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

Dr. Öğr. Üyesi Gülşah BOSTANCI BOZBAYINDIR*

Öz: 2016 tarihinde 2016/679 sayılı Genel Kişisel Verilerin Korunması Tüzüğü'ne (General Data Protection Regulation-GDPR) ek olarak, 2016/680 sayılı Kişisel Verilerin Ceza Adaleti ve Polis İşbirliği Alanında Kullanılmasına Yönelik Gerçek Kişilere Ait Kişisel Verilerin Yetkili Otoriteler Tarafından Suçların Önlenmesi, Soruşturulması ve Tespit Edilmesi veya Cezaların İnfazı Amacıyla İşlenmesi ve Bu Nevi Kişisel Verilerin Serbest Dolaşımı Hakkında Direktif, 27 Nisan 2016 tarihinde kabul edilmiş ve kendisinden önceki 2008/977/JHA sayılı Kararı ilga etmiştir. Bu yeni Direktifin esas amacı (2016/680), gerçek kişilerin kişisel verilerine tutarlı ve yüksek seviyede koruma sağlamanın yanı sıra üye devletlerde yetkili otoriteler arasında kişisel verilerin mübadelesini kolaylaştırmaktır. Kişisel verilerin üye devletler arasında mübadelesi, cezai işlerde adli ve polis işbirliği bakımından önem arz etmektedir. Bu nedenle, gerçek kişilerin kişisel verileri konusunda hak ve özgürlüklerinin korunması ve yetkili otoriteler tarafından, suçların önlenmesi, soruşturulması ve tespit edilmesi veya cezaların infazı amacıyla kişisel verilerin işlenmesine ve değerlendirilmesine ilişkin kuralların yeknesaklaştırılması gerekmektedir. Bu nedenle, Direktif bir yandan önceki direktifin eksikliklerini tadil etmeyi diğer taraftan da bu sahada ortaya çıkan yeni sorunları çözmeyi amaçlamaktadır. Bununla birlikte, 2016/680 sayılı Direktif çok sayıda eleştiriye uğramıştır. Bu çalışmada, 2008 tarihli eski çerçeve karar ve 2016 tarihli yeni Direktifi tahlil edeceğiz ve yeni Direktifle alakalı potansiyel sorunları ve eleştirileri değerlendireceğiz.

Anahtar Kelimeler: Avrupa Birliği Ceza Hukuku, Kişisel Verilerin Korunması, Polis ve Ceza Adaleti

---

* Makale Gönderim Tarihi: 09.10.2018, Makale Kabul Tarihi: 08.11.2018

İstanbul Sabahattin Zaim Üniversitesi Hukuk Fakültesi Ceza ve Ceza Usul Hukuku Anabilim Dalı (ORCID kimlik no: 0000-0003-0602-2713); gulsah_bostanci@yahoo.com.

The Police and Criminal Justice Authorities 2018/680 Directive: Data Protection Standarts with regard to the Processing of Personal Data by Component Authorities and Critics Against the Directive

Abstract: In addition to the General Data Protection Regulation (GDPR), Directive (EU) 2016/680 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*' substantively enacted on 27 April 2016 and repealed the former the Council Framework Decision 2008/977/JHA. The main objective of the new Directive (2016/680) is to ensure a consistent and high level of protection of the personal data of natural persons and facilitating the exchange of personal data between competent authorities of Members States. The exchange of personal data among Member States is crucial in order to ensure effective judicial cooperation in criminal matters and police cooperation. To that end, the level of protection of the rights and freedoms 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, including the safeguarding against and the prevention of threats to public security, should be equivalent in all Member States. On the one hand directive aims to amend the former directive's deficiencies and on the other hand to solve novel issues that has emerged in the field. Thus being so, the 2016 directive has been subject to many critics. In this study, we shall analyse the former 2008 directive and the new 2016 directive, and evualate the potential issues and critics against the new directive.

Keywords: European Criminal Law, Data Protection, Police and Criminal Justice Authorities

I. GİRİŞ

Kişisel verilerin korunması ya da bireylerin kişisel verilerinin işlenmesinin güvence altına alınması uzunca bir süredir Avrupa Birliği hukukunun en önemli meselelerinden birini teşkil etmektedir. Yeni teknolojilerin özel ve kamu sektöründe kullanılması, verilerin hukuka uygun toplanması, işlenmesi ve depolanmasını kolaylaştırmışsa da bu teknolojilerin kötüye kullanımının önüne geçilememiştir[1]. İnternetin yeni gelişmeye başladığı, adeta

1 Franziska Boehm, Information Sharing and Data Protection in the Area of Freedom, Security and Justice, Towards Harmonized Data Protection Principles for Information Exchange at EU Level, Springer, Heidelberg, 2012, s.19.

dijital devrimin gerçekleştiği dönemlerde, internetin bir yandan kötüye kullanımının engellenmesi, bir yandan da suçların önlenmesi, soruşturulması, kovuşturulması ve ayrıca verilerin paylaşımının belli bir standart dâhilinde sağlanması amacıyla 1995 tarihinde 95/46/EC sayılı Direktif kabul edilmişti[2]. 95 sayılı Direktif, kişisel verilerin korunması için atılan çok önemli bir adım olmuştu zira 2000'li yıllardan önce kişisel verilerin korunması genellikle özel hayatın gizliliğine saygı gösterilmesi hakkı çerçevesinde ve onun bir alt unsuru olarak görülmekteydi[3]. Direktiften önce kabul edilen gerek İnsan Hakları Evrensel Beyannamesi gerekse Avrupa İnsan Hakları Sözleşmesi, bilgisayar ve internetin etkin ve yaygın kullanımından çok daha önce kabul edilmiş metinlerdi ve bu metinlerde kişisel verilerin korunmasına ilişkin açık bir hüküm bulunmamaktaydı.

Bilişim teknolojilerinin kullanımındaki hızlı artış, uluslararası metinlerde kabul edilen özel hayatın gizliliği hakkına yönelik olarak ciddi bir tehdit unsuru haline gelmeye başlamıştı. Bu tehdide karşılık, 95 sayılı Direktif ile kişisel bilgilerin kullanılması, toplanması, elde edilen kişisel verilerin gizliliği ve bu bilgilere ilişkin olarak veri sahibine bir takım haklar tesis edilmesi neticesinde yeni bir özel hayatın gizliliği alanı ortaya çıkmış oldu[4]. Böylelikle, kişisel verilerin korunmasını özel hayatın gizliliği hakkının alt unsuru olarak gören anlayış yerini zamanla her iki hakkın -her ne kadar birbirleriyle yakın ilişki içerisinde de olsa- farklı haklar olduğu anlayışına bırakmıştır[5]. Böylelikle, kişisel verilerin güvenliğinin sağlanması hususunda yeni yasal düzenlemelerin önü açılmıştır[6].

---

2 Art.1, 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, O.J. L281/31; European Parliament, "MEPs tighten up rules to protect personal data in the digital era" Press release, 12.03.2014. Available at www.europarl.europa.eu/news/en/news-room/20140307IPR38204/MEPs-tighten-up-rules-to-protect-personal-data-in-the-digital-era; Google Spain C-131/12 EU C 2013, 424, prg.13.

3 Lauri J. Pajunoja, The Data Protection Directive on Police Matters 2016/680, Yayınlanmamış Yüksek Lisans Tezi, Uni. Helsinki, Faculty of Law, 2017, s.65.

4 ECtHR, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, No. 931/13, 27 June 2017, prg. 137. Handbook on European Data Protection Law, European Union Agency for Fundamental Rights and Council of Europe, Luxemburg, 2018, s. 18.

5 Handbook on European Data Protection Law, s.18. Tam tersine kişisel verilerin korunması hakkı, özel hayatın gizliliği hakkını da kapsadığı ve ondan daha geniş bir kapsama sahip olduğu da ifade edilmektedir. Juliane Kokott&Christoph Sobotta, The Distinction between Privacy and Data Protection, International Data Privacy Law, Vol.3, No.4, 2013, s.225.

6 ABAD'ın bazı kararlarında özel hayatın gizliliği klasik bir hak, kişisel verilerin gizliliği ise

Avrupa ülkelerinde kişisel verilerin korunmasına yönelik yasal düzenlemeler, 1970'lerde ortaya çıkmaya başlamıştır[7]. Birlik düzeyinde ise özellikle Avrupa Konseyi 108 numaralı Sözleşme ve 95 tarihli Direktif, kişisel verilerin korunması ve serbest dolaşımının güvenliğinin sağlanması konusundaki öncü metinler olmuştur. 2009'da Lizbon Antlaşması'nın kabul edilmesi, kişisel veriler açısından çok daha önemli bir adımdır. Lizbon Antlaşması ile düzenlenen Avrupa Birliği Antlaşması (ABA) ile Avrupa Birliğinin İşleyişine Dair Antlaşma (ABİA) kişisel verilerin korunmasına yönelik gerçekleşecek olan mevzuata aşikâr bir biçimde yasal zemin hazırlamak suretiyle AB hukuku çerçevesinde kişisel veri kavramının statüsünü güçlendirmiştir. Avrupa Birliği Adalet Divanı (ABAD) da kişisel verileri temel insan haklarından biri olarak kabul ederek, bu hakkın etkin uygulanmasını destekleyici kararlar vermiştir[8].

Avrupa Birliği'nin İşleyişine Dair Antlaşma'nın (ABİA) 16. maddesine dayanarak çıkartılan, 6 Nisan 2016 tarihinde kabul edilen ve 25 Mayıs 2018'de yürürlüğe giren 2016/679 sayılı genel ve ticari amaçlarla kişisel verilerin işlenmesini kapsayan Genel Kişisel Veri Koruma Tüzüğü'ne (GDPR)

---

modern bir hak olarak nitelendirildiği de görülmektedir. CJEU, Joined Cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston, 17 June 2010, prg. 71.

7 Bu hususta ilk düzenleme 1970'de Almanya'nın Hessen eyaletine aittir. Sırasıyla 1973'de İsveç ve 1980'lerde Fransa, Almanya, Hollanda ve İngiltere'de de kişisel verilerin korunmasına yönelik düzenlemeler yapılmıştır.

8 CJEU, Joined Cases Markus und Volker Schecke and Helmut Eifert, C-92/09 C-93/09 2010-662; Digital Rights Ireland Ltd vs. Minister For Communications, Marine and Natural Resources and Others, C-293/12; C-594/12; 2014, 238. Mahkeme, terör, organize suçlar gibi ciddi nitelikte suçlarla mücadele edilmesi, bu suçların işlenmesinin önlenmesi ve soruşturulması amacıyla kişilerin kimliğinin, internete nereden, ne zaman ve ne sıklıkla girdiklerinin tespit edilmesini ve bu bilgilerin altı aydan iki yıla kadar internet sağlayıcıları tarafından saklanabilmesini olanaklı hale getiren 2006'da kabul edilen Veri Koruma Direktifini (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54) geçersiz saymıştır. Mahkeme, direktifte internet kullanıcılarının bütün verilerinin hiçbir ayrıma, kısıtlamaya ya da istisnaya tabii tutulmadan, objektif bir kriter belirlenmeden toplanması ve her ülke hukukunda ayrıca düzenlenmiş "ciddi suçlar" gerekçe gösterilerek en az altı ay en çok iki yıl süre ile saklanmasına izin verilmesinin orantılılık ilkesini aştığı, bunların kötüye kullanılabilmesine karşı herhangi bir güvence de sağlanmadığı gerekçesi ile direktifi geçersiz saymıştır.

ek olarak, polis ve ceza adalet otoriteleri tarafından işlenen kişisel verilerin korunmasına yönelik 2016/680 sayılı yetkili makamlar tarafından suçun önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai süreçlerin yürütülmesi amacıyla işlenen kişisel verilere ilişkin gerçek kişilerin korunmasına ve bu tür verilerin serbest dolaşımına dair direktif kabul edilmiştir. Bu direktif, her ne kadar Genel Veri Koruma Tüzüğü'nün önemi ve haşmeti karşısında daha dar ve özellikli bir uygulama alanı bulmuş olsa da bu durum direktifin önemsiz ya da ikincil nitelikte olduğu anlamına gelmemektedir.

Lizbon Antlaşması ile Avrupa Birliği'nin değişen yapısı göz önünde bulundurularak, 2008 tarihli Veri Koruma Çerçeve Kararı[9]'nın yürürlükte olduğu dönemlerde (2008-2018 arası) ortaya çıkan sorunların gözden geçirilmesi ve yeni bir polis ve ceza adalet alanında kişisel verilerin daha etkin korunması ihtiyacına bir cevap olarak 2018 tarihli Direktif kabul edilmiştir[10].

Çalışmamızda, 'AB Kişisel Verilerin Korunması Hukuku'nda 2016/680 Sayılı Yetkili Makamlar Tarafından Suçun Önlenmesi, Soruşturulması, Tespiti Veya Kovuşturulması Veya Cezai Süreçlerin Yürütülmesi Amacıyla İşlenen Kişisel Verilere İlişkin Gerçek Kişilerin Korunmasına Ve Bu Tür Verilerin Serbest Dolaşımına Dair Direktif'in üye ülkeler düzeyinde uyumlaştırılması, kapsamı, ilkeleri ve uygulanmasına ilişkin hususlara odaklanılmıştır. Neticede ise direktife yönelik eleştiriler üzerinde değerlendirmede bulunmak suretiyle, direktif uygulamasının tutarlılığı ve etkinliği açısından ipuçları ortaya konmuş, Direktifin iç hukuka aktarımında yaşanabilecek sorunlar ve ulusal düzeyde nihai uygulamaları hakkındaki tartışmalar ele alınmıştır.

II. AVRUPA'DA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN GENEL HUKUKİ DÜZENLEMELER

Avrupa düzeyinde kişisel verilerin korunmasına ilişkin düzenlemeler temel olarak iki alanda gerçekleştirilmiştir. Bunlardan biri Avrupa Konseyi'nin üye ülkelerin yanı sıra üye olmayan ülkelerin imzasına da açılan sözleşme-

---

9 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008F0977.

10 2016/680 sayılı Direktif Gerekçe madde 1, 8, 10 ve 11.

leri; bir diğeri de Avrupa Birliği düzeyinde gerçekleştirilen ve üye ülkelerin uyguladığı metinlerdir. Her iki alanda da kişisel verilerin korunması ana hedeftir ancak Avrupa Konseyi çerçevesinde kabul edilen düzenlemelerin AB hukuku düzenlemelerinden temel farkı, bunların sadece Birlik hukuku ve güvenliği alanında değil ulusal güvenlik alanında da uygulanabilir olmalarıdır. Bunun en önemli sonucu, Avrupa Konseyi metinlerine taraf olan devletlerin, kendi ulusal güvenlikleriyle ilgili bir faaliyette bulunuyor olsalar da Avrupa İnsan Hakları Sözleşmesi 8. madde çerçevesinde hareket etmeleri gerektiğidir[11].

A. Avrupa Konseyi Bünyesinde Kabul Edilen Hukuki Düzenlemeler

Avrupa Konseyi çerçevesinde kabul edilen ve kişisel verilerin korunması hakkını içeren düzenlemelerin başında Avrupa İnsan Hakları Sözleşmesi (AİHS) gelmektedir. Sözleşme, 8. maddede yer alan özel hayatın gizliliği hakkı çerçevesinde kişisel verilerin korunması hakkını da ele almaktadır. Maddede herkesin aile ve özel hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkı olduğu ifade edilmektedir. Avrupa İnsan Hakları Mahkemesi (AİHM), kişisel verilerin korunması hakkına ilişkin kararlarını da 8. madde çerçevesinde vermektedir. Mahkemenin kişisel verilere ilişkin yorumu ileride değineceğimiz gerek 95 tarihli Direktif gerekse 108 numaralı Sözleşme'den çok daha geniştir[12]. Bununla birlikte AİHM'in özel hayat kapsamına dahil edilebilecek kişisel bilgiler için gizliliğe ek unsurlar aradığı söylenebilir[13].

---

11 Handbook on European Data Protection Law, s.273.

12 Kokott&Sobotta, s.223.

13 "Mahkeme, söz konusu kişisel verinin çok uzun bir zamanda sistematik olarak toplandığı ve depolandığını, bunun da özel hayat kapsamına girebileceğini ifade etmiştir. Bu tür bilgiler, bir kişinin sadece yakın değil aynı zamanda uzak geçmişini ilgilendirmesi halinde de bu durumun özel hayat kapsamına girmektedir. Mahkeme ayrıca, iç hukukta hangi bilgilerin kaydedilebileceğini, hakkında bilgi toplama ve saklama gibi izleme tedbirleri uygulanabilecek kategorideki kişilerin kimler olduğunu, bu tür tedbirlere başvurulabilecek koşulların neler olduğunu ya da izlenecek usulü açıklayan hiçbir hüküm bulunmadığını kaydetmiştir. İç hukukta tutulan bilgilerin ne kadar bir süreyi kapsayacağına ya da ne kadar uzun süreyle bilgi tutulabileceğine dair sınırlar konmamıştır. Ayrıca, iç hukukta dosyalara erişim yetkisi olan kişilere, dosyaların niteliğine, izlenecek usule ya da bu yolla elde edilen bilgilerin ne şekilde kullanılabileceğine ilişkin açık ya da ayrıntılı hiçbir hüküm mevcut değildir. Bu nedenlerle Mahkeme, Romanya hukukunun kamu makamlarına tanıdığı ilgili takdir yetkisinin kapsamını ve kullanılma biçimini makul bir açıklıkla belirtmediğine kanaat getirmiştir".

Mahkeme'nin, iletişime müdahale[14], kamu ya da özel sektör tarafından gözetleme[15], kamu otoriteleri tarafından kişisel verilerin depolanmasına karşı koruma[16] kararları 8. maddede yer alan gizlilik teriminin geniş yorumlandığı

ECtHR, Rotaru v Romania Başvuru no 28341/95, ECHR 2000-V, prg. 44. Mahkeme daha sonra verdiği bir kararda ceza mahkumiyetine ilişkin kararların başvuranın geçmişine ait özel yaşamının bir parçası olduğunu, başvuranın kendisine verilen uyarı cezasına ilişkin kişisel verilerin süre sınırı olmaksızın tutulmasından ve ifşa edilmesinden dolayı kendisine iş bulma konusunda neden olduğu olumsuz etkisinden şikâyetçi olması karşısında, adli sicil kaydındaki verilerin bir anlamda kamu bilgileri olduğu kabul edilse de, bu verilerin merkezi kayıtlarda sistematik bir şekilde saklanmasının, bunların ilgili kişi dışındaki herkesin söz konusu olayı unutmasının uzun süre sonrasında bile ifşa edilebilecek durumda olduğu anlamına geldiğini ve dolayısıyla 8. maddenin ihlal edildiğini ifade etmiştir. ECtHR, M.M. v UK Başvuru no. 24029/07 (13 Kasım 2012), prg. 188. Handbook on European Data Protection Law, s.44 vd.

