47.
[417] Kolluk Direktifi madde 2(3)(a).
[418] European Commission, "Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", COM(2012) 10 final.
[419] Kolluk Direktifi, Dibace (14). "Bu Direktif, Birlik hukuku kapsamı dışında kalan bir faaliyet sırasında kişisel verilerin işlenmesine uygulanmaması gerektiğinden, ulusal güvenlikle ilgili faaliyetler, ulusal güvenlik konularıyla ilgilenen ajansların veya birimlerin faaliyetleri ve Üye Devletlerin Avrupa Birliği Antlaşması (ABA) Başlık V Bölüm 2 kapsamına giren faaliyetleri yürütürken kişisel verileri işlemesi, bu Direktifin kapsamına giren faaliyetler olarak değerlendirilmemelidir."

üzere "Devletin temel işlevlerini ve toplumun temel çıkarlarını korumayı amaçlayan faaliyetler" ile ilgilidir.[420]

"Kamu güvenliği" kavramının AB hukuku tarafından, özellikle iç pazarın işleyişi ile ilgili[421], ortaya konan temel kural ve özgürlüklere bir istisna olarak düzenlendiği görülmektedir.[422] ABAD tarafından, *Tsakouridis*[423] kararında, kamu güvenliği kavramının "bir üye devletin hem iç hem de dış güvenliğini kapsadığı" vurguladıktan sonra kamu güvenliğinin "kurumların ve temel kamu hizmetlerinin işleyişine ve nüfusun hayatta kalmasına yönelik bir tehdidin yanı sıra dış ilişkilere veya ulusların barış içinde bir arada yaşamasına yönelik ciddi bir rahatsızlık riski veya askeri çıkarlara yönelik bir riskten" etkilenebileceğini tespit etmiştir.[424] Görüldüğü üzere "kamu güvenliği" ve "ulusal güvenlik" kavramları ABAD'ın kararlarında bile birbiri yerine geçebilecek şekilde ifade edilmektedir. Sonuç olarak, ABAD tarafından Kolluk Direktifi özelinde bir "kamu güvenliği" tanımı yapılana kadar, CKKAİ alanında kişisel verilerin korunmasına ilişkin Kolluk Direktifi'nin kapsamı yine ulusal mahkemelerin "AB hukuku kapsamı dışında kalan faaliyet" olan "ulusal güvenlik" kavramını nasıl yorumlayacaklarına ve üye devletlerin CKKAİ alanında kişisel verilerin korunmasına ilişkin Kolluk Direktifi'ni nasıl uygulayacaklarına bağlı olacaktır.[425] Bu doğrultuda, üye devletlerin, Kolluk Direktifi'ni iç hukuklarına aktarırken "ulusal güvenlik" kapsamında işlenen kişisel verileri de Kolluk Direktifi'nin kapsamına dâhil ederek, veri sahibinin hak ve özgürlüklerinin korunması için Kolluk Direktifi'nin sağladığı

[420] Case C-439/19, *B v Latvijas Republikas Saeima*, [2021], EU:C:2021:504, para.67.
[421] ABİHA madde 36, 45, 52 ve 65. Bu hükümler, kamu güvenliği gerekçesiyle sırasıyla malların, işçilerin, hizmetlerin ve sermayenin serbest dolaşımına sınırlamalar getirilmesine izin vermektedir.
[422] VOGIATZOGLOU, PLIXAVRA ve FANTIN, STEFANO, (2019), s.40.
[423] Case C-145/09, *Land Baden-Württemberg v. Panagiotis Tsakouridis*, [2010] ECR I-11979.
[424] Case C-145/09, *Land Baden-Württemberg v. Panagiotis Tsakouridis*, [2010] ECR I-11979, paras.43-44.
[425] MASEA, COSTANZA DI FRANCESCO, (2016), s.7.

güvencelerden daha yüksek güvenceler sağlamasına engel bulunmadığı ve bu yaklaşımı benimseyen üye devletlerin olduğu Komisyon Uzman Grubunca da dile getirilmiştir.[426]

Kolluk Direktifi'nin maddi kapsamı açısından açıklanması gereken ikinci kavram "cezai suç" kavramıdır. Cezaların infazı hariç olmak üzere, Kolluk Direktifi'nde ortaya konan beş veri işleme amacından dördü, yani önleme, soruşturma, tespit ve kovuşturma, "cezai suç" kavramına atıfta bulunmaktadır. "Cezai suç" kavramına Kolluk Direktifi'nin tanımlarında yer verilmemiştir. "Cezai suç" kavramı, veri işlemenin Kolluk Direktifi'nin uygulama kapsamına girip girmediğini belirlerken merkezi bir öneme sahiptir. ABAD'a göre, bir suçun "cezai suç" niteliği taşıyıp taşımadığı değerlendirilirken üç kriter dikkate alınmalıdır: İlk kriter, suçun ulusal hukuktaki hukuki sınıflandırması, ikincisi suçun içsel niteliği ve üçüncüsü de ilgili kişinin maruz kalabileceği cezanın ağırlık derecesidir.[427] Bununla birlikte, ABAD tarafından yapılan yorum esasen farklı üye devlet yasaları kapsamında neyin "cezai suç" teşkil ettiğine dair tüm tanımları içermekle birlikte, Kolluk Direktifi içerisinde "cezai suç" kavramının bir tanımı bulunmamasından kaynaklanan daha somut bir uyumlaştırmanın olmaması, suçların bazı ulusal hukuk düzenlerinde cezai, bazılarında ise idari suç olarak değerlendirilmesine yol açabilecektir.[428] Üye devletlerin "cezai suç" olarak tanımlanan suçların kapsamını belirlemelerine izin verilmesi, Kolluk Direktifi'nin uygulama kapsamının önemli ölçüde genişlemesine ve GDPR tarafından garanti altına alınan genel hakların kısıtlanmasına nesnel olarak ihtiyaç duyulmayan durumları kapsamasına neden olabilecektir.[429] Ancak unutulmamalıdır ki, ceza hukuku alanı

[426] Minutes of the fifteenth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 20 Şubat 2018.
[427] Case C-439/19, *B v Latvijas Republikas Saeima*, [2021], EU:C:2021:504, para 87.
[428] VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, "Assessment of the implementation of the Law Enforcement Directive", European Union Publications Office, 2022, s.19.
[429] BREWCZYŃSKA, MAGDALENA, (2022), s.110.

üye devletlerin tamamen AB'ye devretmek istemedikleri egemenlik alanının önemli bir parçasıdır ve özellikle hangi fiillerin ceza hukuku anlamında suç, hangi fiillerin ise ceza hukuku dışında idari anlamda suç teşkil edeceğine karar vermek Üye Devletlerin takdirindedir. Aksini düşünmek AB çapında tek bir ceza hukuku oluşturmak olacaktır ki bunu sağlamak imkânsıza yakın bir durumdur. Bu değerlendirme ile birlikte yine de Komisyon'un Kolluk Direktifi'ne ilişkin ilk raporunda, Üye Devletlerin, bir suçun niteliğini sadece Kolluk Direktifi'nin kapsamına dâhil edebilmek maksadıyla "cezai suç" olarak belirlememesi gerektiğine vurgu yapılmaktadır.[430]

Kolluk Direktifi'nin maddi kapsamına ilişkin önem arz eden kavramları ve bu kavramların Kolluk Direktifi'nin uygulanması açısından neden olabileceği belirsizlikleri ortaya koyduktan sonra kişisel kapsamına geçilebilir. Bir kişisel veri işleme faaliyetinin Kolluk Direktifi'nin kapsamında olabilmesi için maddi kapsamının yanında kişisel kapsamının da karşılanması gerektiği belirtilmişti. Kolluk Direktifi'nin kişisel kapsamını "yetkili makam" kavramı oluşturmaktadır. Kolluk Direktifi'nde yetkili makam; "kamu güvenliğine yönelik tehditlerin önlenmesi ve bunlara karşı koruma sağlanması da dâhil olmak üzere, cezai suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezai cezaların infazı konusunda yetkili olan herhangi bir kamu makamı"[431] veya "kamu güvenliğine yönelik tehditlerin önlenmesi ve bunlara karşı koruma sağlanması da dâhil olmak üzere, suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezai yaptırımların infazı amacıyla kamu otoritesini ve kamu yetkilerini kullanmak üzere üye devlet hukuku tarafından görevlendirilen diğer herhangi bir kurum veya kuruluş"[432] olarak

[430] "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", s.10.
[431] Kolluk Direktifi madde 3(7)(a)
[432] Kolluk Direktifi madde 3(7)(b).

tanımlanmaktadır. Kolluk Direktifi'nin ilk taslağında[433] "yetkili makam" tanımı dar bir çerçevede "cezai suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezai yaptırımların infazı konusunda yetkili olan herhangi bir kamu makamı" olarak ifade edilmişken, mevcut tanım Konsey tarafından Kolluk Direktifi'ne eklenmiştir.[434]

Kolluk Direktifi'nde "yetkili makam" tanımı yapılırken ikili bir ayrım yapılmıştır. İlk olarak Kolluk Direktifi madde 3(7)(a) kapsamında yetkili makam, madde 1(1)'deki işleme amaçları için "yetkili olan herhangi bir kamu kurumu" şeklinde ortaya konulmaktadır. Bu yetkili makam tanımı, ABİHA madde 87 ışığında okunduğunda, polis, jandarma, sahil güvenlik, gümrük ve diğer uzmanlaşmış kolluk kuvvetleri gibi "geleneksel" kolluk kuvvetleri ile adli makamları kapsamaktadır.[435] İkinci olarak, madde 3(7)(a) kapsamındaki geleneksel kolluk kuvvetleri ve adli makamlara ek olarak, Kolluk Direktifi madde 3(7)(b) kapsamındaki yetkili makam, madde 1(1)'deki işleme amaçları doğrultusunda "üye devlet hukuku tarafından kamu otoritesini ve kamu yetkilerini kullanmak üzere görevlendirilen diğer herhangi bir kurum veya kuruluş" olarak ifade edilmektedir. Bu tanımdan anlaşılacağı üzere Kolluk Direktifi madde 3(7)(b) kapsamındaki yetkili makamın kamu veya özel kurum ve kuruluşlar olabileceği ve kolluk görevlerinin her zaman sadece devlet kurumları

[433] European Commission, "Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", COM(2012) 10 final.

[434] Position (EU) No 5/2016 of the Council at first reading with a view to the adoption of a Directive of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA Adopted by the Council on 8 April 2016, OJ C 158, 3.5.2016, p. 1–45

[435] PURTOVA, NADEZHDA, "Between GDPR and the Police Directive: Navigating through the maze of information sharing in Public-Private Partnership", International Data Privacy Law, Cilt:8, Sayı:1, 2018, s.61.

tarafından yerine getirilmediği bazı üye devletlerin mevcut uygulamalarını[436] yansıtıyor gibi görülmektedir.[437]

Kolluk Direktifi'nin yasalaşma sürecinde hem AVKD hem de Madde 29 Çalışma Grubu, Madde 3(7)(b) kapsamındaki bu ikinci yetkili makam tanımının, kolluk ve ceza adaleti konularıyla kesinlikle ilgisi olmayan idari veya özel kuruluşları da içerebileceğini değerlendirmiş ve GDPR kapsamında olması gereken kurum ve kuruluşlar için Kolluk Direktifi'nin uygulanabilirliğinin potansiyel olarak genişlemesine ilişkin endişelerini dile getirmiştir.[438] Yetkili makam kavramı ile ilgili olarak Kolluk Direktifi'nin dibacesinin 11'inci paragrafında "…Bu tür yetkili makamlar yalnızca adli makamlar, polis veya diğer kolluk kuvvetleri gibi kamu makamlarını değil, aynı zamanda Üye Devlet hukuku tarafından bu Direktifin amaçları doğrultusunda kamu otoritesini ve kamu yetkilerini kullanmakla görevlendirilen diğer herhangi bir kurum veya kuruluşu da içerebilir.[…] Bu Direktif kapsamında söz konusu makamlar adına kişisel verileri işleyen bir kurum veya kuruluş, bir sözleşme veya başka bir yasal işlem ve bu Direktif uyarınca işleyicilere uygulanan hükümlerle bağlı olmalıdır; işleyici tarafından bu Direktif kapsamı dışında kişisel verilerin işlenmesi için (AB) 2016/679 sayılı Tüzüğün uygulanması etkilenmez." denilerek bu endişelere açıklık getirilmeye çalışılsa da çok başarılı olduğu söylenemez. Ayrıca Komisyon'un Kolluk Direktifi'ne ilişkin ilk raporunda da Kolluk Direktifi kapsamındaki yetkili makamlardan "ya devlet organları ya da yasaların bireyler arasındaki ilişkilerde

[436] Bazı AB Üye Devletlerinin yetkili makam yaklaşıma ilişkin bkz. VOGIATZOGLOU, PLIXAVRA ve FANTIN, STEFANO, (2019), s.51-57.
[437] PURTOVA, NADEZHDA, (2018), s.62.
[438] European Data Protection Supervisor (EDPS), "Opinion 6/2015 – a further step towards comprehensive EU data protection: EDPS recommendations on the Directive for data protection in the police and justice sectors", 28 October 2015. s.6; Article 29 Data Protection Working Party, "Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", WP233, 01 Aralık 2015, s.5.

geçerli olan normal kurallardan kaynaklananların ötesinde özel yetkiler verdiği ve/veya zorlama yetkisini kullanma olasılığı bulunan özel kuruluşlar" olarak bahsedilmiştir.[439]

Özetleyecek olursak bir kişisel veri işleme faaliyetinin Kolluk Direktifi kapsamına girebilmesi için hem kişisel kapsamın hem de maddi kapsamın aynı anda karşılaması gerekmektedir. Yukarıda kişisel kapsam ve maddi kapsam ayrıntılı olarak ele alınmış ve bu kapsamlar açısından önemli olan kavramlar açıklığı kavuşturulmaya çalışılmıştır. Ancak söz konusu kavramlara ilişkin belirtilen belirsizlikler özellikle kişisel verilerin işlenmesi açısından hangi durumlarda GDPR hangi durumlarda Kolluk Direktifi'nin uygulanması gerektiğini ortaya koyan sınır çizgisinin bulanıklaşmasına sebep olmaktadır.[440] İlerleyen süreçte ABAD tarafından ortaya konacak içtihat hukuku ışığında bu iki veri koruma mevzuatı arasındaki karşılıklı ilişki daha da netleşecektir.

Kolluk Direktifi'nin "AB hukuku kapsamı dışında kalan bir faaliyet sırasında" kişisel verilerin işlenmesi için geçerli olmadığını yukarıda "ulusal güvenlik" kavramı üzerinden açıklamıştık. Kolluk Direktifi madde 2(3)(b) uyarınca, Kolluk Direktifi, "AB kurumları, organları, ofisleri ve ajansları tarafından" gerçekleştirilen işleme faaliyetleri için de geçerli değildir. Kolluk Direktifi yerine, AB kurumları, organları, ofisleri ve ajansları tarafından gerçekleştirilen kişisel veri işleme faaliyetleri için, "Kişisel verilerin AB kurumları, organları, ofisleri ve ajansları tarafından işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu tür verilerin serbest dolaşımına ilişkin ve 45/2001 sayılı Tüzük ile 1247/2002 sayılı Kararı yürürlükten kaldıran 23 Ekim 2018 tarihli ve 2018/1725 sayılı

[439] "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", s.10.
[440] BOSTANCI BOZBAYINDIR, GÜLŞAH, (2018), s.74; CARUANA, MIREILLE M., (2017), s.5.

Tüzük" (EUDPR)[441] uygulanacak olup, EUDPR ile AB kurumlarınca işlenecek kişisel verilere ilişkin genel bir veri koruma çerçevesi oluşturulmaktadır. EUDPR'nin IX. Bölümü, AB kurumları tarafından, ABİHA'nın "cezai konularda adli işbirliği" veya "kolluk işbirliği" kapsamına giren faaliyetler yürütülürken operasyonel kişisel verilerin[442] işlenmesine ilişkin Tüzükte öngörülen veri koruma kuralları saklı kalmak kaydıyla, bir dizi özel kural öngörmektedir.[443] Europol ve Avrupa Savcılık Ofisi tarafından operasyonel verilerin işlenmesi kendi kuruluş Tüzükleri ile düzenlenmekte olup, EUDPR'ye uygun olarak revize edilmesi gerektiği hüküm altına alınmıştır.[444] Europol Tüzüğü[445], veri işleme faaliyetlerinin yeni Tüzükte belirtilen hükümler saklı kalmak kaydıyla EUDPR'ye tabi olduğunu belirterek değiştirilmiştir.[446] Görüldüğü üzere, ÖGAA kapsamında işlenecek kişisel veriler için geçerli veri koruma kuralları parçalanmış ve kafa karıştırıcı bir düzenleme yığını ile karşı karşıyadır. Bu durum, işleme faaliyetlerinin farklı yetki alanlarına, kuruluşlara veya veri tabanlarına yayıldığı durumlarda veri sahibinin hakkının kullanılmasını olumsuz yönde etkileyebilecektir.[447]

---

[441] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) PE/31/2018/REV/1, OJ L 295, 21.11.2018, s.39–98.

[442] "Operasyonel kişisel veriler; Birlik organları, ofisleri veya ajansları tarafından, bu organları, ofisleri veya ajansları kuran yasal düzenlemelerde belirtilen amaç ve görevleri yerine getirmek üzere ABİHA'nın Üçüncü Kısmının V. Başlığının 4. Bölümü veya 5. Bölümü kapsamına giren faaliyetleri yürütürken işlenen tüm kişisel veriler anlamına gelir." EUDPR madde 3(2).

[443] VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, 2022, s.29.

[444] EUDPR madde 2(3).

[445] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, s.53–114.

[446] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, PE/8/2022/REV/1, OJ L 169, 27.6.2022, s.1–42.

[447] DIMITROVA, DIANA ve DE HERT, PAUL, "The Right of Access Under the Police Directive: Small Steps Forward", MEDINA, MANEL *et.al.*, *Privacy Technologies and Policy*, Springer International Publishing, Switzerland, 2018, s.125.

Kolluk Direktifi'nin kapsamına ilişkin yapılması gereken son bir açıklama bulunmaktadır. Kolluk Direktifi'nin kapsamında her ne kadar kovuşturma çerçevesinde işlenen kişisel veriler yer alsa da kişisel verilerin bir ceza soruşturması ve cezai konulardaki mahkeme işlemleri sırasında işlendiği hallerde, üye devletler bilgi edinme, erişim ve kişisel verilerin düzeltilmesi veya silinmesi haklarının ulusal hukuklarına uygun olarak kullanılmasını sağlayabilecektir.[448]

4.3 Veri Koruma İlkeleri

ABTHŞ ile ayrı bir temel hak olarak düzenlenen kişisel verilerin koruması hakkının temel yönlerini dikkate alan Kolluk Direktifi'nin ikinci bölümü, kişisel verilerin işlenmesine yönelik bir dizi genel veri koruma ilkesini ortaya koymaktadır.[449] Kolluk Direktifi'nin ortaya koyduğu veri koruma ilkeleri, başta GDPR olmak üzere, diğer veri koruma belgelerine benzemekle birlikte, CKKAİ alanında kişisel verilerin işlenmesinin kendine özgü yapısı ve ihtiyaçları göz önünde bulundurularak formüle edilmiştir.[450] Örneğin, "amaç sınırlaması" ve "veri minimizasyonu" ilkeleri GDPR'den farklı bir şekilde formüle edilirken, Kolluk Direktifi, aynı zamanda saklama süresi sınırlamalarının yanı sıra farklı veri sahibi ve veri kategorileri arasındaki ayrıma ilişkin özel hükümler de getirmektedir. Veri kalitesi ilkesinin uyarlanması, kolluk kuvvetleri ve adli makamların özel ihtiyaçlarını karşılamayı ve yalnızca kişisel verilerin korunmasına değil, aynı zamanda yasal sürece de saygı gösterilmesini sağlamayı amaçlamaktadır. Açıkçası, Kolluk Direktifi, kişisel verilerin korunması ile kolluk ve ceza adaleti sürecinin çıkarları arasında bir denge kurmak için yoğun bir çaba

[448] Kolluk Direktifi madde 18 ve dibace (20), (49) ve (107). BOSTANCI BOZBAYINDIR, GÜLŞAH, (2018), s.74; MASEA, COSTANZA DI FRANCESCO, (2016), s.7.
[449] MARQUENIE, THOMAS, (2017), s.330; BOSTANCI BOZBAYINDIR, GÜLŞAH, (2018), s.75.
[450] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2016), s.11.

göstermiştir.[451] Bununla birlikte bazı akademisyenler tarafından, Kolluk Direktifi'nde yer alan veri koruma ilkelerinin, kolluk kuvvetleri için kişisel verilerin korunmasına ilişkin temel belge olan, R (87) 15 sayılı Tavsiye Kararından daha esnek ve daha düşük bir koruma seviyesine sahip olduğu belirtilmiş ve bu durumun kolluk kuvvetleri için yükümlülüklerini gevşetme isteğinin bir yansıması olduğu vurgulanmıştır.[452]

4.3.1 Kişisel Verilerin İşlenmesine İlişkin İlkeler

Kolluk Direktifi, GDPR[453] ile paralel olacak şekilde kişisel verilerin işlenmesine ilişkin ilkeleri düzenlemekle birlikte kolluk ve ceza adaletinin kendine özgü yapısı gereği bazı ilkeleri içerisinde barındırmamakta ya da farklı bir şekilde düzenlemektedir. Kolluk Direktifi kapsamında kişisel veriler; "hukuka uygun ve adil bir şekilde işlenmeli"[454] (hukuka uygunluk ve adillik); "belirli, açık ve meşru amaçlar için toplanmalı" ve "bu amaçlarla uyumlu olmayan bir şekilde işlenmemeli"[455] (amaç sınırlaması); "işlendikleri amaçlarla bağlantılı olarak yeterli, ilgili ve aşırı olmamalı"[456] (veri minimizasyonu); "doğru olmalı ve gerektiğinde güncellenmeli, işlenme amaçları göz önünde bulundurulduğunda yanlış olanlar gecikmeksizin silinmeli veya düzeltilmesini sağlamak için her türlü makul adım atılmalı"[457] (doğruluk); "işlendikleri amaçlar için gerekli olandan daha uzun süre boyunca veri sahiplerinin tanımlanmasına izin verecek bir biçimde tutulmalı"[458] (depolama sınırlaması); "uygun teknik veya organizasyonel önlemler kullanılarak yetkisiz veya yasa dışı işlemeye