14 ECtHR, Malone v. the United Kingdom, Başvuru No. 8691/79, 2 Ağustos 1984; ECtHR, Copland v. the United Kingdom, Başvuru No. 62617/00, 3 Nisan 2007, ECtHR, Mustafa Sezgin Tanrıkulu v. Turkey, Başvuru No. 27473/06, 18 Temmuz 2017., Handbook on European Data Protection Law, s.23.

15 ECtHR, Klass and Others v. Germany, Başvuru No. 5029/71, 6 Eylül 1978; ECtHR, Uzun v. Germany, Başvuru No. 35623/05, 2 Eylül 2010, Handbook on European Data Protection Law, s.23. "Davada, başvuran yetkili mercilere, yazışmalarını ve telefon görüşmelerini sonradan kendilerine haklarında alınan bu tedbirlere ilişkin bilgi vermeksizin takip etme yetkisi tanıyan Alman mevzuatıyla ilgili şikâyette bulunmuştur. Mahkeme, Alman yasama meclisinin Sözleşme'nin 8/1 maddesinde güvence altına alınan hakkın kullanılmasına ilişkin bahse konu mevzuattan kaynaklanan müdahalenin 2. fıkra uyarınca demokratik bir toplumda gerekli olduğunu, ulusal güvenliğin çıkarlarını, düzenin korunması ve suç işlenmesinin önlenmesi amaçlarını gözettiğini değerlendirmek için haklı gerekçelerinin söz konusu olduğunu ifade emiş, Sözleşme'nin özel hayat ve aile hayatına saygı hakkını düzenleyen 8. maddesinin ihlal edilmediğine karar vermiştir. Mahkeme özellikle, vatandaşların gizli şekilde izlenmesine dair yetkilerin, hukuk devleti olmanın bir göstergesi olarak, yalnızca demokratik kurumların korunması için ve kesin bir biçimde gerekli olması halinde, Sözleşme kapsamında imkan sağlanabileceğini tespit etmiştir. Ancak, Mahkeme, günümüzde demokratik toplumların son derece gelişmiş casusluk biçimleri ve terör örgütleri tarafından tehdit edildiğini ve bunun sonucunda Devletin bu gibi tehditlerle mücadele edebilmek için kendi yetki sınırları içerisinde faaliyet gösteren bölücü unsurları gizli bir şekilde izleme görevini üstlenebilmesi gerektiğini kaydederek, mailler, postalar ve iletişim araçları üzerinde gizli teknik takibin yapılmasına imkân veren mevzuatın, istisnai koşullarda, ulusal güvenlik gerekçesiyle ve/veya kargaşa ya da suçun önlenmesi açısından demokratik bir toplumda gereklilik arz ettiğini değerlendirmiştir".

16 ECtHR, Roman Zakharov v. Russia, Başvuru No. 47143/06, 4 Aralık 2015; ECtHR, Szabó and Vissy v. Hungary, Başvuru No. 37138/14, 12 Ocak 2016, Handbook on European Data Protection Law, s. 24. Söz konusu dava, "Rusya'daki cep telefonu görüşmelerinin gizlice dinlenmesine dair bir sistemle ilgilidir. Bir yayınevi şirketinin genel yayın yönetmeni olan başvuran, özellikle Rusya'daki mobil şebeke operatörlerinin kanunen kolluk makamlarının

kararlara örnek olarak gösterilebilir. Mahkeme, özel hayata ilişkin bilgilerin toplanması, depolanması ya da ifşa edilmesini özel hayatın gizliliği hakkının ihlali olduğuna işaret etmektedir[17].

Kişisel verilerin korunması hakkı 8. madde kapsamında değerlendirilmiş olduğundan, bu hak 2. fıkrada yer alan sınırlamalara da tabidir. AİHS 8/2. madde, sınırlandırmanın şartlarını belirtmiştir. Bu müdahale ancak yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın ya da başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.

Avrupa Konseyi düzeyinde kişisel verilerin korunmasına yönelik gerçekleştirilen ve kişisel verilerin işlendiği polis ve ceza adalet alanı da dâhil olmak üzere bütün alanlara uygulanabilir olan sözleşme Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'dir (108 Sayılı Avrupa Konseyi Sözleşmesi)[18]. Sözleşme, temel olarak kişisel verilerin korunmasını ele alan alanında yegâne çok taraflı antlaşmadır. Sözleşme kişisel verilerin sınır ötesi akışı da dâhil verilerin

---

operasyonel-arama faaliyetlerini gerçekleştirmelerine olanak tanıyan bir donanım kurulumu yapmaları gerektiği ve bu durumun da Rusya kanunları kapsamında yeterli güvence sağlanmaksızın, tüm görüşmeleri kapsayan bir dinleme işlemine izin verdiği hususlarda şikâyetçi olmuştur. Mahkeme, Rusya'da haberleşmenin dinlenmesi konusunu düzenleyen kanuni hükümlerin, denetleme yetkisinin keyfi şekilde ve kötüye kullanılma riskine karşı yeterli ve etkili güvenceler sağlamadığını kaydederek, Sözleşme'nin 8. maddesinin ihlal edilmiş olduğuna hükmetmiştir. Denetleme yetkisi, bütün gizli izleme sistemlerinde söz konusu olabilen bir durumdur ve keyfi uygulama ve kötüye kullanma ile Rusya'daki gibi gizli servislerin ve polisin tüm cep telefonu görüşmelerine teknik araçlar vasıtasıyla doğrudan erişiminin olduğu bir sistemde fazlasıyla karşılaşılmaktadır. Mahkeme'nin tespitine göre belli başlı alanlarda, kanuni düzenlemelerde eksiklikler olduğunu tespit etmiştir: Rusya'daki kamu makamlarının gizli izleme tedbirlerine başvurmakla yetkili kılındığı durumlar; bu tür tedbirlerin süresi, özellikle de bu tedbirlerin uygulanmasına son verilmesi gereken durumlar; dinleme işlemi için yetki verilmesinin yanı sıra dinleme yoluyla elde edilmiş verilerin saklanması ve imha edilmesine dair usuller; dinlemenin denetlenmesi. Dahası, haberleşmenin dinlenmesine karşı başvurulabilecek mevcut hukuk yollarının etkililiği, bu hukuk yollarının sadece dinlenildiğine ilişkin kanıt sunan kişilere açık olduğunu ve herhangi bir bildirim sisteminin ya da dinlenme hakkındaki bilgilere erişim imkanının yokluğunda, bu tür bir kanıtı elde edebilmenin mümkün olmadığı gerçeği karşısında sekteye uğramıştır.

17 EctHR, Amann v Switzerland Başvuru no 27798/95, ECHR 2000-II, prg. 69 vd. - 80; Rotaru v Romania Başvuru No 28341/95, ECHR 2000-V, prg. 46.

18 https://eur-lex.europa.eu/legal-content.

işlenmesi sürecinin beraberinde getirebileceği suiistimallere karşı bireylerin haklarının korunmasını öngörmektedir[19]. Sözleşme ile taraf devletler, kamu ve özel sektör ayrımı yapmaksızın otomatik kişisel veri dosyalarının ve kişisel verilerin otomatik işleme tabi tutulması konusundaki uygulamaları kabul eder[20]. Taraflar, kişisel verilerin işlenmesi ile ilgili olarak, tüm bireylerin insan haklarına saygı gösterilmesini sağlamak için gerekli olan şartları ulusal kanunlarına dâhil etmeleri gerekmektedir[21]. Sözleşmede yer alan adil ve hukuka uygun veri toplama ve işleme ilkeleri ile verilerin gerektiğinden daha uzun süre saklanmaması ilkesine aykırı işlemler sözleşmeye aykırılık teşkil edecektir. Sözleşme, özel veri kategorileri de denilen ve kişilerin ırksal köken, dini veya diğer inançlarına ilişkin veriler ile sağlık veya cinsel hayata ilişkin verilerin ya da ceza mahkûmiyetine ilişkin verilerin iç hukukta uygun güvenceler sağlanmadıkça otomatik işleme tabi tutulamayacağını ifade etmektedir[22]. Sözleşme bu kapsamda, verilerin niteliği (madde 5)[23], özel veri kategorileri (madde 6)[24] ve ilgili kişi hakkındaki ek güvenceler (madde 8)[25]'e 9. maddede belirtilen istisnalar ve kısıtlamalar dışında istisna

---

19 Türkiye bu sözleşmeyi 1981'de imzalamış olsa da iç hukukta ancak 2016'da onaylanmıştır. 17.03.2016 tarih ve 29565 sayılı Resmi Gazete.

20 108 no'lu Sözleşme Madde 3.

21 https://eur-lex.europa.eu/legal-content/EN/TXT/. Sözleşme gerçek kişileri kapsamaktadır ancak taraf devletlerin Sözleşmenin kapsamını tüzel kişilere de genişletebilmesine cevaz vermektedir. European Union Agency for Fundamental Rights and Council of Europe, 2014, s.38.

22 108 no'lu sözleşme Madde 6.

23 Otomatik işleme konu olan kişisel veriler:

a. Adil bir biçimde ve yasa yoldan elde edilir ve işlenir;

b. Belli ve meşru amaçlar için kaydedilir ve bu amaçlara aykırı şekilde kullanılmaz;

c. Kaydedilme amaçlarına göre uygun ve yerinde olur ve aşırı olmaz;

d. Doğru bilgileri yansıtır ve gerektiğinde güncellenir;

e. Kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkan veren bir biçimde saklanır.

24 İç hukukta uygun güvenceler sağlanmadıkça, ırksal kökeni, siyasi düşünceleri, dini veya diğer inançları ortaya koyan kişisel veriler ile sağlık veya cinsel hayatla ilgili kişisel veriler, otomatik işleme tabi tutulmaz. Aynı şey ceza mahkumiyeti ile ilgili kişisel veriler için de geçerlidir.

25 Herkes:

a. Otomatik kişisel veri dosyasının mevcudiyetini, temel amaçlarını, dosya yöneticisinin kimliğini ve mutat ikamet yerini veya başlıca işyerini öğrenmek;

b. Makul aralıklarla ve aşırı gecikmeye veya masrafa maruz kalmadan kendisi ile ilgili kişisel

getirilemeyeceğini kabul etmiştir. Bu sınırlama ancak taraf devlet kanunlarında öngörülmüş olması ve demokratik bir toplumda belli hususların sağlanması için gerekli bir önlem oluşturması halinde mümkün olabilecektir. Bu hususlar, devletin güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi; ilgili kişinin veya başkasının hak ve özgürlüklerinin korunmasıdır.

Sözleşme, polis ve ceza adaleti alanındaki kişisel verilerin korunmasına da uygulanabilir niteliktedir. Avrupa Konseyi, bu alana ilişkin daha ayrıntılı bir metin olarak 1987'de 108 numaralı sözleşmeye ek Polis Veri Tavsiye Kararı'nı kabul etmiştir. Karar hukuken taraflar bakımından bağlayıcı değildir ancak polisin veri toplama, işleme, veri girişi, yabancı otoritelerle veri paylaşımı, veri sahibinin haklarının kullandırılması gibi işlemlere yön göstermesi bakımından önem arz etmektedir[26]. Bir başka deyişle, Polis sektöründe kişisel verilerin kullanılmasıyla ilgili R 87 (5) tavsiye karar, ulusal otoriteler tarafından kişisel verilerin işlenmesine yönelik yön gösterici bir özelliğe sahiptir[27]. Gerek 108 numaralı Sözleşme gerekse Tavsiye Karar, AB mevzuatından farklı olarak ulusal güvenlik alanına da uygulanmaktadır[28]. Karar, kural olarak polisin kişisel veriyi gerçek bir tehlike, kamu düzeninin korunması veya belli bir suçun kovuşturulması nedeniyle toplanmasını uygun bulurken, bunun istisnasının kural haline getirilmemesini tavsiye etmektedir. Tavsiye karar, 108 numaralı Sözleşme ile paralel olarak polisin kişisel verileri sınırsız, herhangi bir ayrıma tabi tutulmadan toplanmamasını içermektedir. Kişisel veriler ancak gerçek bir tehlike halinin önlenmesi ya da ceza soruşturması halinde toplanabilecektir. Karara göre, idari nitelikli

---

verilerin otomatik dosyada bulunup bulunmadığının teyidini almak ve bu bilgilerin kendisine anlaşılır bir biçim altında iletilmesini sağlamak;

c. Gerekli olan durumlarda, bu verileri düzelttirmek veya bunların işbu sözleşmenin 5.ve 6. maddelerinde belirtilen temel ilkelere işlerlik sağlayan iç hukuk hükümlerinin ihlali suretiyle işlenmiş olması halinde, söz konusu verileri sildirtmek;

d. İşbu maddenin b ve c fıkralarında öngörülen teyit talebinin veya duruma göre bildirim, düzeltme veya silme talebinin yerine getirilmemesi halinde bir başvuru yolundan yararlanmak hakkına sahiptir.

26 Lauri J. Pajunoja, s.15.

27 Council of Europe Committee of Ministers, Recommendation Rec 87 15 to member states regulating the use of personal data in the police sector, 17/07/1987.

28 Handbook on European Data Protection Law, s.275. 87 (5) sayılı tavsiye karar sırasıyla 1993, 1998 ve 2002 tarihlerinde bir dizi değişiklik geçirmiştir.

tutulan kişisel veriler adli niteliktekilerden ayrı tutulacaktır ve veri sahipleri de farklı kategorilerde ele alınacaktır. Veri paylaşımı ancak meşru bir amaç var ise hukuka uygundur. Uluslararası transferler, güncel bir tehlikenin önlenmesi için gerekli olması haricinde ancak yasal düzenlemeler ve uluslararası sözleşmeler var ise meşrudur[29]. Toplanma da ulusal hukuk mevzuatı ile temellendirilmelidir. Hassas kişisel veriler de ancak toplanması hususunda mutlak bir gereklilik olması durumunda toplanmalıdır. Kişisel verilerinin toplandığını bilmeyen bireye, soruşturmanın bitiminde bilgi verilecektir. Tavsiye karar, suçun önlenmesi, soruşturulması ve kovuşturulması ile cezanın yerine getirilmesi gibi amaçlar doğrultusunda yapılan veri işlemelerde ve polis tarafından kamu güvenliğinin tesisi için gerçekleştirilecek uygulamalarda kullanılacaktır. Tavsiye karar 5. madde çerçevesinde polis verilerinin aktarımı sıkı kurallara tabi kılınmıştır. Ulusal ve uluslararası hukuk çerçevesinde sarih yasal düzenlemelerin mevcudiyeti, eğer yoksa ciddi ve olması yakın ve muhakkak bir tehlikenin önlenmesi veya ciddi bir suçun işlenmesinin engellenmesi için gerekli olması halinde veri aktarımı gerçekleştirilebilecektir. Uluslararası hukuka yapılan atıf, yalnızca cezai konularda karşılıklı yardımla ilgili uluslararası anlaşmalara değil, aynı zamanda Interpol çerçevesinde iş birliğinedir. Ayrıca, bu ilke aynı zamanda, polis organları arasında sınır ötesi veri iletişimini iyileştirmek için tasarlanan komşu devletler arasındaki anlaşmaların varlığını da dikkate almaktadır[30]. Tavsiye karar elbette ki sadece polisin gerçekleştireceği eylemlerde değil aynı zamanda uygulamacı otoriteler ki bunlar yerel kanunlarla kişisel veri işlemeye yetkilendirilmiş özel ve kamu kuruluşları ile savcılık gibi kamu kurumlarının gerçekleştireceği eylemlere de uygulanacaktır[31]. Bu kişiler veri kontrolörü olarak verilerin işlenmesinin her sürecinden sorumludurlar. Toplanacak olan veriler bakımından en önemli husus bunların gereklilik, orantılılık ve belli başlı amaçlar dahilinde toplanmasıdır. Tavsiye karar, yukarıda ifade edildiği

---

29 87 (5) Tavsiye Karar 1-8. maddeler. Polis ve cezai konularda verilerin işlenmesinin kişiler üzerindeki önemli etkileri nedeniyle tavsiye kararın uygulamada polis işlerinde kişisel verilerin kullanılmasına yönelik kullanma kılavuzu yayınlanmıştır.https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5, s.2.

30 Mireille M.Caruana, '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, 2017, s.(1-22), s.15.

31 https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5, s.3.

gibi, adli ve idari veriler arasında bir ayırımı öngörmektedir. Ayrıca, verinin hangi amaçla toplandığını, örneğin veri sahibinin şüpheli ya da fail mi yoksa tanık ya da mağdur mu olduğu belirtilmelidir. Polis sektöründe verilerin bildirimi ya da transferinin gerçekleştirilmesi gereken hallerde bilginin paylaşılması hususunda meşru bir menfaatin olup olmadığı da araştırılmalıdır.

Suçların siber alanda daha sık ve kolay işlenebilir hale gelmesi, yeni suç tiplerinin de oluşmasına yol açmıştır. Sanal dünyada işlenen fiillerin bütün veri işleme sistemlerini de etkiler nitelikte oluşu Avrupa Konseyi'ni Siber Suç Sözleşmesi'[32]ni düzenlemeye sevk etmiştir. Avrupa Konseyi üyesi olmayan ülkelerin de imzasına açılan sözleşme, en önemli ve geniş katılımlı uluslararası sözleşme özelliği sergilemektedir. Bilgi ağı ve internet üzerinde işlenen hukuk ihlallerinin cezalandırılmasını öngören sözleşme, siber suçlarla mücadele yönünde iletişimin ve bilgisayar ağının denetlenmesine de cevaz vermektedir. Sözleşme her ne kadar verilerin korunmasını doğrudan desteklemeyi amaçlamamaktaysa da taraf devletlerden veri sahibinin haklarının korunmasını ihlal edebilecek fiillerin cezalandırmasını talep etmektedir[33].

B. Avrupa Birliği Bünyesinde Kabul Edilen Hukuki Düzenlemeler

Avrupa Birliği düzeyinde kişisel verilerin korunmasına yönelik mevzuat çalışmaları Lizbon Antlaşması öncesinde başlamış ve gerek birincil gerekse ikincil hukuk çerçevesinde birtakım düzenlemeler kabul edilmiştir. Bunların en başında gelen düzenleme, 2000 yılında kabul edilen Avrupa Temel Haklar Şartıdır[34]. Şart, 7. maddede özel hayatın gizliliği hakkını, 8. maddede ise kişisel verilerin korunması hakkını ayrı ayrı düzenlemiş, 8. maddenin 2. fıkrasında kilit veri koruma ilkelerine de atıfta bulunmuştur. Son olarak, 8. maddenin 3. fıkrasında bu ilkelerin uygulanmasını kontrol etmek için bağımsız bir otoriteye atıf yapılmıştır[35].