[451] VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, 2022, s.32.
[452] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2016), s.12; MARQUENIE, THOMAS, (2017), s.331; VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, 2022, s.33; CARUANA, MIREILLE M., (2017), s.20.
[453] GDPR madde 5.
[454] Kolluk Direktifi madde 4(1)(a).
[455] Kolluk Direktifi madde 4(1)(b).
[456] Kolluk Direktifi madde 4(1)(c).
[457] Kolluk Direktifi madde 4(1)(d).
[458] Kolluk Direktifi madde 4(1)(e).

karşı ve kazara kayıp, imha veya hasara karşı koruma dâhil olmak üzere uygun güvenlik sağlanacak şekilde işlenmelidir"[459] (uygun güvenlik). Kolluk Direktifi çerçevesinde kişisel veriler, toplandığı amaç dışında, aynı veya başka bir kontrolör tarafından, Kolluk Direktifi madde 1(1)'de belirtilen amaçlardan herhangi biri için "kontrolörün AB veya üye devlet hukuku uyarınca söz konusu kişisel verileri bu tür bir amaçla işleme yetkisine sahip olması" ve "AB veya üye devlet hukuku uyarınca işleme faaliyetinin gerekli ve söz konusu diğer amaçla orantılı olması" halinde işlenebilir.[460]

Kolluk Direktifi tarafından ortaya konan veri koruma ilkelerinin, GDPR'deki karşılıklarından farklılık gösterdiği önemli alanlardan biri, Kolluk Direktifi'nin 4'üncü maddesinde açıkça yer verilmeyen şeffaflık ilkesidir.[461] Şeffaflık ilkesinin aynen uygulanmasının CKKAİ alanının kendine özgü yapısı ile uyuşmayacağı izahtan varestedir. Bu alanda tam bir şeffaflık her zaman gerçekçi olmayabilir, çünkü gizlilik içerisinde yürütülmesi gereken cezai soruşturmalara müdahale edilebilir, suçların önlenmesi veya ortaya çıkarılması için kolluk tarafından yürütülen gizli operasyonlar ifşa edilebilir, başta terörle mücadele ve organize suçlarla mücadele anlamında kamu güvenliğinin korunması sekteye uğrayabilir. Bu nedenlerle ceza hukukunun ihtiyaçları şeffaflık ilkesinin esnek uygulanması zorunluluğunu ortaya koymaktadır.[462] Ancak, şeffaflık ilkesinin tamamen metinden çıkarılmış olması, bu ilkenin Kolluk Direktifi kapsamında hiç uygulanmayacağı anlamına gelmemektedir. Kolluk Direktifi'nin dibacesinde kişisel verilerin hukuka uygun ve adil bir şekilde işlenirken aynı zamanda şeffaf olunması gerektiği, ancak bu durumun kolluk

[459] Kolluk Direktifi madde 4(1)(f).
[460] Kolluk Direktifi madde 4(2).
[461] VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, 2022, s.33.
[462] LEISER, MARK ve CUSTERS, BART, "The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680", European Data Protection Law Review, Cilt:5, Sayı:3, 2019, s.371.

kuvvetlerinin gizli soruşturmalar veya video gözetimi gibi faaliyetler yürütmesini engellemeyeceği vurgulanmaktadır.[463] Madde 29 Çalışma Grubu, şeffaflığın Kolluk Direktifi'nin 3'üncü bölümü kapsamındaki veri sahibi hakları aracılığıyla desteklendiğini ifade etmektedir.[464] Bununla birlikte, Kolluk Direktifi'nin metninde şeffaflık ilkesinin yer almamasının veri sahiplerinin bilgi edinme haklarının daha zayıf olmasına neden olduğu ileri sürülmüştür.[465]

Kolluk Direktifi'nin düzenlendiği veri koruma ilkelerinden en çok tartışılanı "amaç sınırlaması" ilkesi[466] olmuştur. Amaç sınırlaması ilkesi iki temel kavramdan oluşmaktadır; bunlar "amaç belirleme" (kişisel verilerin belirli, açık ve meşru amaçlar için toplanması) ve "uyumlu kullanım" (daha ileri işlemenin kişisel verilerin toplanma amaçlarıyla uyumsuz olmaması) kavramlarıdır.[467] Komisyon Uzman Grubu'nun on beşinci toplantı tutanaklarında; Kolluk Direktifi madde 1(1) kapsamındaki amaçların genel bir şekilde tanımlandığı, ancak amaçların ise "her bir işleme faaliyetinin arkasında ne olduğunu ve belirli bir işleme faaliyetinin neden gerçekleştirildiğini açıkça ortaya koymak amacıyla, örneğin: bir kişinin biyometrik verilerinin soruşturma amacıyla bir suçun şüphelisi olarak kullanılması suretiyle kimliğinin tespit edilmesi gibi" özel olarak tanımlanması gerektiği belirtilmiştir.[468] AB veri koruma organları ayrıca, her bir işleme amacının ayrıntılı olması gerektiğine, zira "kolluk

[463] Kolluk Direktifi, Dibace (26).
[464] Article 29 Data Protection Working Party, "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)", WP258, 29 Kasım 2017, s.16.
[465] DRECHSLER, LAURA, "Comparing LED and GDPR Adequacy: One Standard Two Systems", Global Privacy Law Review, Cilt:1, Sayı:2, 2020, s.100.
[466] Amaç sınırlaması ilkesi ile ilgili ayrıntılı bilgi için bkz. KONING, MEREL ELIZE, *The purpose and limitations of purpose limitation*, Yayımlanmamış Doktora Tezi, Radboud University Nijmegen, Utrecht, Netherlands, 2020, s.57-88; Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation", WP203, 2 Nisan 2013.
[467] Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation", WP203, 2 Nisan 2013, s.11.
[468] Minutes of the fifteenth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 20 Şubat 2018.

kuvvetlerinin tek başına belirli, açık ve meşru bir amaç olarak değerlendirilemeyeceğine"[469] ve aynı alana ait oldukları için iki kolluk kuvvetinin fiilen uyumlu kabul edilmemesi gerektiğine işaret etmiştir.[470] Kolluk Direktifi'nde belirtilen "amaç sınırlaması" ilkesi kimi akademisyenler tarafından "veri sahibinin haklarını yeterli bir şekilde korumadığı" ve "birincil hukukta yer alan (ABTHŞ madde 8) amaç sınırlaması ilkesinden uzaklaştığı" gerekçeleriyle eleştirilmiş[471], kimi akademisyenler tarafından ise "daha esnek ve daha koruyucu" bir çerçeve sağladığı için yeterli olduğu ifade edilmiştir.[472]

Kolluk Direktifi'nin ortaya koyduğu "amaç sınırlaması" ilkesine ilişkin ABAD'ın *Inspektor v Inspektorata kam Visshia sadeben savet* kararında[473], Kolluk Direktifi madde 1(1)'in lafzının, madde 4(2) ile birlikte okunduğunda, kişisel verilerin bir suçun "tespiti" ve "soruşturulması" amacıyla toplandığı ve daha sonra "kovuşturma" amacıyla işlendiği durumlarda, bu toplama ve işlemenin farklı amaçlara hizmet ettiği sonucu çıkarılabileceğini ifade etmiştir.[474] Kolluk Direktifi'nin 6'ncı maddesinde belirtilen veri sahibi kategorilerinin Kolluk Direktifi'nin kapsamına giren kişisel verilerin işlenme amacına etkisi olmadığı belirtilmiştir.[475] Kolluk Direktifi madde 4(2)(a) ve (b)'de atıfta bulunulan gerekliliklerin

[469] Article 29 Data Protection Working Party, "Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", WP233, 01 Aralık 2015, s.6.
[470] European Data Protection Supervisor, "Opinion on the Data Protection Reform Package", 12 Mart 2012, s.53-54.
[471] JASSERAND, CATHERINE, "Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in Directive 2016/680?", Computer Law & Security Review: The International Journal of Technology Law and Practice, Cilt:34, Sayı:1, 2017, 154-165; JASSERAND, CATHERINE, "Subsequent use of GDPR data for a law enforcement purpose: the forgotten principle of purpose limitation?" European Data Protection Law Review, Cilt:4, Sayı:2, 2018, s.152-167; CARUANA, MIREILLE M., (2017), s.1-22.
[472] DE HERT, PAUL ve SAJFERT, JURAJ, "The Fundamental Right to Personal Data Protection In Criminal Investigations and Proceedings: Framing Big Data Policing Through the Purpose Limitation and Data Minimisation Principles of the Directive (EU) 2016/680", Brussels Privacy Hub Working Paper, Cilt:7, Sayı:31, 2021, s.5.
[473] Case C-180/21, *Inspektor v Inspektorata kam Visshia sadeben savet*, [2022], ECLI:EU:C:2022:967.
[474] Case C-180/21, *Inspektor v Inspektorata kam Visshia sadeben savet*, para 44.
[475] Case C-180/21, *Inspektor v Inspektorata kam Visshia sadeben savet*, paras 47-49.

karşılanması için, kişisel verilerin aynı veya başka bir kontrolör tarafından, bu verilerin toplandığı amaç dışında Kolluk Direktifi madde 1(1)'de belirtilen amaçlardan biri için işlenmesinde bu gerekliliklere uygunluğun değerlendirilmesinin, Kolluk Direktifi madde 1(1)'de atıfta bulunulan amaçların her birinin spesifik ve farklı olarak ele alınması suretiyle gerçekleştirilmesi gerektiği sonucuna varılmıştır.[476] Böylece cezai suçların "önlenmesi", "tespiti" veya "soruşturulması" amacıyla toplanan kişisel verilerin daha sonra, farklı yetkili makamlar tarafından "kovuşturma" veya "cezaların infazı" amacıyla işlenebileceği ortaya konulmuştur.[477] Kolluk Direktifi'nin 4(2) maddesi, Kolluk Direktifi'nin 4(1)(b) maddesinde ortaya konan "amaç sınırlaması" ilkesi kapsamında uyumlu veya uyumsuz amaçların neler olduğunu açıklığa kavuşturmaksızın, müteakip işlemenin koşullarını belirleme görevini üye devletlere bırakmakta ve bu durum üye devletlere geniş bir takdir yetkisi tanınması nedeniyle belirsizliğe yol açacağı ifade edilmektedir.[478]

"Veri minimizasyonu" ilkesinin düzenlendiği Kolluk Direktifi maddde 4(1)(c), kişisel verilerin "yeterli, ilgili ve aşırı olmayan" şekilde işlenmesini öngörmektedir. Bu ifade, GDPR madde 5(1)(c)'de yer alan "yeterli, ilgili ve gerekli olanla sınırlı" ibaresinden farklıdır. Söz konusu farklılık, CKKAİ alanının kendine özgü yapısının bir yansıması olup, özellikle soruşturma gibi hangi verilerin gerekli olduğunun başlangıçta net olmayabileceği cezai prosedürlerde, daha fazla esneklik sağlama ihtiyacının bir sonucudur.[479] Ancak uygulamada, hangi verilerin "aşırı" sayılacağı ile hangilerinin "gerekli olanla sınırlı" kabul edileceği arasındaki sınır her zaman net değildir. Bu durum, veri minimizasyonu ilkesinin esnek

[476] Case C-180/21, *Inspektor v Inspektorata kam Visshia sadeben savet*, para 56.
[477] Case C-180/21, *Inspektor v Inspektorata kam Visshia sadeben savet*, paras 51-52.
[478] VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, 2022, s.36.
[479] SAJFERT, JURAJ ve QUINTEL, TERESA, (2017), s.3.

yorumlarının suistimal riskini artırabileceği endişesini doğurmaktadır.[480] Nitekim Madde 29 Çalışma Grubu'nun Kolluk Direktifi'nin taslağına ilişkin vermiş olduğu görüşünde, veri minimizasyonu ilkesini "belirlenen amaca ulaşmak için yalnızca asgari miktarda kişisel verinin işlenmesi gerektiği" ifadesiyle savunmuştur.[481] Veri minimizasyonu ilkesine ilişkin ABAD'a yapılan bir ön karar başvurusuna ilişkin görüşünde Hukuk Sözcüsü Pitruzella, veri minimizasyonu ilkesini, verilerin işleme amacı için gerekli olan süreden daha fazla tutulmaması ve yalnızca işleme amacının makul bir şekilde başka yollarla yerine getirilememesi halinde tutulması şeklinde ifade etmiştir.[482]

4.3.2 Depolama ve İnceleme İçin Zaman Sınırları

Kolluk Direktifi kapsamında "üye devletler, kişisel verilerin silinmesi veya kişisel verilerin saklanması ihtiyacının periyodik olarak gözden geçirilmesi için uygun zaman sınırlarının belirlenmesini sağlamalıdır."[483] Bu madde, Kolluk Direktifi madde 4(1)(e)'deki depolama sınırlaması ilkesini güçlendiren, depolama için süre sınırlamalarına ve depolama ihtiyacının periyodik olarak gözden geçirilmesine ilişkin özel hükümdür.[484] Madde 29 Çalışma Grubu'na göre, Kolluk Direktifi'nin 5'inci maddesini iç hukuka aktaran ulusal kanunlar, kişisel verilerin daha fazla saklanmasının gerekliliğinin değerlendirilmesine yönelik açık ve şeffaf kriterlerin yanı sıra veri koruma görevlisinin katılımı da dâhil olmak üzere usule ilişkin gereklilikleri belirlemeli ve kontrolörün daha fazla işlemenin gerekli olup olmadığına ilişkin periyodik bir inceleme yapmaması halinde, veriler otomatik olarak

[480] VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, 2022, s.37.
[481] Article 29 Data Protection Working Party, "Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", WP233, 01 Aralık 2015, s.7.
[482] Opinion of Advocate General Pitruzzella of 30 June 2022, *Ministerstvo na vatreshnite raboti*, C-205/21, ECLI:EU:C:2022:507, paras 54-55.
[483] Kolluk Direktifi madde 5.
[484] VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, 2022, s.38.

silinmeli veya anonimleştirilmelidir.[485] Komisyon'un Kolluk Direktifi'ne ilişkin ilk raporunda, Kolluk Direktifi'ni iç hukuka aktaran ulusal veri koruma kanunlarının çoğunluğunun yalnızca 5'inci maddenin genel gerekliliklerini karşıladığını ve bu durumun kişisel verilerin silinmesi veya kişisel verilerin saklanması ihtiyacının periyodik olarak gözden geçirilmesi için zaman sınırlarının veri koruma kanunları yerine sektörel kanunlarca belirleneceği anlamına geleceğini belirtmiştir.[486] ABAD yakın zamanda vermiş olduğu *Direktor na Glavna direktsia "Natsionalna politsia" pri MVR – Sofia* kararında[487] kasıtlı bir suçtan kesinleşmiş mahkûmiyeti bulunan kişilere ait biyometrik ve genetik veriler dâhil olmak üzere kişisel verilerin, kolluk makamları tarafından, suçların önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması ya da cezaların infazı amacıyla, ilgili kişinin ölümüne kadar, hatta o kişinin hukuken itibarının iade edilmiş olması hâlinde dahi saklanmasını öngören ve veri sorumlusuna bu verilerin saklanmasının hâlâ gerekli olup olmadığını periyodik olarak gözden geçirme yükümlülüğünü getirmeyen ya da ilgili kişiye, söz konusu verilerin işlendiği amaçlar açısından artık gerekli olmaması hâlinde bu verilerin silinmesini ya da uygun hâllerde işlenmesinin sınırlandırılmasını talep etme hakkı tanımayan ulusal mevzuatın Kolluk Direktifi ile bağdaşmadığına hükmetmiştir.[488]

4.3.3 Veri Kategorizasyonu ve Kişisel Veri ile Kişisel Verinin Niteliğinin Doğrulanması Arasındaki Ayrım

Kolluk Direktifi'nin 6'ncı maddesi ile üye devletlere "uygulanabilir olduğu hallerde ve mümkün olduğu ölçüde", kontrolörün "şüpheli, hükümlü, mağdur ve tanık gibi" farklı

[485] Article 29 Data Protection Working Party, "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)", WP258, 29 Kasım 2017, s.4.
[486] "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", s.13.
[487] Case C-118/22, *Direktor na Glavna direktsia "Natsionalna politsia" pri MVR – Sofia*, [2024] ECLI:EU:C:2024:97.
[488] Case C-118/22, *Direktor na Glavna direktsia "Natsionalna politsia" pri MVR – Sofia*, para 73.

kategorilerdeki veri sahiplerinin kişisel verileri arasında net bir ayrım yapması yükümlülüğü getirilmiştir. Madde metinde "gibi" ifadesinin kullanılmış olması maddede düzenlenen veri kategorilerinin sınırlı olmayıp üye devletlerce farklı kategorilerin belirlenmesine izin verdiği anlamında gelmektedir. Bu netlik eksikliği veri sahiplerinin hakları açısından tehlikeli ya da daha az koruyucu olabilir.[489] Kolluk Direktifi'nin dibacesinde, Kolluk Direktifi'nin 6'ncı maddesinin, ABAD ve AİHM içtihat hukukunda yorumlandığı üzere, ABTHŞ ve AİHS tarafından güvence altına alınan masumiyet karinesinin uygulanmasını engellememesi gerektiği vurgulanmaktadır.[490] Ancak özellikle soruşturma ve kovuşturma kapsamında kişilerin süreç boyunca sıfatları değişebileceğinden (örneğin kişi mağdurken fail olabilir) Kolluk Direktifi'nin bu hükmünün statik yapısının sorunlara yol açabileceği değerlendirilmektedir.[491]

Veri kalitesi ve doğruluğu, CKKAİ alanında kişisel verilerin işlenmesi bağlamında büyük önem taşımaktadır. Kolluk Direktifi'nin 7'inci maddesi, GDPR'de bulunmayan ek bir gereklilik getirmektedir.[492] Bu kapsamda "üye devletler gerçeklere dayanan kişisel verilerin kişisel değerlendirmelere dayanan kişisel verilerden ayırt edilmesini sağlamalıdır."[493] Ayrıca, "üye devletler, yetkili makamların yanlış, eksik veya artık güncel olmayan kişisel verilerin iletilmemesini veya kullanıma sunulmamasını sağlamak için tüm makul adımların atılmasını sağlamalı" ve "bu amaçla, yetkili makamlar, mümkün olduğu ölçüde, kişisel

[489] COCQ, CELINE C., "EU Data Protection Rules Applying to Law Enforcement Activities: Towards an Harmonised Legal Framework?", New Journal of European Criminal Law, Cilt:7, Sayı:3, 2016, s.267.
[490] Kolluk Direktifi, Dibace (31).
[491] LEISER, MARK ve CUSTERS, BART, (2019), s.375.
[492] Kolluk Direktifi madde 7. Bu madde hakkında ayrıntılı bilgi için bkz. TZANOU, MARIA, "Distinction between personal data and verification of quality of personal data", KOSTA, ELENI ve BOEHM, FRANZİSKA (Eds), *The EU Law Enforcement Directive (LED): A Commentary*, Oxford University Press, Oxford, 2024, s.181-192.
[493] Kolluk Direktifi madde 7(1).

verilerin kalitesini iletilmeden veya kullanıma sunulmadan önce doğrulamalıdır."[494] "Yanlış kişisel verilerin iletildiği veya kişisel verilerin hukuka aykırı olarak iletildiği ortaya çıkarsa, alıcı gecikmeksizin bilgilendirilir" ve "böyle bir durumda, kişisel veriler düzeltilir veya silinir ya da işleme kısıtlanır."[495]

4.3.4 Kişisel Veri İşlemenin Yasallığı ile Özel İşleme Koşulları

Kolluk Direktifi'nin 8'inci maddesinde düzenlenen hukuka uygunluk ilkesi, diğer tüm veri işleme ilkelerini kapsayan ve oluşturan ana ilke olarak görülmektedir.[496] Kolluk Direktifi çerçevesinde kişisel verilerin işlenme faaliyetinin hukuka uygun olabilmesi için Kolluk Direktifi madde 1(1)'de belirtilen amaçlar doğrultusunda yetkili bir makam tarafından yürütülen bir görevin yerine getirilmesi için gerekli olması ve en azından işleme faaliyetinin amaçlarını, işlenecek kişisel verileri ve işleme faaliyetinin amaçlarını belirten AB ya da üye devlet hukukuna dayanması gerekmektedir.[497] Ayrıca Kolluk Direktifi'nin 9'uncu maddesi amaç sınırlaması ilkesinin bir tezahürünü teşkil etmekte ve Kolluk Direktifi'nin maddi veya kişisel kapsamı dışında kalan kişisel veri işleme faaliyetlerine GDPR'nin uygulanacağı düzenlenmektedir.[498] Görüldüğü üzere temel hukuka uygunluk ve amaç sınırlaması ilkelerini detaylandıran bu hükümler, işleme faaliyetlerinin, işlenecek verilerin yanı sıra işleme hedef ve amaçlarını da belirten bir yasayla belirlenen yetkili makamların görevlerinin yerine getirilmesi için gerekli olmasını özellikle