---

32 Convention on Cybercrime CETS no.185, Budapeşte, 23.11.2001.

33 Handbook on European Data Protection Law, s.280.

34 18.12.2000/c 364/01, Charter of Fundamental Rights of the European Union, http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

35 EU (2012), Charter of Fundamental Rights of the European Union, OJ 2012 C 326. Madde 8 Kişisel bilgilerin korunması:

1. Herkes, kendisine ilişkin kişisel bilgilerinin korunmasını isteme hakkına sahiptir.

2. Bu tür bilgiler, belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında top-

2009 tarihinde Lizbon Antlaşması[36]'nın kabul edilmesi ile kişisel verilerin korunması Avrupa Birliği antlaşma metnine dâhil edilmiştir. Bu kapsamda en önemli yenilik Antlaşma ile Avrupa İnsan Hakları Temel Şartı'nın Birliğin birincil hukuk kapsamına dahil edilmesidir[37]. Avrupa Birliği'nin İşleyişine Dair Antlaşma (ABİA) madde 16[38] ile AB kurumlarına kişisel verilerin korunması hususunda mevzuat düzenleme yetkisini tanımaktadır. ABİA 16/2. fıkrası Parlamento ve Konsey'e AB hukuku kapsamında kişisel verilerin işlenmesi alanına uygulanacak olan kuralları belirleyebilmek için yeni bir hukuki temel sunmaktadır. Madde, 2016/679 sayılı Genel Veri Koruma Tüzüğü'ne ve 2016/680 sayılı Direktif'e yasal zemin teşkil etmiştir.

Lizbon Antlaşması öncesi AB ikincil hukukta verilerin korunmasına yönelik temel yasal düzenlemeyi Mayıs 2018'e kadar yürürlükte olan 95 tarihli Direktif oluşturmuştur[39]. AB üye ülkeler arasında kişisel verilerin korunması

---

lanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir.

3. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir.

36 Treaty Of Lisbon Amending The Treaty On European Union And The Treaty Establishing The European Community (2007/C 306/01), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT

37 Lizbon Antlaşması 6. madde: Birlik, 12 Aralık 2007 tarihinde Strazburg'da uyarlandığı haliyle, Antlaşmalar'la aynı hukuki değere sahip olan 7 Aralık 2000 tarihli Avrupa Birliği Temel Haklar Şartı'nda yer alan hakları, özgürlükleri ve ilkeleri tanır. Şart'ta yer alan hükümler, Birliğin Antlaşmalar'da belirlenen yetkilerini hiçbir şekilde genişletmez. Şart'ta yer alan haklar, özgürlükler ve ilkeler; Şart'ın yorumlanması ve uygulanmasının düzenlendiği VII. Başlığı altındaki genel hükümlere uygun olarak ve Şart'ta bu hükümlerin kaynaklarını ortaya koyan açıklamalar gerektiği şekilde göz önünde bulundurularak yorumlanır.

2. Birlik, İnsan Haklarının ve Temel Özgürlüklerin Korunmasına İlişkin Avrupa Sözleşmesi'ne katılır. Bu katılım, Birliğin Antlaşmalar'da belirlenen yetkilerinde değişikliğe yol açmaz.

3. İnsan Haklarının ve Temel Özgürlüklerin Korunmasına İlişkin Avrupa Sözleşmesi tarafından güvence altına alınan ve üye devletlerin ortak anayasal geleneklerinden kaynaklanan temel haklar, Birlik hukukunun genel ilkelerinin parçasıdır.

38 AB'nin işleyişine dair genel ilkelerinin düzenlendiği ABİA 16. maddesine göre;

Herkes, kendisiyle ilgili kişisel verilerin korunması hakkına sahiptir.

Avrupa Parlamentosu ve Konsey, Birlik hukuku kapsamına giren faaliyetlerin yürütülmesinde, Birlik kurum, organ, ofis veya ajansları ile üye devletler tarafından kişisel verilerin işlenmesi sırasında bireylerin korunmasına ve bu bilgilerin serbest dolaşımına ilişkin kuralları olağan yasama usulü uyarınca belirler. Bu kurallara uyulması, bağımsız otoritelerin denetimine tabidir.

39 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 1995 L 281

mevzuatlarını uyumlaştırmayı hedefleyen 95 tarihli Direktif, AB üye ülkeler arasında verilerin etkin paylaşımlarının sağlanması ihtiyacına binaen kabul edilmiştir[40]. 95 tarihli Direktif, 108 numaralı Sözleşmede yer alan hakları güçlendirmeyi de amaçlamıştır[41]. Ancak 95 tarihli Direktif, polis ve cezai konularda adli işbirliği alanına uygulanmamış[42], bu nedenle 2008 tarihinde Kişisel Verilerin Cezai Konularda İşlenmesine İlişkin Çerçeve Karar ile 108 numaralı Sözleşme ve 95 tarihli Direktifin ilkeleri polis ve cezai konular için de kabul edilmiştir. Çerçeve Karar sınır ötesi iş birliğini düzenlemiş, uygulaması iç güvenliğe sirayet etmemiştir. Bir sonraki başlığımızda 2008 tarihli Çerçeve Kararın hükümleri, 2016/680 sayılı Direktif'e kadar olan süreç içerisinde ele alınacaktır.

Avrupa Birliği Adalet Divanı (ABAD) kararları değerlendirildiğinde, Divan'ın AİHM'e paralel olarak özel hayat kavramını dar yorumlamadığı görülmektedir. ABAD'a göre özel hayat tanımlanmış ya da tanımlanabilir bir bilgiye ilişkin her türlü kişisel verilerin korunmasını içermektedir[43]. ABAD, ilk defa 2008'de Şart'a atıf yaparak verilerin korunması hakkına değinmiştir[44]. Mahkeme, Şart'ı daha önceki dönemlerde yasal olarak bağlayıcı olmasa bile, AB hukukunun genel ilkeleriyle bütünleşik olarak kabul edilmemiş olan temel bir hakkı tanımlamak için kullanmıştır[45]. 2008'de Şart Lizbon Antlaşması ile birincil hukuka ait olduğu kabul edilmiş olsa da Birlik mahkemeleri hala temel haklarla ilgili konularda öncelikle AİHM içtihat hukukunu dikkate almaya ve Şart'ın 8. maddesine atıfta bulunmaya devam etmiştir. Örneğin ABAD'ın Promusicae davası, üye devletlerin, hukuk davaları bağlamında telif hakkının etkin bir şekilde korunmasını sağlamak için kişisel verileri iletme yükümlülüğü getirmelerini talep edip etmedikleri konusunda çeşitli AB hükümleri hakkındaydı. Mahkeme kararında, Şart'ın 7. maddesinin AİHS 8. maddesini önemli ölçüde yeniden ürettiğini, Madde 8'in ise kişisel verilerin korunması hakkını açık bir şekilde düzenlediğini

---

40 Handbook on European Data Protection Law, s.29.

41 EU Data Protection Directive 95/46/EC, Gerekçe 11.

42 Direktif 3. madde.

43 CJEU, Joined Cases C–92/09 and C–93/09 Volker und Markus Schecke and Eifert [2010] ECR I-11063, prg.52.

44 CJEU, C-275/06, Promusicae, 29.1.2008, prg.64.

45 G.G.Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Switzerland, Springer International Publishing. 2014.

belirtmiştir[46]. 2008'de Mahkeme Satamedia davası ile 95 tarihli Direktif'i ele almıştır. Mahkeme'ye göre 95 tarihli Direktifin amacı bireylerin temel haklarını ve gizlilik hakkını korumaktır ki bu hak ifade özgürlüğü ile de örtüşmektedir[47]. 2009 tarihinde Mahkeme, Rijkeboer isimli davada bireylerin kişisel bilgilerine erişme hakkını tartışmıştır[48]. Bu davada, Rijkeboer, Rotterdam'daki bir Kolej'e, son iki yıl içindeki kendi kişisel verilerin üçüncü taraflara ifşa edilip edilmediği hakkında bilgi verilmesini talep etmiş ancak kendisine sadece bir yıllık bilgi verilmiştir. Mahkeme, gerek Şart'a gerekse kişisel verilerin korunması hakkına değinmemiş, 95 tarihli Direktif'te yer alan gizlilik hakkına atıfta bulunmuştur.

2009 yılından sonraki kararlarında ise ABAD, Şart'ın yasal olarak uygulanmasının zorunlu olduğu kabulü ile hareket etmiş, AİHS 8. madde yerine Şart'ın 8. maddesine atıflarda bulunmuştur. Özellikle Schecke ve Eifert davasında[49] Mahkeme, AİHS'i ve AİHM'in içtihadını kullanarak ve aynı zamanda Şart'a da dayanarak karar vermeye başladığını göstermiştir. Bunun en temel nedeni Lizbon Antlaşması'nın 6. maddesi'nin Şart'ın birincil hukuka dahil olduğu yönündeki açık ifadesidir. Mahkeme, Şart'ın 7.ve 8. maddesini birlikte değerlendirerek özel hayatın gizliliği hakkını verilerin işlenmesi sırasında korunması hakkıyla bir arada ele almıştır[50]. Mahkeme'nin 8. maddeyi doğrudan referans aldığı en önemli dava Scarlet davasıdır. Davada, Bir İnternet Servis Sağlayıcısı (ISP) şirketi olan Scarlet Extended SA, elektronik haberleşmeyi filtrelemek ve engellemek için bir sistem uygulamak zorunda bırakılmıştır. Mahkemeden bunun AİHS 8. madde ve 10. maddeye ve Şart'ın 11. maddesine dayanarak AB hukuku çerçevesinde yorumlanması istenmiş, Mahkeme de sorunun fikri mülkiyet haklarının korunması ile ilgili olduğu gerçeğine odaklanmış ve bu hakların korunmasının diğer temel haklara karşı dengelenmesi gerektiğini ifade etmiştir. Buna göre, elektronik haberleşmeyi filtrelemek ve engellemek için kullanılan sistem, müşterinin kişisel bilgilerinin korunmasına ilişkin haklarını ve Şart tarafından korunan bilgileri

---

46 CJEU, C-275/06, Promusicae, 29.1.2008, prg.64.

47 CJEU, C-73/07, Satamedia, 16.12.2008, prg. 52-56.

48 CJEU, C-553/07, Rijkeboer, 7.5.2009.

49 CJEU, Joined Cases C–92/09 and C–93/09 Volker und Markus Schecke and Eifert [2010] ECR I-11063, prg.52.

50 Fuster, 2014, s. 235.

alma veya verme özgürlüğünü ihlal edebilir[51]. Mahkeme'nin ilerleyen yıllarda verdiği kararlar ile kişisel verilerin korunması hakkına doğrudan yapılan atıflar içtihat niteliğini kazanmıştır. 2011 yılında Deutsche Telekom davası[52] ile Mahkeme 95 tarihli Direktifin kişisel verileri koruma amacını taşıdığını vurgulamış, Şart'ın ve Avrupa Birliği'nin İşleyişine Dair Antlaşma'nın maddelerine doğrudan atıflarda bulunmaya devam etmiştir[53].

III. AVRUPA BİRLİĞİ BÜNYESİNDE KABUL EDİLEN CEZAİ KONULARDA POLİS VE ADLİ İŞ BİRLİĞİ'NDE KİŞİSEL VERİLERİN KORUNMASI MEVZUATINDAKİ GELİŞMELER

A. 2016/680 Sayılı Direktif Öncesi Düzenlemeler

2016/680 sayılı Polis Ve Adli İşlerde Veri Koruma Direktifi'ne kadar olan süreçte verilerin korunması hakkı özellikle 95 tarihli veri koruma direktifinin kabul edilmesiyle beraber yoğun bir biçimde ele alınmaya başlanmıştır. Polis ve adli konuların da dahil olduğu Lizbon Antlaşması öncesi sütunlu yapıda üçüncü sütunda kalan adalet, özgürlük ve güvenlik alanı, yasal karar alma bakımından birinci sütundan farklılık arz etmekte, çerçeve kararlar ile yürütülmekte idi. Çerçeve kararlarda da üye devletlerden, hükümlerinin kısa bir süre içerisinde uygulanması talep edilmekteydi. AB Antlaşması'na göre, çerçeve kararlar üye devletlerin hukuklarının uyumlaştırılmalarını sağlamak için düzenlenmişti. Bunlar direktiflerden farklı olarak üye devletlerin onaylaması şartına bağlı değillerdi. Tabi, bu neviden bir fark olmakla birlikte, çerçeve kararlar doğrudan etki göstermediklerinden üye devlet vatandaşlarına, çerçeve kararlardan doğan haklar ve yükümlülüklerle ilgili bir durumu mahkeme önüne getirme gücünü vermemekteydi. Bu ve benzeri nedenlerle üye devletler arasında farklı ve birbirinden bağımsız uygulamalar ortaya çıkmaktaydı. Her ne kadar 108 numaralı Sözleşme'ye ilave edilen Polis sektöründe kişisel verilerin kullanılmasıyla ilgili R 87 (5) tavsiye karar ile ulusal otoritelere kişisel verilerin işlenmesine yönelik tavsiyelerde bulunulmuşsa da bunun bağlayıcı bir metin olmaması bu alanda veri korumayı daha da güçleştirmekteydi.

---

51 CJEU, C-70/10, Scarlet, 24.11.2011, prg.30-51

52 CJEU, C-543/09, Deutsche Telekom, 5.5.2011

53 CJEU, C-614/10, Commission v Austria, 16.10.2012.

2016/680 sayılı Direktif'e kadar polis ve cezai konulara ilişkin mevzuat farklı konularda ve ayrı ayrı düzenlenmişti. Bunlarda kişisel verilerin korunması, ilgili politika alanının Topluluk'un yetkisi dahilinde olup olmadığına bağlı olarak farklı şekillerde ele alınmaktaydı. Polis ve adli makamlar tarafından kişisel verilerin korunmasına ilişkin cezai konularda adli ve polis iş birliği çerçevesinde işlenen kişisel verilerin korunmasına yönelik en temel karar olan 2008/977/JHA Çerçeve Karar[54] bu alanda ortak veri koruma standardının getirilmesi hususunda genel bir mevzuat olarak kabul edilmişti. Ancak buna ilave olarak örneğin Ceza hukuku kapsamındaki veri koruması 2006/616/JHA sayılı Çerçeve Karar ile özellikle terörizm ve sınır ötesi suç ile mücadelede sınır ötesi iş birliğinin derinleştirilmesi düzenlenmişti. 2006/960 /JHA sayılı Çerçeve Karar da üye devletlerin önleyici hizmetlerinde bilgi alışverişini basitleştirmeyi amaçlamaktaydı. Bunların yanı sıra Avrupa ceza sektöründe veri koruma ve bilgi alışverişiyle ilgili çok sayıda başka metin yayımlanmıştı. Özellikle 2005/876 / JHA sayılı Sabıka Kayıtlarından çıkartılan bilgi alışverişine ilişkin Çerçeve Karar; 2007/413 / JHA sayılı Schengen Bilgi Sistemi veya Vizeye ilişkin farklı Çerçeve Kararlar çıkartılmıştı. İlaveten Avrupa ceza hukuku alanında AB ajansları, bireysel veri işleme uygulamalarına dair kendi faaliyet alanlarını da belirleme yetkisine sahiptiler.

2008/977/JHA sayılı ceza adaleti ve bunun icrası hususunda kabul edilen veri koruma çerçeve kararı bu nedenlerle tatmin edici düzeyde bir genel çerçeve olarak kabul edilmemekteydi hatta çerçeve karar birçok eksiklik içermesi nedeniyle de sıklıkla eleştirilmişti ve dolayısıyla fiili olarak mevcut üye ülkeler arasındaki mevzuat farklılıklarını da gidememişti[55]. Çerçeve Karara yönelik en önemli eleştiri konusu kararın kapsamıdır. Kararın sadece üye devletlerin soruşturma makamları arasındaki veri alışverişine uygulanması ve üye devletlerin ulusal topraklarında meydana gelen verilerin işlenmesine uygulanmaması bunlardan biridir[56]. Zira, çerçeve karar sadece

---

54 2018 tarihli Direktif'e kadar yürürlükte kalmıştır. 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.

55 Franziska Boehm, s.171.

56 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 record (PNR), http://rivista.eurojus.it/balance-between-

sınır ötesi transfer ve bilgi alışverişine ilişkin olup, polis ve adli otoriteler tarafından ülke içi kişisel verilerin işlenmesi kapsam dışında kalmaktaydı, sınır ötesi transfer durumunda da kişisel verilerin korunması düzeyi oldukça yetersiz addedilmekteydi[57]. Komisyon da 2008 Veri Koruma Çerçeve Kararı'nın sınırlı kapsamının, AB düzeyinde kişisel verilerin korunmasında yasal ve pratik eksikliklere ve aynı zamanda farklı üye devletlerde farklı veri koruma düzeylerine yol açtığını ve yasal belirsizlik yaratacağını açıkça kabul etmiştir[58]. Çerçeve kararlardan doğan yükümlülük ve sorumlulukların ulusal hukuka uygun olacak şekilde belirlenmesi, ülkeler arası farklı uygulamalar ve standartların getirilmesine yol açmıştır. Ayrıca her ne kadar yeknesaklık konusunda birkaç düzenleme içermişse de bunların uyumlaştırılması çerçeve kararların niteliği gereği çok mümkün olamamıştır[59].

Çerçeve kararda ilkeler genellikle gönüllülük esasına dayalı uygulamayı vurgulamakta, bireylerin hakları ile güvenlikle ilgili veri işleme ihtiyacı arasında ilki aleyhine dengesizlik gözetilmekteydi[60]. Örneğin, Çerçeve Kararın 16. Maddesinde, veri sahibinin bilgi edinme hakkı yer almaktaydı. Madde, üye devletlere kişisel bilgilerinin yetkili makamlarca toplandığını veya işlendiğini bireye ancak "ulusal yasalara uygun" olarak bilgilendirilmesini sağlama yükümlülüğü getirmişti ve bu durum nedeniyle üye devletlerin sayısı kadar farklı uygulama kanununun kabul edilmesinin önü açılmıştı[61]. Karar,

---

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/

57 Thomas Marquenie, The Police And Criminal Justice Authorities Directive: Data Protection Standarts and Impact on the Legal Framework, Computer Law and Security Review, 33, 2017, 325.

58 http://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

59 Paul De Hert, Vagelis Papakonstantinou, 'European Parliament Directorate General for Internal Policies: Policy Department Citizen's Rights and Constitutional Affairs, The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area', Brussel, 2014, s.5.

60 Paul De Hert, Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive, A First Analysis', New Journal of European Criminal Law, Vol.7, Issue 1, 2016, s.8.

61 Viviane Reding, 'The European data protection framework for the twenty-first century', International Data Privacy Law, Volume 2, Issue 3, 1 August 2012, (119–129), s.122.

ulusal düzeyde daha yüksek güvencelere izin vermekte ve polis ve adli iş birliğindeki etkili ve akıcı bilgi alışverişine zarar verebilecek üçüncü ülkelerle daha önce gerçekleştirilen iki taraflı anlaşmaları geçersiz kılmaktaydı. Ancak diğer olumsuz durumlar sebebiyle çerçeve karar, ulusal düzeyde etkin uygulanabilirlik, ülkeler arasında yeknesaklık sağlayamaması gibi nedenler ile uygulanabilirliğini sağlayamamıştır[62].

Bütün bu sorunları gidermeye yönelik olarak düzenlenen 2016/680 sayılı Direktifin amacı, 2008/977 sayılı Çerçeve Karar'dan farklı olarak sadece asgari uyum standartlarını ortaya koymak değil aynı zamanda bu sektörde 'Birlik genelinde bireyler için aynı düzeyde koruma' sağlayarak 'kapsamlı bir uyumlaştırmayı' gerçekleştirmek olmuştur[63].

B. 2016/680 Sayılı Direktif

1. Genel Olarak

2016/680 sayılı Polis ve adalet sektöründe veri koruma direktifi, öncelikle bir yandan terörizm ve diğer ciddi suçlarla mücadelede iş birliğini geliştirirken bir yandan da yüksek düzeyde veri koruması sağlamak ve daha önceki çerçeve kararda işaret edilen eksiklikleri gidermek amacıyla kabul edilmiştir. Lizbon Antlaşması yürürlüğe girdikten sonra, kişisel verilerin işlenmesiyle ilgili olarak, gerçek kişilerin verilerinin korunmasının açık temel bir hak olarak kabul edildiğine daha önce değinmiştik. Avrupa kurumlarının yaklaşımına göre, polis ve ceza adalet bağlamında kişisel verilerin işlenmesi ise diğer bütün kişisel verilerin işlenmesinden farklılaştırılmalıdır. Genel Veri Koruma Tüzüğü'nden farklı olarak bu alanın bir direktifle düzenlenmesi, üye devletlerin kendi ulusal yasalarına göre kişisel verilerin işlenmesine yönelik düzenlemelerde belirli bir esneklik seviyesine izin verilmesi bakımından önem arz etmektedir[64].

ABİA 16. maddesi, daha önce de belirttiğimiz gibi beraberinde kişisel verilerin nitelikleri gereği ve bunların polis işbirliği çerçevesinde serbest dolaşımının korunması hususunda özel kuralların alınmasına yasal zemin

---

62 Lauri J. Pajunoja, s.124.

63 Direktif, Gerekçe 12.

64 http://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/

sunmuştur[65]. ABİA 16/2. maddesinde Parlamento ve Konsey'e AB politikalarına uygulanabilecek AB hukuku kapsamında verilerin korunmasına ilişkin mevzuat gerçekleştirebilme imkanı tanınmıştır. Bu sayede Konsey, üye devletlerdeki kişilerin verilerinin işlenmesi halinde, ortak yabancı ve güvenlik politikalarının gereklilikleri kapsamında hareket ettikleri durumlarda ve bunların serbest dolaşımı hallerinde uygulanmak üzere belli başlı kurallar koymuştur[66].

Direktif, Genel Veri Koruma Tüzüğü[67] (GDPR)'ne ek düzenleme şeklinde ortaya çıkmış, böylelikle, GDPR'de yer alan ilkelerin çoğunu aynı şekilde yansıtarak ve bireyler için yüksek koruma sağlayarak gerekli bilgilerin alışverişini engellememek için yasal temelleri belirleme ve üye devletlerin yetkili makamları arasında etkin iş birliğini sağlama amacını da gözetmiştir[68]. GDPR verilerin işlenmesine uygulanabilecek genel kuralları içerirken, Direktif adli uygulamalarda verilerin işlenmesine uygulanacak spesifik kuralları içermektedir. Dolayısıyla bütün AB hukukuna uygulanabilecek tek tip veri koruma kuralları bulunmamaktadır. Dahası GDPR, tüzük olduğundan Direktife göre uyumlaştırmayı sağlayabilmesi daha kolaydır. Ancak Direktif ile Tüzük arasında belli başlı farklılıklar da bulunmaktadır. Öncelikle, alanın kendine has özellikleri nedeniyle, temel veri koruma ilkeleri Direktifte yer alırken, Tüzükte belirtilen ilkelerin bir kısmı Direktife dahil edilmemiştir. Bunlardan ilki bilgi ve kişisel verilere erişim haklarıdır. Bu haklar, en geniş ölçüde kullanıldıklarında, polisin ve yetkili makamların ceza adalet sistemi içindeki çalışmalarının çoğunu zayıflatacaklardır. Örneğin veri sahibinin rızası, suçların önlenmesi, soruşturulması, tespit edilmesi veya yargılanması görevlerini yerine getirmek için yapılan taleplere uymak için yetkili otorite tarafından emredildiğinde kişisel verilerin işlenmesi için gerekli bir koşul değildir. Buna benzer örneklerde bireyin veri koruma hakkı ile polis ve ceza

---

65 EU Decleration No 21 concerning the Charter of Fundamental Rights of the European Union, annexed to the Final Act of the Intergovernmental Conference adopted the Treaty of Lisbon, 2007.

66 Verilerin sınır ötesi boyutta işlenmesine dair Konsey Çerçeve Kararı 2008/977/JHA 27.11.2008.

67 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, https://eur-lex.europa.eu/legal content/EN/TXT.

68 Viviane Reding, s.122.

adaleti sürecindeki menfaatler arasında doğru dengeye uyulup uyulmadığı, her zaman üye devletlerin Direktifte yer alan muafiyetleri nasıl uyguladıklarına bağlı olmuştur. Polis ve ceza adalet sürecindeki menfaatler, bilgi, erişim ve düzeltme haklarına ilişkin sınırlamaları da içermekte olup, bu sayede üye devletler bireyin veri koruma hakkı ile polisin ve diğer ceza adalet sistemi otoritelerinin veri işleme çıkarları ve endişeleri arasında bir denge kurmaya çalışmaktadır.

Direktif 10 bölümden oluşmaktadır. İlk beş bölüm Direktifin kapsamı, veri işlenmesine ilişkin genel ilkeler, kontrolör ve işleyicinin sorumlulukları, kişisel verinin güvenliğini teminini sağlamak için teknik ve organizasyonel düzenlemeler, verilerin üçüncü kişiler ve uluslararası organizasyonlarla paylaşımını oluşturmaktadır. Direktifin ikinci kısmı bağımsız denetim otoritelerinin statülerini, görevlerini ve yetkileri ile denetleyici makamlara şikâyette bulunma hakkı, bir kontrolöre veya işleyiciye karşı etkili bir adli çözüm hakkı ve kişisel verileri yasal olmayan bir şekilde işlenmesi sonucunda maddi veya manevi zarar görmüş herhangi bir kişiye tanınan tazminat hakkıdır. Direktif görünürde geniş bir yaklaşım sergilemektedir ancak gerçek kapsamı daha dardır. Direktifin kapsamı suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai yaptırımların uygulanması amacıyla yetkili makamlar tarafından kişisel verilerin işlenmesi ile sınırlıdır. Kişisel verilerin ceza soruşturması ve kovuşturması esnasında işlenmesi söz konusu olduğu durumlarda üye devletler, kişisel verileri silme ya da bilgi edinme, giriş ve düzeltme haklarını ulusal hukuklarına uygun olan şekilde yerine getirirler. Bu nedenle, Direktifin polis ve adalet alanındaki veri korumaya getireceği gerçek değeri onun ulusal hukuktaki uygulamasına, aynı şekilde Birlik sathındaki ulusal mahkemelerde uygulanmasının sağlanması ise ulusal mahkemelerin Direktifi uygulamaya istekli olmasına bağlıdır.

2. Direktifin Amaçları ve Kapsamı

6 Mayıs 2018'de yürürlüğe giren Direktifin en temel amacı, bireylerin kişisel verilerinin polis ve ceza adaleti yetkilileri tarafından işlenmeleri durumunda, daha iyi nasıl korunabileceğidir. Direktifin kapsamı, suçun önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai süreçlerin yürütülmesi amacıyla işlenen kişisel verilere ilişkin gerçek kişilerin korunması ve bu tür verilerin serbest dolaşımıdır. Bir başka ifadeyle Direktif, Birlik hukuku kapsamındaki (Birlik hukuku dışındaki işleme faaliyetleri ya da Bir-

lik kurumları, ajansları, ofisleri ve organları hariç) 1. ve 2. maddelerde belirtilen yetkili otoriteler tarafından yürütülen kişisel veri işleme faaliyetlerini kapsamaktadır. Bu faaliyetler, kolluk ve ceza adaleti amaçları kapsamında suçun önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezaların yerine getirilmesi ile kamu güvenliğine karşı tehditlerin önlenmesi ve kamu güvenliğinin bu tehditlerden korunmasıdır. Ulusal güvenlik alanının üye devletlerin bizzat sorumlu oldukları alan olarak kaldığı düşünülebilir. Ancak ABAD'ın kişisel verilerin işlenmesine ilişkin bireylerin korunmasına ve bu verilerin serbest dolaşımına dair kuralların, sınır ötesi boyutu olsun ya da olmasın güvenliğe ilişkin olması halinde, uygulanması gerektiği yönünde birçok kararı bulunmaktadır. Bu temelde, Mahkeme, ulusal hukuk kapsamında faaliyetlerinin ulusal bir kontrolör ve ulusal bir mahkeme tarafından işlenmesinin 'Topluluk hukuku kapsamı dışına' düşmediğine ve bu nedenle de Direktifin 3/2. madde istisnası kapsamına girmediğine karar vermiştir[69]. Bu karar, Direktifin taslak metninde yer alan 'ulusal güvenlik konularının da Direktif'in kapsamı dışında kaldığı' ifadesinin ana metinden çıkartılmasına neden olmuştur[70]. Ayrıca direktif ile terörizm ve AB'deki sınır ötesi suçlar gibi suçlara karşı mücadelede iş birliği kapsamında soruşturmaların daha etkin ve verimli olması bakımından Birlik ülkelerinin adli ve polis mercileri arasında bilgi alışverişinin sağlanması amaçlanmaktadır. Direktifin, iç hukuk verilerini de kapsaması bu alandaki kapsamlı Avrupa veri koruma rejiminin oluşturulması bakımından önemli bir adım olarak görülmektedir[71]. Zira Direktif, AB üye ülkelerin polis ve ceza adaleti alanındaki veri koruma kurallarının daha fazla uyumlaştırılmasını amaçladığı için, 95/46 / EC sayılı Direktif ve GDPR'nin yaklaşımını takip ederek, yerel işleme sürecine de

---

69 CJEU Joined Cases C-465/00, C-138/01, and C-139/01 Rechnungshof [2003] ECR I-04989, prg. 41–43; Case C-376/98 Germany v Parliament and Council [2000] ECR I-08419, prg. 85; Case C-491/01 British American Tobacco and Imperial Tobacco [2002] I-11453, prg. 60.

70 Ancak, ulusal güvenlik konularının kapsam dışı olduğu ifadesi Gerekçe14'te varlığını sürdürmektedir. 'Since this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU) should not be considered to be activities falling within the scope of this Directive.' https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680.

71 Thomas Marquenie, s. 330.

başvurmaktadır. Bu, ne Şart'ın 8. Maddesi ne de ABİA 16. maddeden kaynaklanan, yerel ve sınır ötesi işlem süreci arasında bir ayrım yapılmamasına değil ancak AB hukuku kapsamında yer alan işleme faaliyetlerine ve kişisel verilerin serbest dolaşımına atıfta bulunulduğu için gereklidir[72]. Böylelikle, 2008 tarihli çerçeve kararın en çok üzerinde durulan eksikliği de giderilmiş, AB bünyesindeki bütün güvenlikle ilgili otoritelerin kendi rutin kişisel veri işleme faaliyetlerine Direktifte yer alan hükümleri uygulama imkanı ortaya çıkmıştır[73].

Direktifin kapsamı dışındaki bir başka alan olan ortak dış ve güvenlik politikasına ait hususlar Lizbon Antlaşması'nın 39. maddesi ile belirlenmiştir. Maddeye göre *'Avrupa Birliği'nin İşleyişi Hakkındaki Antlaşma'nın 16. maddesine uygun şekilde ve aynı maddenin 2. paragrafına istisna olarak, Konsey, bu Bölüm kapsamındaki faaliyetlerin yürütülmesinde, üye devletler tarafından kişisel verilerin işlenmesi sırasında bireylerin korunmasına ve bu verilerin serbest dolaşımına ilişkin kuralları belirleyen bir karar kabul eder. Bu kurallara uyulması, bağımsız otoritelerin denetimine tabidir.'*

Direktifin 2. maddesi ile kapsam 'kişisel verilerin tamamen ya da kısmen otomatik araçlarla işlenmesine ve kişisel verilerin otomatik araçlar haricinde bir dosyalama sisteminin parçasını oluşturan veya bir dosyalama sisteminin parçasını oluşturması amaçlanan araçlarla işlenmesine uygulanır' şeklinde belirlenmiştir. Şayet kişisel verilerin bir dosyalama sisteminde yer alması ya da bulundurulması amaçlanmışsa, verilerin manüel işlenmesi de madde kapsamında değerlendirilecektir[74]. Dosyalama işlemi için elektronik ortam gerekmemektedir. Otomatik araçlarla veri toplanmasının en tipik örneği iletişimin denetlenmesi, verilerin belli şekillerde zorunlu toplanması, teknik araçla izlemedir[75]. Otomatik araçlarla işlenmesi belli kriterleri taşımalıdır. Dosyalama işlemi belli amaçlarla manuel de gerçekleştirilebilmektedir ancak bunun için belli kriterler olmalıdır. Bu kriterlerin tanımına bağlı olarak, bir dosyaya bir belge numarası verilmesi ve bir şekilde suçun türüne veya

---

72 Vivien Reding, s.123.

73 Paul De Hert&Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive, A First Analysis', s. 10.

74 Direktif Gerekçe 18.

75 Matthias Baecker, 'Gerrit Hornung, Data Processing by Police and Criminal Justice Authorities in Europe-The Influence of the Commission's Draft on the National Police Laws of Criminal Procedure', Computer Law&Security Review, 28, 2012, s.630.

bireyin niteliklerine göre sınıflandırılması yeterli olacaktır. Ancak elektronik işlem sistemlerinin yaygın dağılımı büyük olasılıkla yakın gelecekte Direktifin kapsamına giren ceza adaleti makamları tarafından yürütülen neredeyse tüm veri işlemlerine sirayet edecektir. Ancak o zamana kadar örneğin, bir şüphe üzerine polisin kişiyi durdurup üst aramasında bulunması gibi durumlar Direktifin kapsamı dışındadır[76].

Direktifi uygulayacak olan makamlar 3. madde uyarınca suçun önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai süreçlerin yürütülmesi ile kamu güvenliğinin sağlanması ve kamu güvenliğine karşı tehditlerin önlenmesi hususunda yetkili olan makamlardır. Bununla birlikte, üye devlet hukuku tarafından suçları önleme, soruşturma, tespit etme veya kovuşturma veya kamu güvenliğine yönelik tehditlerin önlenmesi ve bunlara karşı korunmanın dahil olmak üzere cezai yaptırımların uygulanması amacıyla kamu otoritesini ve kamu yetkilerini kullanma yetkisi verilen herhangi bir organ veya tüzel kişilik de yetkili makam olarak kabul edilecektir. Bu çok geniş tanım içerisine polis ve adli makamlar gibi klasik hukuk uygulayıcı makamların yanı sıra sınır görevlileri, özel güvenlik görevlileri gibi özel girişimler ve organizasyonlar da dahil olabilecektir ki bu durum Direktif ile GDPR'nin uygulama alanlarını belirlemeyi bulanıklaştırmaktadır[77]. Ayrıca, üye devletler hukuk uygulamaları ya da idari amaçlarla yetkili otoritelerin faaliyetlerini kendi iç hukuklarına göre belirleyebileceklerdir. Böylelikle aynı neviden veri işleme faaliyetleri, bu faaliyeti idari ceza kapsamında ele almış olan bir üye ülkede GDPR hükümlerine tabi olacak iken adli ceza kapsamında ele almış olan bir başka ülkede Direktifin kapsamında değerlendirilecektir[78].

Direktif, suçların kovuşturulması amacıyla yetkili makamlar tarafından kişisel verilerin işlenmesini düzenlemekle birlikte, kişisel verilerin bir mahkeme kararında, ceza soruşturması veya yargılama sürecinde işlenen kayıt veya dava dosyasında yer alması durumunda, üye devletler AB düzenlemelerinin yerine kendi yasalarında yer alan düzenlemeleri uygulayabilecektir[79].

Direktif ilk bakışta geniş bir uygulama alanına sahip olduğu kanısını

---

76 Baecker&Hornung, s.630.

77 Caruana, s.5.

78 Caruana, s.5.

79 Direktif madde 18.

uyandırsa da birçok açıdan sınırlandırılmıştır. Direktifin kapsamı dışında olan 'ulusal güvenlik' ve direktif kapsamında olan 'kamu güvenliğine karşı tehditlere yönelik korunma' kavramları arasında net bir ayırım ya da kavramlara ait belli başlı tanımların olmaması birer sorun olarak nitelendirilmekte ve bu muğlak istisna üye devletler arasında yeterli veri koruma tedbirleri olmadan gereğinden fazla işleme faaliyetlerini meşrulaştırmak için kullanılmasına neden olmaktadır[80]. Bir diğer sınırlama vesilesi olan üye devletlerin muhakeme işlemleri ve bunların belirli veri koruma gereklilikleri için hareket eden organlar ile Birlik kurum ve kuruluşlarının Direktif kapsamında bulunmaması (Madde 3/3), direktifin kapsamında önemli bir sınırlama teşkil etmektedir. Direktifin uygulanmasına ilişkin somut kuralların eksikliği ve 3. maddedeki istisnalar, Direktifin kapsamını zayıflatacak hususlardır. Bütün bu hususlara rağmen tamamen iç hukuktaki uygulamaların ve yargısal faaliyetlerin veri işleme kapsamına dahil edilmesi, temel veri işleme ilkeleri üzerine inşa edilmiş yeni güvencelerin kabul edilmesi ve teknolojiyle veri işleme yöntemlerinde en güncel değişiklikleri bilerek, önceki Çerçeve Kararda yer alan durumları geliştirmesi, Direktifin en önemli başarılarındandır.