[494] Kolluk Direktifi madde 7(2).
[495] Kolluk Direktifi madde 7(3).
[496] TZANOU, MARIA, "Lawfulness of processing", KOSTA, ELENI ve BOEHM, FRANZİSKA (Eds), *The EU Law Enforcement Directive (LED): A Commentary*, Oxford University Press, Oxford, 2024, s.195.
[497] Kolluk Direktifi madde 8. Bu madde hakkında ayrıntılı bilgi için bkz. TZANOU, MARIA, (2024), s.193-206.
[498] Kolluk Direktifi madde 9. Bu madde hakkında ayrıntılı bilgi için bkz. TZANOU, MARIA, "Specific processing conditions", KOSTA, ELENI ve BOEHM, FRANZİSKA (Eds), *The EU Law Enforcement Directive (LED): A Commentary*, Oxford University Press, Oxford, 2024, s.207-216.

gerektirmektedir.[499] Bu husus Komisyon'un Kolluk Direktifi'ne ilişkin ilk raporunda da öncellikle "Kolluk Direktifi'ni iç hukuka aktaran bazı ulusal veri koruma kanunlarının, işlenecek kişisel verilerin ve işleme amaçlarının kanunda belirtilmesi gerekliliğini yansıtmadığını ve diğer ulusal veri koruma kanunlarının Kolluk Direktifi 8'inci maddeye karşılık gelen tüm hükümleri içermediği" eleştirisinden sonra "ulusal mevzuatta yalnızca Kolluk Direktifi'nin 8'inci maddesinin genel gerekliliklerinin tekrarlanması, belirli bir işleme faaliyeti için yeterli bir yasal dayanak olarak değerlendirilemez: ulusal mevzuat, kişisel verileri işlemeye hangi makamın yetkili olduğunu, söz konusu işlemeyi haklı kılan kamu görevlerini ve işlemenin amacını belirtmelidir" şeklinde ifade edilmiştir.[500]

ABAD *WS v Bundesrepublik Deutschland* kararında[501] Interpol tarafından bir Alman vatandaşı hakkında yayınlanan kırmızı bültenin "*ne bis in idem*" ilkesinin uygulanması bağlamında Kolluk Direktifi'nin 8'inci maddesi kapsamında hukuka uygun olup olmadığını değerlendirmek zorunda kalmıştır. ABAD, AB hukukunun, bir sözleşmeci devlette veya bir üye devlette alınan nihai bir yargı kararıyla söz konusu bildirimin dayandığı eylemler bakımından "*ne bis in idem*" ilkesinin geçerli olduğunun tespit edilmediği durumlarda, söz konusu işlemenin Kolluk Direktifi tarafından belirlenen koşulları karşılaması, özellikle de Kolluk Direktifi madde 8(1) anlamında yetkili bir makam tarafından yürütülen bir görevin yerine getirilmesi için gerekli olması kaydıyla, Interpol tarafından yayınlanan bir kırmızı bültende yer alan kişisel verilerin işlenmesini engellemediğine karar vermiştir.[502] Kolluk Direktifi'nin 9'uncu maddesi ile ilgili ABAD, *Inspektor v Inspektorata kam Visshia sadeben*

[499] BOSTANCI BOZBAYINDIR, GÜLŞAH, (2018), s.76; MARQUENIE, THOMAS, (2017), s.330.
[500] "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", s.14.
[501] Case C-505/19, *WS v Bundesrepublik Deutschland*, [2021], ECLI:EU:C:2021:376.
[502] Case C-505/19, *WS v Bundesrepublik Deutschland*, para 121.

savet kararında[503], bir ceza davası kapsamında savcılık makamı tarafından Kolluk Direktifi çerçevesinde işlenen kişisel verilerin devlete karşı açılan bir tazminat davasında kullanması durumunda söz konusu kişisel veri işleme faaliyetinin Kolluk Direktifi madde 1(1) kapsamında olmaması nedeniyle GDPR'ın uygulanması gerektiğini ifade etmiştir.[504]

Kolluk Direktifi, GDPR'dan farklı olarak[505], madde 8'de belirtilen şekliyle, kişisel verilerin işlenmesi için yalnızca bir yasal dayanak içermektedir. CKKAİ alanının doğası gereği "veri sahibinin rızası" kişisel verilerin işlenmesi için yasal dayanak olarak sayılmamıştır. Başka bir deyişle, Kolluk Direktifi kapsamında kişisel verilerin işlenmesi için rıza gerekli değildir. Bu durum, özellikle verilerinin işlenmesine rıza göstermek istemeyebilecek olan ceza hukuku öznelerinden şüpheli ve sanıklar için anlamlıdır; ancak bu tür bir veri işlemenin kolluk kuvvetlerinin işlerini yapmaları için gerekli olduğu açıktır.[506] Kolluk Direktifi'nin dibacesinde veri sahibinin rızasının yasal dayanak olarak Kolluk Direktifi'nde yer almamasının nedeni şu ifadelerle açıklanmaktadır.[507]

> "*Yasa tarafından yetkili makamlara kurumsal olarak verilen cezai suçları önleme, soruşturma, tespit etme veya kovuşturma görevlerinin yerine getirilmesi, gerçek kişilerden yapılan taleplere uymalarını istemelerine veya emretmelerine izin verir. Böyle bir durumda, GDPR'de tanımlandığı üzere, veri sahibinin rızası, kişisel verilerin yetkili makamlar tarafından işlenmesi için yasal bir zemin oluşturmamalıdır. Veri sahibinin yasal bir yükümlülüğe uymasının gerekli olduğu*

[503] Case C-180/21, *Inspektor v Inspektorata kam Visshia sadeben savet*, [2022], ECLI:EU:C:2022:967.
[504] Case C-180/21, *Inspektor v Inspektorata kam Visshia sadeben savet*, [2022], ECLI:EU:C:2022:967, para 97.
[505] GDPR madde 6.
[506] LEISER, MARK ve CUSTERS, BART, (2019), s.374.
[507] Kolluk Direktifi, dibace (35).

durumlarda, veri sahibinin gerçek ve özgür bir seçimi yoktur, bu nedenle veri sahibinin tepkisi, isteklerinin özgürce verilmiş bir göstergesi olarak kabul edilemez."

4.3.5 Özel Nitelikli Kişisel Verilerin İşlenmesi

Kolluk Direktifi'nin 10'uncu maddesi kapsamında özel nitelikli kişisel verilerin[508] işlenmesine yalnızca "kesinlikle gerekli olduğu durumlarda", "veri sahibinin hakları ve özgürlükleri için uygun güvencelere tabi olarak" ve şu üç durumdan birinin gerçekleşmesi halinde izin verilecektir: "AB veya üye devlet hukuku tarafından yetkilendirildiği hallerde", "veri sahibinin veya başka bir gerçek kişinin hayati çıkarlarını korumak için" veya "söz konusu işleme faaliyetinin veri sahibi tarafından açıkça kamuya açıklanan verilerle ilgili olduğu durumlarda." Kolluk Direktifi'nin 10'uncu maddesi, GDPR'nin 9'uncu maddesi ve EUDPR'nin 10'uncu maddesi ile aynı özel nitelikli kişisel veri listesini tekrarlamaktadır. Ancak Kolluk Direktifi'nce ortaya konan rejim, özel nitelikli kişisel verilerin işlenmesini kural olarak yasaklamadığı için, özel nitelikli kişisel verilerin işlenmesinin kural olarak yasaklandığı ve bazı istisnai durumlarda işlenmesine izin verildiği GDPR ve EUDPR'den farklıdır.[509] Kolluk Direktifi tarafından özel nitelikli kişisel verilerin işlenmesi her ne kadar yasaklanmamış olsa da bu verilerin işlenmesine ancak kesinlikle gerekli olduğu durumlarda ve veri sahiplerinin hak ve özgürlükleri için uygun güvencelere tabi olması şartıyla izin verilmiştir. Aslında Kolluk Direktifi'nin 10'uncu maddesi ile kişisel verileri işlemenin hukuka uygunluğunu ortaya koyan 8'inci maddesinde belirtilen gerekliliklerin yanına özel nitelikli kişisel veriler için iki önemli gereklilik eklenmiştir.[510] Kolluk Direktifi'nin

[508] Kolluk Direktifi kapsamında özel nitelikli kişisel veri: Kişilerin ırkı veya etnik kökeni, siyasi görüşleri, dini veya felsefi inançları, sendika üyeliği, genetik verileri, biyometrik verileri, sağlıkla ilgili verileri veya cinsel yaşamı veya cinsel yönelimi ile ilgili veriler.
[509] JASSERAND, CATHERINE, "Processing of special categories of personel data", KOSTA, ELENI ve BOEHM, FRANZISKA (Eds), *The EU Law Enforcement Directive (LED): A Commentary*, Oxford University Press, Oxford, 2024, s.220.
[510] SAJFERT, JURAJ ve QUINTEL, TERESA, (2017), s.6.

dibacesinde özel nitelikli kişisel veriler için "doğası gereği temel hak ve özgürlükler bakımından özellikle hassas olan kişisel veriler, işlenmeleri bağlamında temel hak ve özgürlükler bakımından önemli riskler yaratabileceğinden özel korumayı hak etmektedir" denilerek Kolluk Direktifi'nin 10'uncu maddesindeki ilave gerekliliklerin gerekçesi ortaya konulmaya çalışılmıştır.[511]

Komisyon Uzman Grubu'nun dokuzuncu toplantısında, üye devletlerden gelen sorulara cevaben, "madde 8 ve 10 arasındaki ilişkinin, özel kategorilerdeki verilerin işlenmesinin her zaman yasayla öngörülmesi gerektiği anlamına geldiğini ve buna ek olarak, yalnızca kesinlikle gerekli olduğunda ve yine yasada belirtilen uygun güvencelere tabi olduğunda izin verildiğini" açıklamıştır.[512] Benzer yaklaşım Madde 29 Çalışma Grubu tarafından da ifade edilmiştir.[513] Komisyon'un Kolluk Direktifi'ne ilişkin ilk raporunda, üye devletlerin çoğunun, özel nitelikli kişisel verilerin işlenmesi için bir ön koşul olarak "kesin gereklilik" şartını aradığını ve üye devletlerin çoğu tarafından Kolluk Direktifi madde 10 (a)-(c) kapsamındaki yasal işleme gerekçelerinin benimsendiğini ifade edilmiştir. Ayrıca bazı üye devletler tarafından bu gerekçelere ilaveten, "kişilerin hayatını, fiziksel bütünlüğünü veya mal varlığını doğrudan tehdit eden bir tehlikeyi önlemek veya bertaraf etmek" gibi gerekçeler öngörüldüğünü belirtilmiştir.[514] ABAD, kolluk kaydı oluşturmak için kasten işlenen bir suçun failinin fotoğraf, parmak izi ve DNA örneklerinin toplanması ve işlenmesiyle ilgili, *Ministerstvo na vatreshnite raboti* kararında[515], yetkili makamın,

[511] Kolluk Direktifi, dibace (37).
[512] Minutes of the ninth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 4 Mayıs 2017.
[513] Article 29 Data Protection Working Party, "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)", WP258, 29 Kasım 2017, s.7.
[514] "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", s.14.
[515] Case C-205/21, *Ministerstvo na vatreshnite raboti*, [2023], ECLI:EU:C:2023:49.

biyometrik ve genetik verilerin toplanmasının öncelikle güdülen belirli amaçlara ulaşmak için kesinlikle gerekli olduğunu ve ikinci olarak bu amaçlara, ilgili kişinin hak ve özgürlüklerine daha az müdahale eden tedbirlerle ulaşılamayacağını doğrulaması ve ortaya koyması yükümlülüğünü öngörmeyen, kasıtlı bir suçla itham edilen herkesin biyometrik ve genetik verilerinin sistematik olarak toplanarak bir kayda geçirilmesini öngören ulusal mevzuatın Kolluk Direktifi'nin 10'uncu maddesi ile bağdaşmadığına hükmetmiştir.[516]

4.3.6 Otomatik Bireysel Karar Verme

Kolluk Direktifi, "AB veya üye devlet hukuku tarafından yetki verilmedikçe" ve "veri sahibinin hakları ve özgürlükleri için uygun güvenceler sağlamadıkça", "veri sahibi ile ilgili olumsuz bir yasal etki yaratan veya onu önemli ölçüde etkileyen profil çıkarma da dahil olmak üzere yalnızca otomatik işlemeye dayanan" kararları yasaklamakta[517] ve "veri sahibinin hak ve özgürlükleri ile meşru menfaatlerinin korunmasına yönelik uygun tedbirler mevcut olmadığı sürece" otomatik bireysel karar verme sürecinde özel nitelikli kişisel verilerin kullanılamayacağını hüküm altına almaktadır.[518] Ayrıca özel nitelikli kişisel verilerin işlenmesi sonucu veri sahibi için ayrımcılıkla sonuçlanabilecek profil çıkarma işleminin yasak olduğu düzenlenmektedir.[519]

GDPR'de otomatik bireysel karar almaya ilişkin çerçeve veri öznesinin haklarının bir parçası olarak öngörülürken[520], Kolluk Direktifi otomatik karar almayı veri koruma ilkeleri altında düzenlemektedir. GDPR'nin 22'inci maddesinde, veri sahiplerinin "kendileriyle ilgili hukuki sonuçlar doğuran veya benzer şekilde kendilerini önemli ölçüde etkileyen profil

[516] Case C-205/21, *Ministerstvo na vatreshnite raboti*, para 136.
[517] Kolluk Direktifi madde 11(1).
[518] Kolluk Direktifi madde 11(2).
[519] Kolluk Direktifi madde 11(3).
[520] GDPR madde 22.

oluşturma da dahil olmak üzere yalnızca otomatik işlemeye dayalı bir karara tabi olmama hakkına sahip olacakları" belirtirken, Kolluk Direktifi'nin 11'inci maddesi, "veri sahibiyle ilgili olumsuz bir hukuki etki doğurması veya kendisini önemli ölçüde etkilemesi" halinde bu tür bir işlemeyi yasaklamaktadır. CKKAİ alanında, istisnai durumlar hariç, otomatik bireysel karar alma yasağının getirilmesi memnuniyetle karşılanmış, ancak doktrinde Kolluk Direktifi'nin 11'inci maddesinin lafzının kâğıt üzerinde GDPR'deki muadiline göre daha sağlam ve koruyucu gibi görünse de özellikle kolluk tarafından kullanılan yöntemlerin teknolojik gelişmeler ışığında veri sahipleri için koruyucu bir çerçeve oluşturmadaki yeterliliği tartışılmıştır.[521]

Kolluk Direktifi'nin 11'inci maddesindeki otomatik bireysel karar vermeye ilişkin yasak, madde lafzından da açıkça anlaşıldığı üzere bireysel karar vermeye ilişkin bir düzenleme olup, toplu veya grup profillemeyi kapsamamaktadır. Bu durum, örneğin suçların hangi bölgelerde yoğunlaştığını tespit edilmesine ilişkin bir analizde, analize konu birey mi yoksa bir bölgede yaşayan grup mu olduğunu ayırt etmeyi zorlaştıran öngörücü kolluk teknolojileri de dâhil olmak üzere çeşitli alanlarda sorunlu olabileceği değerlendirilmektedir. Ayrıca, Kolluk Direktifi'nin 11'inci maddesi, "yalnızca otomatik araçlara dayalı karar verme" ile sınırlı olduğundan ve bir insan müdahalesi (örneğin hem manuel hem de otomatik araçlardan oluşan çok aşamalı karar alma süreçleri) olduğu durumlarda söz konusu madde uygulama alanı bulmayacağından, insan müdahalesinin kapsamının ve niteliğinin ne olduğunun Kolluk Direktifi'nde açık olmaması eleştiriye neden olmuştur.[522]

---

[521] SAJFERT, JURAJ ve QUINTEL, TERESA, (2017), s.8-12; VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, 2022, s.50-53; LYNSKEY, ORLA, "Criminal justice profiling and EU data protection law: precarious protection from predictive policing", International Journal of Law in Context, Cilt:15, Sayı:2, 2019, s.172-175.

[522] LYNSKEY, ORLA, (2019), s.174; SAJFERT, JURAJ ve QUINTEL, TERESA, (2017), s.8.

Sonuç olarak, veri sahiplerinin hak ve özgürlükleri için yüksek düzeyde koruma sağlamak, otomatik bireysel karar verme yetkisi veren AB ve ulusal yasalara ve burada öngörülen güvencelere bağlı olacaktır. Bu bağlamda, Madde 29 Çalışma Grubu ulusal yasa koyucuların kontrolörlere otomatik kararlarla bağlantılı olarak bir Veri Koruma Etki Değerlendirmesi (VKED) gerçekleştirme yükümlülüğü getirmesini tavsiye etmiştir.[523] Komisyon'un Kolluk Direktifi'ne ilişkin ilk raporunda belirtildiği üzere, tüm üye devletlerin Kolluk Direktifi'nin 11'inci maddesini iç hukuka aktaran yasaları, yasayla öngörülmediği sürece yalnızca otomatik işlemeye dayalı bir kararı yasaklayan hükümler içermekte ve ayrımcılıkla sonuçlanan profillemeyi de yasaklamaktadır. Raporda, çoğu üye devletin uyum yasalarının, uygun güvenceler sağlanmadığı sürece bu tür kararların özel kategorilerdeki kişisel verilere dayanmamasını gerekliliğini düzenlediği, ancak bazı üye devlet yasalarının, otomatik karar vermenin yasayla yetkilendirildiği durumlarda veri sahibinin hak ve özgürlükleri için uygun güvencelere atıfta bulunmadığı ifade edilmektedir.[524]

4.4 Veri Sahibinin Hakları

Veri sahibinin hakları, Kolluk Direktifi'nin üçüncü bölümünde düzenlenmektedir. Bu bölümde veri sahibine ait bir dizi hakkın, bunlara uygulanabilecek kısıtlamaların ve bunların veri sahibi tarafından kullanılmasına ve veri sahibine iletilmesine ilişkin usullerin ortaya konulması suretiyle bir kurallar ve usuller dizisi oluşturulmaktadır. Açıkçası, Kolluk Direktifi'ndeki veri sahibinin hakları, kolluk görevlerini ve cezai soruşturmaları korumak için belirli sınırlamaların uygulanması gereken CKKAİ alanına uyarlanmış, güvenlik menfaatleri ile bireylerin hak ve özgürlükleri arasında bir denge kurulmasına çalışılmıştır.

[523] Article 29 Data Protection Working Party, "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)", WP258, 29 Kasım 2017, s.15.
[524] "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", s.14.

Madde 29 Çalışma Grubu tarafından, Kolluk Direktifi'nde, veri sahibi haklarına genel kısıtlamalar getirilmesine izin verilmediği, bunun yerine, söz konusu kısıtlamaların yalnızca gerekli ve orantılı bir tedbir teşkil ettikleri takdirde uygulanması gerektiği ifade edilmiştir.[525] Kolluk Direktifi'nin 12'nci maddesi, veri sahibi haklarının kullanılmasına ilişkin genel usulleri düzenlemekte olup, veri sahibi taleplerinin gereksiz gecikme olmaksızın takip edilmesini ve bilgilerin kısa, anlaşılır, genel olarak ücretsiz ve kolay erişilebilir bir biçimde sunulmasını gerektirerek idari ve pratik yükü azaltmayı amaçlamaktadır.

Kolluk Direktifi madde 13(1) kontrolörün veri sahiplerine sunması gereken bilgileri tanımlamaktadır.[526] Kolluk Direktifi madde 13(1) ile bağlantılı olarak, Kolluk Direktifi'nin dibacesinde, bu bilgilerin nasıl sağlanabileceğine ilişkin örnekler sunulmaktadır: örneğin, yetkili makamın internet sitesinde yayımlanabilir veya örneğin, bir kolluk teşkilatı gözaltı görüntülerinin, vücut kamerası kayıtlarının veya silah ruhsatı bilgilerinin kullanımıyla ilgili gizlilik politikasını yayımlamak isteyebilir.[527] Kolluk Direktifi madde 13(2), madde 13(1)'deki bilgilere ek olarak, bir yasa ile kontrolörün belirli durumlarda veri sahibine haklarının kullanılmasını sağlamak üzere bazı ilave bilgileri[528] vermesini düzenlemektedir. Kolluk Direktifi madde 13(3)'de "ilgili gerçek kişinin temel hakları ve meşru menfaatleri göz önünde bulundurularak, demokratik bir toplumda gerekli ve orantılı bir tedbir teşkil ettiği

[525] Article 29 Data Protection Working Party, "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)", WP258, 29 Kasım 2017, s.24.
[526] Kolluk Direktifi madde 13(1)(a)-(e): "Kontrolörün kimliği ve iletişim bilgileri", "varsa, veri koruma görevlisinin iletişim bilgileri", "kişisel verilerin işlenme amaçları", "bir denetim makamına şikâyette bulunma hakkı ve denetim makamının iletişim bilgileri", "kontrolörden kişisel verilere erişim ve kişisel verilerin düzeltilmesi veya silinmesini ve veri sahibiyle ilgili kişisel verilerin işlenmesinin kısıtlanmasını talep etme hakkının varlığı".
[527] Kolluk Direktifi, dibace (42).
[528] Kolluk Direktifi madde 13(2)(a)-(d): "İşleme için yasal dayanak", "kişisel verilerin saklanacağı süre veya bunun mümkün olmadığı durumlarda bu süreyi belirlemek için kullanılan kriterler", "uygulanabilir olduğu hallerde, üçüncü ülkeler veya uluslararası kuruluşlar da dahil olmak üzere kişisel verilerin alıcı kategorileri", "Gerekli olduğu hallerde, özellikle kişisel verilerin veri sahibinin bilgisi dışında toplandığı hallerde, daha fazla bilgi".