3. Direktifin İlkeleri

Kişisel verilerin korunmasının temel bir insan hakkı olarak öngörülmesi, bunların işlenmesi halinde birtakım ilkelere uygun hareket edilmesini de beraberinde getirmektedir. Polis ve ceza adaleti sektöründe, yerleşik Avrupa veri koruma ilkelerine giriş ve bu ilkelerdeki gelişme önemli bir adım olarak görülmektedir. Direktif bir yandan bu sektördeki veri işlemenin benzersiz niteliğini göz önünde bulundurarak genel ilkeleri desteklemekte bir yandan da kişisel veri sahibinin haklarını korumayı ve veri kontrolörlerine veri işleme esnasında rehberlik etme görevini yükleyerek temel güvenlik önlemlerini belirlemeyi hedeflemektedir[81].

Direktifin ikinci bölümünde buna ilişkin ilkeler yer almaktadır. Bu ilkeler GDPR ile neredeyse aynı niteliktedir. Direktif'in 4. maddesi veri işleme faaliyetlerinin, amaç sınırlaması, veri azaltması, doğruluk, yasallık, adalet,

---

80 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.

81 Thomas Marquenie, s.331.

şeffaflık ile hem dürüstlük hem de gizlilik gereksinimlerini karşılaması gerektiğini belirtmektedir. 8 ve 9. maddeler, işlenecek olan verileri ve aynı zamanda işlemin amaçlarını ve bunların bir yasa tarafından belirlenen yetkili makamların görevlerini yerine getirmesi için gerekli olan işlem faaliyetlerini düzenlemektedir. 5. madde, kişisel verilerin saklanmasına ilişkin zaman sınırlaması öngörmemekte ise de üye devletlere, kişisel verilerin silinmesi veya kişisel verilerin depolanması ihtiyacının periyodik olarak gözden geçirilmesi için uygun zaman sınırlamaları getirmeleri hususunda açık bir çağrıda bulunmaktadır. Bu durum saklama süresine ilişkin uyumlaştırmayı oldukça güçleştirmekte ve Direktifin etkin uyumlaştırmasının önündeki en önemli engellerden biri olarak kabul edilmektedir[82].

Direktifin en önemli maddelerinden biri olan 6. madde, veri sahipleri arasında kategori oluşturan maddedir. Bu doğrultuda Direktif, veri sahibinin suçla ilgisine ve derecesine bağlı olarak verilerin sınıflandırılması ve ele alınmasının önemini kabul etmektedir. Direktif, kanunu uygulayan otoritelere farklı kategorideki insanların verileri arasında net bir ayrım yapılmasını öngörmektedir. Bu kategori şu şekildedir; Ciddi bir suç işleyen ya da işleme şüphesi altında olanlar; Bir ceza mahkûmiyetine uğrayan kişiler; Bir suç mağduru olanlar ya da suç mağduru olduğuna inanlar; Tanıklar. 7. madde gerçeklere dayanan ve kişisel değerlendirmelere dayanan kişisel veriler arasında bir ayrımın korunması gerektiği ve aynı zamanda verilerin ilgili kurumlara iletilmeden veya sunulmadan önce gerçekliğini, güvenilirliğini ve eksiksizliğini doğrulama gerekliliğini belirtmektedir. Bilginin güvenilirliği ve doğruluğu üye devletlere bırakılmıştır. Verilerin doğru olmaması, uyumsuz ya da artık güncel olmaması durumlarında, veriler yetkili üye devletler tarafından iletilmez ya da kullanılmaz. AB Ajansları da üye devletler tarafından sağlanan bilgi kaynağının doğruluğu ve güvenilirliğinden şüphe duyduğunda, yetkili ulusal makamlarca sağlanan bilgileri iletmez ve kullanmaz[83]. Kişisel verilerin yanlış veya yasalara aykırı şekilde aktarıldığına karar verilirse, alıcı gecikmeden bilgilendirilir. Böyle bir durumda, kişisel veriler düzeltilecek, silinecek veya Madde 16'ya göre işlem kısıtlanacaktır.

Direktif 10. madde ile özel kategori verilerin işlenmesi düzenlenmekte-

---

82 Celine C.Cocq, 'EU Data Protection Rules Applying to Law Enforcement Activities, New Journal of European Criminal Law', Vol.7, Issue 3, 2016, s.270.

83 Cocq, s.272.

dir. Direktif'e genetik ve biyometrik verilerin dâhil edilmesiyle dini inançlar, cinsel yaşam, siyasi görüş ve ırksal köken gibi geleneksel hassas kategorilerin kapsamı genişletilmiş, son teknolojik gelişmelere dikkat çekilmiş ve veri sahibinin hayatı üzerinde daha büyük bir etki yaratabilecek hassas verilerin işlenmesine ilişkin özel bir koruma sağlayan uygun bir rejim oluşturulmuştur. 11. madde ile profilleme ve otomatik karar alma hakkında belli başlı kurallar ortaya konmuştur. Bu türden profilleme ve otomatik kararlar genellikle, yalnızca otomatik işlemeye dayalı olduğunda ve veri sahibi için olumsuz yasal etkiler oluşturduğunda veya bunları önemli ölçüde etkilediğinde yasaktır. Profil oluşturma, bir kolluk kuvveti faaliyeti bağlamında veri sahibini olumsuz yönde etkilerken, Direktif, söz konusu kişilerin özel hayatlarına gereksiz müdahaleleri azaltmaya yönelik önlemler sağlamaktadır. Sadece kanun tarafından yetkilendirildiği ve veri sahibinin hak ve özgürlükleri için uygun güvencelerle karşılandığı zaman, veriyi etkileyecek kararlar verilebilir. Bu kararlar özel kategorilerden biri hakkında olduğunda, Direktif veri sahibinin hak ve özgürlükleri ile meşru çıkarlarını korumak için daha fazla uygun önlem alınmasını talep etmektedir. Buna rağmen, bu neviden kararlar kişinin ayrımcılığa uğramasına neden olursa yasaklanacaktır. Özel hassas veriler kategorisinin özellikli durumu nedeniyle, depolama için saklama sürelerinin açık bir şekilde tanınması ile veri türleri ve sahiplerine ilişkin kategoriler oluşturulması, veri sahiplerini korumak ve kolluk kuvvetlerinin etkinlik ve doğruluğunu artırmak için getirilen önemli yeniliklerdir[84]. Direktif kamu otoritelerine verilerin işlenmesi hususunda birtakım ana noktaları hatırlatmaktadır. Bunlar verilerin işlenme sürecinin adil ve hukuka uygun; belli ve meşru bir amaç doğrultusunda; işlendiği amaçla bağlantılı olarak birbiriyle bağlantılı, ölçülü ve yeterli olacak şekilde; gerekli olduğu durumlarda güncellenmiş ve doğru bir biçimde; işlenme amacı için gerekli olduğu süre içinde bireylerin kimliklerinin tutulması; hukuka aykırı ve yetkisi dâhilinde olmayan kişiler tarafından bilgilerin işlenmesine karşı korunmasıdır.

Daha önce belirtildiği gibi, Direktif AB hukuku dışındaki veri işleme sürecine uygulanmaz. Bu hüküm, ulusal güvenlikle ilgili faaliyetlerle, ulusal güvenlik meseleleriyle ilgilenen kurumların veya ulusal güvenliğe dair konularla ilgilenen birimlerin faaliyetleri ve Lizbon Antlaşması 2. Bölüm

---

84 Colonna, Liane, "The new EU proposal to regulate data protection in the law enforcement sector: raises the bar but not high enough", IRI Promemoria 2012, Issue 2, s. 5. https://docplayer.net/31141949-Iri-pm-iri-promemoria-2-2012-liane-colonna.html

V Başlık altındaki aktiviteleri gerçekleştiren üye devletlerin kişisel veri işlemeleri ile ilgili olarak yorumlanmıştır[85]. Ancak bu yorum 1. maddede yer alan kapsamda belirtilen kamu güvenliğine yönelik tehditlerin önlenmesi için öngörülen amaçlarla kısmen çelişki yaratmaktadır. Zira maddede tanımlanmamış olsa bile, kamu güvenliğine yönelik faaliyetler kavramı, kamu güvenliğine yönelik tehditlerin önlenmesi faaliyetlerini de kapsamaktadır.

4. Veri Sahibinin Hakları

Direktifin üçüncü bölümü veri sahibinin hakları ve bunların kullanılmasına ayrılmıştır. Bu bölümde veri sahibine birtakım hakların tanınması, bunlara ilişkin kısıtlamalar, bunların tatbiki ve uygulanma şekilleri ile bir dizi kural ve prosedür yer almıştır. 12. madde bu hakların kullanılmasına yönelik genel usulleri belirtir. 13. madde ve devamında veri sahibine; denetleyicinin kimliğini ve veri işleme görevlisini, işlemin amaçlarını ve denetleyici makamla ilgili bir şikâyette bulunma veya kişisel verilerin düzeltilmesini veya silinmesini isteme hakkı düzenlenmiştir. 14. madde ile veri sahibine, kendileriyle ilgili kişisel verilere erişme ve kişisel verilerini içeren mevcut işleme faaliyetleri hakkında bilgi edinme hakkı verilmektedir. Veri sahibinin talebi üzerine kendisine işlemin amaçları ve hukuki temeli ile ilgili bilgiler verilecektir. Ayrıca verilerin ve veri depolama dönemlerinin kaynağı ve alıcıları hakkında daha fazla bilgi de veri sahibine sağlanacaktır. 16. madde veri sahibine kişisel verilerin düzeltilmesi veya silinmesi ya da bazı hallerde işlenmesini temin etme fırsatı da sunmaktadır. Kişisel verilerin, yasal zorunluluk ya da belli başlı veri koruma standardının ihlali gibi nedenler neticesinde silinmesi veya hatalı olması durumunda düzeltilmesi mümkündür.

Belirtmek gerekir ki GDPR'den farklı olarak, Direktifte yer alan bütün haklar mutlak değildir ve bunlara cezai soruşturma ve kovuşturmaların gizliliği ve bütünlüğünün korunması ve de sınırsız kullanılmalarının polis ve ceza adalet sistemini işlemez hale getirmesi ihtimaline binaen belli başlı sınırlamalar getirilmiştir. Bunlardan biri, kanuni ve cezai usulleri engellemekten, başkalarının hak ve özgürlüklerini korumaktan veya ulusal ya da kamu güvenliğini sağlamak amacıyla, kontrolörün veri sahibine bilgi sunma yükümlülüğü, bu yükümlülüğün ilgili kişilerin temel hak ve meşru çıkarlarına gereken özeni gösterecek şekilde demokratik bir toplumda gerekli ve orantılı

85 Direktif Gerekçe 14.

kanunlarla kısıtlanabilmesi, ertelenebilmesi veya ihmal edilebilmesidir. Bu durumda veri sahibi haklarını kullanmaktan mahrum kalabilecektir. Ancak kısıtlanan bu hak, veri sahibinin ceza adaleti makamlarının eylemleriyle karşı karşıya kaldığında özellikle önemlidir. Bu tür makamlar genellikle veri sahibinin katılımı veya bilgisi olmaksızın büyük miktarlarda kişisel verileri toplama yetkisine sahiptir[86]. Bu nedenle özellikle yerel kanunlarda veri sahibine, gizli soruşturma tedbirlerinin bitiminden sonra bilgi verme yükümlülüğü bulunmaktadır. 15. madde veri sahiplerine veriye girme taleplerinin ya da sınırlama ve silme taleplerinin reddedilmesi halinde bu karara karşı şikâyette bulunma haklarının hatırlatılarak ve reddedilme gerekçesi bildirilerek haberdar edilmesini düzenler. Amaçlardan birine halel gelmediği sürece reddin sebepleri de açıklanır. Bununla birlikte, 17. madde veri sahibinin bilgi edinme, kişisel verilere erişme ve düzeltme ya da silme haklarının yukarıda belirtilen istisnalar ile sınırlandırılması ya da reddedilmesi durumunda, veri sahibine denetim otoritesinin bu hakları kendi yararına kullanılmasını talep etmek hakkını da bahşetmektedir. Direktifin veri sahibinin haklarına ilişkin hükümleri GDPR'ye benzer şekilde kapsamlıdır ve Direktif bu hakların korunmasına ilişkin bir dizi yeterli önlemi sağlamaktadır. Bu hakların kullanılmasında idari ve usuli sınırlamalar da ele alınmaktadır. Veri sahibi kendisine ilişkin veri işleme faaliyetleri hakkında, bu haklarını kullanabilmesi amacıyla, şikâyetlerinin dosyalanması, daha fazla bilgiye erişilmesi, verilerin düzeltilmesi veya silinmesi taleplerinde bulunabilmesi ve gerektiğinde denetim otoritesine de güvenebilmesi konusunda yeterli düzeyde bilgilendirilir. Kamu yararı, başkalarının özgürlükleri ve cezai soruşturmaların bütünlüğü için belirli kısıtlamaların varlığı, bu hakların sağladığı korumayı tamamen geçersiz kılmak adına kullanılamayacaklardır[87].

Yukarıda belirtilen ve kişisel verileri işlenen bireylere, verilerini hangi amaçla ve ne şekilde işlendiğine karar veren yetkili otoritenin adı ve iletişim bilgilerini, verilerinin işleniş amacını, denetleyici kuruma şikâyette bulunma hakkını ve bu otoriteye ait iletişim bilgilerini, kişisel verilerin işlenmesinin sınırlandırılmasını ve ayrıca tamamen silinmesini ya da düzeltilmesini veya bunlara erişim hakkını talep edebilmeleri kamu otoriteleri tarafından sağlanmalıdır.

---

86 Baecker&Hornung, s.631.

87 Thomas Marquenie, s.332.

Risk altında bulunan verilerin güvenliğinin sağlanması için teknik ve örgütsel tedbirlerin de alınması gerekmektedir. Bu kapsamda yetkisiz otoritelerin kişisel verilere müdahale, bunları elde etme ve bunlara giriş yapma teşebbüslerinin reddedilmesine; bunların okunması, kopyalanması, veri ortamının değiştirilmesi ya da silinmesinin önlenmesine; kişisel veri girişinin yetkili olmayan kişilerce yapılmasının önlenmesine; kayıt altına alınmış kişisel verilerin silinmesi ya da okunması ve değiştirilmesinin önlenmesine yönelik tedbirler de alınmalıdır[88].

Daha önce de belirtildiği üzere veri sahibinin rızası, GDPR 7. maddeden farklı olarak, Direktifte yer almamaktadır. Bu nedenle rıza, suçların önlenmesi, soruşturulması, tespit edilmesi veya yargılanması görevlerini yerine getiren yetkili makamlar tarafından kişisel verilerin işlenmesi için gerekli ya da tek başına geçerli bir koşul değildir[89]. Rıza verilerin işlenmesi için yasal bir zemin olarak düzenlenmemiştir ve bu nedenle ceza adalet makamlarının veri işlemeleri için yasal bir gerekçe oluşturamaz[90]. Verilerin işlenmesi için rıza aranmamakta ise de veri sahibi, üye devletlerin kanunlarına göre, Direktifin amaçları doğrultusunda diğer faaliyetlerde kişisel bilgilerinin işlenmesine onay gösterebilecektir. Örneğin soruşturmalarda DNA testleri ya da cezaların infazında elektronik etiketlerle yerini bildirmeye rıza gösterme bunlardan birkaçıdır[91].

5. Veri Denetleyicisinin (Veri Kontrolünün) Yükümlülükleri

a) Genel Yükümlülükler

Direktifin 4. bölümünde veri kontrolörü ve işleyicisinin yükümlülükleri düzenlenmiştir. 19. maddeye göre, işleme faaliyetinin hem doğası hem de amaçlarının yanı sıra veri sahibinin özgürlüklerine karşı potansiyel riskleri göz önüne alarak Direktif ile uyumlu bir biçimde uygun teknik ve organizasyonel tedbirleri sağlamak veri kontrolörünün görevidir. Kontrolör, veri işleme faaliyetlerinin doğasıyla orantılı olduğunda uygun veri koruma politikalarının uygulanması ile görevlendirilecektir. Direktif, üye devletlere özel ve olağan veri korumasını sağlamak için teknik ve organizasyonel ted-

88 Viviane Reding, s.126.

89 Direktif Gerekçe 37.

90 Baecker&Hornung, s.630.

91 Direktif Gerekçe 35.

birlerin ve prosedürlerin uygulanmasını yükümlü kılmıştır. 20'nci maddeye göre, kontrolör, son teknolojilerin uygulama maliyeti ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarını değerlendirir. Bunların yanı sıra işleme faaliyetinin kişilerin hakları ve özgürlükleri açısından teşkil ettiği çeşitli riskleri de dikkate alır. Bu sayede hem işleme yönteminin belirlenmesi esnasında hem de işleme faaliyeti esnasında, veri koruma ilkelerinin etkili bir şekilde uygulanması ve Direktifin gerekliliklerinin yerine getirilmesine yönelik olarak gerekli güvencelerin entegre edilmesi amacı ile tasarlanan takma ad kullanımı gibi uygun teknik tedbirleri uygular. Böylelikle veri sahiplerinin haklarını korur.

Bu koruma yöntemlerinden biri olan olağan veri koruması, verilerin korunmasına izin veren tekniklerin geliştirilmesinde veri koruma değerlendirmesini içeren herhangi bir hizmet veya işletme tarafından kullanılan yöntemi ifade eder. Kontrolör veri korumasını başlangıçtan itibaren destekler. Olağan veri koruması, örneğin bir müşteri yeni bir teknolojik ürün veya hizmet aldığında en katı ayarların otomatik olarak uygulanacağı anlamına gelir. Bir yandan diğer koruma türü olan özel veri koruma kullanılan metotları oluştururken, olağan veri koruması, bu yöntemler yoluyla sağlanan minimum koruma seviyesini oluşturmaktadır[92]. Özel veri koruması bakımından, işleme fiillerine ilişkin gerekli önlemleri uygulamak için teknik ve organizasyonel tedbirler alınmalıdır[93].

Direktif 21 ila 23. maddeler arasındaki düzenlemeler kontrolörler ve veri işlemcileri için ortak özel maddelerdir. Veri işlemcileri kişisel verileri sadece kontrolörün talimatları altında işleyebilir ve veri sahibinin haklarını ve işlem faaliyetinin amaçlarını, niteliğini ve süresini belirleyen bağlayıcı sözleşme ile bu faaliyetleri yürütür. 24 ve 25'inci maddeler, işleme faaliyetlerinin kayıtları ve bunların nasıl tutulması gerektiğini düzenlemektedir. Veri kontrolörü, veri işleyicilerin kayıtların girilmesi ve kayıtların tutulmasını gerektiren ve veri koruma kurallarına uygunluğun gösterilmesini destekleyecek olan, şeffaflık, hesap verebilirlik ve işleme faaliyetlerinin etkin denetimini geliştirecek şekilde ayarlanan kayıt tutma gereksinimlerini belirler. Bu ge-

---

92 Cocq, s.274.

93 Le Métayer, Daniel, 'Privacy by design: a matter of choice' in: Gutwirth, Serge, Yves Poullet and Paul De Hert, Data Protection in a Profiled World, Dordrecht, Springer, 2010, s. 323-326.

reklilikler işleme faaliyetlerinin gerekçelendirilmesi ve eylemin meşruiyetinin uygunluğunun tesis edilmesine yardımcı olacak, aynı zamanda verilerin sorgulanması, ifşa edilmesi ve alınması ile kişinin kimliğinin belirlenmesine yardımcı olacaktır. Ayrıca, Direktifin amacıyla uygunluğun sağlanabilmesi için kayıtlar ve giriş talepleri denetleyici makamlara sunulacaktır.

İşleme faaliyetlerinin kayıt altına alınması halinde bu işlem belli başlı bilgileri de içermelidir. Bunlar, kontrolörün adı ve iletişim bilgileri ile uygulanabilmesi halinde veri koruma memurunun bilgileri; işlemenin amacı; üçüncü ülkeler veya uluslararası kuruluşlardaki alıcılar da dahil olmak üzere, kişisel verilerin açıklandığı veya açıklanacağı alıcı kategorileri; veri sahibi kategorileri ve kişisel veri kategorileriyle ilgili bir açıklama; mümkün ise profillemenin kullanımı; transfer edilen veri kategorileriyle ilgili bir açıklama; kişisel verilerin amaçlandığı transferler de dahil olmak üzere işleme faaliyetinin yasal temeli; mümkün olduğunda, farklı kişisel veri kategorilerinin silinmesi için öngörülen zaman sınırları; mümkün ise Madde 29 (1) 'de belirtilen teknik ve organizasyonel güvenlik önlemlerinin genel bir tanımıdır.

Bir işlem yönteminin bireylerin hak ve özgürlükleri için yüksek bir risk oluşturmasının muhtemel olması halinde 27. madde kontrolörden kişisel verinin korunmasına yönelik işlemin etkisinin önceki değerlendirmesini yönetmesi talep edilir. Bu hal Direktifte 'Veri koruma etki değerlendirmesi (Etki Değerlendirmesi)' olarak nitelendirilmiştir. Bu etki değerlendirmeleri, veri sahipleri ve ilgili kişilerin haklarını ve meşru çıkarlarını göz önünde bulundurmalı, öngörülen işlemleri, geçerli veri koruma önlemlerini ve özgürlüklere yönelik potansiyel riskleri ve bunları yönetmek için kullanılan önlemleri içermelidir. Etki değerlendirmeleri, veri sahiplerinin özgürlük ve hakları için geniş neticeler içermektedir. Ayrıca, kontrolörlerin hesap verilebilirliği ve Direktifte yer alan veri korumayla uygun yükümlülüklere katkıda bulunacaktır. 26 ve 28. maddeler veri kontrolörü ve işlemcilerin denetleyici makamlarla işbirliği yapma ve taleplerin yerine getirilmesine ilişkin gerekli bilgilerin sağlanması yükümlülüğünü getirmektedir.

AB veri koruma modelinin önemli unsurlarından biri, ilgili üye devlette veri koruma yasasının uygulanmasını izleme görevi ile görevlendirilmiş bağımsız bir denetleyici makamın kurulmasıdır. Böylelikle, özel ve olağan veri koruması yoluyla veri koruma ilkelerinin uygulanması ile bir yandan kayıt tutma ve kayıt işlemlerinin gereksinimlerini güçlendirirken bir yandan da

şeffaflığı, hesap verebilirliği ve yasal çerçeveye uyumu teşvik etme amaçlamaktadır[94].

b) Kişisel Verilerin Güvenliği

Bir diğer önemli husus da verilerin güvenliğine ilişkin kurallardır. Gittikçe artan büyük miktardaki verilerin kullanılması ve işlenmesi için kolluk kuvvetleri yetkililerinin modern teknolojileri uygulaması esnasında polis soruşturmalarının bütünlüğünün ve kolluk görevlilerinin kullandıkları kişisel verilerin güvenliğinin sağlanması son derece önemlidir. 29. madde ile 32. madde arasında düzenlenen kişisel veri güvenliği hükümleri ile kontrolörlerden, maliyetler, işleme faaliyetinin doğası ve veri sahibinin hakları üzerinde doğabilecek riskler gibi pratik kaygıları dikkate almak suretiyle riske uygun güvenlik seviyesi sağlamak için teknik ve organizasyonel önlemleri almaları istenmektedir. Bu genel yükümlülüğün yanı sıra veri bütünlüğü için güvenlik önlemleri, veri kurtarma ve ekipman, erişim, iletişim ve depolama kontrolü gibi alınması gereken özel önlemlerin kapsamlı bir listesi de belirtilmiştir. 30. maddeye göre, kişisel veri ihlali halinde, bu ihlalin bireylerin hakları ve özgürlükleri açısından bir riske sebebiyet vermemesi durumu hariç olmak üzere kontrolör, gereksiz gecikmeye mahal vermeden ve uygun olması halinde, ihlalden haberdar olduktan itibaren en geç 72 saat içerisinde yetkili denetim makamına ihlali bildirmekle yükümlüdür. İhlalin, bireylerin hak ve özgürlükleri açısından yüksek risk oluşturmasının muhtemel olduğu durumlarda 31. Madde'ye göre, veri kontrolörü ihlalin niteliğini tanımlayarak ve ilgili bazı bilgileri açıklayarak veri sahibini de bilgilendirmelidir.

Veri güvenliğine ilişkin ayrıntılı düzenlemelerin direktifte yer alması, çerçeve karara nazaran büyük bir iyileştirme adımı olarak görülmektedir. Veri kontrolörleri, veri güvenliğini sağlamak ve denetleyici makamlara ve belli durumlarda veri sahibine de veri ihlallerini bildirmek hususunda katı yükümlülükler altındadırlar. Kontrolör böylelikle şeffaflık, güvenlik ve cezai soruşturmaların bütünlüğüne katkıda bulunmuş olur[95]. Risk altında bulunan verilerin güvenliğinin sağlanması için teknik ve organizasyonel tedbirlerin de alınması gerektiğini ifade etmiştik. Bu tedbirler kapsamına yetkisiz otoritelerin kişisel verilere müdahale, verileri elde etme ve verilere giriş teşeb-

94 Thomas Marquenie, s.333.

95 Thomas Marquenie, s.334.

büslerinin reddedilmesi; bunların okunması, kopyalanması, veri ortamının değiştirilmesi ya da silinmesinin önlenmesi; kişisel veri girişinin yetkili olmayan kişilerce yapılmasının önlenmesi, kayıt altına alınmış kişisel verilerin silinmesi ya da okunması ve değiştirilmesinin önlenmesine yönelik eylemler girmektedir.

6.Yönetim Mekanizması

a) Veri Koruma Görevlisi

Veri kontrolörleri, veri koruma görevlisi olarak nitelendirilen ve kontrolörlere yardımcı olacak kimseleri atamakla görevlidir. 32 ila 34 maddede düzenlenen hükümlere göre bu kimseler veri koruma görevlisidir ve verilerin korunmasıyla ilgili tüm meselelere doğru ve zamanında müdahale etmeleri ve görevlerini etkin bir şekilde yerine getirmeleri için gerekli kaynaklara sahip olmaları gerekmektedir. Veri koruma görevlileri, denetleyicileri bilgilendirecek, tavsiyelerde bulunacak, veri koruma mevzuatına uyulmasını izleyecek, veri sahibi ve veri korumayla ilgili kaygıları olan diğer kişiler için bir iletişim noktası olarak hareket edecektir.

b) Bağımsız Denetim Makamı

Bağımsız denetim makamı, direktifin uygulanmasının izlenmesi ile sorumlu olan ve bu sayede kişilerin Birlik içerisinde kişisel verilerinin akışını kolaylaştırmak ve işleme faaliyetlerine ilişkin temel hak ve özgürlüklerini korumak için üye devletler tarafından belirlenen bir ya da daha fazla kişilerden oluşmaktadır. Denetim makamı, ulusal düzeyde kurulmuştur ve dış etkilerden tamamen bağımsızdır. Direktifte, makamın kuruluşu ve işleyişine dair kurallar ve güvenlik önlemleri de bulunmaktadır. Bağımsız denetim mekanizmalarına görevlerini yerine getirebilmesi için, bu mekanizmaya, kurumlara ve kontrolörlere danışmanlık yapmak, gerekli tüm bilgileri almak ve Direktifin hükümlerine aykırı veri kontrolör faaliyetlerini düzeltmek için yetkili mercilere etkili danışmanlık, soruşturma ve düzeltme yetkileri tanınmıştır. Direktifin 45. maddesinde belirtilen ve denetim makamlarının yetkilerini düzenleyen maddede, her üye devlete, her bir denetim otoritesine, kendi üye devlet topraklarında Direktife uygun olarak verilen görevlerin ve yetkilerin yerine getirilmesi için denetim makamına yetkiler sağlama yükümlülüğü yüklenmektedir.

Direktifteki denetim makamı ile GDPR'de yer alan denetim makamının yetkileri birbiri ile tam olarak örtüşmemektedir. GDPR'de yetkiler uzun bir liste halinde yer almaktayken Direktifte bu liste daha dardır. GDPR'de idari para cezasının kesilmesi yetkisi varken Direktifte böyle bir yetki bahşedilmemiştir. Direktifte, kontrolör ve işleyiciye, Direktife uygun olarak ve uygun bulunması halinde belli bir şekilde ve belirli bir süre içinde, 16. maddeye uyan kişisel verilerin düzeltilmesi veya silinmesi veya işlemin kısıtlanması talimatını vermesi düzenlenmiştir[96]. Her denetim otoritesi, faaliyetlerine ilişkin olarak bildirilen ihlal türlerinin bir listesi ve uygulanan ceza türlerini içeren yıllık bir rapor hazırlayacaktır. Bu raporlar, üye devletlerin ulusal parlamentosuna, hükümetlerine ve diğer makamlara iletilecektir. Bunlar ayrıca kamuya, Komisyona ve Kurul'a da sunulacaktır.

c) Avrupa Veri Koruma Kurulu

Avrupa Veri Koruma Kurulu, bütün üye devletlerin bağımsız denetim makamları ve Avrupa Veri Koruma denetleyicisinden oluşmaktadır. Kurulun, denetleyici makamlar arasında iş birliğini teşvik etmek, Komisyona tavsiyelerde bulunmak ve kuralları yayınlamak gibi Direktifin üye ülkeler tarafından tutarlı bir şekilde uygulanmasına katkıda bulunmak amacıyla bir dizi görevi bulunmaktadır. Kurul, birtakım hükümlerin açıklığa kavuşturulmasına önemli katkılarda bulunur ve Direktifin üye devletler tarafından tekdüze ve kapsamlı bir biçimde uygulanmasını destekleyebilir. Ancak GDPR'de kurulan Kuruldan farklı olarak Direktif'in 51. maddesinde Kurula kolluk kuvvetleri alanında merkezi bir rol biçilmemektedir. Direktif, her üye devletten bir ya da birden fazla kamu yetkilisinin Direktifin uygulanmasını izlemek için görevlendirilmesini talep etmektedir. Bu gözetim, kişilerin temel hak ve özgürlüklerinin sağlanması ve Birlik içinde verilerin güvenli bir biçimde serbest akışının sağlanmasını amaçlamaktadır.

7. Üçüncü Ülkelerle Bilgi Paylaşımı

Kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılmasıyla ilgili olarak, Direktif, bunların serbestçe Birlik dışına çıkışında belli başlı şartların varlığını aramaktadır. Direktif 35. madde ile bir grup genel ilke belirlenmiştir. Transfer, Direktifin işlenme amaçları için gerekli olması

---

96 Caruana, s.11.

ve sadece Direktifte yer alan şartların yerine getirilmesi halinde mümkündür. İletici ve alıcı kontrolörlerin mutlaka yetkili makamlar olması ve transferi gerçekleştiren üye devletlerin diğer üçüncü ülkeler veya kuruluşlara daha ileri transferler için yetkilendirilmiş olması gerekmektedir. Farklı bir üye devletten gelen verilerin iletilmesi durumunda, verilerin kaynaklandığı üye devlet bu transferi, kamu güvenliğine yönelik acil veya ciddi bir tehdidin önlenmesi için gerekli olması hali hariç, onaylamak zorundadır. Direktifin diğer hükümlerine uygun olarak kabul edilmiş olan ulusal hükümlere uygun olarak ve Direktifin 35. maddesinde yer alan şartlar altında gerçekleşen transfer Direktife uygun olacaktır. 36. madde, Avrupa Komisyonu'nun, verilerin transfer edileceği ülkenin Avrupa kişisel verilerin korunması için yeterli koruma sağladığını belirten bir 'yeterlilik kararı' yayınlaması halinde verilerin üçüncü ülkeye transfer edilebileceğini düzenlemiştir[97]. Direktif 36. madde uyarınca, Komisyon'un, alıcı tarafından 'yeterli' seviyede koruma sağladığı yönünde karar vermesi halinde kişisel bilgilerin bir üye devlet tarafından üçüncü bir ülkeye aktarılmasına izin verilir. Yeterli seviyede koruma, üçüncü ülke tarafında iç hukuk ya da uluslararası taahhütleri nedeniyle, esas olarak Avrupa Birliği içinde garanti edilen temel hak ve özgürlüklerin korunmasını sağlaması için gerekli olan yeterli koruma düzeyine eşdeğer

97 Direktif 36/2'ye göre Komisyon, koruma düzeyinin yeterliliğini değerlendirirken, özellikle aşağıdaki hususları dikkate alır:

(a) hukukun üstünlüğü, insan hakları ve temel özgürlüklere saygı, kamu güvenliği, savunma, milli güvenlik ve ceza hukuku ile kamu kuruluşlarının kişisel verilere erişimi de dahil olmak üzere hem genel hem de sektörel mevzuatın yanı sıra söz konusu mevzuatın uygulanması, bir ülke veya uluslararası kuruluşta toplanan kişisel verilerin başka bir üçüncü ülke veya uluslararası kuruluşa transit aktarımına yönelik kurallar da dahil olmak üzere veri koruma kuralları, mesleki kurallar ve güvenlik tedbirleri, içtihadın yanı sıra etkili ve uygulanabilir veri sahibi hakları ile kişisel verileri aktarılmakta olan veri sahiplerine yönelik etkili idari ve adli tazmin;

(b) üçüncü ülkede bulunan veya bir uluslararası kuruluşun tabi olduğu ve yeterli uygulatma yetkileri dahil olmak üzere veri koruma kurallarına uyumluluk sağlanması ve sağlatılması, haklarının kullanımı hususunda veri sahiplerine destek olunması ve tavsiyede bulunulması ve üye devletlerin denetim makamları ile işbirliği yapılmasından sorumlu olan bir veya daha fazla sayıda bağımsız denetim makamının varlığı ve etkili bir şekilde işlev göstermesi ve

(c) ilgili üçüncü ülke veya uluslararası kuruluşun altına girdiği uluslararası taahhütler veya yasal bağlayıcılığı olan sözleşmeler veya belgelerin yanı sıra kişisel verilerin korunması ile ilgili olanlar başta olmak üzere çok taraflı veya bölgesel sistemlere katılımından kaynaklanan diğer yükümlülükler.

koruma anlamına gelmektedir[98]. Komisyon tarafından böyle bir yeterlilik kararının alınmamış olması durumunda, 37. maddeye göre veriyi alan ülkede gerek yeterli ve eşit güvenlik önlemi aldığını teyit etmek gerekse transferi kapsayan tüm ilgili koşulları değerlendirerek, bu tür güvencelerin etkin bir şekilde sağlandığı sonucuna varılması halinde yeterli bir koruma standartlarının bulunmasını sağlamak transfer eden ülkeye düşmektedir. Transfer eden ülkenin veri kontrolörü bu değerlendirmeyi yapacaktır ve bağımsız denetim makamına bildirecektir. Yeterlilik kararı ya da uygun güvenlik önlemlerinin bulunmaması durumunda, 38. maddeye göre veriler sadece bir kimsenin hayati çıkarını korumak, veri sahibinin meşru çıkarlarını korumak ya da kamu güvenliğine yönelik acil ve ciddi tehditleri önlemek için gerekli olması halinde üçüncü ülkeyle paylaşılabilir.

Üçüncü ülkelerdeki verilerin doğrudan özel alıcılara ('alıcı', üçüncü bir kişi olsun veya olmasın, kişisel verilerin açıklandığı bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır) aktarılmasıyla ilgili sadece belli koşulların yerine getirildiği bireysel ve özel durumlarda izin verilecektir. 39. madde, 35 (1) (b) maddede yer alan genel kuraldan saparak[99], üçüncü bir ülkedeki ya da Direktifin amaçları için yetkin olan uluslararası bir organizasyondaki bir otoriteye ("kontrolör") transfer yapılabileceğini kabul etmiştir. Münferit ve özel durumlarda, Madde 3 (7) (a) 'da atıfta bulunulan yetkili makamlar tarafından[100], özel taraflara transfer yapılabilir. Bu durum, üye devletler için yükümlülük oluşturmayan bir seçenek olarak sunulmaktadır. Madde, mevcut uluslararası antlaşmalardan ayrılmamaktadır ve bu aktarımın hukuka uygun olması için Direktifte yer alan diğer yükümlülüklerin yerine getirilmesi gerekmektedir[101]. Madde 40 ile uluslararası iş

---

98 CECJ Schrems case ECLI:EU:C:2015:650, prg 73. Adalet Divanı ayrıca, üçüncü bir ülke tarafından sağlanan koruma seviyesinin yeterliliğine ilişkin takdir yetkisinin, öncelikle temel hakların ışığında kişisel verilerin korunmasının oynadığı önemli rol dikkate alınarak sınırlandırılması gerektiğini belirtmiştir.