ölçüde ve sürece" üye devletler tarafından madde 13(2) uyarınca veri sahibine verilmesi gereken ilave bilgilerin verilmesini belirli durumlarda[529] "geciktiren, kısıtlayan veya ihmal eden" yasal tedbirler kabul edebileceği ifade edilmektedir. Madde 29 Çalışma Grubu ulusal yasa koyuculara, kontrolörlerin madde 13(2)'de belirtilen ek bilgileri hangi durumlarda ve hangi koşullar altında vermeyebileceğini belirlemek için nesnel ölçütler tanımlamaları çağrısında bulunmaktadır.[530] Kolluk Direktifi madde 13(1)'de kullanılan ifadede bilgilerin erişilebilir kılınması gerektiği belirtilirken, madde 13(2)'de belirli durumlarda bilgilerin verilmesi gerektiği ifade edilmiştir. Ancak Kolluk Direktifi'nde "belirli durumların" neyi ifade edebileceği açık değildir. Madde 29 Çalışma Grubu'na göre "bu yükümlülüğün belirli bir veri sahibine değil, belirli bir veri işleme faaliyetinin ve bu faaliyetten potansiyel olarak etkilenen tüm veri sahiplerine ilişkin olduğu ileri sürülebilir."[531]

Kolluk Direktifi madde 14'te veri sahibinin erişim hakkı düzenlenmektedir.[532] Erişim hakkı, ABTHŞ'de yer alan "kişisel verilerin korunması" hakkına ilişkin hükme açıkça dahil edilmiştir.[533] Hem ABAD hem de AİHM, erişim hakkının diğer veri koruma haklarının korunmasında önemli bir rol oynadığını kabul etmiştir. Örneğin, *Rijkeboer* kararında[534] ABAD, erişim hakkının diğer veri sahibi haklarının kullanılması için bir ön koşul olduğunu

[529] Kolluk Direktifi madde 13(3)(a)-(e): "Resmi veya yasal soruşturmaları, incelemeleri veya prosedürleri engellemekten kaçınmak", "suçların önlenmesine, tespit edilmesine, soruşturulmasına veya kovuşturulmasına ya da cezai yaptırımların uygulanmasına halel getirmekten kaçınmak", "kamu güvenliğini korumak", "ulusal güvenliği korumak", "başkalarının hak ve özgürlüklerini korumak".
[530] Article 29 Data Protection Working Party, "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)", WP258, 29 Kasım 2017, s.18.
[531] Article 29 Data Protection Working Party, "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)", WP258, 29 Kasım 2017, s.17.
[532] Kolluk Direktifi madde 14 hakkında ayrıntılı bilgi için bkz. DIMITROVA, DIANA ve DE HERT, PAUL, (2018), s.116-121.
[533] ABTHŞ madde 8(2) "Bu veriler, adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak tutulur. Herkes, kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir."
[534] Case C-553/07, *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer* [2009] ECR I-3889, paras 51-52.

belirtmiştir ve bu görüş ABAD'ın sonraki kararlarında da[535] teyit edilmiştir.[536] Veri sahibinin Kolluk Direktifi kapsamında erişim hakkını kullanması halinde, Kolluk Direktifi madde 15'teki şartlar saklı kalmak koşuluyla, kontrolör öncelikle veri sahibiyle ilgili kişisel verileri işleyip işlemediğini veri sahibine teyit eder. Kontrolör tarafından veri sahibi ile ilgili kişisel verilerin işlendiğinin teyit edilmesi durumunda, veri sahibi, işlemenin amacı ile hukuki dayanağına, işlenen veri kategorilerine, verilerin kimlerle paylaşıldığına (özellikle üçüncü ülkeler veya uluslararası kuruluşlarla), verilerin ne kadar süreyle saklanacağına ya da bu sürenin belirlenmesinde kullanılan kriterlere, kişisel verilerin düzeltilmesi, silinmesi veya işlenmesinin kısıtlanmasını talep etme hakkına, denetim makamına şikâyette bulunma hakkı ile bu makamın iletişim bilgilerine ve verilerin kaynağına ilişkin mevcut tüm bilgilere erişim hakkına sahiptir.[537] Kolluk Direktifi kapsamında veri sahiplerine, doğrudan erişim hakkının tanınması, 2008/977 sayılı Çerçeve Karar kapsamındaki önceki duruma kıyasla önemli bir ilerleme olarak görülmektedir.[538]

Kolluk Direktifi madde 14'te düzenlenen veri sahibinin erişim hakkı mutlak bir hak değildir. Kontrolör, Kolluk Direktifi madde 15'te belirtilen dört koşulun yerine getirilmesi halinde, bu verileri tamamen veya kısmen kısıtlayabilir. İlk olarak, sınırlama üye devletler tarafından kabul edilen bir yasama tedbirine dayanmalıdır. İkinci olarak, kısıtlama sadece "demokratik bir toplumda gerekli ve orantılı bir tedbir teşkil ettiği sürece" uygulanabilir. Üçüncü olarak, veri sahibinin temel haklarına ve meşru menfaatlerine gereken saygı

[535] Joined Cases C-141/12 and C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* [2014] EU:C:2014:2081, para 57; Case C 434/16, *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994, para 57.
[536] VOGIATZOGLOU, PLIXAVRA *et.al.*, "From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives", Journal of Intellectual Property, Information Technology and E-Commerce Law, Cilt:11, Sayı:3, 2020, s.285.
[537] Kolluk Direktifi madde 14 (a)-(g).
[538] SAJFERT, JURAJ ve QUINTEL, TERESA, (2017), s.12; DIMITROVA, DIANA ve DE HERT, PAUL, (2018), s.124.

gösterilmelidir.[539] Bu bağlamda veri sahibinin haklarına yönelik her türlü kısıtlama, sırasıyla ABAD ve AİHM içtihat hukukunda yorumlandığı şekliyle ABTHŞ ve AİHS'ye uygun olmalı ve özellikle bu hak ve özgürlüklerin özüne saygı göstermelidir.[540] Dördüncü olarak, kısıtlama Kolluk Direktifi madde 15 (1)(a)-(e)'de belirtilen meşru amaçlardan en az birini takip etmelidir. Bu amaçlar şunlardır: "resmi veya yasal soruşturmaları, incelemeleri veya prosedürleri engellemekten kaçınmak"; "cezai suçların önlenmesi, tespiti, soruşturulması veya kovuşturulmasına ya da cezai yaptırımların uygulanmasına halel getirmekten kaçınmak"; "kamu güvenliğinin korunması"; "ulusal güvenliğin korunması" veya "başkalarının hak ve özgürlüklerinin korunması". Söz konusu meşru amaçlar oldukça geniş bir şekilde ifade edilmiş olup, kontrolör bu istisnalardan yararlanırken geniş bir takdir marjına sahip olacaktır. Bu bağlamda, erişim hakkına getirilen kısıtlamalar, ilgili veri sahiplerinin erişim hakkının etkinliğini kolayca azaltabilecektir.[541]

Üye devletler muafiyete tabi olabilecek işleme kategorileri hakkında yasal tedbirler kabul edebilir.[542] Kontrolörün belirli bir veri sahibinin erişim hakkını tamamen veya kısmen kısıtlaması halinde, veri sahibini kararın gerekçeleri de dahil olmak üzere erişimin tamamen reddedilmesi veya kısıtlanması konusunda bilgilendirmesi gerekir. Bu bilgiler veri sahibine "yazılı olarak" ve "gereksiz gecikme olmaksızın" iletilmelidir. Bu tür bilgilerin açıklanması kısıtlamaya ilişkin meşru gerekçelerden birine zarar verecekse, veri sorumlusu bu bilgileri açıklamayabilir. Ancak, veri sahibini bir denetim makamına şikayette bulunma ve yargı yoluna başvurma hakkı konusunda bilgilendirmek zorundadır.[543] Kontrolörün ret kararı

[539] Kolluk Direktifi madde 15(1).
[540] Kolluk Direktifi, dibace (46).
[541] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2016), s.13; DIMITROVA, DIANA ve DE HERT, PAUL, (2018), s.122.
[542] Kolluk Direktifi madde 15(2).
[543] Kolluk Direktifi madde 15(3).

vermesi halinde bu kararın dayandığı maddi ve hukuki gerekçeleri belgelemesi ve bunları denetim makamının erişimine açık tutması gerekmektedir.[544] Kontrolörün veri sahibini erişimin tamamen reddedildiği konusunda bilgilendirmesi gerektiği açık olmakla birlikte, Kolluk Direktifi madde 15(4) hükmünün lafzı, kısmi bir ret durumunda kontrolörün veri sahibini en azından talebinin hangi kısmının reddedildiği konusunda bilgilendirip bilgilendirmeyeceğini veya hem bu bilgiyi hem de kısmi ret nedenlerini bildirip bildirmeyeceğini netleştirmemektedir.[545]

Kolluk Direktifi madde 16'da kişisel verilerin düzeltilmesinin, silinmesinin ve işlenmesinin kısıtlanmasına ilişkin veri sahibinin hakları ve kontrolörün yükümlülükleri düzenlenmektedir. Veri sahibi, kendisiyle ilgili yanlış kişisel verilerin düzeltilmesini veya işleme faaliyetinin Kolluk Direktifi hükümlerini ihlal ettiği durumlarda kendisi ile ilgili verilerin silinmesini talep edebilir.[546] Kontrolör, silme işlemi yerine, "kişisel verilerin doğruluğuna veri sahibi tarafından itiraz edilmesi ve bunların doğruluğunun veya yanlışlığının tespit edilememesi" veya "kişisel verilerin kanıt amacıyla muhafaza edilmesi" durumlarında işleme faaliyetini kısıtlayabilecektir.[547] Üye devletler, veri sahibinin, "temel hakları ve meşru menfaatleri göz önünde bulundurularak demokratik bir toplumda gerekli ve orantılı bir tedbir teşkil ettiği ölçüde", Kolluk Direktifi madde 16 (4)(a)-(e)'de belirtilen gerekçelerle, bu tür bilgileri sağlama yükümlülüğünü tamamen veya kısmen kısıtlayan yasal tedbirler kabul edebilecektir.[548] İşlenen kişisel verilerin yanlış olduğunun teyit edildiği durumlarda düzeltilmesi için bu durum yetkili makamlara iletilecektir.[549] Ayrıca kişisel

[544] Kolluk Direktifi madde 15(4).
[545] DIMITROVA, DIANA ve DE HERT, PAUL, (2018), s.122.
[546] Kolluk Direktifi madde 16(1)-(2).
[547] Kolluk Direktifi madde 16(3).
[548] Kolluk Direktifi madde 16(4).
[549] Kolluk Direktifi madde 16(5).

verilerin, düzeltildiği veya silindiği ya da işleme faaliyetinin kısıtlandığı hallerde, kontrolörün alıcıları da bilgilendirerek aynı işlemin yapılmasını sağlamalıdır.[550]

Kolluk Direktifi madde 17'de veri sahiplerinin Kolluk Direktifi kapsamındaki haklarını denetim makamı aracılığı ile kullanabileceği düzenlenmektedir. Söz konusu madde hem yetkili makamlar hem de veri sahipleri için "bir güvenlik ağı" olarak öngörülmektedir.[551] Yetkili makamlar devam eden soruşturmaları korumak amacıyla herhangi bir işleme doğrulamasını açıklamamaya karar verebilirken,[552] veri sahiplerine en azından veri işlemelerinin hukuka uygunluğunun denetim makamı tarafından doğrulanması fırsatı verilmektedir.[553] Madde 29 Çalışma Grubu tarafından, Kolluk Direktifi madde 17'nin belirsiz ifadesine rağmen, denetim makamlarına ulusal hukuk tarafından yalnızca erişim hakkını değil, veri sahipleri adına düzeltme, silme ve kısıtlama haklarını da kullanma yetkisi verilmesi gerektiğini savunulmuştur.[554] Denetim makamları, veri sahipleri ile yetkili makamların menfaatleri arasındaki hassas dengeyi koruyarak, Kolluk Direktifi madde 17 uyarınca gelen talepleri ve cevapları azami özenle ele almalıdır.[555] Ancak pratikte bu dengenin sağlanması oldukça zor olabilir; denetim makamı her zaman verilerin Kolluk Direktifi'ne uygun işlenip işlenmediğini tespit edebilecek veya verilerin düzeltilmesini sağlayabilecek bir konumda olmayabilir. Bu durumda, verilerine erişimi olmayan ve denetim makamının herhangi bir usulsüzlüğü giderip gidermediğini bilmeyen bir veri sahibinin yetkili

[550] Kolluk Direktifi madde 16(6).
[551] DRECHSLER, LAURA, (2020), s.102.
[552] Kolluk Direktifi madde 13(3), 15(3), 16(4).
[553] Kolluk Direktifi madde 17(3).
[554] Article 29 Data Protection Working Party, "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)", WP258, 29 Kasım 2017, s.23.
[555] SAJFERT, JURAJ ve QUINTEL, TERESA, (2017), s.14.

makama karşı açacağı davasını mahkemede nasıl takip edebileceği sorusu ortaya çıkmaktadır.[556]

Veri sahibinin haklarına ilişkin önemli bir sınırlama, üye devletlerin "kişisel verilerin cezai soruşturma ve kovuşturmalar sırasında işlenen bir yargı kararında veya kaydında veya dava dosyasında yer alması halinde" hakların kullanılması için geçerli çerçeve olarak ulusal hukuku belirlemelerine imkân tanıyan Kolluk Direktifi madde 18 kapsamında öngörülmektedir. Veri sahibinin Kolluk Direktifi'nde belirtilen haklarından ulusal ceza muhakemesi yasaları vasıtasıyla feragat etme imkânı Kolluk Direktifi'nin dibacesinde de yinelenmektedir.[557]

Kolluk Direktifi'ne ilişkin Komisyon'un ilk raporunda; tüm üye devletlerin, veri sahiplerinin kişisel verilerine erişim hakkı başta olmak üzere veri sahiplerinin haklarını kısıtlamak için Kolluk Direktifi tarafından öngörülen istisnaları, kısıtlamaların uygulanacağı durumları veya koşulları daha fazla belirtmeksizin sadece Kolluk Direktifi'nin genel dilini kullanacak şekilde, kullanmayı seçtiği ifade edilmiştir. Ayrıca raporda, Üye Devletlerin çoğunun, veri sahiplerinin haklarını bir denetim makamı aracılığıyla kullanabilmelerini sağlamak için Kolluk Direktifi'nin gerekliliğine uyduğu ve ulusal ceza soruşturmaları ve kovuşturmaları bağlamında veri sahiplerinin haklarının ulusal hukuka uygun olarak kullanılmasını şart koşma seçeneğini kullandığı belirtilmiştir.[558]

[556] DIMITROVA, DIANA ve DE HERT, PAUL, (2018), s.123.
[557] Kolluk Direktifi, dibace (49) ve (107).
[558] "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", s.14-15.

4.5 Kontrolörün Yükümlülükleri

4.5.1 Genel Yükümlülükler

Direktifin dördüncü bölümü, veri kontrolörleri ve işleyicilerine bir dizi yeni yükümlülük getirmektedir. Kolluk Direktifi madde 19 uyarınca, "işleme faaliyetinin niteliği, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlüklerine yönelik değişen olasılık ve ciddiyetteki riskleri dikkate alarak işleme faaliyetinin" Kolluk Direktifi ile uyumluluğunun sağlanması için uygun teknik ve kurumsal tedbirlerin alınması kontrolörün sorumluluğundadır. Buna ek olarak, kontrolör, veri işleme faaliyetlerinin niteliği ile orantılı olduğunda, uygun veri koruma politikalarının uygulanması ile görevlendirilir.

Kolluk Direktifi madde 20 kapsamında, üye devletler, kontrolörlerin kişisel veri işleme faaliyetlerinde teknolojinin durumu, maliyet, işlemenin niteliği ve haklara yönelik riskleri dikkate alarak veri koruma ilkelerini (örneğin veri minimizasyonu) etkili biçimde uygulamalarını ve uygun teknik ve kurumsal önlemleri (örneğin takma ad kullanımı) hayata geçirmelerini sağlamakla yükümlüdür. Ayrıca, kontrolörlerin varsayılan olarak yalnızca belirli amaçlar için gerekli olan kişisel verileri işlemesini sağlayacak tedbirleri uygulaması gerekir. Bu yükümlülük, toplanan veri miktarı, saklama süresi ve veriye erişim kapsamını kapsar. Özellikle, kişisel verilerin bireylerin müdahalesi olmadan geniş kitlelerce erişilebilir hale gelmesi önlenmelidir.

Kolluk Direktifi madde 21, iki veya daha fazla veri sorumlusunun işleme faaliyetlerinin amaç ve araçlarını ortaklaşa belirlemesi durumunda bir dizi kural ortaya koymaktadır. Kontrolörlerin sorumlulukları AB ve üye devletler hukuku ile belirlenmediği sürece, kontrolörlerin, Kolluk Direktifi ile ilgili sorumluluklarını bir düzenleme (protokol

vb.) yoluyla belirlenmeli ve veri sahipleri için tek bir irtibat noktası tayin edilmelidir.[559] Ayrıca üye devletler, kontrolörlerin, sorumluluklarını belirleyen düzenlemenin şartlarına bakılmaksızın, veri sahibinin, haklarını kontrolörlerin her birine karşı kullanmasını sağlamalıdır.[560] Kolluk Direktifi söz konusu düzenlemenin içeriği bakımından GDPR'den ayrılmaktadır. GDPR kapsamında, bu düzenlemenin veri sahipleri açısından "ilgili rolleri ve ilişkileri gerektiği gibi yansıtması" ve aralarındaki anlaşmanın "özünü" ortaya koyması gerekmektedir.[561] Kolluk Direktifi madde 21'de böyle bir hükmün yer almaması eleştirilmiş ve böyle bir hükmün yer alması veri sorumlularını daha fazla öz denetim uygulamaya ve veri koruma hukuku kapsamındaki yükümlülükleri konusunda daha yüksek bir farkındalığa sahip olmaya teşvik edeceği dile getirilmiştir.[562]

Kolluk Direktifi madde 22 ve 23 uyarınca, veri işleyenler, kişisel verileri yalnızca kontrolör ve işleyicinin verdiği talimatlar doğrultusunda işleyebilecektir. Ayrıca veri işleyenler, "işleme faaliyetinin konusu ve süresi, işleme faaliyetinin niteliği ve amacı, kişisel verilerin türü ve veri sahibi kategorileri ile kontrolörün yükümlülükleri ve haklarını ortaya koyan" bağlayıcı bir sözleşmeye tabi olmalıdır. Ayrıca, veri işleyenlerin diğer veri işleyenlerle ilişki kurması ve işbirliği yapması için kontrolör tarafından önceden yazılı olarak yetkilendirilmesi de gerekmektedir.

Kolluk Direktifi'nin temel amaçlarından biri kişisel verilerin işlenmesinde yüksek düzeyde hesap verebilirliği teşvik etmek olduğundan, yetkili makamların Kolluk Direktifi ile uyumluluğu gösterebilmeleri ve denetim makamları tarafından işleme faaliyetlerinin hukuka

[559] Kolluk Direktifi madde 21(1).
[560] Kolluk Direktifi madde 21(2).
[561] GDPR madde 26(2).
[562] RADTKE, TRISTAN, "The Concept of Joint Control under the Data Protection Law Enforcement Directive 2016/680 in Contrast to the GDPR", Journal of Intellectual Property, Information Technology and Electronic Commerce Law, Cilt:11, Sayı:3, 2020, s.247.

uygunluğunu gözden geçirebilmeleri hayati önem taşımaktadır. Bu amaçla, Kolluk Direktifi'nin IV'üncü Bölümü işleme faaliyetine ilişkin kayıtların tutulması ve log kayıtlarına ilişkin hususları ortaya koymaktadır.

Kolluk Direktifi madde 24 işleme faaliyetine ilişkin tutulması gerek kayıtları ve usullerini düzenlemekte olup, bu madde uyarınca, kontrolörler ve işleyiciler sorumlulukları altındaki tüm işleme faaliyeti kategorilerine ilişkin bir kayıt tutmalıdır. Bu kayıtlar işleme amaçları, ilgili yasal dayanak, verilerin saklanması ve güvenliği, diğer alıcılara aktarım ve ilgili veri sahibi ve kişisel veri kategorileri hakkında bilgi içermelidir. Dolayısıyla, bu madde hükmü yetkili makamların faaliyetlerini belgelemesini ve talep üzerine bu bilgileri denetim makamlarına sunmalarını gerektirmektedir.[563]

Kolluk Direktifi madde 25 kapsamında, üye devletler, en azından bilgisayar sistemlerinde kişisel verilerin toplanması, değiştirilmesi, açıklanması, birleştirilmesi ve silinmesi de dahil olmak üzere, otomatik işleme sistemlerindeki çeşitli işleme faaliyetlerine ilişkin log kayıtlarının tutulmasını sağlamalıdır. Danışma ve açıklama kayıtları, işlemenin gerekçesinin, tarihinin ve zamanının belirlenmesine ve mümkün olduğu hallerde verilere danışan, açıklayan veya verileri alan kişilerin kimliklerinin tespit edilmesine olanak sağlamalıdır. Bu bilgiler talep üzerine yetkili makamlara sunulmalıdır ve yalnızca işlemenin yasallığının doğrulanması, kendi kendini izleme, kişisel verilerin bütünlüğünün ve güvenliğinin sağlanması ve cezai kovuşturmalar için kullanılmalıdır. Esas olarak log kayıtlarının tutulması, yetkili makamların bilgi teknoloji sistemlerinde, kişisel verilerin kim tarafından ne zaman ve hangi amaçla işlendiğine dair belirli bilgileri içeren, meta verileri üretmelerini ve muhafaza etmelerini gerektirmektedir.

[563] VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, 2022, s.69.

Log kayıtlarının tutulması yükümlülüğü, GDPR'de eşdeğer bir hükmü bulunmayan Kolluk Direktifi'nin belirgin bir özelliğidir. Başta kolluk kuvvetleri olmak üzere yetkili makamların veri tabanlarının çok sayıda kişiye ait yüksek hacimde bilgi içermesi ve bunların çoğunun hassas verilerden oluşması, bu tür veri tabanlarının kötüye kullanılmaması ve yalnızca hukuka uygun amaçlar doğrultusunda yetkili kişiler tarafından erişilmesinin sağlaması açısından log kayıtlarının merkezi bir rol oynayacağı değerlendirilmektedir.[564] Ayrıca Madde 29 Çalışma Grubu tarafından, özellikle danışma ve ifşa kayıtları için gerekçe gerekliliğinin hesap verebilirliğe yönelik güçlü bir adım olduğu belirtilmiş ve bu gerekliliğin tüm işleme faaliyetleri için öngörülmesi tavsiye edilmiştir.[565]

AB'nin veri koruma reformları, yasal düzenlemelere uyumu daha net bir şekilde göstermek ve olumsuz etkileri ortaya çıkmadan önlemek için yüksek riskli veri işleme faaliyetlerinden önce bir VKED yapılmasını zorunlu hale getirmiştir. Hem GDPR'de hem de Kolluk Direktifi'nde belirtilen bu yükümlülük, kontrolörlerin veri işleme faaliyetlerinin bireylerin hak ve özgürlükleri üzerindeki potansiyel etkisini önceden değerlendirmesini ve belirlenen risklere karşı uygun önlemleri alarak veri sahiplerinin çıkarlarını korumasını gerektirmektedir.[566] Kolluk Direktifi madde 27, kolluk ve adli makamlar bağlamında bu prosedürün kapsamını, ayrıntılarını ve gerekliliklerini belirlemektedir. Özellikle yeni teknolojilerin kullanımını içeren bir işleme türünün, işleme faaliyetinin niteliği, kapsamı, bağlamı ve amaçları dikkate alındığında gerçek kişilerin hak ve özgürlüklerine yönelik yüksek bir riskle sonuçlanmasının muhtemel olduğu durumlarda bir VKED'nin gerekli

[564] SAJFERT, JURAJ ve QUINTEL, TERESA, (2017), s.14.
[565] Article 29 Data Protection Working Party, "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)", WP258, 29 Kasım 2017, s.26.
[566] VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, 2022, s.72.

olduğunu belirtmektedir.[567] Bu değerlendirme, işleme faaliyetinden önce yapılmalı ve öngörülen faaliyetlerin bir tanımını, veri sahiplerinin hak ve özgürlüklerine yönelik risklerin bir değerlendirmesini ve bu riskleri ele almak ve kişisel verilerin korunmasını sağlamak için kullanılan tedbirler, güvenceler ve mekanizmalara genel bir bakışı içermelidir.[568] Bu nedenle, Kolluk Direktifi'nin dibacesinde de belirtildiği üzere VKED münferit vakalarla ilgilenmez, bunun yerine prosedürleri, sistemleri ve genel işleme faaliyetlerini değerlendirmeyi amaçlar.[569] VKED'ler, veri sahiplerinin hak ve özgürlüklerine ilişkin geniş kapsamlı sonuçları dikkate alırken, kontrolörlerin hesap verebilirliğine ve Kolluk Direktifi'ndeki veri koruma yükümlülüklerine uyulmasına katkıda bulunduğundan, yeni gözetim ve işleme teknolojilerinin yönetiminde özellikle önemli bir rol oynayacaktır.[570] VKED'lerin kolluk kuvvetlerinin veri işlemesinde güvenlik seviyesini artırdığını, Komisyon'un Kolluk Direktifi'ne ilişkin ilk raporunda da belirtmiştir.[571] Ancak GDPR ve Kolluk Direktifi, VKED'ler konusunda önemli farklılıklar içermektedir. GDPR madde 35, VKED'nin gerekli olduğu durumları açıkça belirtip, veri koruma görevlisinin sürece dahil olmasını zorunlu kıldıktan sonra ulusal denetim makamlarının yönlendirilmesini öngörürken; Kolluk Direktifi madde 27, GDPR'nin aksine bu seviyede ayrıntı sunmamakta ve yalnızca risklerin belirlenmesine ilişkin Kolluk Direktifi'nin dibacesinde[572] konuya ilişkin açıklama yapmakla

[567] Kolluk Direktifi madde 27(1).
[568] Kolluk Direktifi madde 27(2).
[569] Kolluk Direktifi, dibace (58).
[570] DEMETZOU, KATERINA, "Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation", Computer Law & Security Review, Cilt:35, Sayı:6, 2019, s.2; MARQUENIE, THOMAS, (2017), s.334.
[571] "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", s.19.
[572] Kolluk Direktifi, dibace (51) "Gerçek kişilerin hak ve özgürlüklerine yönelik risk, değişen olasılık ve şiddette, özellikle fiziksel, maddi veya maddi olmayan zarara yol açabilecek veri işlemeden kaynaklanabilir: İşlemenin ayrımcılık, kimlik hırsızlığı veya dolandırıcılık, mali kayıp, itibarın zedelenmesi, mesleki gizlilikle korunan verilerin gizliliğinin kaybedilmesi, takma adın yetkisiz bir şekilde tersine çevrilmesi veya diğer önemli ekonomik veya sosyal dezavantajlara yol açabileceği durumlar; veri sahiplerinin hak ve özgürlüklerinden veya kişisel verileri üzerindeki kontrollerini kullanmaktan mahrum bırakılabileceği durumlar; ırk veya etnik köken,

yetinmektedir. Ayrıca Kolluk Direktifi madde 28 ile yüksek riskli veya yeni teknolojiler içeren veri işleme faaliyetlerinin başlamasından ve veri işlemeye ilişkin bir yasama tasarrufunun hazırlanması aşamasında denetim makamının bilgilendirilmesini ve danışılmasını, gerekirse müdahale etmesini düzenlemektedir. Sonuç olarak Kolluk Direktifi açısından bu alanın aydınlatılması üye devletlere ve özellikle denetim makamlarına düşmektedir.

4.5.2 Kişisel Verilerin Güvenliği

CKKAİ alanındaki veri koruma çerçevesine yapılan bir diğer önemli katkı da veri güvenliğine ilişkin düzenlemelerdir. Kolluk birimleri ve adli makamlar, giderek artan kişisel veri hacmini işlemek amacıyla modern teknolojilere başvurdukça, hem yürütülen soruşturmaların bütünlüğünün korunması hem de işlenen kişisel verilerin güvenliğinin sağlanması büyük önem taşımaktadır.[573] Bu kapsamda Kolluk Direktifi Bölüm IV'ün ikinci kısmı, kontrolörlere işleme güvenliği ve kişisel veri ihlallerinin yönetimi ile ilgili ek yükümlülükler getirerek "uygun güvenlik" ilkesini[574] genişletmektedir.[575]

Kolluk Direktifi madde 29 uyarınca, kontrolörler, "teknolojinin geldiği noktayı, uygulama maliyetlerini ve işleme faaliyetinin niteliği, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlüklerine yönelik değişen olasılık ve ciddiyetteki riskleri dikkate alarak, riske uygun bir güvenlik düzeyi sağlamak üzere uygun teknik ve kurumsal

---

siyasi görüşler, din veya felsefi inançlar veya sendika üyeliğini ortaya çıkaran kişisel verilerin işlendiği durumlar; bir kişiyi benzersiz bir şekilde tanımlamak için genetik verilerin veya biyometrik verilerin işlendiği veya sağlıkla ilgili verilerin veya cinsel yaşam ve cinsel yönelimle ilgili verilerin veya cezai mahkumiyet ve suçların veya ilgili güvenlik önlemlerinin işlendiği; kişisel profillerin oluşturulması veya kullanılması için özellikle işteki performans, ekonomik durum, sağlık, kişisel tercihler veya ilgi alanları, güvenilirlik veya davranış, konum veya hareketlerle ilgili hususların analiz edilmesi ve tahmin edilmesi gibi kişisel hususların değerlendirildiği; özellikle çocuklar olmak üzere savunmasız gerçek kişilerin kişisel verilerinin işlendiği veya işlemenin büyük miktarda kişisel veri içerdiği ve çok sayıda veri sahibini etkilediği durumlarda."

[573] BOSTANCI BOZBAYINDIR, GÜLŞAH, (2018), s.83.

[574] Kolluk Direktifi madde 4(1)(f).

[575] VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, 2022, s.75.

tedbirleri" uygulamakla yükümlüdür.[576] Bu kapsamda otomatik veri işleme bakımından güvenlik tedbirlerinin benimsenmesi yoluyla sağlanması gereken, "ekipman erişim kontrolü", "veri ortamı kontrolü", "saklama kontrolü", "kullanıcı kontrolü", "veri erişim kontrolü", "iletişim kontrolü", "girdi kontrolü", "aktarım kontrolü", "kurtarma", "güvenilirlik" ve "bütünlük" olmak üzere toplam on bir özel garanti ve bilgi kontrol şekli öngörülmektedir.[577] Kolluk Direktifi'nin bu hükmü, kolluk kuvvetleri ile ceza adaleti makamlarının sıklıkla işlediği verilerin özellikle hassas yapısı göz önüne alındığında, GDPR'deki karşılığına[578] nazaran belirgin şekilde daha güçlü güvenceler sağladığı için memnuniyetle karşılanmıştır.[579]

Kolluk Direktifi çerçevesinde yapılan işleme faaliyeti sonucu bir kişisel veri ihlalinin meydana gelmesi durumunda, Kolluk Direktifi madde 30'a göre, kontrolörlerin ve işleyicilerin, "kişisel veri ihlalinin gerçek kişilerin hak ve özgürlüklerine yönelik bir riske yol açmasının muhtemel olmadığı hâller haricinde" kişisel veri ihlalini, gecikmesizin ve en 72 saat içerisinde denetim makamına bildirmesi gerekmektedir. Eğer 72 saat içinde denetim makamına bildirim yapılamamışsa bunun nedenleri de denetim makamına kişisel veri ihlali bildirilirken iletilecektir. Buna ek olarak, ihlalin gerçek kişilerin hak ve özgürlüklerine yönelik yüksek bir riskle sonuçlanmasının muhtemel olduğu tespit edilirse, Kolluk Direktifi madde 31 uyarınca, kontrolörün ihlalin niteliğini açıklayarak ve ilgili belirli bilgileri ifşa ederek veri sahibini bilgilendirmesini de gerektirmektedir. Ancak, kontrolörün yüksek riskin gerçekleşmesini önlemek için müteakip adımları atması veya koruma tedbirlerinin verileri

[576] Kolluk Direktifi madde 29(1).
[577] Kolluk Direktifi madde 29(2).
[578] GDPR madde 32.
[579] MARQUENIE, THOMAS, (2017), s.334; VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, 2022, s.75.

anlaşılmaz hale getirmesi halinde, veri sahibine bu bildirimin yapılması artık gerekli olmayacaktır.

Veri güvenliğinin sağlanması kapsamında ayrıntılı kuralların getirilmesi, bu alandaki önceki yasal düzenlemelere kıyasla kayda değer bir ilerleme olarak değerlendirilmektedir. Kontrolörlere ve işleyicilere getirilen, veri güvenliğini sağlama ve meydana gelen veri ihlallerini denetim makamlarına ve belirli koşullarda ilgili kişilere bildirme yükümlülüğü, ceza soruşturmalarında daha yüksek düzeyde şeffaflık, güvenlik ve bütünlük sağlamayı amaçlamaktadır.[580]

Kolluk Direktifi'nin 32 ila 34'üncü maddeleri uyarınca, kontrolörler, kişisel verilerin korunmasına yardımcı olmak üzere kamuya açık bir "Veri Koruma Görevlisi" atamak zorundadır. Bu görevlilerin veri koruma ile ilgili tüm konulara uygun ve zamanında dahil olmaları ve görevlerini etkin bir şekilde yerine getirebilmeleri için gerekli kaynaklara sahip olmaları gerekmektedir. Bu görevler arasında kontrolörün bilgilendirilmesi ve tavsiyelerde bulunulması, veri koruma mevzuatına uyumun izlenmesi, VKED'lere katılması, denetim makamları ile işbirliği yapılması ve veri sahipleri ve veri koruma ile ilgili endişeleri olan diğer aktörler için bir irtibat noktası olarak hareket edilmesi yer almaktadır.

4.6 Kişisel Verilerin Üçüncü Ülkelere veya Uluslararası Kuruluşlara Aktarılması

Kolluk Direktifi'nin V. Bölümü, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılmasıyla ilgilidir. AB veri koruma hukukunun önemli bir amacı, AB vatandaşlarının kişisel verilerini AB sınırları dışında da korumak olduğundan, üçüncü ülkelerde bulunan yetkili makamlara yapılan aktarımların hukuka uygun olması için belirli

[580] MARQUENIE, THOMAS, (2017), s.334; BOSTANCI BOZBAYINDIR, GÜLŞAH, (2018), s.83.

koşullara uyması ve yeterli güvenceler kapsamında olması gerekmektedir.[581] Bu amaçla, Kolluk Direktifi madde 35 kişisel verilerin aktarılması için gerekli genel ilkeleri ortaya koymaktadır. Bu kapsamda kişisel verilerin yetkili makamlar tarafından üçüncü ülkelere veya uluslararası kuruluşlara aktarılması için "aktarımın madde 1(1)'de belirtilen amaçlar için gerekli olması"; "kişisel verilerin üçüncü bir ülkedeki bir kontrolöre veya madde 1(1)'de atıfta bulunulan amaçlar bakımından yetkili bir makam olan uluslararası bir kuruluşa aktarılması"; "kişisel verilerin başka bir üye devletten aktarıldığı veya kullanıma sunulduğu durumlarda, söz konusu üye devletin ulusal hukukuna uygun olarak aktarıma önceden izin vermiş olması"; "Komisyon'un 36'ncı madde uyarınca bir yeterlilik kararı almış olması veya böyle bir kararın olmaması halinde 37'nci madde uyarınca uygun güvencelerin sağlanmış veya mevcut olması veya 36'ncı madde uyarınca bir yeterlilik kararının ve 37'nci madde uyarınca uygun güvencelerin olmaması halinde 38'inci madde uyarınca belirli durumlar için derogasyonların geçerli olması" ve "başka bir üçüncü ülkeye veya uluslararası kuruluşa aktarılması durumunda, asıl aktarımı gerçekleştiren yetkili makam veya aynı üye devletin başka bir yetkili makamı, suçun ciddiyeti, kişisel verilerin asıl aktarılma amacı ve kişisel verilerin aktarıldığı üçüncü ülkedeki veya uluslararası kuruluştaki kişisel veri koruma düzeyi de dahil olmak üzere ilgili tüm faktörleri gerekli şekilde dikkate alması" gerekmektedir.

Kolluk Direktifi'nin bu hükmü GDPR'nin bu konudaki mimarisini[582] kendine örnek almakta ve kişisel verilerin AB dışına aktarılmasına yönelik üç kademeli bir yaklaşım oluşturmaktadır. Bu kademelendirme uyarınca, bu aktarımlar ancak Komisyon'un yeterli düzeyde veri koruması sağlayan bir ülkeye aktarımlara izin veren bir yeterlilik kararı alması veya böyle bir kararın olmaması durumunda kişisel verilerin korunmasına ilişkin uygun

[581] DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2016), s.14.
[582] GDPR madde 44-50.

güvencelerin mevcut olması veya bu tür güvencelerin olmaması durumunda belirli durumlar için belirli derogasyonların geçerli olması halinde gerçekleşebilir. Buna ek olarak, Bölüm V, belirli koşullar karşılandığında kişisel verilerin doğrudan üçüncü ülkelerdeki yetkin olmayan alıcılara aktarılması imkanını da sağlamaktadır.[583] AB sınırları ötesinde kişisel veri aktarımını düzenleyen Kolluk Direktifi V. Bölüm, farklı menfaatler arasında hassas bir denge kurmaya çalışmaktadır. Üçüncü ülkelerdeki yetkili makamlarla işbirliği üye devlet kolluk kuvvetleri ve adli makamlarının etkinliği açısından önemli olduğundan, bir yandan veri koruma kuralları belirli bir esneklik sağlamalı ve CKKAİ alanının yetkili makamlarının ihtiyaçlarını karşılamalı, diğer yandan AB dışına kişisel verilerin aktarımının veri sahipleri açısından taşıdığı riskler göz önünde bulundurularak, veri sahiplerinin hak ve menfaatlerini korumak için sağlam ve uygulanabilir güvenceler gerektirmektedir.[584]

4.6.1 Yeterlilik Kararı Temelinde Aktarımlar

Kolluk Direktifi tarafından düzenlenen üç kademeli yapının ilk kademesini Komisyon tarafından alınan "yeterlilik kararı" kapsamında kişisel verilerin aktarımı oluşturmaktadır. Kolluk Direktifi madde 36'da Komisyon tarafından yeterlilik kararının hangi değerlendirmeler ve usul çerçevesinde alınacağı düzenlenmektedir. Komisyon, bir üçüncü ülke ya da uluslararası kuruluşun kişisel verilerin korunmasına ilişkin yeterli düzeyde koruma sağlayıp sağlamadığını değerlendirirken öncelikle o ülkenin veya kuruluşun hukuki çerçevesini ve uygulama pratiğini dikkate alır. Bu kapsamda "hukukun üstünlüğü, insan hakları ve temel özgürlüklere saygı, kamu güvenliği, savunma, ulusal güvenlik ve ceza hukuku" gibi alanlardaki düzenlemeler ile kişisel verilere kamu makamlarınca erişim kuralları göz önünde bulundurulur. Ayrıca, genel ve sektörel veri koruma mevzuatı, bu

[583] VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, 2022, s.78.
[584] CARUANA, MIREILLE M., (2017), s.15.

mevzuatın uygulanma şekli, veri aktarımına ilişkin kurallar, güvenlik önlemleri, içtihat hukuku, veri sahiplerine tanınan haklar ile idari ve yargısal başvuru yolları da değerlendirmeye dahil edilir. Komisyon ayrıca, söz konusu ülkede veya kuruluşta yeterli yaptırım yetkilerine sahip, bağımsız şekilde işleyen bir ya da daha fazla denetim makamının varlığını, bu makamların veri koruma kurallarının uygulanmasını sağlama ve veri sahiplerine yardımcı olma kapasitelerini da dikkate alır. Son olarak, ilgili ülkenin ya da kuruluşun kişisel verilerin korunmasına yönelik uluslararası yükümlülükleri, taraf olduğu bağlayıcı sözleşmeler ve çok taraflı ya da bölgesel sistemlere katılımı da değerlendirme sürecinde önemli rol oynar.[585] Komisyon tarafından üçüncü bir ülke veya uluslararası bir kuruluş için yeterlilik kararı alınması durumunda artık üye devletler tarafından kişisel verilerin, hakkında yeterlilik kararı alınan taraflara aktarılması için ayrıca özel bir izin gerekmemektedir.[586]

Kolluk Direktifi'nin dibacesinde de belirtildiği üzere Komisyon tarafından yeterlilik kararı alınabilmesi için ilgili üçüncü ülke veya uluslararası kuruluş tarafından AB'deki veri koruma düzeyine "eşdeğer" bir veri koruma sağlanmalıdır.[587] Esasa ilişkin olarak, yeterlilik kararları, Kolluk Direktifi madde 36'da belirtilen değerlendirme kriterleri ışığında, ilgili üçüncü ülkenin mevcut mevzuatının teoride ve uygulamada bir bütün olarak değerlendirilmesine odaklanmalıdır. Bu nedenle, eşdeğer bir korumaya ilişkin anlamlı bir analiz için "uygulanabilir kuralların içeriği ve bunların pratikte etkili bir şekilde uygulanmasını sağlamaya yönelik araçlar" olmak üzere iki temel unsuru bulunmaktadır.[588] ABAD'ın *Schrems*[589] kararında belirttiği üzere, yeterli koruma düzeyi terimi, üçüncü

[585] Kolluk Direktifi madde 36(2).
[586] Kolluk Direktifi madde 36(1).
[587] Kolluk Direktifi, dibace (67).
[588] European Data Protection Board, "Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive", 2 Şubat 2021, s.8.
[589] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, [2015], ECLI:EU:C:2015:650, (Schrems I).

ülkenin, iç hukuku veya uluslararası taahhütleri nedeniyle, ABTHŞ ışığında AB'de garanti edilen temel hak ve özgürlüklere esasen eşdeğer bir koruma düzeyi sağlamasını gerektirdiği şeklinde anlaşılmalıdır. Üçüncü ülkedeki koruma düzeyinin AB'de garanti edilen koruma düzeyine esasen eşdeğer olması gerekirken, bu bağlamda, söz konusu üçüncü ülkenin bu tür bir koruma düzeyi amacıyla başvurduğu araçlar AB'de kullanılanlardan farklı olabilir ancak bu araçlar yine de uygulamada etkili olmalıdır.[590] Bu doğrultuda Komisyon tarafından üçüncü ülkelerde ve uluslararası kuruluşlarda aranacak yeterlilik standardı, AB mevzuatını bire bir yansıtmayı değil, bu mevzuatın temel gerekliliklerini karşılamayı gerektirmektedir.[591]

Kolluk Direktifi ile ortaya konan kademelenmenin ilk adımını oluşturan yeterlilik kararları, veri koruma seviyesini değerlendirmek için bu konuda donanımlı olan Komisyon'a güvenerek, Kolluk Direktifi'nin ve ilkelerinin daha tutarlı bir şekilde uygulanmasıyla üçüncü ülkelere ve uluslararası kuruluşlara veri aktarımlarında sağlam veri koruma standartlarının varlığına ilişkin belirgin ve resmi bir güvence işlevi görecektir.[592] Komisyon, GDPR kapsamında birçok ülke ile ilgili yeterlilik kararı almış olsa da[593], Kolluk Direktifi kapsamında yeterlilik kararı, yalnızca Birleşik Krallık ile Haziran 2021'de kabul

[590] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, paras 73 ve 74.
[591] European Data Protection Board, "Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive", 2 Şubat 2021, s.5.
[592] DRECHSLER, LAURA, "Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context", International Data Privacy Law, Cilt:11, Sayı:2, 2021, s.188.
[593] Avrupa Komisyonu şimdiye kadar GDPR kapsamında Andorra, Arjantin, Kanada (ticari kuruluşlar), Faroe Adaları, Guernsey, İsrail, Man Adası, Japonya, Jersey, Yeni Zelanda, Kore Cumhuriyeti, İsviçre, Birleşik Krallık, Amerika Birleşik Devletleri (AB-ABD Veri Gizliliği Çerçevesine katılan ticari kuruluşlar) ve Uruguay'ın yeterli koruma sağladığını kabul etmiştir. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#adequacy-decisions-latest, Erişim Tarihi: 25.05.2025.

edilmiştir.[594] Sonuç olarak, uygun güvencelerin veya derogasyonların Birleşik Krallık dışındaki üçüncü ülkelere veri aktarımını haklı kılıp kılmadığını değerlendirmek üye devletlere ve onların yetkili makamlarına kalmıştır. Bu durumun AB genelinde hukuki belirsizliğe ve tutarsızlığa yol açabileceği ve bu nedenle, temel hakların ve AB veri sahiplerinin menfaatlerinin AB sınırları ötesinde korunmasını sağlamak için Kolluk Direktifi kapsamında yeterlilik kararlarının gerekli olduğu vurgulanmaktadır.[595] Görünüşe göre Komisyon da bu niyeti paylaşmaktadır. Komisyon'un Kolluk Direktifi'ne ilişkin ilk raporunda, Komisyon "diğer kilit uluslararası ortaklarla yeterlilik bulguları olasılığını aktif bir şekilde teşvik ettiğini" ve "Kolluk Direktifi kapsamında gelecekteki yeterlilik kararları için diğer olası adayları [...] değerlendireceğini" belirtmekte ve Kolluk Direktifi'nin yakın zamanda kabul edilmesini ve kolluk kuvvetlerinde veri koruma kurallarının devam eden küresel yakınsamasını mevcut yeterlilik kararlarının sayısının düşük olmasının nedenleri olarak göstermektedir.[596]

4.6.2 Uygun Koruma Önlemlerine Tabi Aktarımlar ile Özel Derogasyonlar

Kolluk Direktifi tarafından düzenlenen üç kademeli yapının diğer iki kademesini Kolluk Direktifi madde 37'de düzenlenen "uygun koruma önlemlerine tabi aktarımlar" ile Kolluk Direktifi madde 38'de düzenlenen "özel durumlar için derogasyonlar" oluşturmaktadır. Kolluk Direktifi madde 36 çerçevesinde Komisyon tarafından alınmış bir yeterlilik kararının bulunmaması halinde, yetkili makamlar, uygun güvencelerin bulunması

[594] Commission Implementing Decision (EU) 2021/1773 of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (notified under document C(2021) 4801), C/2021/4801, OJ L 360, 11.10.2021, s.69–107.
[595] DRECHSLER, LAURA, (2021), s.190.
[596] "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", s.26.

veya bu tür güvencelerin yokluğunda belirli özel durumlar için derogasyonların geçerli olması halinde kişisel verileri üçüncü ülkelere ve uluslararası kuruluşlara aktarabilir.

Kolluk Direktifi madde 37 uyarınca, Komisyon tarafından alınmış bir yeterlilik kararının bulunmaması halinde, üye devlet yetkili makamları, "kişisel verilerin korunmasına ilişkin uygun güvencelerin yasal olarak bağlayıcı bir belgede öngörülmüş olması"[597] veya "kontrolör kişisel verilerin aktarımını çevreleyen tüm koşulları değerlendirmiş ve kişisel verilerin korunmasına ilişkin uygun güvencelerin mevcut olduğu sonucuna varmış olması"[598] durumunda kişisel verileri aktarabilir. Böyle bir öz değerlendirme durumunda, kontrolörün "aktarım kategorileri hakkında" denetim makamını bilgilendirmesi ve denetim makamına "aktarımın tarihi ve saati, alıcı yetkili makam hakkında bilgi, aktarımın gerekçesi ve aktarılan kişisel verileri" içeren belgeleri sağlaması gerekmektedir.[599] Kolluk Direktifi madde 38 kapsamında, yetkili makamlar, yalnızca veri sahibinin belirli menfaatlerini korumak, kamu güvenliğine yönelik acil ve ciddi bir tehdidi önlemek için aktarımın gerekli görülmesi halinde veya veri sahibinin haklarının söz konusu kamu menfaatlerinin önüne geçmediği Kolluk Direktifi madde 1(1)'de belirtilen amaçlara ilişkin münferit durumlarda, bir yeterlilik kararı veya uygun güvenceler gerekliliğinden istisna yapabilir ve kişisel verileri aktarabilir.

Uluslararası anlaşmalar haricinde uygun koruma tedbirlerine ilişkin neredeyse tüm seçeneklerin Komisyon veya denetim makamının iznini gerektirdiği GDPR'nin[600] aksine, Kolluk Direktifi bu tür bir düzenleyici gözetim öngörmemektedir. Ayrıca, GDPR uygun

[597] Kolluk Direktifi madde 36(1)(a). Bu tür yasal olarak bağlayıcı araçlar, örneğin, üye devletler tarafından akdedilen ve hukuk düzenlerinde uygulanan ve veri sahipleri tarafından uygulanabilen, veri koruma gerekliliklerine ve etkili idari veya adli tazminat elde etme hakkı da dahil olmak üzere veri sahiplerinin haklarına uyulmasını sağlayan yasal olarak bağlayıcı ikili anlaşmalar olabilir. Kolluk Direktifi, dibace (71).
[598] Kolluk Direktifi madde 36(1)(b).
[599] Kolluk Direktifi madde 36(2) ve (3).
[600] GDPR madde 46 ve 47.

güvenceler olarak kullanılabilecek somut yasal araçları listelerken[601], Kolluk Direktifi bu tür uygun güvencelerin tam olarak ne olduğu konusunda hiçbir ayrıntı vermemektedir. Uygulamada, Kolluk Direktifi madde 37'deki uygun güvenceler, özel durumlar için derogasyonların sınırlı uygulama alanı ve yukarıda bahsedilen yeterlilik kararlarının eksikliği göz önüne alındığında, üçüncü ülkelere ve uluslararası kuruluşlara aktarım için varsayılan yöntem olarak hizmet etmektedir.[602]

Kolluk Direktifi'nde, üçüncü taraflara aktarıma ilişkin Kolluk Direktifi'ndeki usullerin uygulanmamasına neden olacak bir boşluk bulunmaktadır. Kolluk Direktifi madde 61'e göre, 6 Mayıs 2021 tarihinden önce akdedilmiş kişisel verilerin aktarımına ilişkin uluslararası anlaşmalar değiştirilene, yenilenene veya iptal edilene kadar yürürlükte kalacaktır. Bu durum, bu belgelerde öngörülen veri koruma standartlarının potansiyel yetersizliğine ilişkin açık bir risk oluşturmaktadır. Üye devletlerin, Kolluk Direktifi tarafından belirlenen modern standartlardan önce akdedilmiş olabilecek anlaşmalar temelinde gizli ve hassas kolluk verilerini aktarmaya etmeye devam etmesi, Avrupalı veri sahiplerinin hak ve özgürlüklerinin bu aktarımlar sırasında yeterince korunmasının pek mümkün olmadığı için eleştirilmiştir.[603] Bu risk göz önünde bulundurularak, Avrupa Veri Koruma Kurulu (AVKK) yakın zamanda bir bildiri yayınlamış ve AB mevzuatı, içtihat hukuku ve AVKK rehberliği ile daha fazla uyum sağlanmasının gerekip gerekmediğini belirlemek amacıyla üye devletleri "kişisel verilerin uluslararası transferini içeren uluslararası anlaşmalarını değerlendirmeye ve gerektiğinde gözden geçirmeye" davet

[601] GDPR madde 46(2).
[602] DRECHSLER, LAURA, "The Achilles Heel of EU data protection in a law enforcement context: international transfers under appropriate safeguards in the law enforcement directive.", Cybercrime: New Threats, New Responses (Proceedings of the XVth International Conference on Internet, Law & Politics, Universitat Oberta de Catalunya, Barcelona, 1-2 July, 2020), 2020, s.54.
[603] VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, (2022), s.84; DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, (2016), s.15; DRECHSLER, LAURA, (2020), s.56.

etmiştir.[604] AVKK tarafından Kolluk Direktifi madde 37'nin nasıl uygulanması gerektiğine açıklık getiren kılavuz ilkeler yayınlanmıştır.[605] Kılavuz ilkeler, üçüncü ülkelere veya uluslararası kuruluşlara veri aktarımı için gerekli olan "uygun güvencelere" ilişkin yasal standarda odaklanmaktadır. AVKK, uygun güvencelerin yeterlilik kararlarıyla aynı standartta tutulmasını yani bu tür transferlerin AB içinde olduğu gibi esasen eşdeğer bir veri koruma seviyesi sağlaması gerektiğini vurgulamaktadır.[606] Üye devletler bu kılavuz ilkeler ışığında Kolluk Direktifi madde 37'yi uygulayacaktır.

4.6.3 Özel Alıcılara ve Kolluk Dışı Kurumlara Yapılan Aktarımlar

Genel kural olarak, yetkili makamlar kişisel veri aktarımlarını kolluk kuvvetleri veya ceza adaleti yetkisi olan alıcılarla sınırlandırmalıdır. Bunun nedeni, kolluk verilerinin genellikle hassas ve son derece gizli olması nedeniyle özel kuruluşlarla veya kolluk olmayan kamu kurumlarıyla paylaşılmasının engellemesidir.[607] Üçüncü taraflara aktarımlarla ilgili olarak, bu ilke Kolluk Direktifi 35(1)(b) maddesinde açık bir şekilde ortaya konulmuştur. Bununla birlikte, istisnai durumlarda, yetkili makamlar, kişisel verilerin üçüncü ülkelerdeki yetkili olmayan alıcılarla paylaşılmasının, yakın bir tehdidi önlemek veya cezai bir suça yanıt vermek için veri sahibinin haklarına müdahaleyi gerektiren bir kamu yararı için gerekli olduğunu belirleyebilir. Kolluk Direktifi Bölüm V'in en yenilikçi hükmü olarak görülen madde 39, AB üye devletlerindeki kolluk kuvvetlerinin doğrudan üçüncü ülkelerdeki özel tarafların veri talepleri için veri koruma çerçevesi sağlamaktadır.[608] Kolluk Direktifi madde

[604] European Data Protection Board, Statement 04/2021 on international agreements including transfers, Adopted on 13 April 2021.
[605] European Data Protection Board, Guidelines 01/2023 on Article 37 Law Enforcement Directive Version 2.1 Adopted on 19 June 2024.
[606] European Data Protection Board, Guidelines 01/2023 on Article 37 Law Enforcement Directive Version 2.1 Adopted on 19 June 2024, s.3.
[607] VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, (2022), s.87.
[608] SAJFERT, JURAJ ve QUINTEL, TERESA, (2017), s.19.

39 kapsamında, kişisel verilerin kolluk kuvvetleri tarafından üçüncü ülkelerdeki yetkili olmayan alıcılara (kolluk kuvvetleri veya ceza adaleti yetkisi olmayan kuruluşlar) "münferit ve özel durumlarda" aktarılmasına ilişkin kuralları belirlemektedir. Kolluk Direktifi'nin 39'uncu maddesinin uygulanabilmesi için, Kolluk Direktifin diğer tüm koşullarının yerine getirilmesi gerekmektedir. Bu tür transferler için yasal dayanak AB veya üye devlet hukukunda ortaya konmalı ve yukarıda açıklanan kademelendirme doğrultusunda madde 36 kapsamında bir yeterlilik kararı, madde 37 uyarınca uygun güvenceler veya madde 38'den bireysel bir derogasyon mevcut olmalıdır. Buna ek olarak, belirli bir suçun soruşturulması için kesinlikle gerekli olmalıdır. Bu gereklilik, aktaran makamın ana görevleri ile kişisel verilerin aktarılması gerekliliği arasında güçlü bir bağ olmasını gerektirmektedir. Veri sahibinin temel hak ve özgürlükleri, aktarımın gerçekleştirildiği amaçlar için kamu yararının önüne geçemez ve hizmet sağlayıcılar aktarılan verilerin işlenebileceği amaçlar hakkında bilgilendirilmelidir.[609]

Komisyon Uzman Grubu tarafından da belirtildiği üzere[610], Kolluk Direktifi madde 39 üçüncü ülkelerde yetkili olmayan alıcılara aktarım yapılmasına izin verme zorunluluğu getirmemektedir. Bunun yerine, üye devletlerin kendi yetkili makamlarının bu tür aktarımlarda bulunmasına izin vermeleri durumunda sadece bir dizi asgari standart sağlamaktadır. Her ne kadar doğası gereği isteğe bağlı olsa da bu durum yine de ulusal bir yasal dayanağın varlığına ilişkin belirsizlik yaratabilir.[611]

[609] Kolluk Direktifi madde 39(1).
[610] Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 7 Kasım 2016,
[611] MARQUENIE, THOMAS, (2017), s.336.

4.7 Bağımsız Denetim Makamları

4.7.1 Bağımsız Statü

Bağımsız denetim makamları, ilk günlerinden itibaren Avrupa veri koruma düzenlemelerinin merkezinde yer almaktadır. Kolluk Direktifi de bu anlayış ile kişisel verilerin en üst seviyede korumasını ve Kolluk Direktifi'nin ortaya koyduğu düzenlemelerin uygulanmasını sağlamak amacıyla, yasal uyumluluğu izlemek ve uygulamak için kilit bir önlem olarak bağımsız denetim makamlarını tanıtmaktadır.[612] ABAD'ın *Schrems*[613] kararında da teyit ettiği üzere, bu kurumlar tarafından yerine getirilen denetim faaliyeti, veri koruma hakkının kritik bir yönü ve veri sahiplerinin menfaat ve özgürlüklerinin korunması için vazgeçilmez olarak kabul edilmektedir.[614] Denetim makamlarının kendisine verilen görevleri etkili bir şekilde yerine getirebilmelerini sağlamak amacıyla, Kolluk Direktifi bu makamların kuruluşu, bağımsızlığı ile yetki ve sorumluluklarına ilişkin kuralları belirlemiştir.

Öncelikle Kolluk Direktif ile üye devletlere "işleme faaliyetine ilişkin olarak gerçek kişilerin temel hak ve özgürlüklerini korumak ve AB içerisinde kişisel verilerin serbestçe akışını kolaylaştırmak amacıyla, bu Direktif'in uygulanmasının izlenmesinden sorumlu olacak" bağımsız denetim makamı oluşturma yükümlülüğü getirilmektedir.[615] Ancak Kolluk Direktifi üye devletlerin hem GDPR hem de Kolluk Direktifi için yetkili olan tek bir denetim makamı kurmasına izin vermektedir.[616] Denetim makamları tam bir bağımsızlık içinde hareket etmelidir ve tam bağımsızlıklarının nasıl sağlanacağına ilişkin hükümler (üyelerinin

[612] DE HERT, PAUL ve SAJFERT, JURAJ, (2018), s.243.
[613] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, paras 40-44.
[614] CARUANA, MIREILLE M., (2017), s.9.
[615] Kolluk Direktifi madde 41(1).
[616] Kolluk Direktifi madde 41(3).

bağımsızlığı, personel, yeterli bütçe vb. dahil olmak üzere) GDPR ile aynıdır.[617] Kolluk Direktifi madde 42, denetim makamlarının tüm dış etkilerden ari olmalarını ve dış kaynaklardan talimat almamalarını gerektirmektedir. Ayrıca, görevlerini etkin bir şekilde yerine getirebilmeleri için yeterli kaynaklara sahip olmaları ve kendi personellerini seçmekte özgür olmaları gerekmektedir. Ayrıca, üyeleri birbiriyle bağdaşmayan işlerle uğraşmamalı, görevlerini etkin bir şekilde yerine getirebilmeleri için yeterli kaynak sağlanmalı ve kuruluşların tabi olduğu herhangi bir mali kontrol bağımsız yapılarını etkilememelidir. Bu hükümlerin iç hukuka aktarılması incelendiğinde, bu gerekliliklerin ulusal yasal çerçevelere tam olarak dahil edildiği görülmektedir. Komisyon'un Kolluk Direktifi'ne ilişkin ilk raporunda, tüm üye devletlerin Kolluk Direktifi'ni iç hukuka aktaran yasalarında denetim makamları için bağımsızlık koşulunu öngördükleri kaydedilmiştir.[618]

Tam bağımsızlık gerekliliği, denetim makamlarının belirli bir temel hakkın koruyucusu olarak kararları üzerinde etkisi olabilecek herhangi bir yönlendirme veya her ne şekilde olursa olsun başka bir dış etkiden bağımsız olarak görevlerini yerine getirmelerine izin vermelidir. Denetim makamlarının görevlerini etkili bir şekilde yerine getirebilmeleri için, bağımsız bir şekilde faaliyet göstermeleri hayati önem taşımaktadır.[619] ABAD'ın *Komisyon/Almanya*[620] kararında, ABAD denetim makamlarının "tam bağımsızlık" kavramını tanımlamış ve bunun denetim makamlarının görevlerini yerine getirmelerini sorgulayabilecek doğrudan veya dolaylı herhangi bir yönlendirmeyi veya başka bir dış etkiyi

[617] Kolluk Direktifi madde 42, GDPR madde 52.
[618] "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", s.11.
[619] DE HERT, PAUL ve SAJFERT, JURAJ, (2018), s.248.
[620] Case C–518/07, *European Commission v Federal Republic of Germany*, [2010], ECLI:EU:C:2010:125.

engellemek olduğunu ifade etmiştir.[621] Ayrıca ABAD tarafından *Komisyon/Avusturya*[622] kararında, "işlevsel bağımsızlığın" tek başına dış etkinin yokluğunu garanti etmek için yeterli olmadığı belirtilmiş ve Avusturya veri koruma otoritesinin, yönetici üyesinin aynı zamanda hiyerarşik olarak daha üst bir pozisyonda bulunan bir federal yetkili olması nedeniyle tamamen bağımsız olarak değerlendirilemeyeceğine karar vermiştir.[623]

Uygulamada denetim makamlarının, kolluğun işleyişinin gözetiminin genellikle aynı denetim makamı içindeki farklı organlar tarafından gerçekleştirildiği göz önüne alındığında, tam ve gerçek bir bağımsızlık elde etmesinin özellikle kolluk bağlamında zor olabileceği değerlendirilmektedir. Ayrıca CKKAİ alanının kendine özgü doğası nedeniyle, denetim makamlarının bu alandaki kurumlarla yakın çalışamaması veya bu kurumlardan personel alamaması halinde kolluk faaliyetleri konusunda gerekli uzmanlığı elde etmesi zor olacağından bu durum denetim makamının görevini yetirmesinde zorluklara yol açabilecektir.[624] Kolluk bağlamında denetim makamlarının bağımsızlığına ilişkin ilave bir endişe nedeni de yeterli kaynağın sağlanıp sağlanamaması ile ilgilidir. Bu makamların bağımsız olmaları tek başına yeterli olmayıp, görevlerini layıkıyla yerine getirebilmeleri için gerekli kaynaklara, altyapıya, insan gücüne ve finansmana da sahip olmaları gerekmektedir. Bu husus, Komisyon'un Kolluk Direktifi'ne ilişkin ilk raporunda da vurgulanmış, ancak aynı raporda Kolluk Direktifi ile ilgili sorumlulukların ulusal denetim makamları arasında genellikle bir öncelik olmadığı sonucuna varmış ve bunların çoğunun Kolluk Direktifi

[621] Case C–518/07, *European Commission v Federal Republic of Germany*, [2010], ECLI:EU:C:2010:125, para 30.
[622] Case C-614/10, *European Commission v Republic of Austria*, [2012], ECLI:EU:C:2012:631.
[623] Case C-614/10, *European Commission v Republic of Austria*, [2012], ECLI:EU:C:2012:631, paras 42-50.
[624] MARQUENIE, THOMAS, (2017), s.335; DRECHSLER, LAURA, (2020), s.102.

kapsamında görevlerini yerine getirmek için yeterli kaynak ve uzmanlıktan yoksun olduklarını belirtmiştir.[625]

4.7.2 Yetki Kapsamı, Görev ve Yetkiler

Kolluk Direktifi'nin 45 ila 47'inci maddeleri denetim makamlarının yetki kapsamını, görevlerini ve yetkilerini düzenlemektedir. Kolluk Direktifi madde 45(1), her denetim makamının kendi ülkesinde Kolluk Direktifi uyarınca kendisine verilen görevlerin yerine getirilmesi ve verilen yetkilerin kullanılması konusunda yetkili olacağını öngörmektedir. Kolluk Direktifi madde 45(2) uyarınca, adli sıfatıyla mahkemelerin kişisel verileri işleme faaliyeti denetim makamlarının yetki kapsamı dışında kalmaktadır. Bu istisnanın gerekçesi Kolluk Direktifi'nin dibacesinde "hakimlerin yargısal görevlerini yerine getirirken bağımsızlıklarını korumak amacıyla" şeklinde açıklanmaktadır.[626] Buna ek olarak, Kolluk Direktifi Üye Devletlerin "adli sıfatıyla hareket eden diğer bağımsız adli makamların" da denetim makamının yetki kapsamı dışında bırakabileceğini düzenlenmektedir. Pek çok "diğer adli makam" bağımsız olarak nitelendirilmeyeceğinden, bu seçenek kısıtlayıcı bir şekilde yorumlanmalıdır. Üye devletlerin gelenekleri ve ceza hukuku sistemlerindeki farklılıklar nedeniyle, bu isteğe bağlı muafiyet, hakimlerle aynı bağımsız statüye sahip ulusal makamların (örneğin savcılar) ihtiyaçlarını karşılamaktadır.[627] Üye devletlere bırakılan bu takdir yetkisi, özellikle üye devletlerin yargı sistemlerindeki önemli farklılıklar göz önünde bulundurulduğunda, savcıların ne zaman ve ne ölçüde "bağımsız yargı makamları" oldukları

[625] "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", s.21.
[626] Kolluk Direktifi, dibace (80).
[627] DE HERT, PAUL ve SAJFERT, JURAJ, (2018), s.249.

ve faaliyetlerinin ne zaman ve ne ölçüde "yargı faaliyetleri" teşkil ettiği her zaman net olmadığı için eleştirilmiştir.[628]

Kolluk Direktifi madde 46 denetim makamlarının görevlerini düzenlemektedir. Bu kapsamda, her üye devlet, ulusal denetim makamının bir dizi görevi yerine getirmesini sağlamalıdır. Bunlar arasında Kolluk Direktifi'nin uygulanmasının izlenmesi ve uygulanması[629], veri koruma hakları ve yükümlülüklerine ilişkin kamu ve kurumsal farkındalığın teşvik edilmesi[630], kişisel verilerin korumasına ilişkin düzenlemeler hakkında ulusal kurumlara tavsiyelerde bulunulması[631], şikayetlerin ele alınması ve soruşturulması[632], veri işlemenin yasallığının kontrol edilmesi ve diğer denetim makamlarıyla işbirliği yapılması[633] yer almaktadır. Ayrıca, veri korumayı etkileyen teknolojideki gelişmeleri takip etmeli, belirli işleme faaliyetlerine ilişkin rehberlik sağlamalı ve AVKK'nın çalışmalarına katkıda bulunmalıdırlar.[634] Yetkili makamların elektronik ortam da dahil olmak üzere şikayet başvurularını kolaylaştırması ve hizmetlerini veri sahiplerine ve veri koruma görevlilerine ücretsiz olarak sunması gerekmektedir[635]; ancak tekrar eden veya açıkça temelsiz talepler söz konusu olduğunda makul bir idari ücret uygulanabilir veya yetkili makamın bu kararı gerekçelendirebilmesi koşuluyla talep reddedilebilir.[636]

Denetim makamlarının görevlerine ilişkin olarak, Kolluk Direktifi kapsamında GDPR'de olduğundan daha az sorumluluğu olduğu açıktır.[637] Eksik görevlerin çoğu CKKAİ

[628] CARUANA, MIREILLE M., (2017), s.10.
[629] Kolluk Direktifi madde 46(1)(a).
[630] Kolluk Direktifi madde 46(1)(b) ve (d).
[631] Kolluk Direktifi madde 46(1)(c).
[632] Kolluk Direktifi madde 46(1)(f) ve (i).
[633] Kolluk Direktifi madde 46(1)(g) ve (h).
[634] Kolluk Direktifi madde 46(1)(j), (k) ve (l).
[635] Kolluk Direktifi madde 46(3).
[636] Kolluk Direktifi madde 46(4).
[637] GDPR kapsamında denetim makamının görevleri için bkz. GDPR madde 57.

alanı ile ilgisi olmayan hükümlere karşılık geldiği için haklı görülebilirken, Kolluk Direktifi madde 46(1)(g) GPDR'de bulunmayan ve denetim makamının veri işleme faaliyetlerinin hukuka uygunluğunu veri sahipleri adına ve veri sahiplerinin talebi üzerine gözden geçirmesini gerektiren ek bir ödev getirerek kolluk ve ceza adaleti alanına özgü bazı görevler belirleyerek bunu bir şekilde telafi etmektedir.[638] Bu doğrultuda, Kolluk Direktifi kapsamında denetim makamının pozisyonunun GDPR'ye kıyasla muhtemelen daha zayıf görünmesine rağmen, doğası gereği hala "oldukça güçlü" olduğunu düşünülmektedir.[639]

Kolluk Direktifi madde 47'ye göre Üye Devletler, denetim makamlarının, soruşturma için etkili yetkilere[640], etkili düzeltici yetkilere[641] ve etkili tavsiye yetkilerine[642] sahip olmasını sağlamalıdır. Denetim makamlarının yetkilerini kullanması etkili yargı yolu ile güvence altına alınmalıdır.[643] Ayrıca denetim makamlarının Kolluk Direktifi'nin ihlali hâlinde yasal işlem başlatma veya müdahil olma yetkisinin bulunması yasayla sağlanmalıdır.[644]

Kolluk Direktifi madde 47 ile denetim makamlarına verilen yetkiler GDPR'deki muadili olan madde 58'de listelenen yetkilerle uyumlu değildir. GDPR madde 58 uzun bir yetki listesi sıralarken, Kolluk Direktifi madde 47 nispeten sınırlıdır ve açık bir gerekçe olmaksızın bazı yetkiler vermemektedir. Örneğin, GDPR'nin aksine, Kolluk Direktifi, veri sahibinin taleplerine uyulmasını emretme ve idari para cezaları uygulama yetkisini atlayarak denetim makamının düzeltici yetkilerini önemli ölçüde kısıtlamaktadır. Ayrıca üçüncü bir ülkedeki bir alıcıya veya uluslararası bir kuruluşa veri akışını askıya alma yetkisi de Kolluk

[638] VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, (2022), s.93.
[639] DRECHSLER, LAURA, (2020), s.102.
[640] Kolluk Direktifi madde 47(1).
[641] Kolluk Direktifi madde 47(2).
[642] Kolluk Direktifi madde 47(3).
[643] Kolluk Direktifi madde 47(4).
[644] Kolluk Direktifi madde 47(5).

Direktifi'nde yer almamaktadır. Bu eksiklikler, GDPR ile kıyaslandığında Kolluk Direktifi kapsamındaki denetim makamlarının "göreceli zayıflığı" ile sonuçlandığı şeklinde yorumlanmıştır.[645]

Denetim makamları ile ilgili hükümlerin Kolluk Direktifi ve GDPR'de bu kadar farklı bir şekilde düzenlenmiş olması genel olarak eleştirilmiştir. Örneğin AVKD, GDPR ve Kolluk Direktifi kapsamında "veri koruma otoritelerine verilen yetkiler arasında ayrım yapmaya gerek olmadığını" savunmuştur. Denetimin veri koruma hakkının hayati bir yönü olduğuna dikkat çekerek, denetimin seviyesi ve yoğunluğunun veri işlemenin gerçekleştiği sektöre bağlı olmaması gerektiğini ileri sürmüştür.[646] Bu görüş Madde 29 Çalışma grubu tarafından da paylaşılmıştır.[647] Ayrıca kolluk faaliyetleri bireysel veri koruma hakları ve toplumsal özgürlükler üzerinde önemli bir etkiye sahip olduğundan, kolluğun faaliyetleri çerçevesinde kişisel verileri işlemesinin güçlü bir şekilde denetlenmesinin tartışmasız diğer devlet kurumlarının faaliyetlerinden daha önemli olduğu değerlendirilmektedir.[648]

4.8 Hukuki Yollar, Sorumluluk ve Yaptırımlar

Kolluk Direktifi, CKKAİ alanında verilerin işlenmesi bağlamında veri sahiplerinin haklarının etkili bir şekilde korunmasını sağlamak için kapsamlı bir çerçeve sunmaktadır. Kolluk Direktifi madde 52, kişisel verilerinin hukuka aykırı bir şekilde işlendiğini düşünen bireylerin, konuyu soruşturması ve şikayet sahibini hem prosedür hem de sonuç hakkında bilgilendirmesi gereken bağımsız bir denetim makamına şikayette bulunmalarına izin vermektedir. Buna ek olarak, Kolluk Direktifi madde 53 ve 54 veri sahiplerinin sadece

[645] CARUANA, MIREILLE M., (2017), s.15.
[646] European Data Protection Supervisor (EDPS), "Opinion 6/2015 – a further step towards comprehensive EU data protection: EDPS recommendations on the Directive for data protection in the police and justice sectors", 28 October 2015. s.8.
[647] Article 29 Data Protection Working Party, "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)", WP258, 29 Kasım 2017, s.30.
[648] CARUANA, MIREILLE M., (2017), s.11.

denetim makamlarına karşı değil aynı zamanda veri kontrolörleri ve işleyicilerine karşı da yargı yoluna başvurma hakkını garanti altına almaktadır. Bu, şikayetler üzerine harekete geçmeyi reddetmeleri veya yaptırım yetkilerini kullanmaları da dahil olmak üzere, bu kuruluşlar tarafından alınan kararlar için yargı denetimine erişim sağlar. Kolluk Direktif madde 55, kamu yararına çalışan kâr amacı gütmeyen kuruluşların bireyler adına hareket etmesini sağlayarak veri sahibi haklarını daha da güçlendirmektedir. Bu hüküm, bireyleri haklarını aramaktan caydırabilecek idari ve usuli yüklerin hafifletilmesi açısından özellikle önemlidir.

Hukuka aykırı işleme durumunda, Kolluk Direktifi madde 56, üye devletlerin hem maddi hem de manevi zararlar için tazminat ödemesini gerektirmektedir. Ayrıca, Kolluk Direktifi madde 57 uyarınca, veri koruma kurallarının ihlalinden sorumlu olan hem bireyler hem de tüzel kişiler için etkili, orantılı ve caydırıcı yaptırımlar uygulamalıdırlar. Bu hükümler toplu olarak, erişilebilir hukuk yollarını, üçüncü taraf temsilini ve katı hesap verebilirlik önlemlerini bir araya getirerek veri sahibi haklarının uygulanmasını güçlendirmekte ve böylece Kolluk Direktifi'nin uygulanmasında şeffaflığı ve yasal kesinliği artırmaktadır.[649]

4.9 Değerlendirme

Kolluk Direktifi, CKKAİ alanında kişisel verilerin korunmasında önemli bir ilerlemeyi temsil etmektedir. Kendinden önceki kişisel verilerin korunmasına ilişkin yasal araçlar üzerine inşa edilen Kolluk Direktifi, kolluk kuvvetleri ve adli makamlar tarafından gerçekleştirilen hem sınır ötesi hem de yerel kişisel veri işleme faaliyetleri için veri koruma güvencelerini tek bir belgede bir araya getiren ilk AB yasal aracıdır. Bunu yaparken, yüksek

[649] CARUANA, MIREILLE M., (2017), s.15.

standartlardan oluşan sağlam bir çerçeve oluşturmuş ve veri sahibi haklarının korunması ve kullanılmasına güçlü bir vurgu yapmıştır. Kolluk Direktifi, kişisel verilerin korunması hakkına güçlü bir şekilde odaklanan kapsamlı bir çerçeve oluşturmakta ve genel veri koruma ilkelerine bağlılık, veri sahiplerinin güçlendirilmesi, yetkili makamlara getirilen yükümlülükler, kişisel verilerin üçüncü ülke alıcılarına aktarılması ve bu normlara yasal uyumun bağımsız denetimi ile ilgili benzer ilkeleri içeren GDPR'den büyük ölçüde yararlanmaktadır.

Kolluk Direktifi ile kaydedilen ilerlemeler övgüye değer olmakla birlikte, Kolluk Direktifi'nin etkinliği, güvenilirliği ve gücü yine de çeşitli eksiklikler nedeniyle engellenmektedir. Bir Tüzük yerine bir Direktifin tercih edilmesi, veri koruma standartlarına yönelik çok sayıda farklı yaklaşımın ortaya çıkmasına dolayısıyla bazı durumlarda yasal belirsizliğin devam etmesine neden olmuştur. Bu durum, kilit kavramların ulusal yoruma tabi kalması ve dolayısıyla kamu güvenliği, cezai suç ve yetkili makam gibi kritik kavramların son derece tutarsız uygulamalarına yol açması nedeniyle daha da kötüleşmektedir.

GDPR'de mevcut olan bazı genel ilkelerin eksikliğinden ve kişisel verilerin yeniden kullanımı, depolanması ve kategorize edilmesine ilişkin muğlak hükümlerin ve tutarsız bir şekilde uygulanan hükümlerin etkisinden kaynaklanan sorunlar da gözlemlenmiştir. Veri sahibi haklarının kullanılmasına ilişkin olarak, özellikle üye devletlerin bu bağlamda sahip olduğu geniş takdir yetkisi göz önünde bulundurulduğunda, belirli sorumlulukların bulunmaması ve belirli hakların kullanılması ve kısıtlanmasına ilişkin bazı hükümlerin kusurlu bir şekilde aktarılması konusunda endişeler dile getirilmiştir.

Ayrıca, kontrolörlere getirilen somut yükümlülükler, GDPR'deki muadillerine kıyasla genellikle eksiktir, farklı ulusal uygulamalar ve pratik zorluklarla karşı karşıyadır ve yetkili makamlara sağlanan somut rehberliğin yokluğundan muzdariptir. Bu durum özellikle

müşterek kontrolörlük, veri koruma etki değerlendirmeleri ve işleme faaliyetlerinin kayıt altına alınmasına ilişkin hükümlerde dikkat çekmektedir. Üçüncü taraflara yapılan aktarımlara gelince, yeterlilik kararlarının eksikliği AB'nin temel haklarının AB sınırları ötesinde korunmasını zayıflatma riski taşımaktadır. Veri koruma standartlarını karşılama olasılığı düşük mahiyetteki önceden var olan kişisel verilerin aktarımına ilişkin anlaşmalara güvenmeye devam edilmesi ve kapsamlı bir rehberlik olmaksızın karmaşık yeterlilik ve yeterli koruma konularının çözümünden üye devletlerin yetkili makamlarının sorumlu tutulmasıyla ilişkili riskler bu durumu daha da kötüleştirmektedir.

Kolluk Direktifi'nce, üye devletlere, mahkemeler ve adli makamlar tarafından gerçekleştirilen işleme faaliyetlerine uyulup uyulmaması konusunda geniş bir takdir yetkisi tanınmış olması, bu tür makamların denetim makamının denetiminden kaçınması gibi bir risk oluşturabilecektir. Bu sorunlar, Kolluk Direktifi'nin Avrupa veri koruma çerçevesine yaptığı önemli katkıları geçersiz kılmasa da yasal kesinlik ve AB veri sahiplerinin hak ve özgürlüklerine zarar verecek şekilde gücünü ve tutarlılığını zayıflatma riski taşımaktadır.

SONUÇ

CKKAİ alanında kişisel verilerin korunması, AB içerisinde derin bir evrim geçirmiştir. Bu evrim, AB'nin daha geniş kapsamlı yasal, kurumsal ve normatif gelişiminin yanı sıra dijital teknolojilerin artan önemine, sınır ötesi kolluğa ve kamu güvenliği amacıyla kişisel verilere artan bağımlılığa verdiği yanıtı yansıtmaktadır.

Bu tezin ilk bölümü, 2009 yılında Lizbon Antlaşması'nın yürürlüğe girmesinden önce, AB'nin kolluk kuvvetleri bağlamında veri koruma yaklaşımının parçalı ve kurumsal olarak kısıtlı olduğunu göstermiştir. Maastricht Antlaşması'nın Üçüncü Sütunu altında faaliyet gösteren CKKAİ alanı büyük ölçüde hükümetlerarası kalmış, bu da sınırlı ulusüstü gözetim, eşit olmayan uygulama ve bireysel hakların zayıf uygulanabilirliği ile sonuçlanmıştır. Avrupa Konseyi'nin 108 sayılı Sözleşmesi ve R(87)15 sayılı Tavsiye Kararı gibi ilk araçlar, CKKAİ alanında veri koruma için önemli normatif temeller atmış ancak üye devletler arasında tek tip uygulamayı garanti etmek için gerekli bağlayıcı güçten yoksun kalmıştır. Veri Koruma Direktifi iç pazarda sağlam bir veri koruma çerçevesi getirirken, kolluk faaliyetlerini kapsam dışında bırakmıştır. 2008/977 sayılı Çerçeve Karar'ın kabul edilmesi, AB'nin bu boşluğu gidermek için ilk girişimi olmuş, bununla birlikte, hükümetlerarası niteliği, sınırlı uygulama mekanizmaları ve genel veri koruma ilkeleri ile tutarlı olmaması, uygulamada büyük ölçüde etkisiz kalmasına neden olmuştur.

İkinci bölüm, Lizbon Antlaşması'nın AB veri koruma hukukunun evriminde, özellikle de CKKAİ alanında nasıl belirleyici bir dönüm noktası olduğunu göstermiştir. Lizbon Antlaşması sütunlu yapıyı ortadan kaldırarak ve kolluk ve adli işbirliğini AB'nin olağan yasama usulleri altına alarak, daha fazla yasal tutarlılık, demokratik hesap verebilirlik ve adli gözetim sağlamıştır. Lizbon Antlaşması ile ABTHŞ'nin birincil hukuk statüsüne çıkarılması ile yasal olarak bağlayıcı bir güç kazanması, AB'nin kişisel verilerin temel bir

hak olarak korunması konusundaki kararlılığını daha da pekiştirmiştir. Lizbon Antlaşması sonrası bu bağlamda, CKKAİ alanındaki yetkili makamlar tarafından kişisel verilerin işlenmesini özel olarak düzenlemek üzere Kolluk Direktifi kabul edilmiştir. GDPR'yi tamamlayan Kolluk Direktifi, uyumlaştırılmış kurallar, daha güçlü güvenceler, bağımsız denetim makamları ve bireyler için uygulanabilir haklar getirmiştir. Ayrıca, ABAD, her ne kadar bu alana ilişkin içtihat hukukunu yeni oluşturmaya başlamış olsa da Kolluk Direktifi'nin uygulanmasına ilişkin yol gösterici rol oynamaktadır.

Kolluk Direktifi, AB'nin iç hukuk düzeninin ötesinde aynı zamanda CKKAİ alanında AB ile daha yakın işbirliği arayışında olan devletler için de bir ölçüt oluşturmaktadır. AB ile adli ve güvenlik işbirliğini derinleştirmeyi uzun zamandır arzulayan ve terörizm, organize suçlar ve düzensiz göç gibi sınır aşan tehditlerle mücadelede kilit bir ortak olmaya devam eden Türkiye için, AB'nin veri koruma standartlarına uyum stratejik bir gereklilik haline gelmiştir. Kolluk Direktifi, Türkiye'nin vatandaşlarına Schengen Bölgesi içerisinde vizesiz seyahat hakkı tanınması için yerine getirmesi gereken 72 kriterin ana hatlarını belirleyen AB-Türkiye Vize Serbestisi Diyaloğu bağlamında da doğrudan ilgilidir. Kilit kriterlerden biri, özellikle adli ve kolluk işbirliği bağlamında, kişisel verilerin yeterli düzeyde korunmasının sağlanmasıyla ilgilidir. AB, vize serbestisi konusunda kaydedilen ilerlemeyi, bağımsız bir veri koruma otoritesinin kurulması ve veri sahiplerinin haklarına yönelik güvenceler de dâhil olmak üzere, Türkiye'de Kolluk Direktifi ile uyumlu mevzuatın kabul edilmesine açıkça bağlamıştır.[650] Bu haliyle Kolluk Direktifi, sadece AB hukukunun iç tutarlılığını güçlendirmekle kalmamakta, aynı zamanda AB'nin dış ilişkileri için siyasi ve hukuki bir referans noktası olarak işlev görmekte ve daha geniş işbirliği anlaşmalarının bir parçası

[650] "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", s.28.

olarak veri koruma standartlarının teşvik edilmesinde AB'nin normatif gücünü pekiştirmektedir.

Bu tez, yasal-tarihsel ve analitik bir yaklaşımla, CKKAİ çerçevesinde kişisel verilerin korunmasına yönelik birleşik, hak temelli ve uygulanabilir bir AB rejiminin kademeli olarak ortaya çıkışının izini sürmeye çalışmıştır. Parçalı yasal çerçevelerden ve hükümetlerarası koordinasyondan ulusüstü bir yasal düzene geçiş, yalnızca dijital çağda veri korumanın artan önemini değil, aynı zamanda AB'nin hukukun üstünlüğünü destekleme, temel hakları koruma ve üye devletler arasında karşılıklı güveni artırma yönündeki daha geniş arzusunu da yansıtmaktadır. Sonuç olarak, AB'nin veri koruma rejiminin CKKAİ çerçevesinde kişisel verilerin korunması bağlamında geçirdiği evrim, AB'nin kamu güvenliği ile bireysel hakların korunması zorunluluklarını dengeleyerek yasal mimarisini çağdaş zorluklara uyarlama becerisini örneklemektedir.

KAYNAKÇA

KİTAP

BACHE, IAN, GEORGE, STEPHAN ve BULMER, SIMON, *Politics in the European Unıon*, 3th Edition, Oxford University Press, Oxford, 2011.

BAYKAL, SANEM ve GÖÇMEN, İLKE, *Avrupa Birliği Kurumsal Hukuku*, 1.Baskı, Seçkin Yayıncılık, Ankara, 2016.

BLASI CASAGRAN, CRISTINA, *Global Data Protection in the Field of Law Enforcement: An EU Perspective*, Routledge Taylor & Francis Group, London, 2018.

BOEHM, FRANZISKA, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Springer Science & Business Media, Heidelberg, 2012.

CRAIG PAUL ve DE BÚRCA GRAINNE, *Eu Law: Text. Cases, and Materials*, 7th Edition, Oxford University Press, Oxford, 2020.

FIJNAUT, CYRILLE, *A Peaceful Revolution: The Development of Police and Judicial Cooperation in the European Union*, Cambridge: Intersentia, 2019.

FUSTER, GLORIA GONZÁLEZ, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer Science & Business, 2014.

GÖÇMEN, İLKE, *Avrupa Birliği Hukukunda Direktiflerin Bireyler Arasındaki İlişkilere Etkileri*, Yetkin Yayınevi, Ankara, 2008.

HIJMANS HIELKE, *The European Union as Guardian of Internet Privacy; The Story of Art 16 TFEU*, Springer International Publishing, Switzerland, 2016.

LYNSKEY, ORLA, *The Foundations of EU Data Protection Law*, 1st Edition, Oxford University Press, Oxford, 2015.

MITSILEGAS, VALSAMIS, *EU Criminal Law*, 2th Edition, Hart Publishing, Oxford, 2022.

MITSILEGAS, VALSAMIS, *Eu Criminal Law After Lisbon: Rights, Trust and the Transformation of Justice In Europe*, Hart Publishing, Oxford, 2016.

ÖZCAN, MEHMET, *Avrupa Birliği Sığınma Hukuku - Ortak Bir Sığınma Hukukunun Ortaya Çıkışı*, 1.Baskı, USAK Yayınları, İstanbul, 2005.

PEERS, STEVE, *EU Justice and Home Affairs Law Volume II: EU Criminal Law, Policing, and Civil Law*, 5th Edition, Oxford University Press, Oxford, 2023

RIPOLL SERVENT, ARIADNA, *The European Parliament*, 1st Edition, Palgrave and Macmillan, London, 2018.

KİTAP BÖLÜMÜ/MAKALE

ARAT, TUĞRUL *et.al.*, "Avrupa Bütünleşmesi: 1957 – 1993 Arası", AKÇAY, BELGİN ve GÖÇMEN, İLKE (Eds.), *Avrupa Birliği: Tarihçe, Teoriler, Kurumlar ve Politikalar*, 3.Baskı, Seçkin Yayıncılık, Ankara, 2016, s.59-82.

BAYKAL, SANEM ve GÖÇMEN, İLKE, "Avrupa Birliği Hukukunun Kaynakları Bakımından Normlar Hiyerarşisi", *Prof Dr Erdal Onar'a Armağan*, Ankara Üniversitesi Basımevi, 2013, s.317-365.

BAYKAL, SANEM ve GÖÇMEN, İLKE, "Avrupa Bütünleşmesi: 1993 Sonrası", AKÇAY, BELGİN ve GÖÇMEN, İLKE (Eds.), *Avrupa Birliği: Tarihçe, Teoriler, Kurumlar ve Politikalar*, 3.Baskı, Seçkin Yayıncılık, Ankara, 2016, s.83-110.

BAYKAL, SANEM, "Reform Antlaşması ve Getirdikleri: Kurumsal Yapı Çerçevesinde Genel Bir Değerlendirme", Ankara Avrupa Çalışmaları Dergisi, Cilt:7, No:1, 2007.

BAYKAL, SANEM, "Temel Haklar", AKÇAY, BELGİN ve ÖZÇELİK, GÜLÜM BAYRAKTAROĞLU (Eds.), *Lizbon Antlaşması Sonrası Avrupa Birliği: Serbest Dolaşım ve Politikalar*, 2.Baskı, Seçkin Yayıncılık, Ankara, 2012, s.383-412.

BOEHM, FRANZISKA, "Information Sharing in the Area of Freedom, Security and Justice—Towards a Common Standard for Data Exchange Between Agencies and EU Information Systems", GUTWİRTH, SERGE, *et.al.*, *European data protection: in good health?*, Springer Science & Business Media, 2012, s.143-183.

BOSTANCI BOZBAYINDIR, GÜLŞAH, "Avrupa Birliği Ceza Hukuku'nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Sayı:2, 2018, s.51-104.

BREWCZYŃSKA, MAGDALENA, "A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation", KOSTA, ELENI ve LEENES, RONALD, *Research Handbook On EU Data Protection Law*, Edward Elgar Publishing, Cheltenham, 2022, s.91-114.

CARUANA, MIREILLE M., "The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement", International Review of Law, Computers & Technology, Cilt:33, Sayı:3, 2017, s.1-22.

COCQ, CELINE C., "EU Data Protection Rules Applying to Law Enforcement Activities: Towards an Harmonised Legal Framework?", New Journal of European Criminal Law, Cilt:7, Sayı:3, 2016, s.263-276.

CRAIG, PAUL, *The Lisbon Treaty: Law, Politics, and Treaty Reform*, Oxford University Press, Oxford, 2013.

DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, "The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal

matters – A modest achievement however not the improvement some have hoped for", Computer Law & Security Review, Cilt:25, Sayı:5, 2009, s.403-414.

DE HERT, PAUL ve PAPAKONSTANTINOU, VAGELIS, "The New Police and Criminal Justice Data Protection Directive: A First Analysis", New Journal of European Criminal Law, Cilt:7, Sayı:1, 2016, s.7-19

DE HERT, PAUL ve SAJFERT, JURAJ, "The Fundamental Right to Personal Data Protection In Criminal Investigations and Proceedings: Framing Big Data Policing Through the Purpose Limitation and Data Minimisation Principles of the Directive (EU) 2016/680", Brussels Privacy Hub Working Paper, Cilt:7, Sayı:31, 2021, s.1-17.

DE HERT, PAUL ve SAJFERT, JURAJ, "The Role of the Data Protection Authorities in Supervising Police and Criminal Justice Authorities Processing Personal Data", BRIERE, CHLOE ve WEYEMBERGH, ANNE (Eds.), *The Needed Balances in EU Criminal Law: Past, Present and Future*, Hart Publishing, Oxford, 2018, s.243-255.

DE HERT, PAUL, *et.al.*, "Data protection in the third pillar: Cautious pessimism", MARTIN, MAIK (Ed.), *Crime, Rights and the EU: The Future of Police and Judicial Cooperation*, Justice, London, 2007, s.121-194.

DEMETZOU, KATERINA, "Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation", Computer Law & Security Review, Cilt:35, Sayı:6, 2019, s.1-14.

DIMITROVA, DIANA ve DE HERT, PAUL, "The Right of Access Under the Police Directive: Small Steps Forward", MEDINA, MANEL *et.al.*, *Privacy Technologies and Policy*, Springer International Publishing, Switzerland, 2018, s.111-130.

DRECHSLER, LAURA, "Comparing LED and GDPR Adequacy: One Standard Two Systems", Global Privacy Law Review, Cilt:1, Sayı:2, 2020, s.93-103.

DRECHSLER, LAURA, "The Achilles Heel of EU data protection in a law enforcement context: international transfers under appropriate safeguards in the law enforcement directive.", Cybercrime: New Threats, New Responses (Proceedings of the XVth International Conference on Internet, Law & Politics, Universitat Oberta de Catalunya, Barcelona, 1-2 July, 2020), 2020, s.47-65.

DRECHSLER, LAURA, "Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context", International Data Privacy Law, Cilt:11, Sayı:2, 2021, s.182-195.

ERDEM, MUSTAFA RUHAN, "Lizbon Antlaşması ve Avrupa Ceza Hukuku'nun Geleceği: Treaty of Lisbon and the Future of European Criminal Law", Yaşar Üniversitesi E-Dergisi, Cilt:8, Sayı: Özel, 2013, s.1019-1098.

FLETCHER, MARIA, "Impact of the Pupino Decision on Eu Law" MITSILEGAS, VALSAMIS *et.al.*(Eds.), *The Court of Justice and European Criminal Law: Leading Cases in a Contextual Analysis*, Hart Publishing, 2019, s.67-82.

GÖÇMEN, İLKE ve ŞEKER, EMRİYE ÖZLEM, "Kişisel Verilerin Korunması Tüzüğü'ne İlişkin Avrupa Birliği Adalet Divanının İlk Kararları", ŞENOCAK, KEMAL, *Muhtelif Yönleriyle Kişisel Verilerin Korunması Hukuku*, Yetkin Yayıncılık, Ankara, 2022, s.239-288.

GÖÇMEN, İLKE, "Avrupa Birliği Adalet Divanı", AKÇAY, BELGİN ve GÖÇMEN, İLKE (Eds.), *Avrupa Birliği Tarihçe, Teoriler, Kurumlar ve Politikalar*, 3. Baskı, Seçkin Yayıncılık, Ankara, 2016, s.261-288.

GÜNEŞ, AHMET M, "Lizbon Antlaşması Sonrasında Avrupa Birliği", Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt:12, Sayı:1, 2008, s.739-772.

HERLIN-KARNEL, ESTER, "The European Court of Justice as a game-changer: fiduciary obligations in the area of freedom, security and justice", RIPOLL SERVENT, ARIADNA ve TRAUNER, FLORIAN (Eds.), *The Routledge Handbook of Justice and Home Affairs Research*, 1st Edition, Routledge Taylor & Francis Group, London, 2018, s.396-408.

HIJMANS, HIELKE ve SCIROCCO, ALFONSO, "Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to help?", Common Market Law Review, Cilt:46, Sayı:5, 2009, s.1485-1525.

JASSERAND, CATHERINE, "Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in Directive 2016/680?", Computer Law & Security Review: The International Journal of Technology Law and Practice, Cilt:34, Sayı:1, 2017, s.154-165.

JASSERAND, CATHERINE, "Processing of special categories of personel data", KOSTA, ELENI ve BOEHM, FRANZISKA (Eds), *The EU Law Enforcement Directive (LED): A Commentary*, Oxford University Press, Oxford, 2024, s.217-230.

JASSERAND, CATHERINE, "Subsequent use of GDPR data for a law enforcement purpose: the forgotten principle of purpose limitation?" European Data Protection Law Review, Cilt:4, Sayı:2, 2018, s.152-167.

KÖKTAŞ, ARİF, "Özgürlük, Güvenlik ve Adalet Alanı", AKÇAY, BELGİN ve GÖÇMEN, İLKE (Eds.), *Avrupa Birliği Tarihçe, Teoriler, Kurumlar ve Politikalar*, 3.Baskı, Seçkin Yayıncılık, Ankara, 2016, s.491-523.

KONING, MEREL ELIZE, *The purpose and limitations of purpose limitation*, Yayımlanmamış Doktora Tezi, Radboud University Nijmegen, Utrecht, Netherlands, 2020.

KOSTA, ELENI, "A divided European data protection framework: A critical reflection on the choices of the European legislator post-Lisbon", KOSTA, ELENI ve LEENES, RONALD (Eds.), *Research Handbook On EU Data Protection Law*, Edward Elgar Publishing, Cheltenham, 2022, s.68-90.

KOSTA, ELENI, *et.al*, "Data Protection in the Third Pillar: In the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive", International Review of Law, Computers & Technology, Cilt:21, Sayı:3, 2007, s.347-362.

KUNER, CHRISTOPHER, *et.al.*, "Background and Evolution of the EU General Data Protection Regulation (GDPR)", KUNER, CHRISTOPHER, *et.al.* (Eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, s.1-47.

LABAYLE, HENRI, "The institutional framework", MITSILEGAS, VALSAMIS et.al. (Eds.), *Research Handbook on EU Criminal Law,* Edward Elgar Publishing Limited, Cheltenham, 2016, s.29-48.

LAURSEN, FINN, "The Lisbon Treaty: Overview of Institutional Choices and Beginning Implementation", LAURSEN, FINN (Ed.), *The EU's Lisbon Treaty: Institutional Choices and Implementation*, Ashgate Publishing, Farnham, 2012, s.2-17.

LEISER, MARK ve CUSTERS, BART, "The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680", European Data Protection Law Review, Cilt:5, Sayı:3, 2019, s.367-378.

LYNSKEY, ORLA, "Criminal justice profiling and EU data protection law: precarious protection from predictive policing", International Journal of Law in Context, Cilt:15, Sayı:2, 2019, s.162-176.

MARQUENIE, THOMAS, "The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework", Computer Law & Security Review, Cilt:33, Sayı:3, 2017, s.324-340.

MASEA, COSTANZA DI FRANCESCO, *Balance between security and fundamental rights protection: an analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name records (PNR)*, 2016, https://rivista.eurojus.it/balance-between-security-and-fundamental-rights-protection-an-analysis-of-the-directive-2016680-for-data-protection-in-the-police-and-justice-sectors-and-the-directive-2016681-on-the-use-of-passen/, Erişim Tarihi: 10.04.2025, s.1-17.

MITSILEGAS, VALSAMIS, "The Third Wave of Third Pillar Law: Which Direction for EU Criminal Justice?", Queen Mary School of Law Legal Studies Research Paper No. 33/2009, European Law Review, Cilt:34, Say:4, 2009, s.522-560.

MONAR, JÖRG, "Justice and Home Affairs: The Treaty of Maastricht as a Decisive Intergovernmental Gate Opener", Journal of European Integration, Cilt:34, Sayı:7, 2012, s.33-50.

MOORE, DOMINIQUE, "Article 99. Entry into force and application", KUNER, CHRISTOPHER, *et.al.* (Eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, s.1320-1321.

O'NEILL, MARIA, "The Issue of Data Protection and Data Security in the (Pre-Lisbon) EU Third Pillar", Journal of Contemporary European Research, Cilt:6, Sayı:2, 2010, s.211-235.

PEERS, STEVE, “EU Criminal Law and Police Cooperation”, CRAIG PAUL ve DE BÚRCA GRAINNE (Eds.), *The Evolution of the EU Law*, 3th Edition, Oxford University Press, Oxford, 2021, s.752-769.

PEERS, STEVE, “Finally 'Fit for Purpose'? The Treaty of Lisbon and the End of the Third Pillar Legal Order”, Yearbook of European Law, Cilt:27, Sayı:1, 2008, s.47-64.

PEERS, STEVE, “Salvation Outside The Church: Judicial Protection In The Third Pillar After The *Pupino* And *Segi* Judgments”, Common Market Law Review, Cilt:44, Sayı:4, 2007, s.883-929.

PEERS, STEVE, “The European Union and substantive criminal law: reinventing the wheel?”, Netherlands Yearbook of International Law, Volume 33, 2002, s.47-73.

PEERS, Steve*, The ‘Third Pillar acquis’ after the Treaty of Lisbon enters into force*, Statewatch Analysis, 1 Aralık 2009.

PIRIS, JEAN-CLAUDE, *The Lisbon Treaty: A Legal and Political Analysis*, Cambridge University Press, Cambridge, 2010.

PURTOVA, NADEZHDA, “Between GDPR and the Police Directive: Navigating through the maze of information sharing in Public-Private Partnership”, International Data Privacy Law, Cilt:8, Sayı:1, 2018, s.52-68.

QUINTEL, TERESA ve KOSTA, ELENI, “Background and evolution of the LED”, KOSTA, ELENI ve BOEHM, FRANZISKA (Eds.), *The EU Law Enforcement Directive (LED): A commentary*, Oxford University Press, Oxford, 2024, s.1-8.

RADTKE, TRISTAN, “The Concept of Joint Control under the Data Protection Law Enforcement Directive 2016/680 in Contrast to the GDPR”, Journal of Intellectual Property, Information Technology and Electronic Commerce Law, Cilt:11, Sayı:3, 2020, s.242-251.

RIPOLL SERVENT, ARIADNA, "The European Parliament in justice and home affairs: becoming more realistic at the expense of human rights?", RIPOLL SERVENT, ARIADNA ve TRAUNER, FLORIAN (Eds.), *The Routledge Handbook of Justice and Home Affairs Research*, 1st Edition, Routledge Taylor & Francis Group, London, 2018, s.385-395.

SAJFERT, JURAJ ve QUINTEL, TERESA, "*Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities*", 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873, Erişim Tarihi:5.4.2025, s.1-22.

SPAVENTA, ELEANOR, "Fundamantel Rights in the European Union", BARNARD, CATHERINE ve PEERS, STEVE (Eds), *European Union Law*, Oxford University Press, Oxford, 2014 s.226-254.

TEZCAN, ERCÜMENT, "Avrupa Birliği'nde Politika Yapımı/Karar Alma", AKÇAY, BELGİN ve GÖÇMEN, İLKE (Eds.), *Avrupa Birliği Tarihçe, Teoriler, Kurumlar ve Politikalar*, 3. Baskı, Seçkin Yayıncılık, Ankara, 2016, s.343-382.

TZANOU, MARIA, "Distinction between personal data and verification of quality of personal data", KOSTA, ELENI ve BOEHM, FRANZİSKA (Eds), *The EU Law Enforcement Directive (LED): A Commentary*, Oxford University Press, Oxford, 2024, s.181-192.

TZANOU, MARIA, "Lawfulness of processing", KOSTA, ELENI ve BOEHM, FRANZİSKA (Eds), *The EU Law Enforcement Directive (LED): A Commentary*, Oxford University Press, Oxford, 2024, s.193-206.

TZANOU, MARIA, "Specific processing conditions", KOSTA, ELENI ve BOEHM, FRANZİSKA (Eds), *The EU Law Enforcement Directive (LED): A Commentary*, Oxford University Press, Oxford, 2024, s.207-216.

VIOLA DE AZEVEDO CUNHA, MARIO, "Privacy, Security and the Council Framework Decision 2008/977/JHA", Law Technology, Cilt:43, Sayı:4, 2010, s.2-18.

VOGIATZOGLOU, PLIXAVRA *et.al.*, "From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives", Journal of Intellectual Property, Information Technology and E-Commerce Law, Cilt:11, Sayı:3, 2020, s.274-302.

VOGIATZOGLOU, PLIXAVRA ve FANTIN, STEFANO, "National and Public Security Within and Beyond The Police Directive", VEDDER, ANTON *et.al.*(Eds.), *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, Intersentia, Cambridge, 2019, s.44-62.

VOGIATZOGLOU, PLIXAVRA ve MARQUENIE, THOMAS, "Assessment of the implementation of the Law Enforcement Directive", European Union Publications Office, 2022, s.1-120.

VOGIATZOGLOU, PLIXAVRA ve VALCKE, PEGGY, "Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law", KOSTA, ELENI ve LEENES, RONALD, *Research Handbook On EU Data Protection Law*, Edward Elgar Publishing, Cheltenham, 2022, s.11-49.

YAKUT, BAHADIR, "Lizbon Sonrası AB'nin Yeni Kurumsal Yapısı ve Karar Alma Süreçlerinin Özgürlük, Güvenlik ve Adalet Alanındaki Yansımaları", Türkiye Adalet Akademisi Dergisi (TAAD), Yıl:1, Sayı:2, 2010, s.53-85.

YAKUT, BAHADIR, "Lizbon Sonrası Avrupa Birliğinin Cezai Meselelerde Yetkisinin Kapsamı", Ankara Avrupa Çalışmaları Dergisi, Cilt:9, No:2, 2010, s.169-207.

AKADEMİK TEZLER

BİLGİN, AHMET BURAK, *Avrupa Birliği'nde İnsan Haklarının Gelişimi ve Korunması*, Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2015.

CAN, NESLİHAN, *Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması*, Yayımlanmamış Tez, İstanbul Üniversitesi, İstanbul, 2020.

KAMARA, IRENE, *Data protection standardisation: The role and limits of technical standards in the EU data protection law*, Doktora Tezi, TILT, Vrije Universiteit Brussel – LSTS, 2021.

MÖLLER, CAROLIN, *The Evolution of Data Protection and Privacy in the Public Security Context-An Institutional Analysis of Three EU Data Retention and Access Regimes*, Yayımlanmamış Doktora Tezi, Queen Mary University of London, London, 2017.

ÖZET

Bu tez, kolluk ve ceza adaleti alanında AB'de kişisel verilerin korunması rejiminin evrimini incelemektedir. Kolluk ve adli işbirliğinin AB'nin Üçüncü Sütunu altında yönetildiği Lizbon Antlaşması öncesi dönemden Lizbon Antlaşması'nın yürürlüğe girmesinden sonra bu alanın AB hukukunun anayasal çerçevesine dahil edildiği yasal ve kurumsal dönüşümü incelemektedir.

İlk bölüm, Avrupa Konseyi'nin 108 sayılı Sözleşmesi ve R(87)15 sayılı Tavsiye Kararı gibi erken dönem uluslararası belgelerin yanı sıra Veri Koruma Direktifi ve 2008/977 sayılı Çerçeve Karar'ın cezai konularda kolluk ve adli işbirliği alanındaki ugulamalarına odaklanarak Lizbon Antlaşması öncesinde veri korumanın parçalı ve hükümetlerarası yapısını analiz etmektedir. İkinci bölüm, ABTHŞ'nin bağlayıcılığı ve GDPR ve Kolluk Direktifi'nin kabulü de dâhil olmak üzere Lizbon Antlaşması ile getirilen yasal ve yapısal reformları ele almaktadır. Kolluk Direktif, cezai konularda kişisel verilerin yetkili makamlar tarafından işlenmesine yönelik özel kurallar getirmekte, güvenceleri, gözetimi ve bireysel hakları güçlendirmektedir.

Tez, tarihsel-karşılaştırmalı ve yasal-analitik bir yaklaşımla, AB'nin ulusal ve hükümetlerarası önlemlerden oluşan bir yamalı bohçadan, hassas kolluk kuvvetleri ve ceza adaleti alanında daha tutarlı ve uygulanabilir bir veri koruma rejimine nasıl ilerlediğini göstermektedir.

Anahtar Kelimeler: Veri koruma, Avrupa Birliği, Lizbon Antlaşması, kolluk ve ceza adaleti, GDPR, Kolluk Direktifi.

ABSTRACT

This thesis examines the evolution of the personal data protection regime in the EU in the field of law enforcement and criminal justice. It examines the legal and institutional transformation from the pre-Lisbon Treaty period, when law enforcement and judicial cooperation were governed under the EU's Third Pillar, to the post-Lisbon Treaty period, when this area was incorporated into the constitutional framework of EU law.

The first part analyzes the fragmented and intergovernmental nature of data protection prior to the Lisbon Treaty, focusing on the application of the Data Protection Directive and Council Framework Decision 2008/977 in the field of law enforcement and judicial cooperation in criminal matters, as well as early international instruments such as Convention 108 and Recommendation R(87)15 of the Council of Europe. The second part addresses the legal and structural reforms introduced by the Lisbon Treaty, including the binding nature of the Charter of Fundamental Rights of the European Union and the adoption of the GDPR and the Law Enforcement Directive. The Law Enforcement Directive introduces specific rules for the processing of personal data by competent authorities in criminal matters, strengthening safeguards, oversight and individual rights.

Through a historical-comparative and legal-analytical approach, the thesis shows how the EU has moved from a patchwork of national and intergovernmental measures to a more coherent and enforceable data protection regime in the sensitive field of law enforcement and criminal justice.

Keywords: Data protection, European Union, Lisbon Treaty, law enforcement and criminal justice, GDPR, Law Enforcement Directive.