99 35/1-b: Kişisel veriler, Madde 1 (1) 'de belirtilen amaçlar için yetkili bir makam olan üçüncü bir ülke veya uluslararası kuruluştaki bir denetleyiciye aktarılır

100 3/7-a: suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması veya kamu güvenliğine yönelik tehditlerin önlenmesi ve bunlara karşı korunmanın önlenmesi de dahil olmak üzere cezaların infazı için yetkili herhangi bir kamu makamı.

101 Komisyon uzman grubu, bu Madde'nin bir istisna olarak kalması gerektiğini ancak buna rağmen, veri korumaya ihtiyaç duyulduğunda veya kredi kartı sahtekarlığıyla mücadelede ya da siber suçla mücadele gibi acil durumlarda bir kural haline geldiğini belirtmiştir. Caruana, s.18.

birliğini teşvik etmek ve uluslararası mübadele için daha kapsamlı bir veri koruma çerçevesine uygun adımları belirleyerek bilgi alışverişini kolaylaştırmak için bir dizi temel kural ortaya konulmuştur.

8. Çözüm Yolları, Sorumluluk ve Yaptırımlar

Direktifin 8. bölümünde Direktifte yer alan düzenlemelerin uygulanması ve veri sahibinin başvurabileceği yargı yolları için belli mekanizmalar belirlenmiştir. Direktif kapsamında veri sahibi verilerinin korunmasını sağlamak için belli başlı imkanlara sahip olmuştur. 52. madde uyarınca veri sahibinin, verilerinin işlenmesi esnasında işlenen Direktif ihlallerinin bağımsız denetim makamına şikayet etme hakkı doğmaktadır. Bağımsız denetim makamı, veri sahibini bilgilendirmeden önce mevcut şikayeti değerlendirir, soruşturur ve neticede süreç ve sonuçları kendisine bildirir. 52. maddeye göre diğer herhangi bir idari veya yargı yoluna halel getirmeksizin, üye devletler, veri sahibine, verilerinin işlenmesi esnasında Direktifin hükümlerine aykırı hareket edildiği kanaatinde ise bunu bağımsız denetim makamına şikayette bulunma hakkını sağlayacaktır. 53 ve 54. maddelerde hem denetleyici otoriteye hem de veri kontrolör ve işlemcilerine karşı etkili bir yargı yoluna başvurma hakkı da sağlanmıştır. Bu sayede, denetleyici otoritenin bütün bağlayıcı kararlarının yargısal olarak gözden geçirilmesi sağlanacaktır ve yapılan veri işleme faaliyetlerinin meşruluğunun ayrıntılı bir değerlendirmesinin yapılması imkanlı hale gelecektir. 55. madde ile veri sahibine, diğer başvuru yollarına gitme ve bunun getireceği idari ve pratik yükü azaltmak adına kamu yararına yasal amaçlara sahip olan ve kar amacı gütmeyen bir kuruluş tarafından kendi adlarına haklarını kullandırma fırsatı tanınmaktadır. Hukuka aykırı işleme faaliyetinin gerçekleşmesi halinde, 57 ve devamı maddeler uyarınca üye devletler, veri sahibinin maddi ve manevi zararlarından dolayı tazminat talep etme haklarını tanımalı ve ihlali gerçekleştiren tüzel ya da gerçek kişilere karşı etkili, orantılı ve caydırıcı cezaları uygulamalıdır.

Bu bölüm altında düzenlenen çözüm yolları, yaptırımlar ve sorumluluklar, veri sahibinin haklarının korunması ve uygulanmasını desteklemek amacıyla getirilmiştir. Bağımsız bir kurumu içeren şikayet mekanizmasının olması ve denetim makamı, veri kontrolörleri ve işlemcilerin yargısal denetime tabi olması, veri sahibinin haklarını güçlendirdiği gibi verileri üzerinde

daha fazla kontrol sağlaması bakımından önemlidir[102]. İhlallerin ceza hukuku yoluyla yaptırıma tabi tutulması ve etkin, caydırıcı ve orantılı nitelikte olması da Direktifin hükümlerinin üye devletler tarafından uygulanması amacına hizmet etmektedir. Direktifin 60. maddesi mevcut yürürlükte olan Birlik hukukunun uygulanabilirliğine ilişkindir. Maddeye göre, Direktiften önce yürürlüğe giren, adli iş birliği alanında üye devletlerin Antlaşmalara göre kurulan bilgi sistemlerine girişlerine ilişkin işleme faaliyetlerine dair Birlik mevzuatı ve de uygulamaya yönelik olası farklılıklar da gündemde kalmaya devam edecektir.

IV. DİREKTİFE YÖNELİK ELEŞTİRİLER

Direktif henüz çok yakın bir zamanda yürürlüğe girmiş olsa da -yaklaşık iki yıl önce kabul edildiği 2016 yılından bu yana- birtakım soru işaretlerini beraberinde getirmiştir. Her şeyden önce yukarıda da kısaca bahsettiğimiz gibi, direktifte geniş istisnaların yer alması ve bunların uygulanmasına ilişkin genel ve muğlak terimlerin kullanılmasının, üye ülkelerde farklı uygulamalara neden olması ve direktiften beklenen etkilerin aşınabileceği riskini taşımaktadır. Bir diğer endişe Direktifin 2008 tarihli Çerçeve kararın meydana getirdiği sorunları ortadan kaldırıp kaldıramayacağı ve farklı hukuk sistemleri arasında uyumlaştırmayı sağlayabilecek etkinlikte bir mevzuat meydana getirip getiremeyeceğidir[103]. Zira ancak bu yolla adalet ve polis alanında güçlü veri koruması sağlanacaktır. Çerçeve karar, daha önce de belirtildiği üzere üye devletler arasında bağdaşmayan uygulamalara yol açmıştı ve sınır ötesi bilgi alışverişine uygulanır niteliğe sahipti. Bu itibarla denilebilir ki, Direktifin getirdiği en önemli yenilik yerel sürecin de Direktif kapsamına dâhil edilecek biçimde genişletilmiş olmasıdır[104]. Dolayısıyla yerel süreçteki işlemler de AB hukuku ve dolayısıyla genel veri koruma kurallarına tabi hale gelmiştir.

Direktif, ulusal hukuk sistemlerinde doğrudan etkili olmakla ve üye devletlerin mahkemelerinde uygulanabilir olmakla kalmayıp aynı zamanda veri koruma hakkı ihlallerine karşı güçlü bir koruma sağlamakta ve genel

---

102 Thomas Marquenie, s.337.

103 Thomas Marquenie, s.328.

104 Direktif 1.ve 2. maddeler

veri koruma standartları da ortaya koymaktadır[105]. Bu kapsamda veri sahibi haklarına ilişkin daha iyi bilgi sahibi olacak, daha etkin bir gözlem mekanizması kurulacaktır. Genel ilkelere getirilen istisna ya da sınırlamalar gereklilik ve orantılılık ilkelerine daha sıkıya bağlanmıştır. Direktif geniş bir biçimde çerçeve karardan daha iyi düzenlenmiş, tutarlılık, uyumlaştırma ve veri koruma standartlarındaki düzeyi daha da arttırmıştır. Ancak bütün bu olumlu yönlerine rağmen temel olarak belli başlı hususlarda da eleştirilmekten kurtulamamıştır.

Bunlardan ilki, çerçeve kararda olduğu gibi alanın düzenlenmesi için seçilen enstrümanın niteliğidir. Direktif ile bu alanın düzenlenmesi neticesinde ilk kez Avrupa Parlamentosu'nun sürece katılmasını sağlamıştır. Direktifler de bağlayıcı olmakla birlikte, uygulamaları üye devletlere bırakılan ve iç hukukta hangi alanda düzenleneceği devletlerin geniş takdir yetkisine bağlı olan bir AB hukuku enstrümanıdır. Özellikle Direktif'te, öncelikle üye devletlere ve onların yetkili ulusal makamlarına, kişisel verilerin işlenmesi ve aktarılmasının gerekli ve orantılı olup olmadığına karar vermesi hususunda geniş bir takdir hakkı verilmiştir. Bu yetki, üye devletlere bağlı olan veri işleme ve aktarma kategorileri arasında tutarsızlıklara yol açabilir[106]. Ayrıca direktifin uygulama alanı olan üye devletlerin adli mekanizmaları kendi tarih ve kültürlerine göre farklılıklar arz etmektedir. Buna ilaveten teknolojik yeterlilikleri ve polis ve adalet sistemlerinde yeni teknolojileri kullanma yaklaşımları Birlik üye ülkeleri arasında farklı uygulamaların da doğmasına neden olabilecektir[107]. Adli ve polis konularının bir tüzük ya da GDPR içinde bir bölüm olarak kabul etmek yerine direktif olarak düzenlenmesi, ulusal düzeydeki farklı mevzuat uygulamalarını önlemenin önündeki en büyük engel olmuştur[108]. Zira Direktif'in iç hukuka uygulanması, üye ülkelerin farklı hukuk geleneklerinin de uygulamaya dahil edilmesi anlamına gelecek, bu durum da potansiyel uyuşmazlığa neden olabilecektir[109]. Komisyon'un, polis ve ceza adalet alanında verilerin işlenmesinin diğer bütün alanlardan farklılık arz etmesi gerektiği yönündeki kararı, ayrı bir mevzuat ile bu alanın düzenlenmesi yaklaşımı ile hayat bulmuş ve bir yandan genel bir yandan

105 Thomas Marquenie, s.328.

106 Cocq, s.275.

107 Paul De Hert&Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive, A First Analysis', s.10.

108 Thomas Marquenie, s.329.

109 Cocq, s.264.

da özel veri koruma mevzuatının oluşumu ile neticelenmiştir[110]. Direktifle bir taraftan yüksek minimum standartlar kurulmaya ve mümkün olduğunca ilkelerin ve kişisel veri sahibinin güvencelerine yönelik potansiyel istisnalar daraltılmaya çalışılırken bir taraftan da direktiflerin uygulamasını üye devletlere bırakarak, çerçeve karar düzeyinde olmasa da ülkeler arası veri koruma rejimleri arasında önemli derecede farklılıklara neden olunması eleştiri konusudur[111].

Bir diğer mesele ise GDPR ve direktif arasında ortaya çıkan farklılıklardır. Direktifte yer alan amaçlar dışındaki yetkili otoritelerin işlediği veriler hakkında GDPR uygulanacaktır[112]. Bu tür bir ayırım, gerek veri sahibi gerekse veri kontrolörünün durumundaki yasal belirsizlik polis ve adli otoriteleri arasında iki farklı ve bağımsız kurallar manzumesine neden olmakta, bunların uygulanmasında zorluklara da yol açmaktadır[113]. Bu farklılığın nedeni, polis ve ceza adalet alanında veri işlemenin farklı karakteristik özellik sergilemesine bağlanabilir. Genel veri işlemeden farklı olarak güvenlikle ilişkili süreç belli bir esnekliği gerektirmektedir. Örneğin, verinin niteliğine ilişkin kurallar, söz konusu tanık verilerine dayandığında sıkı bir biçimde uygulanamayabilir ya da bilgi verme ve giriş hakkı, en geniş biçimiyle kullanılması durumunda şüphelinin gözetlenmesi faaliyetlerini kullanılamaz hale getirebilecektir[114]. Ayrıca belirtmemiz gerekir ki GDPR'de öngörülen hak-

---

110 Paul De Hert&Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive, A First Analysis', s.8.

111 Thomas Marquenie, s.329.

112 Direktifle, sorumluluklarının daha düşük seviyede kalmasının veri ihlalleri ve veri sahibinin haklarının zedelenmesi hem GDPR hem de Direktife göre işlem yapan veri kontrolörü için birtakım zorluklara neden olacağı belirtilmiştir. Bu nedenle, hukuki metnin şekline bakılmaksızın tutarlı ve tek bir mevzuat olarak değerlendirilmelidir. WP29 opinion relating to the core topics in the view of trilogue, 17 June 2015, s.3. http://ec.europa.eu/justice/data-protection/article-29/documentation/other,document/files/2015/20150617_ appendix_core-issues_plenary_en.pdf) Böylelikle karışıklık ve özellikle bireylerin haklarının korunma düzeyi eşit derecede sağlanmış olacaktır. Özellikle tanımlar, ilkeler, yükümlülükler, bireylerin hakları ve denetim otoritesi tutarlı olmalı ve direktifteki istisnalar sıkı gereklilik koşuluna bağlanmalıdır.http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf

113 http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf, s.5.

114 Paul De Hert&Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive, A First Analysis', s.9.

lar, Direktif'te öngörülen haklardan fazladır ancak eğer GDPR'de yer alan haklar ceza hukuku kapsamında mümkün olan en fazla ölçüde hatta aynen uygulanırsa cezai soruşturmaları fiilen olanaksız hale gelebilecektir[115].

Direktifte verilerin hukuka uygun ve adil bir biçimde işleneceği ifade edilmektedir. Ancak GDPR'de olduğu gibi bunların hangi yasal zeminde gerçekleşeceği düzenlenmemiştir[116]. Direktif bunun yerine sadece 8. mad-

---

115 http://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/

116 GDPR 6. maddesine göre veri işleme şu hallerde hukuka uygundur:

1. İşleme faaliyeti, ancak aşağıdaki hususlardan en az biri geçerli olduğunda ve olduğu ölçüde, hukuka uygundur:

(a) veri sahibinin bir ya da daha fazla sayıda spesifik amaca yönelik olarak kişisel verilerinin işlenmesine onay vermesi;

(b) veri sahibinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce veri sahibinin talebiyle adımlar atılması için, işleme faaliyetinin gerekli olması;

(c) kontrolörün tabi olduğu bir yasal yükümlülüğe uygunluk sağlanması amacı ile işleme faaliyetinin gerekli olması;

(d) veri sahibinin veya başka bir gerçek kişinin hayati menfaatlerinin korunması amacı ile işleme faaliyetinin gerekli olması;

(e) kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya kontrolöre verilen resmi bir yetkinin uygulanması hususunda işleme faaliyetinin gerekli olması;

(f) özellikle veri sahibinin çocuk olması halinde veri sahibinin kişisel verilerin korunmasını gerektiren menfaatleri veya temel hakları ve özgürlüklerinin bir kontrolör veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır basması haricinde, söz konusu menfaatler doğrultusunda işleme faaliyetinin gerekli olması.

Ilk alt paragrafın (f) bendi kamu kuruluşları tarafından görevlerinin yerine getirilmesi hususunda gerçekleştirilen işleme faaliyetine uygulanmaz.

2. Üye devletler, Bölüm IX'te belirtilen diğer spesifik işleme durumları da dahil olmak üzere işleme faaliyetine ilişkin daha kati gereklilikler ve hukuka uygun ve adil işlemenin sağlanmasına yönelik diğer tedbirler belirlenmesi suretiyle, bu Tüzük'ün işleme faaliyetine ilişkin kurallarının uygulamasını 1. paragrafın (c) ve (e) bentlerine uygun olacak şekilde uyarlamak üzere daha spesifik hükümler uygulamaya devam edebilir veya uygulamaya koyabilir.

3. 1. paragrafın (c) ve (e) bentlerinde belirtilen işleme dayanağı (a) Birlik hukuku veya (b) kontrolörün tabi olduğu üye devlet hukuku ile ortaya konur.

İşleme amacı söz konusu yasal dayanakta belirlenir veya, 1. paragrafın (e) bendinde atıfta bulunulan işleme faaliyeti ile ilgili olarak, kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya kontrolöre verilen resmi bir yetkinin uygulanması hususunda gereklidir. Söz konusu yasal dayanak bu Tüzük kurallarının uygulamasının uyarlanmasına yönelik spesifik hükümler ihtiva edebilir: bunun yanı sıra, kontrolör tarafından gerçekleştirilen işleme faali-

dede işlemenin üye devletler tarafından meşru ve 1. maddede belirtilen üye devlet ve Birlik hukukuna dayanan amaçlar doğrultusunda yetkili otoritelerin görevlerini yerine getirmesi için gerekli olması halinde işlem hukuka uygun kabul edilmektedir. Hukuka uygunluk sadece bu kritere bağlanmış görünmektedir[117]. Ayrıca Direktif, GDPR'nin sağladığı belli başlı hakları, örneğin unutulma hakkı, veri taşınabilirliği hakkı gibi, veri sahibine sağlamamaktadır.

Direktif, yetkili mercilerce kişisel verilerin işlenmesine ilişkin olarak, veri konusunun haklarının ve özgürlüklerinin korunması için üye devletlerin direktifle belirlenen asgari seviyedeki güvencelerden daha yüksek güvenceler sağlamasını engellememektedir[118]. Direktife göre, daha yüksek standartlar getirmek engellenmemekteyse de bu durum bir yanda daha yüksek standartlara sahip ülkeler bir yanda da buna gönüllü olmayan ülkeler kategorisi oluşmasına neden olacak, üye ülkeler arasında etkin iş birliği ve bilgi alış

---

yetinin hukuka uygunluğunu düzenleyen genel koşullar; işleme faaliyetine tabi veri türleri; ilgili veri sahipleri; kişisel verilerin açıklanabileceği kuruluşlar ve açıklanma amaçları; amacın sınırlandırılması; saklama süreleri ve Bölüm IX'te belirtilen diğer spesifik işleme durumlarına yönelik tedbirler gibi hukuka uygun ve adil işlemenin sağlanmasına yönelik tedbirler de dahil olmak üzere işleme faaliyetleri ve işleme usulleri Birlik veya üye devlet hukuku kamu yararı hedefini karşılar ve gözetilen meşru amaçla orantılıdır.

4. Kişisel verilerin toplanma amacı dışında bir amaca yönelik olarak yapılan işleme faaliyetinin veri sahibinin rızasına veya 23(1) maddesinde atıfta bulunulan hedeflerin güvence altına alınmasına yönelik olarak demokratik bir toplumda gerekli ve ölçülü bir tedbir teşkil eden bir Birlik veya üye devlet kanununa dayanmaması durumunda, kontrolör, başka bir amaca yönelik işleme faaliyetinin kişisel verilerin asıl toplanma amacına uygun olup olmadığını değerlendirmek üzere, bunun yanı sıra aşağıdaki hususları dikkate alır:

(a) kişisel verilerin toplanma amaçları ile planlanan diğer işleme amaçları arasındaki herhangi bir bağlantı;

(b) veri sahipleri ve kontrolör arasındaki ilişki başta olmak üzere kişisel verilerin toplandığı bağlam;

(c) 9. madde uyarınca özel kategorilerdeki kişisel verilerin işlenip işlenmediği veya 10. madde uyarınca mahkumiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin işlenip işlenmediği başta olmak üzere kişisel verilerin mahiyeti;

(d) planlanan diğer işleme faaliyetlerinin veri sahiplerine olası yansımaları;

(e) şifreleme veya takma ad kullanımı da dahil olmak üzere uygun güvencelerin bulunması.

117 Paul De Hert&Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive, A First Analysis', s.11.

118 Direktif madde 1.

verişini engelleyecek duruma gelme riski taşınacaktır[119]. Komisyon, Direktif yoluyla bu alanı düzenlemek suretiyle, üye devletlerin polis ve yargı makamları için daha fazla esnekliğe ihtiyaç duyulduğunu ve böylece bu alanların spesifik doğasını ele aldığını ifade etmiştir. Ancak Direktif veri koruma hedeflerini güvenlik politikası hedefleriyle dengelemeyi ve daha az parçalanmış bir genel çerçevenin oluşturulmasına katkıda bulunmayı amaçlarken, daha önce ortaya çıkan tüm eksiklikleri çözemez hale gelebilecektir[120]. Direktifin Birlik hukuku dışındaki faaliyetlerin yanı sıra Birlik kurumları, organları, ofisleri ve ajanslarının (Europol, OLAF, Schengen ya da Customs Information System gibi) gerçekleştirdiği faaliyetlere uygulanmaması, bunların her birinin kendi veri koruma rejimlerini uygulamaya devam edecekleri anlamına gelmektedir[121].

Direktifin 2008 Çerçeve Kararından farklı olarak sadece üye ülkeler arasında veri alışverişi değil aynı zamanda üye devletlerde kişisel verilerin işlenmesini düzenleyecektir ancak 1. maddenin 3. fıkrası nedeniyle Direktif, ceza alanında veri işlemenin maksimum uyumunun sağlanmasından hala uzaktır.

Direktifte yer alan genel ilkelerin, polis ve ceza adalet alanına uygulanması, daha önce yürürlükte olan çerçeve karardaki aksaklıklar dikkate alındığında önemli bir adım olarak görülmesine rağmen, Direktif'te verilerin toplandıkları amaçlardan farklı amaçlar için ileriki dönemlerde gerçekleşebilecek veri işlemelerine yönelik ilave korumanın az olması; denetleyici ulusal yasalar tarafından yeterli bir şekilde yetkilendirildiği sürece ve işlemin diğer amaçlar için gerekli ve orantılı olduğu sürece, kişisel verilerin başka amaçlar için işlenebilmesi; somut kuralların eksikliği veya ek gerekliliklerin olmayışı, orantılılık ve zorunluluk kavramlarına ilişkin farklı ulusal yorumlar ne yazık ki verilerin farklı amaçlarla kullanılması hususunda gereklilik ve orantılılık ilkelerine ulusal otoriteler tarafından farklı yaklaşımların benimsenmesini ve verilerin yeterli önlemler alınmadan farklı amaçlar için iş-

---

119 Thomas Marquenie, s.329.

120 Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, as annexed to the Final Act of the Intergovernmental Conference which adopted the Lisbon Treaty.

121 Paul De Hert&Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive, A First Analysis', s.11.

lenmesini engelleyememektedir[122]. Kişisel verilerin saklanması ihtiyacının periyodik olarak gözden geçirilmesi için somut kriterlerin olmaması ve açık bir zaman çizelgelemesinden ziyade 'uygun' zaman sınırlarının gerekliliği, ABAD kararları karşısında uyumsuz bir ifade olarak görülmektedir. ABAD, verilerin tutulması konusunda açık bir karar vermiştir. Zira Veri Saklama Direktifi'ni iptal ettiği kararında, kısmen, veri kategorileri ile kişiler arasında bir ayrımın olmayışı, aynı zamanda, verileri saklama sürelerini belirleyen nesnel ölçütlerin olmaması nedeniyle, Direktifi feshetmiştir[123].

Direktifle ilgili getirilen bir diğer eleştiri konusu da 10. maddede özel veri koruma kategorilerine ilişkin olarak çocuk haklarına özel önem verilmemesi ve özel veri kategorisinin sadece 'Birlik veya Üye Devlet hukuku tarafından yetkilendirildiği durumlarda'; veri konusu veya başka bir gerçek kişinin hayati çıkarlarını korumak veya bu tür işlemlerin, veri konusu tarafından açıkça kamuya açıklanmış verilerle ilgili olması durumunda 'uygun güvencelere' tabi olarak kişisel verilerin işlenmesi şeklinde, geniş kapsamlı ve muğlak ifadelerle düzenlenmiş olmasının hassas verilerin işlenmesi için 'torba' bir zemin oluşturduğudur. Dolayısıyla direktif, insan haklarının korunması için daha güçlü koruma mekanizması olmaksızın profil oluşturma faaliyetleri için hassas kişisel verilerin kullanılmasına izin vermektedir[124]. Bu müdahaleye karşı tek ilave şart 11. maddede hassas kişisel verilerin profillenmesi için bunların sadece uygun olması yeterli olmamakta, ayrıca belli bir kullanım ya da amaç için uygun olması ve meşru çıkarların da korunması gerekmektedir[125].

Direktifte, üçüncü ülkelerle veri alışverişi için basamaklı kurallar ve prosedürlerin kurulması, kolluk kuvvetlerinin ve adli makamların uluslararası işbirliğinde önemli bir adım olarak kabul edilmektedir[126]. Ancak aktarım

---

122 Article 29 Data Protection Working Party (Working Party 29), "Opinion 03/2013 on Purpose Limitation", 2 April 2013.

123 CJEU, Digital Rights Ireland and Seitlinger and Others, Joined Cases C-293/12 and C-594/12, O.J. C258, 8 April 2014.

124 Thomas Marquenie, s.332.

125 11/2: 'Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place'.

126 CJEU, Maximilian Schrems v Data Protection Commissioner, Case C-362/14, O.J. C351, 6

yapan ülkeler tarafından uygun güvencelerin oluşturulmasına ilişkin ifadelerin muğlak olması, üye devletlerin farklı yeterlilik standartlarını uygulamalarının ve kullanılmalarının önünü açmaktadır[127]. Örneğin, kamu güvenliğine yönelik acil bir tehdit, veri sahibinin hayati çıkarlarını koruma ihtiyacının varlığı, üye ülkelerin üçüncü ülkelerdeki veri koruma standartlarını değerlendirmesinin talep edilmesi herhangi bir kritere dayanmamaktadır. Ancak GDPR, 46. maddesinde bu kriterler belirtilmiştir[128].

Direktifin son bölümlerinde mevcut mevzuat ile ilişkisine değinilmektedir. 61. maddeye göre daha önce gerçekleştirilmiş olan bu alandaki Birlik düzeyindeki mevzuat değiştirilmeyecek, üye devletler arasında ya da üçüncü ülkeler veya organizasyonlarla gerçekleştirilmiş olan ikili antlaşmalar da değiştirilmedikçe, ilga edilmedikçe ya da mülga edilmedikçe yürürlükte kalacaktır. Direktifin taslak metinlerinde her ne kadar Direktif'in yürürlüğe girmesinden itibaren beş yıl içinde bu anlaşmaların tadil edilmesi ve yeni

---

October 2014; European Commission, "Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions: Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century", Brussels, 25 January 2012, 11.

127 Cocq, s.271.

128 Madde 46:

1. 45(3) maddesi uyarınca alınan bir karar olmaması halinde, ancak bir kontrolör veya işleyicinin uygun güvenceler sağlamış olması halinde ve uygulanabilir veri sahibi hakları ve veri sahiplerine yönelik etkili kanun yollarının mevcut olması koşuluyla, söz konusu kontrolör veya işleyici bir üçüncü ülke veya uluslararası bir kuruluşa kişisel veri aktarabilir.

2. 1. paragrafta atıfta bulunulan uygun güvenceler, bir denetim makamından spesifik bir onay alınmasına gerek olmaksızın, aşağıdakilerle sağlanabilir:

(a) kamu kuruluşları veya organları arasında yasal bağlayıcılığı bulunan ve uygulanabilir bir belge;

(b) 47. madde uyarınca bağlayıcı kurumsal kurallar;

(c) 93(2) maddesinde atıfta bulunulan inceleme usulü uyarınca Komisyon tarafından kabul edilen standart veri koruma şartları;

(d) 93(2) maddesinde atıfta bulunulan inceleme usulü uyarınca bir denetim makamı tarafından kabul edilen ve Komisyon tarafından onaylanan standart veri koruma şartları;

(e) 40. madde uyarınca onaylı davranış kuralları ile birlikte üçüncü ülkedeki kontrolör veya işleyicinin veri sahibinin hakları ile ilgili de olmak üzere uygun güvenceler uygulamaya ilişkin bağlayıcı ve uygulanabilir taahhütleri veya

(f) 42. madde uyarınca onaylı bir belgelendirme mekanizması ile birlikte üçüncü ülkedeki kontrolör veya işleyicinin veri sahibinin hakları ile ilgili de olmak üzere uygun güvenceler uygulamaya ilişkin bağlayıcı ve uygulanabilir taahhütleri.

veri koruma kurallarına uygun hale getirilmesi zorunlu kılınmışken, mevcut metin böyle bir yükümlülük içermemektedir. Dolayısıyla Direktif ve GDPR'den önceki dönemde imzalanmış ve Direktif ve GDPR'den daha az koruma sağlayan anlaşmaların varlığını sürdürüyor olması yeni mevzuat ile planlanan daha güçlü veri koruma standartlarının göz ardı edilmesine ve aşılmasına neden olma ihtimalini doğurmaktadır[129]. Bu antlaşmalar aynı zamanda Direktifte yer alan üçüncü ülkelere veri transferi için gerekli olan yeterli korumanın da sağlanamama ihtimalini kuvvetlendirmektedir[130].

Netice olarak denilebilir ki Direktif, GDPR ile birlikte AB kişisel verilerin korunması bakımından önemli bir adım olmuştur. Lizbon Antlaşması'nın kabul edilmesiyle birlikte sütunlu yapının da kalkması sayesinde hükümetler arası iş birliği alanına dahil olan adli ve polis konularındaki iş birliği Birlik hukuku kapsamına alınmış, böylelikle Direktif üye ülke ulusal hukuklarında doğrudan uygulama alanı bulmuştur. Direktif, hukukun uygulanmasına ilişkin verilerin işlenmesi sürecinin özel ihtiyaçları ve özellikli karakterinin farkında olarak veri koruma ilkelerini ayrıntılı bir biçimde düzenlemiş, bireylerin hakları ile adli ve polis adalet sürecinin gereklilikleri arasında bir denge bulmaya çalışmıştır. Örneğin, 7. maddede üye devletler gerçeklere dayanan kişisel verilerle kişisel değerlendirmelere dayanan kişisel verilerin birbirinden mümkün olduğunca ayırt edilmesini sağlamakla yükümlüdür. 6. madde de üye devletlere, kontrolörlere mümkün olduğu hallerde farklı kategorilerdeki veri sahiplerinin kişisel verileri arasında net bir ayrım yapmalarını isteme yükümlülüğü getirmiştir. Bu ve yukarıda genel hatları ile izah etmeye çalıştığımız Direktifin ilkeleri, tanımları, veriler arasındaki farklılıklar, uyuşmazlıklarda çözüm yolları, yargısal mekanizmalar, veri işleyicilerinin sorumlulukları gibi kimi daha önceki çerçeve kararda olan ve geliştirilen kimi de ilk kez Direktifle düzenlenen hükümler önemli birer unsur olarak Direktifin öne çıkan olumlu özellikleri şeklinde kabul edilmektedir. Ancak yine yukarıda izah etmeye çalıştığımız, yeni yürürlüğe giren ve hakkında

---

129 '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', Data Protection Working Party, art.29, 1 December 2015, s.16.

130 Paul De Hert&Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive, A First Analysis', s.15.

ABAD kararlarının henüz oluşmadığı Direktife yönelik çekinceler de mevcuttur. Daha önce de belirttiğimiz üzere bu çekincelerin ortadan kalkması ya da sorunların aşılması ulusal düzeydeki uygulamalar ve mevzuatlar arasındaki uyumla mümkün olacaktır.

KAYNAKÇA

Article 29 Data Protection Working Party (Working Party 29), "Opinion 03/2013 on Purpose Limitation", 2 April 2013.

Baecker, M. Hornung, G., Data Processing by Police and Criminal Justice Authorities in Europe-The Influence of the Commission's Draft on the National Police Laws of Criminal Procedure, Computer Law&Security Review, 28, 2012.

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 record (PNR), http://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/

Boehm, F., Information Sharing and Data Protection in the Area of Freedom, Security and Justice, Towards Harmonized Data Protection Principles for Information Exchange at EU Level, Springer, Heidelberg, 2012.

Caruana, M. 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, 2017, s.(1-22).

Case C-376/98 Germany v Parliament and Council [2000] ECR I-08419.

Case C-491/01 British American Tobacco and Imperial Tobacco [2002] I-11453.

CJEU Joined Cases C-465/00, C-138/01, and C-139/01 Rechnungshof [2003] ECR I-04989.

CJEU, C-275/06, Promusicae, 29.1.2008.

CJEU, C-73/07, Satamedia, 16.12.2008.

CJEU, C-553/07, Rijkeboer, 7.5.2009.

CJEU, Joined Cases C–92/09 and C–93/09 Volker und Markus Schecke and Eifert [2010] ECR I-11063.

CJEU, Joined Cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston, 17 June 2010.

CJEU, C-70/10, Scarlet, 24.11.2011.

CJEU, C-543/09, Deutsche Telekom, 5.5.2011.

CJEU, C-614/10, Commission v Austria, 16.10.2012.

CJEU, Digital Rights Ireland and Seitlinger and Others, Joined Cases C-293/12 and C-594/12, O.J. C258, 8.4.2014.

CJEU, Maximilian Schrems v Data Protection Commissioner, Case C-362/14, O.J. C351, 6.10.2014.

Cocq, C. C., EU Data Protection Rules Applying to Law Enforcement Activities, New Journal of European Criminal Law, Vol.7, Issue 3, 2016.

Colonna, Liane, "The new EU proposal to regulate data protection in the law enforcement sector: raises the bar but not high enough", IRI Promemoria 2012, Issue 2, s. 5. https://docplayer.net/31141949-Iri-pm-iri-promemoria-2-2012-liane-colonna.html

Convention on Cybercrime CETS no.185, Budapeşte, 23.11.2001.

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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008F0977.

Council of Europe Committee of Ministers, Recommendation Rec 87 15 to member states regulating the use of personal data in the police sector, 17/07/1987.

Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, as annexed to the Final Act of the Intergovernmental Conference which adopted the Lisbon Treaty.

De Hert, P.&Papakonstantinou, V., 'European Parliament Directorate General for Internal Policies: Policy Department Citizen's Rights and Constitutional Affairs, The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area', Brussel, 2014.

De Hert, P.&Papakonstantinou, V., The New Police and Criminal Justice Data Protection Directive, A First Analysis, New Journal of European Criminal Law, Vol.7, Issue 1, 2016.

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 proces-

sing of personal data and on the free movement of such data, OJ 1995 L 281.

ECtHR, *Klass and Others v. Germany*, No. 5029/71, 6.9.1978.

ECtHR, *Malone v. the United Kingdom*, No. 8691/79, 2.8.1984.

ECtHR, *Rotaru v Romania* App no 28341/95, ECHR 2000-V.

ECtHR, *Amann v Switzerland* App no 27798/95, ECHR 2000-II.

ECtHR, *Copland v. the United Kingdom*, No. 62617/00, 3.4. 2007.

ECtHR, *Uzun v. Germany*, No. 35623/05, 2.9. 2010.

ECtHR, *M.M. v UK* App no. 24029/07 13.10.2012.

ECtHR, *Roman Zakharov v. Russia*, No. 47143/06, 4.12. 2015.

ECtHR, *Szabó and Vissy v. Hungary*, No. 37138/14, 12.1. 2016.

ECtHR, *Mustafa Sezgin Tanrıkulu v. Turkey*, No. 27473/06, 18.7. 2017.

ECtHR, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, No. 931/13, 27.6. 2017.

European Union Agency for Fundamental Rights and Council of Europe, 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/.

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", 28.10. 2015.

European Commission, "Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions: Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century", Brussels, 25.1. 2012

EU Council Framework Decision 2008/977/JHA, of 27.11.2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. OJ 2008 L 350, 30.12.2008.

EU Decleration No 21 concerning the Charter of Fundamental Rights of the European Union, annexed to the Final Act of the Intergovernmental Conference adopted the Treaty of Lisbon, 2007.

European Parliament, "MEPs tighten up rules to protect personal data in the digital era" Press release, 12.03.2014. Available at www.europarl.

europa.eu/news/en/news-room/20140307IPR38204/MEPs-tighten-up-rules-to-protect-personal-data-in-the-digital-era

Fuster, G.G., The Emergence of Personal Data Protection as a Fundamental Right of the EU, Switzerland, Springer International Publishing. 2014.

Google Spain C-131/12 EU C 2013, 424.

Handbook on European Data Protection Law, European Union Agency for Fundamental Rights and Council of Europe, Luxemburg, 2018.

Kokott, J.& Sobotta, C., The Distinction between Privacy and Data Protection, International Data Privacy Law, Vol.3, No.4, 2013.

Le Métayer, Daniel, "Privacy by design: a matter of choice" in Gutwirth, Serge, Yves Poullet and Paul De Hert, Data Protection in a Profiled World, Dordrecht, Springer, 2010.

Marquenie, Thomas, The Police And Criminal Justice Authorities Directive: Data Protection Standarts and Impact on the Legal Framework, Computer Law and Security Review, 33, 2017.

"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", Data Protection Working Party, art.29, 1 December 2015,

Pajunoja, L. J., The Data Protection Directive on Police Matters 2016/680, Yayınlanmamış Yüksek Lisans Tezi, Uni. Helsinki, Faculty of Law, 2017.

Reding, V., 'The European data protection framework for the twenty-first century', International Data Privacy Law, Volume 2, Issue 3, 1 August 2012.

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, https://eur-lex.europa.eu/legal content/EN/TXT.

Treaty Of Lisbon Amending The Treaty On European Union And The Treaty Establishing The European Community (2007/C 306/01) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT

WP29 opinion relating to the core topics in the view of trilogue, 17.6. 2015.

18.12.2000/c 364/01, Charter of Fundamental Rights of the European Union, http://www.europarl.europa.eu/charter/pdf/text_en.pdf

http://ec.europa.eu/justice/data-protection/article-29/documentation/other document/files/2015/20150617_ appendix_coreissues_plenary_en.pdf)

http://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

https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680.

http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf