

KOLLUK TEŞKİLATINDA VE CEZA YARGILAMALARINDA KİŞİSEL VERİLERİN KORUNMASI: “UNUTULAN” DİREKTİFİN KAPSAMLI VE KARŞILAŞTIRMALI ANALİZİ^(*)

Doç. Dr. Mural Volkan DÜLGER^(**)
Stj. Av. Onur ÖZKAN^(***)

Öz: Avrupa Birliği Veri Koruma Reformu, 27 Nisan 2016 tarihinde kabul edilen iki düzenleme ile gerçekleşti. Bu düzenlemelerden ilki, dünya çapında büyük etki yaratmış; birçok çalışmaya, işleme, görüşe ve karara konu olmuş ve büyük bir ilgiyle karşılanmıştır. İkinci düzenleme ise kendine çok fazla tartışma ve çalışma alanı bulamamış, gösterilen ilgiyi “akran”ına kaptırmış ve ilk düzenlemenin gölgesinde kalmıştır. Bu düzenlemelerden ilki, henüz ismi dahi söylenmeden hemen akla gelmektedir: Avrupa Birliği Genel Veri Koruma Tüzüğü. Ancak ikinci düzenleme tabir-i caizse unutulmuştur: 2016/680 sayılı Direktif. Makalemizin odak noktasında yer alan bu “unutulan” düzenleme, kolluk ve cezai yargılama alanında kişisel verilerin korunmasını düzenler. Bu çalışmayla hedeflenen, Direktifin kapsamlı ve karşılaştırmalı analizinin okuyucuya sunularak, düzenlediği önemli konuların açığa kavuşturulmasıdır.

Anahtar Kelimeler: Kişisel Verilerin Korunması Hukuku, Kolluk ve Cezai Yargılama, Bilgi Paylaşımı, Avrupa Birliği Ceza Hukuku, Polis Direktifi.

DATA PROTECTION IN THE FIELD OF LAW ENFORCEMENT AND CRIMINAL JUSTICE: COMPREHENSIVE AND COMPARATIVE ANALYSIS OF THE “FORGOTTEN” DIRECTIVE

Abstract: The European Union Data Protection Reform took place on April 27, 2016 with two legal regulations. The first of these regulations has had a huge impact worldwide. It has been subject to many studies, process, opinions and decisions and received great interest. The second regulation did not find much discussion and research field and it has lost the all shown interest to its “peer”. In this sense, it can be said that it is overshadowed by first regulation. The first of these regulations comes to mind immediately without mentioning its name: European Union General Data Protection Regulation. However, the second regulation is “forgotten”: Directive 2016/680. This “forgotten” Directive, which is the focus of our article, regulates the protection of personal data in the field of law enforcement and criminal justice. The aim of this study is to present comprehensive and comparative analysis to the reader and to clarify the important issues regulated by the Directive.

Keywords: Data Protection Law, Law Enforcement and Criminal Justice, Information Sharing, European Union Criminal Law, Police Directive.

^(*) Makalenin Gönderiliş Tarihi: 24.03.2020,
Makalenin Birinci Hakem Tarafından Kabul Tarihi: 29.03.2020,
Makalenin İkinci Hakem Tarafından Kabul Tarihi: 06.04.2020.

^(**) İstanbul Aydın Üniversitesi, Hukuk Fakültesi, Ceza Hukuku ve Ceza Muhakemesi Hukuku Anabilim Dalı,
E-posta: volkan.dulger@dulger.av.tr; [Orcid no: https://orcid.org/0000-0003-4034-5436](https://orcid.org/0000-0003-4034-5436).

^(***) İstanbul Barosu; İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Bölümü, Yüksek Lisans Öğrencisi,
E-posta: onur.ozkan@dulger.av.tr; [Orcid no: https://orcid.org/0000-0002-3391-4728](https://orcid.org/0000-0002-3391-4728).

Giriş

Bugün teknoloji dendiği zaman aklımıza gelen ilk kavramlardan biri de “insan hakları”. Oysa teknoloji, gelişiminin ilk aşamalarında insan hakları ilişkin olan ya da etik tartışmalardan uzakta ve gelecek kaygıları ile değil; aksine, parlak bir geleceğe ilişkin büyük umutlar ile ilerledi. Bugün Bilişim Çağı (Information Age, Informationszeitalter) şeklinde ifade ettiğimiz nokta; bir taraftan pek çok farklı üretim, ifade biçimlerini ve paylaşım imkânlarını beraberinde getirse de öte yandan, bizatihi bizleri tanımlayan veya bizlerle ilişkili birçok verinin ortaya saçılmasına sebep oldu ve bu bakımdan, yeni bir denetim ve gözetim alanının oluşması sonucunu doğurdu.

Foucault’nun öznelleştirme sürecini başlattığı bilgi ekseni bugün, yalnızca bilim statüsü kazanmaya çalışan araştırma kiplerinden ibaret değil.¹ Etrafımızı çepeçevre saran bu bilgi dalgası “bölücü pratiklerini”,² tanıdığımız tanımadığımız birçok kişinin değer yargısı ile gerçekleştiriyor ve bizi bir özne olarak kurma sürecinin tam da merkezinde yer alıyor. Bilgi ve öznenin, dolayısıyla da iktidarın bu girift ilişkisinde; denetim bilgi ve bilgi vasıtaları üzerinde gerçekleşiyor, iktidar gündelik yaşam pratiklerine dâhil oluyor ve bu amaçla izleme faaliyetlerini sürdürüyor.³ Bilgi vasıtalarının çok büyük ölçüde dijitalleştiği günümüzde, bu yeni vasıtalar, büyük gözetimin erişimini, gücünü ve kapasitesini arttırarak mahremiyetimize ilişkin kaygılarımızı derinleştiriyor.⁴

Çalışma konumuzun temel noktasında yer alan ceza yargılamasındaki ve kolluk teşkilatındaki veriler, kişilerin temel hak ve özgürlükleri ihlal etme tehlikesini en yüksek derecede taşıyan ve dolayısıyla da korunmaya muhtaç kişisel verilerdir. Özellikle devlet kurumlarının sahip olduğu suç işlenmesinin önlenmesi ve işlenmiş olanların ortaya çıkarılması gayesi; güvenlik kaygılarının öne çıktığı bir toplumda, herkesi denetimin bir objesi haline getirmesi sonucunu doğurabilir. Böyle bir durumda günümüzde artık saklanacak herhangi bir yer kalmamıştır.⁵

¹ Michel Foucault, *Özne ve İktidar*, Seçme Yazılar 2, (Çev: Işık Ergüden/Osman Akınhay), 4. Bası, Ayrıntı, İstanbul, 2014, s. 58.

² Bölücü pratikleri, kişiyi birbirine bağlı karşıtlar arasında kuran ve Foucault’nun tabiriyle, iktidarın “normalleştirme” için uygun alanı oluşturan değer yargıları şeklinde açıklayabiliriz. Yazar buna örnek olarak, deli ile akıllı, hasta ile sağlıklı, suçlular ile “iyi çocuklar”ı saymaktadır. Bunlar, bizi ve deneyimlerimizi belli alanlara sıkıştıran, bu alanlarla tanımlayan ve sosyal gruplandırmayı (social sorting) doğuran diyalektik nesneleştirme araçlarıdır.

³ Anthony Giddens, *The Nation-State and Violence: Volume Two of a Contemporary Critique of Historical Materialism*, Polity Press, Cambridge, 1985, s. 309.

⁴ David Lyon, “Surveillance, Power, and Everyday Life”, in: Danny Quah/Chrisanthi Avgerou/Robin Mansell/Roger Silverstone (eds.), *The Oxford Handbook of Information and Communication Technologies*, Oxford University Press, Oxford, 2007, s. 451.

⁵ Gazeteci ve hukukçu Glenn Greenwald’ın, 2013 yılında yapmış olduğu ifşaatlar ile gündeme gelen eski National Security Agency (NSA) çalışanı Edward Snowden ile yapmış olduğu mülakatlar, günümüzde gözetlemenin hangi boyuta eriştiğini ve artık bundan saklanacak herhangi bir yerimizin kalmadığını ortaya koymaktadır. Bkz: Glenn Greenwald, *No Place to Hide*, Penguin Books, London, 2014.

İşte yaşanan tüm bu süreç, temel ve bağımsız bir insan hakkı olarak kişisel verilerin korunması hakkını ortaya çıkardı.

Kişisel verilerin korunması hukuku, kendisine ilişkin ilk düzenleyici metinlerin ortaya çıkmasından bu yana, birçok ülkenin birbiriyle etkileşimi ile geliştirilen az sayıdaki ve nispeten yeni hukuk alanları arasında sayılabilir. 1960'ların sonlarından başlayarak, benzer yaklaşımları uygulayan veri koruma kanunları, dünyanın çeşitli ülkelerinde ortaya çıkmıştır. Bu gayri resmi sınırlar arası gelişimi, hızlı bir şekilde resmi uluslararası araçlar izlemiştir.⁶

Kıta Avrupası barındırdığı Avrupa Birliği, Avrupa Konseyi ve Avrupa Komisyonu gibi kurumlarıyla, bu alandaki pek çok hukuki metnin yaratıcısı, hakkın gelişimi ve ilerleyeceği yönün belirleyicisidir. Kişisel verilerin gerek kamu gerek özel sektör tarafından işlenmesine ilişkin bugüne kadar yapılmış birçok düzenleme bulunmasına rağmen, Direktifin kabul edilmesine kadar; ceza yargılamasında ve kolluk teşkilatı alanında işlenen verilere ilişkin kapsamlı ve kişilere yeterli güvenceyi sağlayabilen bir düzenleme yoktur. Bu durum özellikle 11 Eylül Sonrası ortaya çıkan politiko-jüridik atmosfer, ulusların küresel terör tehdidine karşı yürüttüğü ve gizli soruşturmalar ile ağır yaptırımları içeren dönem ile son derece bağlantılıydı. Ancak günümüzde şartlar değişmiş, kişiler özel alanlarına ve mahremiyetlerine karşı maruz kaldığı sık ve ağır müdahaleler neticesinde, mahremiyet haklarının sağlanmasına yönelmişlerdir. Temelde bu gelişmeler, Avrupa Birliği çerçevesinde yeni bir veri koruma reformuna ve özelde, kolluk ve ceza yargılamasında alanda işlenen verilerini daha güçlü şekilde koruyabilecek bir düzenlemeye olan ihtiyacı doğurdu.

Direktife duyulan ihtiyaçta üç ana etken rol oynar.⁷ Bunlardan birincisi, internet üzerinden veya internet vasıtasıyla işlenen suçlarda görülen büyük artıştır.⁸

⁶ Paul de Hert/Vagelis Papakonstantinou, "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency", *I/S: A Journal of Law and Policy for the Information Society*, V. 9., I. 2, s. 272, (Three Scenarios).

⁷ Juraj Sajfert/Teresa Quintel, "Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities", in: Mark Cole/Franziska Boehm (eds.), *GDPR Commentary*, Edward Elgar Publishing, Cheltenham, 2019, Forthcoming, s. 2 (Çevrimiçi) <https://ssrn.com/abstract=3285873>, (Erişim Tarihi: 01.04.2019).

⁸ Bize göre, internet üzerinden veya vasıtasıyla işlenen suçlar ya da diğer bir ifadeyle bilişim suçları ile, bilişim sistemlerinin ve dijital verilerin gizliliği, bütünlüğü ve kullanılabilirliğinin korunması amaçlanır. Kişilik hakkının yanında kişilerin bilişim sistemlerinin kesintisiz ve düzgün işleyeceğine olan güveni de koruma kapsamındadır. Aynı yönde bkz: Thomas Weigend, "Information Society and Penal Law: General Report", *Revue Internationale de Droit Penal*, Vol. 84, 2013/1-2, s. 53. İnternetin hayatımızdaki yerinin artmasıyla doğru orantılı olarak, bu suçların işlenme oranlarında önemli artışlar gözlemlenmektedir. Birleşik Krallık hükümetinin Dijital, Kültür, Medya ve Spor Departmanı tarafından yayınlanan 2019 Siber Güvenlik İhlali Araştırmasına göre, işletmelerin yaklaşık üçte biri (% 32) ve on yardım kurumundan ikisi (% 22) son 12 ay içinde siber güvenliğinin ihlal edildiğini veya siber güvenlik saldırısına uğradığını bildirmiştir. Her bir işletme ihlaller neticesinde yıllık £4,180 zarara uğrarken, bu miktar yardım kuruluşları için £9,470 olmaktadır. İstatistikler için bkz: UK Government Department for Digital, Culture,

Bununla birlikte, soruşturma makamları da özellikle suçluların bıraktığı dijital izleri takip edebilmek adına büyük veri analizleri başta olmak üzere, pek çok teknolojik ve yeni araştırma tekniklerini benimsemiştir. Dolayısıyla ikinci etken, kolluk ve cezai yargılama alanında dijital soruşturma sistemlerinin yoğun biçimde kullanımıdır.⁹ Son olarak, eski düzenlemelerin uyumlulaştırma ve icra edilebilirlik anlamında beklenen etkiyi sağlayamaması, bu alanda düzenlenecek yeni bir hukuki metne ihtiyacı doğurmuştur.

§ I. Ceza Yargılamasında ve Kolluk Teşkilatında Verilerin Korunmasına İlişkin 2016/680 Sayılı Direktif

A. Genel Olarak

Avrupa Birliği (AB) Hukuku'nda, kolluk ve cezai yargılama alanında kişisel verilerin işlenmesini düzenleyen günümüzdeki birincil hukuki metin, 2016/680 sayılı Direktiftir (Bundan sonra yalnızca "Direktif" olarak anılacaktır).¹⁰ Direktif, 27 Nisan 2016'da GDPR ile birlikte, veri koruma reform paketinin bir parçası olarak kabul edildi. Reform hareketinin ilgi odağında yer alan GDPR, yarattığı küresel etki ile kamu kurumlarını ve özel sektörü son derece meşgul etmiş; üzerine çokça tartışmayı ve öğretide birçok çalışmayı beraberinde getirmişken, Direktif için benzer bir durumdan bahse-

Media and Sport (DCMS) / University of Portsmouth, "Cyber Security Breaches Survey 2019", (Çevrimiçi) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/791940/Cyber_Security_Breaches_Survey_2019_-_Main_Report.PDF (Erişim Tarihi: 01.04.2019). Benzer bir çalışmada, İngiliz Kimlik Avı Koruması Çalışma Grubu'nun (Anti-Phishing Working Group) 2018 yılında yayımladığı Siber Suçlara Küresel Karşılığın Birleştirilmesi (Unifying the Global Response To Cybercrime) raporlarında, bir buçuk milyondan fazla sayıda siber güvenlik saldırısı tespit edilmiştir. APWG, "Unifying the Global Response To Cybercrime", (Çevrimiçi) <https://www.antiphishing.org/resources/apwg-reports/> (Erişim Tarihi: 01.04.2019).

⁹ Bilişim suçları ya da bir başka deyişle siber suçlar, geleneksel fiziksel suçlardan farklı olarak; kitlesel mağduriyet, küresel erişim, eylem ve sonuç arasındaki bölgesel kopukluk, teknolojik gelişmelerin sürekliliği nedeniyle ceza hukuku mevzuatındaki ortaya çıkan ve kapanamayan boşluklar ile karakterize edilmektedir. Usule ilişkin sorunlar, siber suçların yetersiz raporlanmasına yol açmakta; suçluların tespit edilmesi ve dijital delillerin toplanmasında yaşanan zorluklar, yargısal ikilemler ve yargılamanın süjeleri hakkında teknik bilgi eksikliği şeklinde kendini göstermektedir. Bu nedenle, siber suçlulukla mücadele için tüm çabalara rağmen, yeni siber ortamda eski araçları kullandığımız sürece tatmin edici sonuçlar elde edemeyeceğimiz açıktır. Bu konuyu ayrıca Ceza Hukuku ve Ceza Muhakemesi Hukukunun temel ilkeleri bakımından ele alan bir çalışma için bkz: Vanja Bajovic, "Criminal Proceedings in Cyberspace: The Challenge of Digital Era", in: Emilio C. Viano (ed.), *Cybercrime, Organized Crime, and Societal Responses: International Approaches*, Springer, Heidelberg, 2017, s. 87-103.

¹⁰ 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 (Çevrimiçi) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG (Erişim Tarihi: 01.04.2019).

dilemez. 2015 AB yasama yılının bir numaralı gündem maddesini oluşturmuş bu reform paketinin içerisinde iki hukuki düzenleme yer alsa da 2016/680 sayılı Direktifin, GDPR’ın gölgesinde kaldığı ve hatta “unutulduğu”¹¹ rahatlıkla söylenebilir.¹²

GDPR, 95/46/EC sayılı “*Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunması*”na ilişkin Direktifin yerini alır. Makalemizin konusunu oluşturan 2016/680 Sayılı Direktif ise Avrupa Konseyi’nin 2008 tarihli Çerçeve Kararının (2008/977/JHA) yerine geçer. Dolayısıyla çalışmamızın konusunu oluşturan düzenleme, eski düzenlemeden farklı olarak çerçeve karar değil, bir direktif hükmündedir. Bu sayede düzenlemedeki esaslı noktaların üye devletlerin ulusal mevzuatına aktarılmaması halinde kişiler, bu konudaki şikâyetlerini ulusal mahkemelerinde ileri sürebilirler. Bu bakımdan Direktif, AB çapında normatif uyumlulaştırmanın sağlanması bakımından önem arz eder.¹³ GDPR da doğrudan uygulanabilir olması, bağlayıcılık içermesi ve kişisel verilerin korunma hakkı bakımından temel kriter ve ilkeleri ortaya koyması itibarıyla, değerlendirmelerimizde büyük rol oynayacağı belirtilmelidir.

Direktif, kolluk ve ceza yargılamasında makamlar tarafından; suçların işlenmesini önleme, suçu tespit etme, soruşturma, kovuşturma veya ceza mahkumiyetlerinin infazı, kamu güvenliğini koruyucu faaliyetler ile kamu güvenliğini tehlikeye düşüren hallerin önlenmesi amaçlarıyla kişisel verilerin işlenmesini konu eder (Direktif m. 1). Bununla birlikte, kolluğun olayın ceza hukuku bakımından “fiil” oluşturup oluşturmadığı konusunda bilgisi olmadan kendi faaliyeti çerçevesinde veri işlemesi ve yine gösteri, büyük spor etkinlikleri ve isyanlarda zorlayıcı tedbir alma veya kamu güvenliğinin korunması amacıyla veri işlemesi hallerine de Direktif uygulanır.¹⁴

Öğretide beklendiği gibi,¹⁵ ulusal güvenliğin sağlanması amacıyla işlenen verilere düzenlemenin uygulanmayacağı, bu anlamda istihbarat teşkilatlarının faaliyetlerinin kapsam dışında tutulduğu ve bu hususun üye devletlerin takdir

¹¹ Marc Leiser, “The Law Enforcement Directive: The ‘Forgotten Directive’s Delicate Interplay with the GDPR”, Avrupa ve Türk Hukukunda Kişisel Verilerin Korunmasına İlişkin Güncel Sorunlar Sempozyumu, Yeditepe Üniversitesi, 9 Aralık 2018.

¹² Bu yönde bkz: Paul de Hert/Vagelis Papakonstantinou, “The New Police and Criminal Justice Data Protection Directive: A First Analysis”, *New Journal of European Criminal Law*, Intersentia, 2016, V. 7., I. 1, s. 7 (A First Analysis); Sajfert/Quintel, s. 2.

¹³ Paul de Hert/Juraj Sajfert, “Police, Privacy and Data Protection from a Comparative Legal Perspective” in: Monica den Boer (ed.), *Comparative Policing from a Legal Perspective*, Edward Elgar Publishing, Cheltenham, 2018, s. 323; Ayrıca krş. Viviane Reding, “Privacy Matters - Why the EU Needs New Personal Data Protection Rules”, EU Commission, (Çevrimiçi) http://europa.eu/rapid/press-release_SPEECH-10-700_en.htm?locale=en (Erişim Tarihi: 01.04.2019).

¹⁴ Directive 2016/680 Recital 12.

¹⁵ de Hert/Papakonstantinou, A First Analysis, s. 10.

alanına bırakıldığı görülür.¹⁶ Direktifin 14 sayılı gerekçesinde (Recital) de bu hususa vurgu yapılmıştır.¹⁷

Direktifin uygulanacağı veriler ise yetkili makamlar tarafından, kısmen veya tamamen otomatik olarak işlenen veriler olarak belirlenmiştir. Esasen otomatik olarak işlenen veriler, AB Hukukunda uzun süredir konu edilmektedir. Kişisel veriler hakkında çok taraflı bağlayıcılık içeren ilk ve halen tek hukuki metin,¹⁸ Avrupa Konseyi tarafından 28 Ocak 1981 tarihinde Strazburg'da imzaya açılan, “*Kişisel Verilerin Otomatik İşlenme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi*”dir.¹⁹ 108 sayılı Sözleşme ana hatlarıyla, üye ülkelerdeki gerçek kişilerin kişisel verilerinin kamu ve özel sektörlerdeki otomatik bilgi işlemesine tabi tutulması karşısında veri koruma haklarını güvence altına almayı amaçlar.²⁰

¹⁶ Bu yönde bkz: Gülşah Bostancı Bozbayındır, “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”, *GSÜHFD*, Beta, İstanbul, 2018/2, s. 72.

¹⁷ Directive 2016/680 Rec. 14: “AB hukuku kapsamı dışında kalan bir faaliyet için kişisel verilerin işlenmesi, ulusal güvenlik ile ilgili faaliyetler, ulusal güvenlik ile bağlantılı kurum ya da birimlerin faaliyetleri ve kişisel verilerin Avrupa Birliği Antlaşması’nın 5. Başlığının 2. Bölümündeki ortak dış ve güvenlik politikalarına ilişkin faaliyetlerin yürütülmesi çerçevesinde kişisel verilerin işlenmesi, bu Direktifin kapsamına giren faaliyetler olarak değerlendirilmemelidir.” Ulusal güvenliğin yanında, Direktifin 2. maddesinin 3. fıkrası ile AB kurum, kuruluş ve organları da kapsam dışına alınmıştır. Düzenleme uyarınca, Europol ve Eurojust gibi AB kurumlarının Direktifin kapsamı dışında kalmakta ve bu anlamda, AB kanun koyucusu Direktif ile, tüm AB çapındaki asgari kural ve kriterleri belirleme şansını değerlendirmemektedir. Ayrıca bkz: Cristina Blasi Casagran, *Global Data Protection in the Field of Law Enforcement: An EU Perspective*, Routledge Research in EU Law, Routledge, Oxford, 2016, s. 46.

¹⁸ de Hert/Papakonstantinou, *Three Scenarios*, s. 278; Elif Küzeci, *Kişisel Verilerin Korunması*, 3. Bası, Turhan Kitabevi, Ankara, 2019, s. 126.

¹⁹ Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. (Çevrimiçi) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>, (Erişim Tarihi: 10.04.2019). 1 Ekim 1985 tarihinde yürürlüğe giren Sözleşme, Türkiye tarafından 28 Ocak 1981 tarihinde imzalanmış ancak otuz beş yıl sonra, 17 Mart 2016 tarihli ve 29656 sayılı Resmî Gazete’de yayımlanan onay kanunu ile ülkemiz açısından bağlayıcı hale gelmiştir. Onay kanunu tasarındaki gerekçede, Sözleşmenin kırk yedi ülke tarafından imzalandığı ve Türkiye’nin taraf olmasına karşın sözleşmeyi onay işlemleri tamamlayıp sözleşmeyi yürürlüğe koymayan tek ülke olduğuna dikkat çekilmiştir. Bu durumun gerekçesi olarak ise öncelikle, uluslararası hukuktaki ilgili düzenlemelerin takip edilerek, ulusal hukukta kişisel verilerin korunması hakkının düzenlenmesi ve ancak sonrasında iç hukukta Sözleşmenin yürürlüğe sokulması yönündeki tercih gösterilmiştir. 2010 Anayasa Değişikliği ile kişisel verilerin korunması hakkının, anayasal bir hak olarak güvence altına alınması ve Sözleşmenin onaylanması sürecinde 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile ilgili gelişmeler, Sözleşmenin onaylanarak iç hukukta yürürlüğe girmesi gerekliliğini doğurmuştur. TBMM Başkanlığı, “Kişisel Verilerin Otomatik İşlenme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı”, (Çevrimiçi) <https://www2.tbmm.gov.tr/d24/1/1-0966.pdf>, 1/8/2014, (Erişim Tarihi: 01.04.2019).

²⁰ Sylvia Kierkegaard/Nigel Waters/Graham Greenleaf/Lee A. Bygrave/Ian Lloyd/Stephen Saxby, “30 Years on - The Review of the Council of Europe Data Protection Convention 108”, *Computer Law & Security Review: The International Journal of Technology Law and Practice*, Elsevier, London, 2011, V. 27, I. 3, s. 223 vd.; Handbook on European Data Protection Law: 2018 Edition,

Bunun yanında, otomatik olarak işlenmeyen, yani elle işlenen veriler de şayet bir dosyalama sistemi oluşturuyorsa Direktif kapsamına girer.

Düzenleme ile amaçlanan ise kamusal makamların işleyişinde kişisel verileri korumak, üye devletlerin yetkili makamları arasında kişisel verilerin aktarılmasını ve bu anlamda mülga 2008/977/JHA sayılı Kararda da olduğu gibi kolluk ve ceza yargılamasında alanda iş birliğini sağlamaktır (Direktif m. 1/2). İş birliği konusunda AB kanun koyucusu, kişisel verilerin korunması hakkı kaygılarıyla, bu iletişimi kesintiye uğratmayı değil; aksine veri akışına ilişkin genel bir çerçeve çizmeyi hedefler.²¹ Sonuç olarak, Direktif temel olarak iki ana hedef üzerine kurgulanmıştır: Kolluk ve cezai yargılama alanlarında kişisel verilerin korunması hakkına daha güçlü bir koruma sağlamak ve üye devletler arasındaki veri akışını ve iletişimini geliştirmek.²²

B. Direktifi Karşılaştırılmalı Olarak İncelemek: Eski Rejim, Yenilikler ve GDPR

Özel hayata saygı hakkı ile kişisel verilerin korunması hakları birbiriyle yakın ilişkilidir ancak farklılıkları sebebiyle birbirinden ayrı iki temel hakkı ve hukuksal alanı oluştururlar. Mahremiyet hakkı ya da AB Hukukunda tercih edilen ifadesiyle özel hayata saygı hakkı, 10 Aralık 1948 tarihli İnsan Hakları Evrensel Bildirgesi (Bildirge) ve 4 Kasım 1950 tarihli Avrupa İnsan Hakları Sözleşmesi (AİHS) ile ortaya çıkan uluslararası insan hakları hukukunun yapı taşlarından birini oluşturur. Ancak gerek Bildirgenin gerekse AİHS'in modern bilişim teknolojilerinin ve bilgi toplumunun çok öncesinde kaleme alınmış olması, kişileri verilerinin işlenmesi karşısında da koruyacak özellikli ve farklı hukuki belgelere ihtiyacı doğurmuştur.²³

Avrupa Konseyi ve AB, hakkın temellerinin atılması ve çerçevesinin çizilmesinde öncülük eden kuruluşlardır.²⁴ Yukarıda anılan, Avrupa Konseyi'nin ha-

Publications Office of the European Union, Luxembourg, 2018, s. 24-26; Murat Volkan Dülger, Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi, İstanbul, 2019, s. 55; Hüseyin Murat Develioğlu, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha, İstanbul, 2017, s. 9; Küzeci, (3), s. 126; A. Çiğdem Ayözger Öngün, Kişisel Verilerin Korunması Hukuku: Elektronik Haberleşme Sektörüne İlişkin Düzenlemeler Dahil, 2. Bası, Beta, İstanbul, 2019, s. 74.

²¹ de Hert/Papakonstantinou, A First Analysis, s. 11.

²² Krş. Sajfert/Quintel, s. 3; Handbook on European Data Protection Law, 2018 Edition, s. 32; European Commission, Proposal for a Directive of the European Parliament and of the Council on the Protection of Individual 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, s. 4, (Çevrimiçi) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF>, (Erişim Tarihi: 01.04.2019) (Avrupa Komisyonu Tasarısı); Directive 2016/680 Rec. 8, 10.

²³ Handbook on European Data Protection Law: 2018 Edition, s. 18.

²⁴ Esasında, veri koruma alanında ilk düzenlemeyi Almanya'nın Hessen Eyâleti'nin 1970 yılında (*Datenschutz*) getirdiği belirtilmelidir. Ancak bu düzenlemenin uygulama alanı da Hessen Eyâleti ile sınırlı idi. Öte yandan, ulusal kapsamdaki ilk veri koruma kanunu (*Datalag*) 1973 yılında İsveç'te yürürlüğe girmiştir. Avrupa Konseyi ve AB'nin öncülüğüne ilişkin tespitimizde, bu hususta

zırlamış olduğu 1981 tarihli 108 sayılı Sözleşme ve 13 Aralık 1995 tarihinde yürürlüğe giren 95/46/EC sayılı AB Veri Koruma Direktifinin yanında, 2000 tarihli AB Temel Haklar Şartı'nın 8. maddesinde kişisel verilerin korunması hakkının ayrı ve temel bir hak olarak kabul edilmesi ve 2009 tarihinde Lizbon Antlaşması ile bu hakkın Avrupa Birliği'nin İşleyişi Hakkında Antlaşma (TFEU) kapsamına alınması, günümüzde bu konuyu “görünür” kılan ve tartışmamıza olanak sağlayan kilometre taşı niteliğinde gelişmelerdir.²⁵

Kişisel verilerin korunması hakkının gelişimi ile birlikte, belki de bu hakkın en ağır ve en yoğun müdahaleye maruz kaldığı, kolluk ve cezai alanlardaki veri işleme faaliyetleri de AB yasama ajandasına çeşitli zamanlarda konu olmuştur. Konumuz bakımından, 108 sayılı Sözleşmeye ek, 17 Eylül 1987 tarihli ve R (87) 15 sayılı Tavsiye Kararı²⁶ ve 95 sayılı Direktif döneminde düzenlenmiş 27 Kasım 2008 tarihli ve 2008/977/JHA sayılı Çerçeve Kararı²⁷ önem arz eder.

1. Direktif Öncesi AB Hukukunda Benimsenen Rejim

İlk olarak, 108 sayılı Sözleşme, 3. maddesinde; *“Taraflar, işbu Sözleşmeyi kamu sektöründe ve özel sektörde, otomatik kişisel veri dosyalarına ve kişisel verilerin otomatik işleme tabi tutulması konusunda uygulamayı taahhüt ederler.”* denmekte ve ilk bakışta, kolluk ve cezai yargılama alanında uygulanabilir ve bağlayıcı nitelikte olduğu görülür.²⁸ Ancak Sözleşmenin “İstisnalar ve kısıtlamalar” başlıklı 9. maddesinde; devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatlerinin korunması ve suçların önlenmesi amacıyla veri işlenmesinin, taraf devletlerce müstesna tutulabileceğinin düzenlenmesi, uygulanabilirlik konusunda soru işaretleri yaratmaktaydı.²⁹

Buna karşılık yukarıda anılan Tavsiye Karar, doğrudan kolluk güçlerindeki kişisel verileri konu etmektedir. Karar; kolluğun veri toplaması, işlemesi, yabancı otoritelerle iş birliği çerçevesinde veri paylaşması, veri ilgisinin haklarının kul-

hazırlamış oldukları hukuki metinlerin, gerek kendi sınırlarını aşan (extra - territorial) ve pek çok ülkenin hukuk politikasına yön veren etkileri gerekse de ilk elden detaylı düzenlemeleri içermeleri göz önünde bulundurulmuştur.

²⁵ Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Law, Governance and Technology Series 16, Springer, Heidelberg, 2014, s. 1-15; Orla Lynskey, *The Foundations of EU Data Protection Law*, Oxford Studies in European Law, Oxford University Press, Oxford, 2015, s. 3-45.

²⁶ Recommendation R (87) 15 of the Committee of Ministers to Member States Regulating the use of Personal Data in the Police Sector, (Çevrimiçi) <https://rm.coe.int/168062dfd4>, (Erişim Tarihi: 01.04.2019).

²⁷ Council Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters, (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977>, (Erişim Tarihi: 01.04.2019).

²⁸ Diana Alonso Blas, “First Pillar and Third Pillar: Need for a Common Approach on Data Protection?”, in: Serge Gutwirth/Yves Poullet/Paul de Hert/Cecile de Terwangne/Sjaak Nouwt (eds.), *Reinventing Data Protection?*, Springer, Heidelberg, 2009, s. 226; Bostancı Bozbayındır, s. 60.

²⁹ Joseph Cannataci/Mireille Caruana, Report: Recommendation R (87) 15 - Twenty-Five Years Down the Line, Council of Europe, 2013, s. 5.

landırılması gibi işlemler için esas ilkeleri belirler, özellikle amaca bağlılık ilkesiyle günümüzde bile bu konudaki AB düzenlemelerine rehberlik eder.³⁰ Tavsiye karar, sekiz temel ilkedен oluşur.

Tavsiye Karar ilk ilkesinde, kolluk güçleri dışında kurulması gereken bağımsız kontrol ve denetleme mekanizmalarının oluşturulmasını tavsiye etmektedir. Bu makam, yalnızca bir danışma makamı şeklinde konumlandırılmıştır. Her ne kadar danışma olarak da olsa böyle bir makama yer verilmesi, kolluk güçlerini veri koruma mevzuatının “ruhuna” uymasını sağlamak için gerekli önlemleri almaya itmesi ve bu alanda gelişen yeni teknolojileri kamuoyunun tartışmasına açma ihtimali bakımından önemli bir gelişmeydi.³¹ Tavsiye Karar, ikinci ilkesiyle verilerin işlenmesini yalnızca gerçek bir tehlikenin veya belirli bir suçun işlenmesi amaçlarıyla sınırlandırır.³² Kişisel veriler kolluk güçleri tarafından “bir gün ihtiyaç olursa” düşüncesiyle, kişileri “işlemek” için işlenemez. O günkü şartlarda bu ilke, temel insani ve hukuki değerler yönünden büyük bir kazanım olarak görülebilir. O dönem yaygınlaştırılması amaçlanan demokratik polislik (democratic policing) anlayışına hizmet etmektedir.³³

Kararın üçüncü ilkesi, verilerin yalnızca gerekli ve doğru olduğu ölçüde saklanabileceğini, dördüncü ilkesi amaca bağlılığı, beşinci ilkesi veri dolaşımına ilişkin esasları, altıncı ilkesi veri ilgililerinin haklarını, yedinci ilkesi veri saklama süreleri ile verilerin güncellenmesini, sekizinci ve son prensibi ise veri güvenliğini düzenler.³⁴

AB hukukunun bu konudaki ilk hukuki düzenlemesi olan Tavsiye Karar, kolluk alanındaki veri işlemeye ilişkin temel ama oldukça önemli ilkeleri ortaya koyar. Günümüzde de temel olarak bu ilkeler takip edilmektedir. Bağımsız bir denetleme makamının öngörülmüş olması ise bu ilkelere uyulmasını sağlayacak en önemli araçtır.³⁵ Bunun yanında, veri toplamasının katı surette, amaca bağlılıkla sınırlandırılmış olması ve bu ilkenin veri saklaması açısından da benimsenmesi son derece önemli kazanımlardır.

³⁰ Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-Level*, Springer, Heidelberg, 2011, s. 96; Cannataci/Caruana, s. 5; Bostancı Bozbayındır, s. 60; Lauri Pajunoja, *The Data Protection Directive on Police Matters 2016/680 Protects Privacy - The Evolution of EU's Data Protection Law and Its Compatibility with the Right to Privacy*, Yayınlanmamış Yüksek Lisans Tezi, University of Helsinki, Helsinki, 2017, s. 15.

³¹ Bu yönde bkz: Boehm, s. 97; Cannataci/Caruana, s. 12-14; Recommendation R (87) 15 para. 31-35.

³² Boehm, s. 97-98; Cannataci/Caruana, s. 15-17; Recommendation R (87) 15 para. 43-48.

³³ Bu yönde bkz: Cannataci/Caruana, s. 5; Demokratik polislik kavramı, kolluk güçlerinin görevlerini yaparken; demokratik, hukuki ve insan haklarına saygılı bir bakış açısına sahip olmasını ve toplumun tümüne karşı duyarlı biçimde, hizmetini derhal, eşit ve tarafsız olarak sunmasını ifade etmektedir. “Demokratik polislik” üzerine detaylı bir çalışma ve rehber için bkz: The Organization for Security and Co-operation in Europe (OSCE), *Guidebook on Democratic Policing*, (Çevrimiçi) <https://www.osce.org/secretariat/23804?download=true> (Erişim Tarihi: 01.04.2019).

³⁴ Recommendation R (87) 15 para. 49-100.

³⁵ Bu yönde bkz: Boehm, s. 101-102.

Direktif öncesi AB rejimindeki ikinci nesil ve Direktif ile ilga edilen, 2008/977/JHA sayılı Çerçeve Karardır. 11 Eylül sonrası özellikle “Küresel Teröre Karşı Savaş” doktrininin gelişmesi, dönemin güvenlik kaygıları etrafında, AB kurum ve üye devletleri arasında gerek AB vatandaşları gerekse de üçüncü ülkenin vatandaşlarının kişisel verilerinin yoğun bir dolaşımını beraberinde getirmektedir.³⁶ Ancak benzer gerekçelerle, kişilerin haklarına ilişkin yeterli güvenceleri sağlayamamaktaydı. Nitekim Çerçeve Karar, özellikle sınırlı bir kapsamı içermesi ve yalnızca veri dolaşımına ilişkin düzenlemeleri barındırması dolayısıyla öğreti ve AB kurumlarınca dahi eleştirilmekteydi.³⁷

Çerçeve Karara ilişkin tasarı 2005 yılında sunulduğunda; veri ilgililerinin hakları, denetleyici makam, veri işleme ve dolaşımına ilişkin olarak, döneminin temel veri koruma düzenlemesi 95/46/EC sayılı Direktif ile benzer hükümler getirmektedir. Ancak sonrasında yapılan değişiklikler, Kararı olumsuz anlamda baştan sona farklı bir metin haline getirmiştir.³⁸

Karar, veri işlenmesinde hukuka uygunluk, ölçülülük ve amaca bağlılık gibi ilkeler içermekte; kişilere bazı şartlar altında düzeltme, silme ve engelleme taleplerini sunma imkânı tanımakta ise de hemen hemen her ilke, kolluğun aksini yapmasını ve kişilerin haklarının kısıtlanmasına ilişkin bir istisnayı da barındırdığından, bu hükümler de uygulanamamıştır.³⁹

³⁶ Avrupa Komisyonu, Çerçeve Kararın ve terörle mücadele amaçlarıyla özellikle DNA profilleri, parmak izleri ve araç kayıt verileri gibi kişisel verilerin sınır ötesi dolaşımını ve işbirliğini düzenleyen 2005 tarihli Prüm Kararının tetikleyicisi olarak Avrupa ve Amerika çapındaki küresel terör eylemlerini göstermektedir. Bkz: European Commission, “Communication from the Commission to the European Parliament and the Council: Overview of Information Management in the Area of Freedom, Security and Justice”, (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0385&from=EN>, 20/7/2010, s. 2-3, (Erişim Tarihi: 01.04.2019).

³⁷ Blasi Casagran, s. 42; Paul de Hert/Vagelis Papakonstantinou, “The Data Protection Framework Decision of 27 November 2008 regarding Police and Judicial Cooperation in Criminal Matters - A Modest Achievement However not the Improvement Some Have Hoped for”, *Computer Law & Security Review: The International Journal of Technology Law and Practice*, Elsevier, London, 2009, V. 25, I. 5, s. 403-404 (Not the Improvement Some Have Hoped For); Hielke Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU*, Springer, Heidelberg, 2016, s. 133; Boehm, s. 114; Sajfert/Quintel, s. 3; de Hert/Papakonstantinou, *A First Analysis*, s. 8; Ángeles Gutiérrez Zarza, *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Springer, Heidelberg, 2015, s. 23; Bostancı Bozbayındır, s. 67; Michele Nino, “The Protection of Personal Data in the Fight Against Terrorism: New Perspectives of Pnr European Union Instruments in the Light of the Treaty of Lisbon” *Utrecht Law Review*, Utrecht, 2010, V. 6, No. 1, s. 69; Avrupa Komisyonu Tasarısı, s. 2; Pajunoja, s. 22; European Data Protection Supervisor (EDPS), “Opinion of the European Data Protection Supervisor for a Directive of the European Parliament and of the Council regarding the European Investigation Order in Criminal Matters”, (Çevrimiçi) [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010XX1229\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010XX1229(01)), 29/12/2010, para. 52, (Erişim Tarihi: 10.04.2019).

³⁸ Blasi Casagran, s. 42; de Hert/Papakonstantinou, *Not the Improvement Some Have Hoped For*, s. 407; González Fuster, s. 221.

³⁹ de Hert/Papakonstantinou, *Not the Improvement Some Have Hoped For*, s. 411.

Bunun yanında eleştirilen bir başka durum olarak, Karar yalnızca üye devletler arasındaki veri dolaşımına uygulanabilmekte, ceza yargılamasında ve kolluk makamlarının yerel bazda kişisel veri işlemesi kapsam dışında kalmaktaydı.⁴⁰ Üstelik, düzenlenen sınır ötesi transfer durumunda da kişisel verilerin korunması düzeyi oldukça yetersiz ve gerekli güvencelerden yoksundu.⁴¹ Tüm bunlar, Karar kapsamındaki uluslararası veri aktarımı ağının hukuki takibini son derece zorlaştırmakta, kontrolüne ise takibe nazaran olanak dahi bırakmamaktaydı.⁴²

Çerçeve Karar, gönüllülük esasına dayandığından normatif uyumlulaştırmayı sağlayamamıştır. Dahası, alınacak tedbirlerin üye devletlerin iç hukukunca belirleneceği öngörüldüğünden, her biri birbirinden farklı çok sayıda uygulama ortaya çıkmasına sebep olmuş ve bu nedenle hukuki denetimi oldukça zorlaştırmıştır.⁴³

Kapsamın yukarıda belirtildiği gibi sınırlı olmasının yanında, herhangi bir netlik içermemesi de kolluk güçlerinin veri işleme faaliyetinin ne zaman yalnızca yerel bir faaliyetin konusunu ne zaman sınır ötesi bir dolaşımın konusunu oluşturacağından emin olamamasına ve bu nedenle uygulanabilirlik sorunlarına yol açmıştır.⁴⁴ Kararın tabir-i caizse üzerine inşa edildiği ya da *edilmesi gerektiği*, 95 sayılı Direktif ile dahi herhangi bir uyumluluk içermemesi, bir başka eleştiri konusudur.⁴⁵ Son olarak belki de en önemli sorun, Karardaki yetersiz tüm bu ilkelere dahi politik gerekçelerle vazgeçilebilmesidir.⁴⁶

Nihayet Direktif, tüm bu durumu değiştirmeyi vaat etmektedir.⁴⁷

⁴⁰ Paul de Hert/Rocco Bellanova, Data Protection in the Area of Freedom, Security and Justice: A System Still to be Fully Developed?, European Parliament, (Çevrimiçi), [http://www.europarl.europa.eu/RegData/etudes/note/join/2009/410692/IPOL_LIBE_NT\(2009\)410692_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/note/join/2009/410692/IPOL_LIBE_NT(2009)410692_EN.pdf), Mart 2009, s. 6, (Erişim Tarihi: 10.04.2019).

⁴¹ Thomas Marquenie, "The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework", *Computer Law and Security Review: The International Journal of Technology Law and Practice*, Elsevier, London, 2017, V. 33, I. 3, s. 325.

⁴² de Hert/Papakonstantinou, Not the Improvement Some Have Hoped For, s. 412.

⁴³ Boehm, s. 171; Viviane Reding, "The European Data Protection Framework for the Twenty-First Century", *International Data Privacy Law*, Oxford Academic, Oxford, 2012, V. 2, I. 3, s. 122; Bostancı Bozbayındır, s. 68.

⁴⁴ European Commission, "Safeguarding Privacy in a Connected World a European Data Protection Framework for the 21st Century", (Çevrimiçi) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF>, 25/1/2012, s. 10, (Erişim Tarihi: 10.04.2019).

⁴⁵ de Hert/Papakonstantinou, Not the Improvement Some Have Hoped For, s. 407; de Hert/Bellanova, s. 7; Boehm, s. 138-144; Nino, s. 67-69.

⁴⁶ Statewatch, Implementing the "principle of availability": The European Criminal Records Information System, The European Police Records Index System, The Information Exchange Platform for Law Enforcement Authorities, (Çevrimiçi) <http://www.statewatch.org/analyses/no-145-ecris-epris-ixp.pdf> s. 21, (Erişim Tarihi: 10.04.2019).

⁴⁷ de Hert/Papakonstantinou, A First Analysis, s. 8.

2. Direktif ile Getirilen Yenilikler

Direktif, veri ilgililerinin hakları konusunda gelişmeler içerir⁴⁸ ve hak sahiplerine iki boyutlu bir koruma sunar.⁴⁹ Korumanın ilk boyutunda, kural olarak, veri ilgililerine doğrudan veri sorumlularına başvurabilme ve haklarını kullanabilme imkânı tanınır. Korumanın ikinci boyutunda ise hem düzenleme hem de yargı makamı olarak konumlandırılmış denetleyici makamlar bulunur. Kişiler şikâyetlerini bu makamlar önünde dile getirebilecek, haklarını arayabilecek ve tazminat talep edebilecektir. Dolayısıyla, Çerçeve Kararın aksine Direktif, kişisel verilerin korunması hakkı ile kamu güvenliği menfaati arasında adil ve makul bir denge kurmaya çalışmaktadır.⁵⁰

Direktif ayrıca ilkeler bakımından daha detaylı düzenlemeler içerir ve bu ilkelerden cayılmasına da izin vermez. Veri sorumluları için daha kapsamlı bir sorumluluk yükü getirilmiş olup, Direktif bu yükü veri işleme faaliyetlerinin ilk aşamasına kadar taşır. Veri sorumlusu makamların başlangıçtan itibaren veri koruması (data protection by default) ve tasarımdan itibaren veri koruması (data protection by design) ilkelerine uymaları, mahremiyeti ön planda tutmaları gerekir.

Veri koruma etki değerlendirmesi (data protection impact assessment) de Direktif ile tanınan yeniliklerdendir. Böylece temel hak ve özgürlükler bakımından yüksek risk taşıyan faaliyetlerde ön denetimi sağlanır. Gerek veri sorumlusu gerekse de denetleyici makamlar tarafından kontrol mekanizması öngörülerek, kişi hakları yönünde bir düzenleme getirilmiştir. Ayrıca Direktif, 32. maddesi ile üye devletleri veri koruma görevlisi (data protection officer) atamakla yükümlü kılarak, kolluk ve cezai yargılama alanında kişisel verilerin korunması hakkının hayata geçirilmesi hususunda önemli bir atılım daha gerçekleştirir.

Ayrıca 2008 Çerçeve Kararında ve GDPR'da da bulunmayan, özel bir yükümlülük olarak⁵¹ veri ilgililerinin sınıflandırılması, Direktifle ilk defa tanınmıştır. Direktifin 6. maddesi uyarınca üye devletler, topladıkları kişisel verileri; şüpheli, sanık, hükümlü, mağdur ve tanık gibi kişilerin yargılama sürecindeki rollerine dayanarak sınıflandıracaktır. AB kanun koyucusu söz konusu hükmü getirerek, veri ilgisinin suçla ilgisine ve derecesine bağlı olarak verilerin sınıflandırılması istemektedir.⁵² Bu ayırım özellikle hiçbir şekilde suça dâhil olmamış kişilerin de verilerinin bu kapsamda işlenmesinden doğacak ağır tedbir ve kısıt-

⁴⁸ Statewatch, The Directive on Data Protection and Law Enforcement: A Missed Opportunity?, (Çevrimiçi) <https://www.statewatch.org/analyses/no-176-leas-data%20protection.pdf>, s. 5, (Erişim Tarihi: 10.04.2019).

⁴⁹ Sajfert/Quintel, s. 13.

⁵⁰ de Hert/Papakonstantinou, A First Analysis, s. 12.

⁵¹ Sajfert/Quintel, s. 6.

⁵² Bostancı Bozbayındır, s. 76.

lamalardan daha az zarar görmesi düşüncesinden kaynaklanır.⁵³ Böyle bir ayırım verilerin tasnifi ve organizasyonu açısından faydalar içerse de, sınıflandırmanın “karanlık” tarafında yer alan, suçla bağlantılı kişiler için ise ayrımcılık, kişisel verilerin korunması hakkına olan müdahalelerde keyfilik ve hakkın korunma çabasında azalmaya neden olma ihtimali açısından da eleştirilebilir.⁵⁴

Bir başka ayırım da Direktifin 7. maddesi uyarınca, olgulara dayanan kişisel veriler ile değerlendirmeye dayanan kişisel veriler arasında yapılmalıdır. Bu tasnif de verilerin doğru olmasını öngören ilkenin bir uzantısı olarak anlaşılabilir.

Direktif ile uygulama alanı da genişlemiştir. Çerçeve Kararın aksine yalnızca üye devletler arasındaki veri dolaşımına değil, öngörülen amaçlarla yapılacak gerek yerel gerekse de sınır ötesi tüm veri işleme faaliyetleri için Direktif uygulanır.

Başka bir yöndeki olumlu gelişme; Karara ilişkin eleştirilerimizin aksine, Direktif getirmiş olduğu düzenlemelerle veri koruma ana düzenlemesi ile ihtiyaç duyulan yeknesaklığı da sağlamayı başarmıştır.⁵⁵ Nihayet Direktifin, içerdiği kapsamlı ve ileriye dönük kurallar, hedeflediği yüksek veri koruma seviyesi ile Bilişim Çağının doğurduğu ihtiyaçları karşılayabilecek nitelikte olduğu kanaatindeyiz ancak bazı eksik noktalarda bulunmaktadır. Direktife ilişkin değerlendirmelerde hem olumlu hem de olumsuz yönleri değineceğiz.

3. GDPR ve Direktif Arasındaki Hukuki İlişkinin Boyutu

Uygulama kapsamı son derece geniş olan GDPR, kişisel verilerin işlenmesi için genel kuralları ortaya koyar. Bu nedenle AB Kişisel Verilerin Korunması Hukuku bakımından genel bir düzenlemedir (lex generalis). Öte yandan, Direktif ise ceza yargılamasının ve kolluk alanının özel yapısını dikkate alır. Dolayısıyla Direktif, özel düzenleme (lex specialis) olarak ve GDPR’ın bir tamamlayıcısı olarak uygulanacaktır.⁵⁶

⁵³ The Article 29 Working Party, “The Future of Privacy”, (Çevrimiçi) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf, 01/12/2009, s. 26, (Erişim Tarihi: 10.04.2019).

⁵⁴ Bu yönde bkz: Emmanuel Salami, “The Impact of Directive (EU) 2016/680 on 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 on the Existing Privacy Regime” (Çevrimiçi) <http://dx.doi.org/10.2139/ssrn.2912449>, s. 4, (Erişim Tarihi: 10.04.2019).

⁵⁵ de Hert/Papakonstantinou, A First Analysis, s. 10.

⁵⁶ Bu yönde bkz: Bart Custers/Alan M. Sears/Francien Dechesne/Illina Georgieva/ Tommaso Tani/ Simone van der Hof, *EU Personal Data Protection in Policy and Practice*, Information Technology and Law Series Volume 29, Springer, Heidelberg, 2019, s. 217; Paolo Balboni, “Personal Data Protection and the Use of Information to Fight Online Terrorist Propaganda Recruitment and Radicalization: Part III”, (Çevrimiçi), <https://www.paolobalboni.eu/index.php/2019/02/10/personal-data-protection-and-the-use-of-information-to-fight-online-terrorist-propaganda-recruitment-and-radicalization-part-iii/> (Erişim Tarihi: 01.04.2019).

Nitekim bu hususa GDPR'nın 19 sayılı gerekçesinde de değinilmekte ve *"Yetkili makamlarca suçların işlenmesini önleme, suçu tespit etme, soruşturma, kovuşturma veya hükmün infazı, koruyucu faaliyetler, kamu güvenliğini tehlikeye düşüren hallerin önlenmesi amaçlarıyla gerçek kişilerin verilerinin işlenmesi ve bu türden verilerin serbest dolaşımı, belirli ve başka bir AB düzenlemesinin (yazar notu: 2016/680 sayılı Direktif) konusudur. Bu nedenle GDPR, sayılan amaçlarla gerçekleştirilen veri işleme faaliyetleri için geçerli olmamalıdır."* denilmektedir.⁵⁷

Direktif ve GDPR arasındaki çizginin belirlenmesi kimi zaman oldukça karmaşık olabilir. Bu açıdan sözgelimi, düzensiz sınır geçme ve göç hareketlerinin suç olarak düzenlendiği ülkelerde, kolluğun bu hareketleri tespit etmek ve suçu önlemek için kişisel veri işleme halinde Direktif uygulanır. Öte yandan düzensiz göçmen, iltica başvurusunda bulunduktan sonra; başvurusunun işleme konması ve bu çerçevedeki veri işleme faaliyeti açısından, başlatılan cezai işleme bakılmaksızın, GDPR uygulanır.⁵⁸

Elbette bu örnek, somut olay karşısında; GDPR ile Direktif arasında hangisinin uygulanacağı konusundaki karmaşıklığı ortaya koyar. Bunun yanında Direktif öncesi, üye ülkelerin kendi mevzuatını uygulamasının yaratmış olduğu karmaşayı da gözler önüne serer. İşte temelde bu nedenlerle Direktif hükmünde bir düzenlemeye geçilmiştir. Kanımızca ileride konu ettiğimiz Direktif tıpkı GDPR gibi, Tüzük olarak düzenlenerek, AB Hukukunun ve üye devletler için bağlayıcı ve doğrudan uygulanabilir hale getirilecektir.

Bunun yanında, üstte andığımız gerekçe bizi başka bir sonuca daha sevk etmektedir: Direktife göre yetkili makamlar tarafından kişisel verilerin söz konusu amaçlar dışında işlenmesi halinde, üye devletlerin Direktifin sağladığı esnek veri işleme şemsiyesinden faydalanmaması gerekir. Esasında Direktifin 1. maddesi ve GDPR'nın 19 sayılı gerekçesinin mefhum-ı muhalifinden (argumentum a contrario) çıkan bu sonuca, Direktifin 9. maddesinin 2. fıkrasında da yer verilmiştir.

Buna göre, AB veya üye devletin mevzuatında ayrıca bir düzenleme bulunmadığı sürece, yetkili makamların Direktifin amaçları dışında kişisel verileri işleme halinde bu faaliyete GDPR uygulanacaktır. Keza anılan maddenin 2. fıkrasına göre de yetkili makamlar tarafından, kamu yararı ya da bilimsel veya tarihi araştırma amaçlarıyla veya istatistiksel amaçlarla verilerin arşivlenmesi halinde Direktif değil, GDPR uygulama alanı bulmalıdır. Nitekim GDPR'nın 5. maddesinde kişisel verilerin söz konusu amaçlarla arşivlenmesinin veri işlenmesi amaçlarına uygun olacağı belirtilirken, bu yönde bir düzenlemeye Direktifte yer verilmediği görülür.

⁵⁷ GDPR Recital 19, bkz: (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679> (Erişim Tarihi: 01.04.2019).

⁵⁸ Örnek için bkz. Sajfert/Quintel, s. 4.

Sonuç olarak, AB kanun koyucusu Direktifin kapsamını sınırlamak niyetindedir. Adli makamlar veya kolluk makamları tarafından işlenen her kişisel veri, Direktif kapsamına girmemelidir. Kanun koyucu, GDPR’ın daha geniş çapta ve genel olarak uygulanmasını sağlamak amacındadır. Zira GDPR, kişilere daha büyük ölçüde hukuki korumalar tanıır ve kişisel verilerin korunması ile çelişkili olabileceği diğer temel hak ve özgürlükler arasında kurulacak adil ve makul dengeye kişisel verilerin korunması hakkı açısından yaklaşır.

§ II. Kişisel Verilerin İşlenmesine İlişkin İlkeler

Direktif, “*Kişisel verilerin işlenmesine ilişkin ilkeler*” başlıklı 4. ve devamı maddeleri ile verilerin işlenmesine ilişkin esas ilkeleri belirlenir.

Verilerin işlenmesine hâkim ilkelere değinmeden önce bu ilkelerin uygulama alanı bulacağı kişisel veri ve bu verilerin işlenmesi kavramlarını açıklayacağız. Direktifin 3. maddesinde tanımlara yer verilir. Anılan madde uyarınca, kişisel veri; tanımlanmış ve tanımlanabilir herhangi bir kişi ile bağlantılı bilgiyi ifade eder. Buna göre, doğrudan veya dolaylı olarak, özellikle ad, kimlik numarası, konum verisi, çevrimiçi tanımlayıcı veya fiziksel, fizyolojik özelliklere ve genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğe özgü faktörlerin atfıyla bulunulabilen ve tanımlanabilen bir kişiyi ortaya koyan bilgiler, kişisel veri sayılır.

Kişisel verilerin işlenmesi ise kişisel veriler üzerinde gerçekleştirilen her türlü faaliyeti ifade eder. Buna örnek olarak Direktif; verilerin toplanması, kaydı, organize edilmesi, yapılandırılması, depolanması, uyarlanması veya değiştirilmesi, geri alınması; danışma amacıyla kullanılması, aktarma yollarıyla açıklanması, yayılması veya başka şekillerle sıralanması veya birleştirilmeye uygun hale getirilmesi ile veriler üzerinde kısıtlama, silme veya imha etme işlemlerinin gerçekleştirilmesini sayar.

Söz konusu tanımlar, GDPR ile herhangi bir anlam ve söylem farklılığı içermez. AB kanun koyucusu, tanımlar konusunda yeknesaklığın sağlanmıştır. Buna binaen, tanım maddesinin 2008/977/JHA sayılı Karara nazaran daha detaylı düzenlemeler içerdiği ancak kişisel veri ve veri işleme gibi ana kavramları yine benzer şekilde düzenlediği görülür.

A. Veri İşlenmesine Hâkim Olan İlkeler

Direktif ile öngörülen ilkeler, GDPR’ın veri işlenmesine ilişkin ilkeleri ile birçok noktada bağdaşır. Ancak Direktifin özellikli durumu ve düzenlenme amacı göz önünde bulundurulduğundan, birtakım farklılıkları da içerisinde barındırır. Konumuz bakımından bu başlık altında söz konusu ilkeleri, özellikle GDPR ile ayrıştığı ve bu anlamda farklılık içerdiği hususlar bazında ele almaya ve Direktifin “ratio legis”ini ortaya koymaya çalışacağız.

- Kişisel veriler hukuka uygun ve adil işlenmelidir.

Kişisel veriler, her ne kadar kamu güvenliğinin sağlanması amaçları ile işleniyor olsa da, bağımsız ve temel bir insan hakkının konusu oldukları unutulmamalıdır.⁵⁹ Dolayısıyla hukuka uygunluk ve adalet ilkesine uyulmalıdır. Hukuka uygunluk ilkesi Direktif özelinde öngörülen amaçlarla kişisel verilerin işlenmesidir. Zira başka amaçlarla verilerin işlenmesi halinde GDPR uygulama alanı bulacak ve GDPR'ın ilgili hükümler uyarınca, veri işleme şartlarını taşıma gerekecektir.

Söz konusu madde GDPR ile karşılaştırmalı olarak incelendiğinde, burada Direktifin getirilme amacı ile bağdaşan bir değişikliğin bulunduğu görülür. GDPR, verilerin işlenmesi hususunda hukuka uygunluk ve adalet ilkelerinin yanında ayrıca, “şeffaflık” (=transparency) ilkesini de tanımış ve hatta büyük önem atfetmişken;⁶⁰ bu ilkeye Direktifte yer verilmemiştir. Şeffaflık ilkesi ana hatlarıyla, kamuya veya veri ilgisine işleme ve işlemenin amaçları hakkında bir bilgilendirme yapılmasını ve bu bilgilendirmenin öz, kolay erişilebilir ve anlaşılabilir olmasını ve sade bir dili içermesi gerektiğini ifade eder.⁶¹

Kanımızca, bu ilkeye Direktifte yer verilmemesi uygundur. Şeffaflık ilkesinin uygulanması kimi durumlarda kamu güvenliğinin sağlanması amacı ile bağdaşmayabilir. Sözgelimi, uluslararası çapta aranan bir suçlunun, kişisel verilerinin çeşitli ülkelerin savcılık kurumları tarafından işlendiği ve bu kurumlar arasında verilerin dolaşımının gerçekleştirildiği yönünde bilgilendirilmesi ve bu verilere erişiminin sağlanması halinde, söz konusu suçlunun yakalanmasının ve yargılanmasının mümkün olamayabileceği, şeffaflığın bu süreçte vurabileceği açıktır.

Söz konusu durumun bir sonucu olarak, Direktifin 13. maddesinin 3. fıkrasında veri ilgililerinin bilgilendirilme haklarının ve 15. maddesinde veri ilgililerine veriye erişim haklarının; demokratik toplumun gereklilikleri ölçüsünde ve bu gereklilikler süresince, tamamen veya kısmen kısıtlanabileceği belirtilmiştir.

⁵⁹ Dülger, s. 45; Küzeci, (3), s. 65. Kişisel verilerin korunması hakkı, oldukça geniş bir alanı kapsayan ve bu alana özgülenmiş bağımsız idari otoriteler tarafından düzenlemesi ve adli takibi gerçekleştirilen, özel hayatın gizliliğinden farklı, temel ve bağımsız bir insan hakkıdır. Kişisel verilerin korunması hakkının insan hakkı olduğu konusunda geniş bilgi için bkz: Eşref Barış Börekçi, Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu, Yayınlanmamış Yüksek Lisans Tezi, Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2019, s. 19 vd.

⁶⁰ Develioğlu, s. 45.

⁶¹ Dülger, s. 115; Develioğlu, s. 45; Estelle Dehon/Peter Carey, “Fair, Lawful and Transparent Processing”, in: Peter Carey (ed.), *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, Oxford, 2018, s. 44; The Article 29 Working Party, “Guidelines on Transparency Under Regulation 2016/679”, (Çevrimiçi), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227, 22/08/2018, s. 7-9, (Erişim Tarihi: 10.04.2019).

- Kişisel veriler belirli, açık ve meşru amaçlara yönelik toplanmalıdır.

Bu ilke, kişisel verileri işlemekle yetkili makamların ulaşmak istediği hedeflerin belirli ve açık olmasını, meşruiyet ise yasal dayanak ve dürüstlük kuralına uygunluğu ifade eder.⁶²

Esasında bu ilkenin, hukukun temel ilkelerinden “hukuki belirlilik” ilkesinin kişisel verilerin korunması hukukundaki yansımasıdır. Hukuk sisteminin hak ve yükümlülükleriyle donatılmış sükeleri olarak kişiler, devletin veri işleme gibi temel hak ve özgürlüklerine müdahale niteliği taşıyan faaliyetlerini sürdürürken bir rasyonelite, istikrar ve tutarlılık gösterdiğini bilmelidir. Ancak böylece hukuk normunun hüküm ve sonuçları toplum üyelerince öngörülebilir olur ve hukuk devleti ilkesi uygulanabilir.

Söz konusu ilke, kolluk alanına giren böylesi önemli ve kişilerin güvenliği açısından sakıncalı olabilecek veri işleme faaliyetinin ancak belirli ve meşru bir amaca sahip olmasını gerektirdiğinden Direktif özelinde ayrı bir önem taşır. Zira belirli, somut ve meşru toplumsal güvenlik amaçlarına yönelik olmadan; kişilerin verilerinin muğlak amaçlarla sürekli olarak işlenmesi, toplumun her bir üyesini potansiyel suçlu olarak görüldüğü ve herkesin denetlenmenin öznesi haline getirildiği bir polis devletini doğurur.⁶³

Nitekim AİHM’in, insan hakları örgütü Liberty tarafından yapılan başvuruda vermiş olduğu karar da bu doğrultudadır.⁶⁴ Karara konu somut olaya göre Birleşik Krallık Savunma Bakanlığı, büyük ve gizli gözetim amaçlarıyla yürüttüğü Elektronik Test Tesisi (Electronic Test Facility) ile insan hakları örgütlerinin, 1990 ve 1997 yılları arasında birbirileriyle gerçekleştirdiği telefon görüşmelerini, faks ile e-mail iletişimindeki bilgileri ele geçirmiştir.⁶⁵

Savunma Bakanlığının bu faaliyeti, 1985 tarihli İletişimin Ele Geçirilmesi Kanunu’na (Interception of Communications Act 1985) uyarınca gerçekleştirdiği savunmasında bulunmuştur. Faaliyet Savunma Bakanlığına, “ciddi suçları önlemek veya tespit etmek amacıyla” iletişimin denetlenmesi emri çıkarma imkânı tanıyan, Kanunun m. 3/2-b maddesine dayanmaktadır. Aynı maddeyle, milli güvenlik menfaatini sağlamak veya Birleşik Krallık’ın ekonomik refahını korumak amacıyla da Savunma Bakanlığına iletişimin denetlenmesi emri çıkarabilme imkânı tanınmıştır.⁶⁶

⁶² Dülger, s. 117-123; Küzeci, (3), s. 200; Develioğlu, s. 46; Nilgün Başalp, Kişisel Verilerin Korunması ve Saklanması, Yetkin, Ankara, 2004, s. 37; Ayözger Öngün, s. 134; Peter Carey, “Data Protection Principles”, in: Peter Carey (ed.), *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, Oxford, 2018, s. 34.

⁶³ Bu yönde bkz: Küzeci, (3), s. 203.

⁶⁴ AİHM, Liberty ve Diğerleri v. Birleşik Krallık, Başvuru no: 58243/00, K. T. 1 Ekim 2008.

⁶⁵ Liberty ve Diğerleri v. Birleşik Krallık, para. 5

⁶⁶ Liberty ve Diğerleri v. Birleşik Krallık, para. 16-19.

1999 yılında bir TV programının Capenhurst, Cheshire’de bulunan Elektronik Test Tesisini haberleştirmesiyle durum açıklığa kavuşmuş ve insan hakları örgütleri bu faaliyete karşı hukuki girişimlerde bulunmuşlardır.⁶⁷

AIHM başvuru üzerine, haberleşmelerin gizlice izlenmesine olanak tanıyan mevzuatın, herkes için bir gözetleme tehdidi oluşturduğuna ve bireylerin mahremiyetini ortadan kaldırdığına hükmetmiştir.⁶⁸ AIHM’e göre, kanunun belirlilik içermemekte; kişilere verilen bu yetkinin kötüye kullanılması halinde yeterli güvenceyi sağlayamamakta ve devlet yetkililerine haberleşmeyi denetleme ve ele geçirme konusunda çok geniş bir takdir yetkisi tanımaktadır.⁶⁹ Sonuç olarak Mahkeme, Birleşik Krallık’ın AIHS’in 8. maddesini ihlal ettiğine hükmetmiştir.⁷⁰

Son olarak, Direktifte, GDPR’dan farklı olarak, verilerin arşivlenmesine ilişkin düzenlemeye yer verilmemiştir. Yukarıda belirttiğimiz üzere, Direktifteki amaçlara uygun olarak işlenen verilerin, kamu yararı ya da bilimsel veya tarihi araştırma amaçlarıyla veya istatistiksel amaçlarla arşivlenmesi; Direktifin kapsamına alınmamış ve veri işleme amaçları arasında sayılmamıştır. Bu durumda Direktif değil, GDPR uygulanacaktır.

- Kişisel veriler işlendikleri amacı aşmamalı, amaçla bağlantılı ve ölçülü olmalıdır.

Söz konusu ilke “veri minimizasyonu” şeklinde de ifade edilmektedir.⁷¹

Bu ilke, GDPR’a göre bir farklılık bulunur. GDPR amaçla sınırlı olma ilkesini esas almışken, Direktif amaca göre aşırı olmama ilkesini esas alır. GDPR sonradan ortaya çıkan ve verilerin toplanma amacına uygun düşmeyen yeni verilerin işlenmesini sınırlar ve bu veriler için bütün şartların tekrar sağlanması ararken,⁷² Direktif bu konuda daha geniş bir kriter olarak, aşırı olmamayı kabul eder.

Bu değişikliğin nedeni ise kamu güvenliğinin sağlanması adına ortaya çıkan yeni birtakım verilerin izlenmesi ve işlenmesi gerekebilecektir. Bu verilerin işlendikleri amacın sınırlarını aşabilir, ancak amaca göre aşırı olmamalıdır. Direktifin getirilme amacı göz önünde bulundurulduğunda, GDPR’dan daha farklı kriterlerin benimsenmesi doğaldır. Son olarak, başlangıçta Direktifteki amaçlar doğrultusunda toplanmış kişisel verilerin daha sonra başka bir amaçla işlenmesi halinde, bu faaliyetin GDPR hükümlerine tabi olacağı ifade edilmelidir.⁷³

⁶⁷ Liberty ve Diğerleri v. Birleşik Krallık, para. 6.

⁶⁸ Liberty ve Diğerleri v. Birleşik Krallık, para. 56.

⁶⁹ Liberty ve Diğerleri v. Birleşik Krallık, para. 69.

⁷⁰ Liberty ve Diğerleri v. Birleşik Krallık, para. 70.

⁷¹ Paul Voigt/Axel von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer, Heidelberg, 2017, s. 90; Carey, s. 35; Dülger, s. 124; Küzeci, (3), s. 208.

⁷² Dülger, s. 126; Ayözger Öngün, (2), s. 138.

⁷³ Directive 2016/680 Rec. 12; de Hert/Papakonstantinou, A First Analysis, s. 9.

- Veriler doğru ve gereken hallerde güncel olmalıdır.

Bu ilke, verilerin herhangi bir şekilde yanıltıcı ve yanlış bilgiler içermemesi- ni; verilerin güncelliğini yitirmesi ve artık doğru ve gerçek durumu yansıtmaması halinde verilerin güncellenmesini ve verilerin yanlışlığının fark eden yetkili makamların verilerin düzeltilmesi veya silinmesi için gerekli her adımı gecikmeksizin atması gerektiğini ifade eder.⁷⁴

Bu çerçevede, yetkili makamlar verileri elde ettiği kaynakları belirlemeli, kaynakların doğruluğunu sınamalı ve bu ilkeye ilişkin olarak ortaya çıkan talepleri değerlendirmede makul önlem ve hazırlıklarını yapmış olmalıdır.⁷⁵ Bu ilkeye, gerek GDPR'ın 5. maddesinde gerek mülga 95/46/EC sayılı Direktifin 6. maddesinde gerekse de yürürlükten kalkan 2008 Çerçeve Kararının 4. maddesinde rastlamak mümkündür.

- Veriler işlendikleri amaç için gerekli süre kadar tutulmalıdır.

Bu ilke yetkili makamların, kişisel verileri topladığı ve daha sonra işlediği amaçlar için gerekli olan süreden daha uzun bir süre tutamayacaklarını düzenler. Direktifin veri işleme için öngördüğü amaçlar cezai yargılama ve kamu güvenliğinin sağlanması hususlarına yöneliktir. Öyleyse, verilerin tutulması söz konusu amaçlara hizmet etmiyor ise bu verilerin artık silinmesi gerekir.

Bu ilkenin bir uzantısı olarak Direktifin 5. maddesi, üye devletlerin Direktif uyarınca işledikleri verilerin silinmeleri veya periyodik olarak gözden geçirilmeleri için bir makul süre (time-limits for storage and review) belirlemeleri gerektiğini belirtir. Kişisel verilerin tutulması pek çok veri ihlali riskini de beraberinde getirir ve veri güvenliğini olumsuz yönde etkileyebilir.⁷⁶ Veri güvenliğine ilişkin politikalar geliştirmek, üye devletlerin takdirindedir. Ancak burada sorun, “suçun önlenmesi” amacıyla depolanan veriler için bu makul sürenin nasıl belirleneceği noktasında çıkacaktır. Madde 29 Çalışma Grubu, ancak belirli bir veri ilgisine ait risk değerlendirme raporlarının bulunması halinde verilerin bu amaçla depolanabileceğini belirtmektedir.⁷⁷

Cezai kovuşturmalar sırasında işlenen verilerin aksine, önleyici amaçlarla veri depolandığında bu faaliyetin muhakkak sona ermesi gereken belirli bir an bulunmaz. Ancak gereklilik ilkesi, kamu makamlarının veriyi işlerken yaptıkları

⁷⁴ Dülger, s. 130; The Information Commissioner's Office (ICO), Guide to the General Data Protection Regulation (GDPR), (Çevrimiçi) <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>, s. 33-34, 36 (Erişim Tarihi: 10.04.2019).

⁷⁵ Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, (Çevrimiçi) <https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler>, s. 6, (Erişim Tarihi: 10.04.2019).

⁷⁶ Küzeci, (3), s. 215; Ayözger Öngün, (2), s. 146.

⁷⁷ The Article 29 Working Party (WP29), “Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680)”, (Çevrimiçi) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178, 29/11/2017, s. 10, (Erişim Tarihi: 10.04.2019).

ilk tespiti; verilerin işlenmesi gerçekten bu amaca hizmet ediyor mu ya da veri ilgisi toplum açısından tehlikelilik arz ediyor mu yönünde gözden geçirmesini gerektirir. Zira artık suçun önlenmesi amacına hizmet etmeyen ve gereklilik ilkesini karşılayamayan veriler, derhal silinmelidir. Çalışma Grubu ayrıca, kişisel veri kategorileri arasında bir ayırım yapılmasını ve azami saklama sürelerinin her bir veri kategorisine özgü olarak belirlenmesini tavsiye etmektedir.⁷⁸

Söz konusu ilke, AİHS'in 8. maddesinde düzenlenen "özel hayata saygı hakkı" ile yakın ilişkilidir. Gereklilik ilkesine uyulmaması nedeniyle özel hayata saygı hakkının ihlal edildiği AİHM kararlarını bu alt başlıkta ele alacağız.

AİHM'e yapılan bir başvuruda, başvuruçuların biyometrik verileri (parmak izleri, hücresel numuneler ve DNA profili) haklarında ceza soruşturması yürütülmesi sebebiyle kolluk kuvvetleri tarafından kaydedilmiştir. Başvuruçulardan birisi hakkındaki dava, müştekinin uzlaşma sonucu şikâyetini geri çekmesiyle düşmüştür. Diğer başvuruçu hakkında mahkeme, başvuruçunun beraatine karar vermiştir.

Birleşik Krallık hukukunun bir parçasını oluşturan 2001 tarihli Cezai Yargılama ve Polis Kanunu'nun (2001 Criminal Justice and Police Act) 82. maddesi uyarınca, kişilerin beraat ettiği bazı durumlarda dahi verileri depolanabilmektedir. İç hukuktaki düzenlemeye dayanan Birleşik Krallık kolluk makamları, söz konusu biyometrik verileri kalıcı olarak depolamıştır. AİHM bu faaliyet nedeniyle, başvuruçuların özel hayata saygı haklarının (AİHS m. 8) ihlal edildiğine karar vermiştir.⁷⁹ Karara göre, kişisel verilerin korunması hakkı ile kamu güvenliği menfaati arasında kurulması gereken makul dengede üye devlet, takdir alanı sınırlarının üzerinde bir kanuni düzenleme getirmiştir. Mahkeme, başvuruçuların özel hayatına yapılan böyle bir müdahalenin demokratik bir toplumun gereklilikleri ile bağdaşmayacağı kanısındadır.⁸⁰

AİHM'e yapılan bir başka başvuruda ise avukat olan başvuruçu, henüz öğrenci iken 1946 yılında, ülkesinde ifade özgürlüğüne olan müdahaleleri protesto eden ülkesi Romanya'daki Komünist rejim karşısı iki mektup kaleme almıştır. Aynı yıl, bu eyleminden ötürü Vaslui Halk Mahkemesi tarafından mahkûm edilmiştir.

Romanya İstihbarat Teşkilatı, başvuruçu hakkında gizli dosya oluşturmuş ve bu dosyada, başvuruçunun aşırı sağcı ve Yahudi düşmanı olan bir grubun mensubu olduğunu belirtilmiştir. Başvuruçu bu bilgilerin halen tutulduğunu, rejimin

⁷⁸ WP29, Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680), s. 5.

⁷⁹ AİHM, S. ve Marper v. Birleşik Krallık, Başvuru no: 30562/04, 30566/04, K. T. 4 Aralık 2008, para. 129.

⁸⁰ S. ve Marper v. Birleşik Krallık, para. 125. Karara ilişkin geniş bilgi için bkz: Ragıp Barış Erman, "Adli Yargı Sisteminde DNA Örnekleri ve Profilleri - S. ve Marper - Birleşik Krallık Davası", *Fasikül Hukuk Dergisi*, Seçkin, Ankara, 2010, C. 2, S. 10, s. 20-23.

devrilmesinden sonra açtığı tazminat davasında İçişleri Bakanlığının vermiş olduğu bilgiler neticesinde öğrenmiştir.⁸¹

AİHM kararında, söz konusu kişisel verinin çok uzun süredir sistematik olarak toplandığı ve depolandığını belirtmiş ve bir kişinin sadece yakın değil, aynı zamanda uzak geçmişini ilgilendirmesi halinde de bu durumun özel hayat kapsamına gireceğini ifade etmiştir.⁸²

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.⁸³ Ayrıca verilerin ne kadar süre ile saklanacağı, erişim yetkisi olan kişilere, dosyaların niteliğine, izlenecek usule ya da bu yolla elde edilen bilgilerin ne şekilde kullanılabilirliğine ilişkin açık ya da ayrıntılı hiçbir hüküm mevcut değildir.⁸⁴ Bu nedenlerle Mahkeme, S. ve Marper başvurusunda Birleşik Krallık için verdiği karara benzer şekilde, Romanya'nın kamu makamlarına tanıdığı ilgili takdir yetkisinin kapsamını ve kullanılma biçimini makul bir açıklıkla belirtmediğine kanaat getirmiştir.⁸⁵

Sonuç olarak, yetkili makamlar kişisel verileri hukuka uygun işlemekle yükümlüdür. Veriler belirli ve meşru amaçlara yönelik olarak toplanmalı, veriler doğru ve gerçek durumu yansıtmalıdır. Veriler, bağlantılı olma ve ölçülülük bağlamında gerekli asgari düzeyde tutulmalıdır. Direktifin ortaya koyduğu bu ilkelerin, özellikle düzenlenen alanın özel ihtiyaç ve karakteristiği göz önüne alındığında; kişilerin hakları ile kolluk ve cezai yargılama alanlarının gereklilikleri arasındaki dengenin kurulmasına olumlu bir etki sunacağı söylenebilir.⁸⁶

B. Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebepleri

Direktifin 8. maddesi, verilerin işlenmesinde hukuka uygunluk nedenlerini düzenler. GDPR'ın belki de en önemli ve öğreti ile uygulamanın üzerinde en çok durduğu konu olan hukuka uygunluk, Direktifin düzenlediği alan ve arz ettiği özellikler nedeniyle, son derece kısa ve açık bir şekilde kendisine yer bulmaktadır. Örneğin, Direktif uyarınca, rızanın varlığı kişisel verilerin işlenmesinde hukuka uygunluk nedeni olamaz.⁸⁷

⁸¹ AİHM, Rotaru v. Romanya, Başvuru no: 28341/95, K. T. 4 Mayıs 2000, para. 7-14.

⁸² Rotaru v. Romanya, para. 43-45.

⁸³ Rotaru v. Romanya, para. 50.

⁸⁴ Rotaru v. Romanya, para. 57.

⁸⁵ Rotaru v. Romanya, para. 60.

⁸⁶ de Hert/Papakonstantinou, A First Analysis, s. 11.

⁸⁷ Bostancı Bozbayındır, s. 70.

Buna göre, veri işleme ancak Direktifin 1. maddesinde yer alan; suçların işlenmesini önleme, suç tespit etme, soruşturma, kovuşturma veya hükmün infazı, kamu güvenliğini koruyucu faaliyetler ile kamu güvenliğini tehlikeye düşüren hallerin önlenmesi amaçları için gerekli ise hukuka uygundur. Ayrıca üye devletler, Direktifi iç hukuklarına aktarıırken getirecekleri yasal düzenlemelerde; işlenecek verilere, veri işlemenin amaçlarına ve bu faaliyetler ile ulaşılması istenen hedeflere, özellikli durumlarını ve kapsamlarını belirleyerek yer vermelidirler. Kısaca, veri işlemenin hukuka uygun olması için veri yetkili makamlar tarafından işlenmeli (*kişi unsuru*) ve Direktifte öngörülen amaçları (*amaç unsuru*) gözetilmelidir.⁸⁸

Bunun yanında Direktifin 9. maddesi, birtakım özel veri işleme koşullarına da yer verir. Düzenlemenin ilk fıkrasında, yetkili makamların Direktifin amaçları doğrultusunda topladıkları verilerin, şayet üye devletin iç hukukunda aksi yönde düzenleme yoksa başka bir amaçla işlenemeyeceği düzenlenmektedir. Böyle bir durumda AB Hukukunda söz konusu işlemeye uygulanacak düzenleme GDPR olacaktır. Yine ikinci fıkra uyarınca, üye devletlerin yetkili makamlarını Direktifteki amaçlar dışında veri işlemesi için yetkilendirmesi durumunda da söz konusu veri işlemeye GDPR'ın ilgili hükümleri uygulanacaktır.

Ayrıca üye devlet, kendi iç hukukuna dayanarak işlediği verileri başka bir üye devlete ve yetkili makama aktarırken, verilerin özel veri işleme koşullarına tabi olduğunu ve bu özel koşulların ihtiyaç duyduğu gereklilikleri alıcı yetkili makama iletmelidir.

C. Direktif Kapsamında Özel Nitelikli (Hassas) Kişisel Verilerin İşlenmesi ve Otomatik Karar Mekanizması

Direktif, 10. maddesi ile özel nitelikli (hassas) kişisel verilerin işleme şartlarını belirler. Öncelikle Direktif, hassas verileri GDPR ile aynı şekilde sınıflandırmaktadır. Buna göre; kişinin ırk ve etnik kökeni, siyasi düşüncesi, dini veya felsefi inancı, sendika üyeliği, genetik ve biyometrik verileri, sağlık durumu, cinsel hayatı ve yönelimleri hassas kişisel veriler kapsamındadır.

Hassas kişisel veriler ancak bu verilerin işlenmesi; üye devletin veya AB mevzuatında buna ilişkin bir düzenleme olduğu hallerde, söz konusu veri ilgilisi tarafından aleni hale getirilmişse veya veri işlemesi veri ilgisinin hayati menfaatlerini korumak için kesin surette gerekli (*strictly necessary*)⁸⁹ ise, veri ilgisinin

⁸⁸ Krş. Sajfert/Quintel, s. 3.

⁸⁹ Belirtmek gerekir ki, katı surette gerekli deyiminden ne anlaşılması gerektiği net değildir. Bu yönde bkz: WP29, "Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680)", s. 7. Ancak gerekliliğin, temel hakların kullanılmasını engelleyebileceği için çok geniş bir şekilde yorumlanmaması gerektiği belirtilmektedir. Öte yandan, son derece dar algılanması halinde de başvurulmasını güçleştireceğinden, meşru faaliyetler için de veri işlemesini aşırı zorlaştıracığı ifade edilmektedir. Bkz: WP29, "Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector", (Çevrimiçi) <https://www.pdpjournals.com/docs/88168.pdf>, 27/02/2014, s. 6, (Erişim Tarihi: 10.04.2019). Bu bakım-

temel hak ve özgürlüklerine ilişkin güvencelerin de sağlanması suretiyle işlenebilir. Hassas nitelikte kişisel veriler işlenirken, ortaya çıkabilecek ayrımcılık risklerinin düşürülmesi adına üye devletlerin gerekli güvencelere ulusal hukukunda yer vermesi tavsiye edilmektedir.⁹⁰

Hassas veriler arasında biyometrik verilerin özellikle DNA örneklerinin ve parmak izlerinin, kolluk güçlerince kullanımının son çeyrek asırda olağanüstü artış gözlemlenmekte, gelecekte de bu artış trendinin yükselerek devam edeceği düşünülmektedir.⁹¹ Biyometrik verilerin teknolojiyle birlikte son derece artan çeşitliliği ve yaygınlığının, kişilerin mahremiyeti ve veri koruma hakları üzerinde yarattığı riskler göz önünde bulundurulduğunda güvenliğe olan menfaat ile kişilik haklarının makul bir dengeye oturtulması gerekir.⁹²

Direktifin 11. maddesi tartışmaya açık ve dikkat çekici hükümlerden biridir. Otomatik karar mekanizmalarına ilişkin düzenlemeyi içeren maddeye göre; şayet veri ilgilisi hakkında “olumsuz bir yasal etki” (an adverse legal effect) doğurabilecek ise yalnızca otomatik işlemler yoluyla elde edilen bilgilere dayanarak, yetkili makamların veri ilgililerini etkileyecek kararları veremeyeceği ve profil oluşturamayacağı (profiling)⁹³ belirtilmektedir.⁹⁴ Ancak üye devletler iç hukuklarında bu hususu düzenleyerek ve veri ilgililerin temel hak ve özgürlüklerine ilişkin güvenceleri sağlayarak ve en azından verilerin işlenmesinde elle müdahale talebi hakkını da tanıyarak, otomatik olarak işlenen verileri karar alma süreçlerinde değerlendirebileceklerdir.

dan “katı surette” gerekliliğinin, temel haklar ve meşru menfaatler arasındaki dengede ilkinde daha ağırlık vererek yorumlanması gerektiği kanaatindeyiz.

⁹⁰ WP29, Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680), s. 10.

⁹¹ Simon Cole, *Suspect Identities: A History of Fingerprinting and Criminal Identification*, Harvard University Press, Cambridge, 2002, s. 292-295.

⁹² Erik Zouave/Jessica Schroers, “You’ve been Measured, You’ve been Weighed and You’ve been Found Suspicious: Biometrics and Data Protection in Criminal Justice Processing” in: Ronald Leenes/Rosamunde van Brakel/Serge Gutwirth/Paul De Hert (eds.), *Data Protection and Privacy: The Internet of Bodies*, Computers, Privacy and Data Protection Series, V. 11, Hart Publishing, Oxford, 2018, s. 2-3.

⁹³ Profil oluşturma, sonradan verilecek kararlara konu edilmesi açısından, veriler arasındaki korelasyonların (ilintilerin) tespit edilerek bilgi artışının amaçlandığı otomatik veri işleme tekniğidir. Bu anlamda profil, bir kimseyi veya bir topluluğu temsil eden bir dizi ilişkili veri iken; profil düzenleme ise büyük veri kümelerinde veriler arasındaki bilinmeyen kalıpları keşfetme süreci şeklinde ifade edilebilir. Ayrıca bkz: Francesca Bosco/Niklas Creemers/Valeria Ferraris/Daniel Guagnin/Bert-Jaap Koops, “Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities”, in: Serge Gutwirth/Ronald Leenes/Paul de Hert (eds.), *Reforming European Data Protection Law*, Law, Governance and Technology Series 20, Springer, Heidelberg, 2015, s. 8-12.

⁹⁴ Otomatik karar verme mekanizması, hiçbir şekilde insan dahil olmadan alınan kararları ifade eder. Bkz: The Article 29 Working Party, “Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679”, (Çevrimiçi) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, 06/02/2018, s. 20, (Erişim Tarihi: 10.04.2019).

Direktif aracılığıyla, veri ilgililerinin hakları geniş çapta güçlendirilmiş de olsa, söz konusu hükmün düzenleme konusu alanın ihtiyaçlarına cevap verdiği ancak kişilere yeterli güvenceyi sağlamadığı görülür.⁹⁵ Öncelikle, olumsuz yasal etkiden neyin anlaşılması gerektiği ortaya konulmuş değildir.⁹⁶ Bu sebeple, kavramın yarattığı belirsizliğin kötüye kullanılması mümkündür. Bu ihtimalin önüne geçilebilmesi için olumsuz yasal etkiyi tanımlayan bir maddeye ihtiyaç bulunduğunu düşünüyoruz. Zira verilerin ezici çoğunluğu otomatik olarak işlenirken, hangi yasal olumsuz etkileri oluşturabilecek kararların bu verilere dayanılarak verilemeyeceği açıkça düzenlenmelidir.

Bununla birlikte Direktif, 38 sayılı gerekçesinde “uygun önlemler” deyişiminden ne anlaşılması gerektiğini açıklamaktadır. Buna göre, kararın gerekçesini talep etme hakkı da dâhil olmak üzere; kişiler hakkında yapılan bu işlemler hakkındaki özellikli bilgileri talep edebilecek, ayrıca karara itiraz edebilme hakları tanınacaktır. Ancak gerekçelerin bağlayıcı olmaması sebebiyle, bu hakların uygulanabilirliği tartışmalıdır.⁹⁷

Son olarak, hassas kişisel veriler işlenirken otomatik profil oluşturma yoluyla ayrımcılığa yol açmak 11. maddenin son fıkrası uyarınca yasaklanmıştır.⁹⁸ Ayrıca hassas verilerin otomatik olarak işlenmesi yoluyla alınacak kararlar, yukarıda belirtilen şartların yanında; meşru menfaatlerin ve veri ilgisinin temel haklarının güvence altına alınması için gerekli önlemlerin alınması ile verilebilecektir.

§ III. Veri İlgililerinin Hakları

Direktif, veri ilgililerinin haklarına 12 ile 18’inci maddeleri arasında yer vermektedir. Aşağıda detaylıca inceleneceği üzere, veri ilgililerinin hakları; bilgilendirilme hakkı, erişim hakkı, düzeltmeyi talep etme ve silinmeyi talep etme hakkıdır.

Bununla birlikte bu hakların icra edilebilirliği hususunda, Direktifin 8. Bölümündeki hukuki çarelere değinmek gerekirse; veri ilgililerinin bu haklarının tanınmaması ya da veri sorumluları tarafından yükümlülüklerle aykırı davranılması halinde, veri ilgilileri şikâyetlerini 52. madde uyarınca denetleyici makamlara

⁹⁵ Sajfert/Quintel, s. 8.

⁹⁶ Öğretide Bygrave, yasal etkiyi; bir kişinin hak veya yükümlülüklerini değiştiren veya belirleyen etki olarak tanımlamaktadır. Bkz: Lee A. Bygrave, “Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling”, *Computer Law & Security Review: The International Journal of Technology Law and Practice*, Elsevier, London, 2001, V. 17, I. 1, s. 17. Bu tanımdan yola çıkılarak olumsuz yasal etkinin belirlenmesi halinde kapsamın muhtemelen genişlikte olacağı açıktır. Bu nedenle açık bir düzenlemeye ihtiyaç bulunur.

⁹⁷ Bu yönde bkz: Sajfert/Quintel, s. 10.

⁹⁸ Madde 29 Çalışma Grubu’na göre, hassas nitelikli verilerin tabiatı ve otomatik karar mekanizmalarının doğurduğu aşikâr ayrımcılık risklerinin ortadan kaldırılması için üye devletler Direktifi iç hukuklarına aktarırken, bu konuda katı önlemler almalıdırlar, WP29, “Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680)”, s. 13.

iletebileceklerdir. Şikâyet neticesinde veri ilgililerinin hem denetleyici makamlardan hem de veri sorumlusu ve işleyenlerden etkili hukuki çözümleri talep etme hakları bulunur. Son olarak, 56. madde uyarınca veri ilgilileri, haklarının ihlalin-den doğan zararlarının tazminini de talep edebilirler.

A. Veri İşlemesi Hakkında Bilgilendirme Hakkı

Direktifin 12. maddesi uyarınca, üye devletler veri ilgililerine yapacakları bilgilendirme ve iletişimlerde öz, kolay erişilebilir ve anlaşılabilir olmalı ve sade bir dil kullanmalıdır.

GDPR'daki bilgilendirme hakkı düzenlemesinden farklı olarak, ilk göze çarpan husus “şeffaflık” ifadesine burada yer verilmeyiştir. Buna paralel olarak yurkarıda, veri işlenmesine hâkim ilkelerde de şeffaflık ifadesine yer verilmediğine dikkat çekilmiştir.

Buna karşılık, Direktifin 26 sayılı gerekçesi ise açıkça her veri işlemenin hukuka uygun, adil ve şeffaf olması gerektiğini belirtmektedir.⁹⁹ Bu durum karşısında, şeffaflık ilkesinin ve bu ilkenin somut olarak vücut bulduğu bilgilendirme hakkının Direktifte kendisine yer bulduğu ve GDPR uyarınca yapılan açıklamaların burada da küçük farklarla da olsa, geçerli olacağı kabul edilmelidir.¹⁰⁰

Bilgilendirme hakkı kapsamında, veri ilgisine sağlanması gereken ilk bilgi, veri sorumlusunun kimliği ve iletişim bilgileridir. Varsa, veri koruma görevlisinin (data protection officer) iletişim bilgileri de iletilmelidir. Veri işlemenin amacı hakkında da veri ilgilisi bilgilendirilmelidir. Ancak burada GDPR'dan farklı olarak, sunulacak ilk bilgilerde veri işlemenin hukuki dayanağına ve veri işlemeyle hedeflenen meşru menfaat bilgisinin ilgiliye sunulması hükmüne Direktifte yer verilmemiştir.

Yine, veri ilgisine yapılacak bilgilendirmede, denetim makamına şikâyetle bulunma hakkının bulunduğu belirtilmelidir. Ayrıca veri ilgisine hakları hatırlatılmalıdır.

Direktif, anılan maddenin 2. fıkrasında, bazı durumlarda, birtakım ek bilgilerin veri ilgisine sunulacağını düzenler. Bu bilgiler; veri işlemenin hukuki dayanağı, kişisel verilerin ne kadar süre ile saklanacağı veya bu bilginin sağlanması mümkün değilse, ilgili sürenin belirlenmesinde kullanılacak kriterler, veri-

⁹⁹ Directive 2016/680 Recital 26: “Kişisel veriler, ilgili gerçek kişilerle bağlantılı olarak hukuka uygun, adil ve şeffaf şekilde ve yalnızca yasalarla belirtilen özel amaçlar uyarınca işlenmelidir. Bu hüküm tek başına, kolluk kuvvetlerinin gizli soruşturma veya video gözetimi gibi faaliyetlerde bulunmasını engellemez. Bu tür faaliyetler, yasal dayanağı olduğu ve ilgili kişinin de meşru menfaatleri de göz önünde bulundurularak, demokratik bir toplum açısından gerekli ve makul bir tedbir özelliği taşıdığı sürece; suçların önlenmesi, soruşturulması, tespit edilmesi, kovuşturulması, mahkemeler tarafından verilen ceza hükümlerinin infazı ve yasaların öngördüğü şartlar altında kamusal ve ulusal güvenliğine yönelik tehditlerin önlenmesi de dâhil olmak üzere, üye devletler tarafından gerçekleştirilebilir (...)”.

¹⁰⁰ Bu yönde bkz: WP29, “Guidelines on Transparency Under Regulation 2016/679”, s. 4.

ler üçüncü bir ülke ve uluslararası kuruluşlar dâhil olmak üzere, üçüncü kişilere aktarıldığında veri alıcılarının kategorisi ve veri ilgisinin bilgisi olmaksızın veri toplanması durumunda gerekli ise başka birtakım ek bilgilerin sağlanacağını içermelidir. Başka bir hususa dikkat çekmek gerekir ki, Direktif, GDPR'dan farklı olarak, veri işlenirken, oluşturulan profiller ve otomatik olarak verilen kararların altında yatan mantık konusundaki anlamlı ve açıklayıcı bir bilginin sunulmasını bilgilendirme hakkı kapsamına almamıştır.¹⁰¹

Bilgilendirme hakkı ile AB kanun koyucusu, veri ilgililerinin verilerin işlenmesiyle müdahale edilen temel hak ve özgürlükleri karşısında bir güvence olmayı ve bu iki menfaat arasında makul bir dengenin sağlanmasını hedeflemektedir. Bunun yanında söz konusu hakkın kabul edilmesi ve şeffaflığın sağlanması, kişisel verilerin dolaşımını son derece kolaylaştıran profil oluşturma, veri madenciliği (data mining¹⁰²) ve bu yönde çok sayıda teknolojik gelişmeler; verilerinin kim tarafından, neye dayanarak, nerede ve hangi amaçlar ve araçlar vasıtasıyla işlendiği konusunda haberdar edilmesini çok daha önemli kılmaktadır.¹⁰³

Kişiler elbette, verilerinin işlenmesinin taşıdığı riskler ve bu yöndeki kuralardan haberdar edilmelidir. Herkes sahip olduğu güvenceler ve haklar konusunda aydınlatılmış olmalı ve bu haklarını nasıl kullanılacağına ilişkin yeterli bilgi kendilerine sağlanmalıdır. Kişilerin mahremiyetinin korunması, veri sorumlularının faaliyetlerini şeffaflıkla sürdürmelerine bağlıdır.¹⁰⁴ Ancak bu şekilde hesap verilebilirlik sağlanacak, temel hak ve özgürlüklerinin kısıtlanmasında keyfiliğin önüne geçilebilecektir.

Ancak bilgilendirme hakkına istisna tanındığı haller de bulunur. Direktif m. 13/3 uyarınca, bazı durumlarda üye devletlerin aydınlatma yükümlülüğünün yerine getirmelerini erteleyebilecekleri veya ihmal edebilecekleri ve bilgilendirme hakkının kullanımını kısıtlayabilecekleri düzenlenir. Anılan madde uyarınca, veri ilgililerinin bilgilendirilmesi; resmi ve yasal soruşturmaları, tahkikatları veya prosedürleri veya suçların önlenmesi, tespit edilmesi, soruşturulması veya kovuşturulmasını ve cezaların infaz edilmesi amaçlarını engelleyebilecek nitelikteyse veya kamusal ve ulusal güvenlik ile başkalarının hak ve özgürlüklerini korunmasını güçleştirecek ise üye devletler, getirecekleri yasal düzenlemeler ile söz konusu hakların kullanımını tamamen veya kısmen kısıtlayabilecektir.

¹⁰¹ Zouave/Schroers, s. 17.

¹⁰² *Veri madenciliği*, çok sayıda veri arasından örüntüleri tespit etme, bu verileri analiz etme ve bir sonuç çıkarma işlemidir.

¹⁰³ WP29, "The Future of Privacy", s. 16.

¹⁰⁴ Roger Taylor, "No Privacy without Transparency" in: Ronald Leenes/Rosamunde van Brakel/Serge Gutwirth/ Paul De Hert (eds.), *Data Protection and Privacy: The Age of Intelligent Machines*, Computers, Privacy and Data Protection Series, V. 10, Hart Publishing, Oxford, 2017, s. 85.

AB kanun koyucusu, kişisel verilerin korunması hakkı ile kamu güvenliği- nin sağlanması menfaati arasındaki dengeyi kurmada; veri ilgililerine söz konusu hakların tanınmasının, ulaşılması hedeflenen menfaatleri zarara uğratabileceği hallerde, bu hususu üye devletlerin takdir alanına dair bir konu olarak değerlendirmiştir. Söz konusu maddenin son fıkrası uyarınca da üye devletler, bu veri işleme faaliyetlerini sayma yoluyla belirterek iç hukukunda düzenleyebilir. Dolayısıyla, üye devletler ulusal hukuklarında getireceği düzenlemeler ile bu hakkı, birtakım veri işleme faaliyetleri özelinde tamamen veya kısmen kısıtlama yoluna gidebileceklerdir. Burada önemli olan, düzenlemenin iç hukuka aktarılırken üye devletlerin, bu yetkiyi kullanacağı şartların objektif kriterlerle uyarınca belirlenmesidir.¹⁰⁵

B. Veriye Erişim Hakkı

Direktif m. 14, veriye erişim hakkını düzenler. Buna göre, veri ilgilileri, veri sorumlusundan kişisel verilerinin işlenip işlenmediğine dair bilgi isteyebilir. Verileri işlenmekteyse bunların neler olduğuna ve birtakım bilgilere erişme hakkı bulunur. Üye devletler, bu hakkın kullanılması için gerekli adımları atmalıdır.

Erişim hakkı ana hatlarıyla, bilgilendirme hakkını tamamlayarak kişisel verilerin ne şekilde işlendiğine ilişkin veri ilgililerinin bilgi sahibi olmasına ve haklarını kullanmalarını amaçlar.¹⁰⁶ Erişim hakkının kural olarak doğrudan veri sorumlusuna karşı kullanılabilmesi oldukça önemli bir gelişmedir.¹⁰⁷

Üye devletler, verilere erişimin yanında veri ilgililerine birtakım bilgileri sunmalıdır. Bunlar; işlemenin amaç ve hukuki dayanağı, ilgili kişisel verinin kategorisi, kişisel verilerin ifşa edildiği veya edileceği, alıcılar veya alıcı kategorileri, mümkünse kişisel verilerin saklanacağı süre veya bu mümkün değilse sürenin belirleneceği esaslar, veri ilgisinin veri sorumlusuna ve denetim makamına karşı sahip olduğu haklar ile verilerin kaynağı hakkındaki bilgilerdir. Elbette bilgilerin sunumu, “anlaşılabilir biçimde” (in an intelligible form) olmalıdır. Avrupa Konseyi, erişim hakkının adil bir şekilde kullanılmasını sağlamak için anlaşılır biçimdeki iletişimin içeriğe olduğu kadar üslubuna da yani, standart bir dijital iletişim diline de uygulanacağını belirtmektedir.¹⁰⁸

¹⁰⁵ WP29, “Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680)”, s. 18.

¹⁰⁶ Develioğlu, s. 87.

¹⁰⁷ Paul de Hert/Diana Dimitrova, “The Right of Access Under the Police Directive: Small Steps Forward”, in: Manel Medina/Andreas Mittrakas/Kai Rannenberg/Erich Schweighofer/Nikolaos Tsourolas (eds.), *Privacy Technologies and Policy, 6th Annual Privacy Forum, APF 2018, Barcelona, Spain, June 13-14, 2018, Revised Selected Papers*, Springer, Heidelberg, 2018, s. 123.

¹⁰⁸ The Council of Europe (CoE), Practical Guide on the use of Personal Data in the Police Sector (Çevrimiçi) <https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5>, s. 7, (Erişim Tarihi: 10.04.2019).

Yine de hakkın tabir-i caizse çekirdeğini oluşturan profil oluşturma ve otomatik olarak işleme ile alınan kararlar ve hakkındaki bilgiler erişim hakkı kapsamında değildir. Bu hususların erişim hakkı kapsamında yer almaması öğretide eleştirisi konusudur.¹⁰⁹

Esasında düzenleme, GDPR ile hemen hemen aynı iken, ondan ayrılan ve hakkın içeriğini etkileyen bir başka düzenlemeyi de barındırmaktadır. Erişim hakkı da tıpkı bilgilendirme hakkı gibi *nispidir*: Aynı şartlarla, üye devletlerce tamamen ve kısmen kullanımı kısıtlanabilir. Dolayısıyla, erişim hakkının da mutlak bir hak olmadığı görülmektedir. Buna rağmen, Direktif ile getirilen düzenleme ile henüz bu konuda atılması gereken adımlar olsa da, üye devletlerin veri işleme faaliyetlerinde hesap verilebilirliği ve şeffaflığı ön plana taşıyan önemli bir girişim olduğu söylenmelidir.¹¹⁰

C. Verilerin Düzeltmesini ve Silinmesini Talep Etme Hakkı

Direktif kapsamında kişisel verileri işlenen veri ilgililerinin sahip olduğu belki de en önemli ve etkili hak, verilerin düzeltilmesini (the right to rectification) ve silinmesini (the right to erasure) üye devletler ve onların yetkili makamlarından talep etme haklarıdır.

Üye devletler, yetkili makamlardan elde etmiş oldukları verilerin, veri ilgilisi hakkında yanlış bilgiler içermesi durumunda gecikmeksizin, kişinin *düzeltilme hakkını* tanımalıdır (Direktif m. 16/1). Böyle bir durumda üye devletler veri ilgililerine, ihtiyaç halinde ek bir beyan ile tamamlatılmak suretiyle, kendi verilerinin tamamlanmasını ve düzeltilmesine yönelik imkânları sunmakla yükümlüdürler.

Aynı maddenin 2. fıkrası ise veri ilgililerine üye devletlerden hukuka aykırı olarak işlenen verilerinin silinmesini talep etme hakkını düzenler. Maddeye göre üye devletler, Direktifin 4., 8. veya 10. maddelerine aykırı şekilde verilerin işlenmesi halinde kişilere verilerinin *silinmesini talep hakkını* tanıma ve yetkili makamların verileri silmesini sağlama yükümlülüğü altındadırlar. Buna göre, silme hakkından bahsedebilmek için bu aykırılık hallerinin ortaya konulması gerekir.

¹⁰⁹ de Hert/Dimitrova, s. 127.

¹¹⁰ de Hert/Dimitrova, s. 125; Hesap verilebilirlik ve şeffaflık ya diğer bir ifadeyle "açıklık" ilkeleri, OECD'nin 1980 tarihli "Mahremiyet Çerçeve Kararı" ile ilk defa kendisine yer bulmuştu. Bkz: The Organization for Economic Cooperation and Development (OECD), "The OECD Privacy Framework" s. 15-16, (Çevrimiçi) https://www.oecd.org/internet/economy/oecd_privacy_framework.pdf (Erişim Tarihi: 10.04.2019). OECD ilkelerinden bu yana hukuki metinlerde kendisine yer bulmuş bu ilkelerin hem etik hem de pratik bir boyutu bulunur. Gerek düzenlemeler gerekse de ilkeler, yalnızca normatif nitelik taşımazlar. Bunlar kişisel verilerin korunması hukukunun gelişimi ve zihinlerde belirginleşmesi için kültürel değişim zeminini de oluştururlar. Kamuoyunun bilinçlendirilmesine hizmet ederler. Krş. Hielke Hijmans/Charles D. Raab, "Ethical Dimensions of the GDPR" in: Mark Cole/Franziska Boehm (eds.), *Commentary on the General Data Protection Regulation*, Edward Elgar 2019, Forthcoming, s. 2-3 (Çevrimiçi) <https://ssrn.com/abstract=3222677> (Erişim Tarihi: 10.04.2019).

Öncelikle, Direktifin 4. maddesi kişisel verilerin işlenmesine hâkim olan ilkeleri düzenlerken, 8. madde verilerin hukuka uygunluğunu ve 10. maddesi ise hassas nitelikli kişisel verilerin işlenmesinde uyulacak şartları düzenler. Öyleyse sözgelimi 4. madde çerçevesinde ortaya çıkabilecek aykırılık, verilerin belirli olmayan amaçlarla ve “bir gün ihtiyaç olursa” şeklindeki bir düşünceyle işlenmesi olabileceği gibi verilerin depolanmasının artık veri elde edilmesindeki amaca hizmet etmiyor olması şeklinde olabilir. Keza 8. madde uyarınca, Direktifte belirtilen amaçların gözetilmeden verilerin elde edilmesi de verileri hukuka aykırı kılacaktır. Son olarak, hassas nitelikli kişisel verilerin işlenmesi veri ilgisinin hayati menfaatlerini (the vital interests of the data subject) korumalıdır. Aksi takdirde, bu verilerin işlenmesi de hukuka aykırıdır ve yetkili makamlar bu verileri gecikmeksizin silme yükümlülüğü altındadır.

Anılan maddenin 3. fıkrasına göre üye devletler, bazı hallerde verileri silmek yerine verilerin işlenmesini kısıtlayabilirler. Kişisel verilerin doğruluğuna ilişkin veri ilgisinin bir şikâyeti varsa ve bu durum verilerin doğruluğuna ilişkin bir belirsizliğe yol açmışsa, verilerin silinmesi yerine işlenmesi kısıtlanabilir. Bu durumda üye devlet, kısıtlama kararını kaldırmadan önce veri ilgisini bilgilendirmelidir. İkinci ihtimalde, silinmesi talep edilen verinin, delil olarak saklanması gerekiyorsa üye devlet silinme yerine kısıtlama tedbirine başvurabilir.

Bu noktada belirtilmesi gerekir ki, GDPR’da veri işlemenin sınırlandırılması hakkı, veri ilgisinin talep edebileceği ayrı bir hak şeklinde düzenlenmişken Direktifte ise üye devletlerin bazı durumlarda verileri silme yerine başvurabilecekleri alternatif bir tedbir olarak kendine yer bulmuştur. Ayrıca gerek düzeltme gerek silme gerekse de işlemenin kısıtlanması halinde, verilerin aktarıldığı alıcılarda da söz konusu işlemler paylaşılmalı ve alıcılar kendi sorumlulukları altında bulunan verilerde bu işlemleri gerçekleştirmelidir. Bir başka farklılık olarak, GDPR’da öngörülen veri işlemeye itiraz hakkına doğal olarak, Direktifte yer verilmemiştir.

Anılan maddenin 4. fıkrası uyarınca üye devletler, verinin düzeltilmesi veya silinmesi yönündeki talepleri reddetmeleri halinde bir veri işlemeye ilişkin bilgiler ve talebin reddine dair bir gerekçe sunmakla yükümlüdürler. Ancak söz konusu yükümlülüğün, tıpkı bilgilendirme ve erişim haklarında olduğu gibi ve aynı şartlara dayanarak, üye devletlerce tamamen veya kısmen kaldırılabilmesi belirtilmiştir. Buna karşılık, kişilerin denetleyici makama şikâyet hakkı ve üye devletlerin kişilere karşı, veri ilgililerinin başvurabileceği hukuki çareler konusunda bilgilendirme yükümlülüğü sürmektedir.

Nihayet, veri ilgisinin Direktif kapsamında sahip olduğu haklar; bilgilendirilme hakkı, erişim hakkı, düzeltmeyi talep hakkı ve silinmeyi talep etme hakkı şeklinde sayılabilir. Veri ilgililerinin bilgilendirme ve erişim hakları, mutlak nitelikte

olmayıp üye devletlerce kısıtlanabilecektir.¹¹¹ Buna karşılık aynı durum düzeltme ve silinme hakları için geçerli değildir. Şayet, veri işlenirken yanlış bilgilere yer verildiyse veriler doğrusu ile düzeltilmeli ve veri işlenmesinde hukuka aykırılıkların varlığı halinde ve gerekli şartlar sağlanmakta ise veriler silinmelidir.

§ IV. Direktif Uyarınca Veri Sorumlusu ve Veri İşleyene İlişkin Hükümler

Direktif GDPR’da da olduğu gibi, veri işleme faaliyetinin aktörlerinden veri sorumlusu ve veri işleyene ilişkin ayrıntılı düzenlemeler içerir. Bu düzenlemelerin detayına girmeden önce, veri sorumlusunu ve veri işleyeni tanımlayacağız.

Direktif’in 3. maddesi, bir tanım maddesidir. Veri sorumlusu Direktife göre, muhakkak bir yetkili makam olması gerektiğinden, öncelikle yetkili makamı tanımlamak gerekir. Yetkili makam; suçların önlenmesi, soruşturulması, tespit edilmesi, kovuşturulması, mahkemeler tarafından verilen ceza hükümlerinin infazı ve kamusal ile ulusal güvenliğine yönelik tehditlerin önlenmesi hususunda görevli kamusal makamı veya üye devlet tarafından bu hususlarda yetkilendirilmiş ve kamu gücünü kullanan herhangi başka organ veya tüzel kişiyi ifade eder.

Veri sorumlusu ise kişisel verilerin işleme amaçlarını ve araçlarını tek başına ya da başkalarıyla müştereken belirleyen yetkili makamdır. Bu anlamda veri sorumluluğunun paylaşılabileceği de kabul edildiğinden, müşterek sorumluluk esası (ortak veri sorumlusu) da söz konusu olabilir.

Veri işleme faaliyetinin diğer aktörü olarak veri işleyen ise veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi, kamu otoritesi, kurumu veya diğer başka birimler şeklinde tanımlanır.

Bu başlık altında incelenecek önemli kurumlardan biri de denetleyici makamdır (supervisory authority). Zira veri sorumlusu ve veri işleyenin, faaliyetlerin üçüncü bir aktörü denetleyici makamlar ile iş birliği halinde çalışmaları bir yükümlülük olarak Direktifin 26. maddesi ile getirilir. Makam, gerek kişisel verilerin işlenme sırasında gerekse de işlenme sonrasında ortaya çıkabilecek hukuki uyumsuzluklarda önemli bir rol üstlenir. Denetleyici makam, veri koruma kurallarının uygulanmasını soruşturma ve düzeltme yetkileriyle denetleyen bağımsız idari otorite olarak tanımlanabilir.¹¹² Denetleyici makam hem GDPR, Direktif ve

¹¹¹ Buna karşılık, bu hakların sınırlandırılması ancak üye devletlerinin bu durumu belgelendirmesi ve gerekçelendirmesi ile mümkündür, bkz: WP29, Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680), s. 25.

¹¹² Bu noktada belirtmek gerekir ki, 2004 ile 2014 yılları arasında Avrupa Veri Koruma Denetçisi (European Data Protection Supervisor) olarak görev yapmış *Peter Hustinx*, denetleyici makamların ancak etkili olabileceklerini sağlayan yasal bir çerçeveye ve stratejik bir yaklaşım ve fark yaratabilme becerisine sahip olmaları halinde efektif bir kurum olarak ihtiyaçları karşılayabileceğini belirtmektedir, bkz: Peter Hustinx, “The Role of Data Protection Authorities”, in: Serge Gutwirth, Yves Poullet, Paul de Hert, Cecile de Terwangne, Sjaak Nouwt (eds.), *Reinventing Data Protection?*, Springer, Heidelberg, 2009, s. 131.

ilgili ulusal kanunların ihlaline ilişkin bireysel şikâyetleri ele almaları itibarıyla yargısal, hem de yetkili bulunduğu hususlarda uzman olmaları ve ilke kararlar alabilmeleri itibarıyla de düzenleyici bir kurum niteliğindedir.

Direktifin 41. maddesine göre, her üye devletin en az bir denetleyici makamı bulunması gerekir. Örnek olarak Birleşik Krallık'ta *The Information Commissioner's Office* (ICO), Almanya'da *Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (BFDI) ve Fransa'da ise *Commission Nationale de l'Informatique et des Libertés* (CNIL) ulusal veri koruma otoritesidir. Ülkemizde de Kişisel Verilerin Korunması Kanunu ile birlikte kurulan, idari ve mali özerkliğe sahip ve kamu tüzel kişiliğini haiz *Kişisel Verileri Koruma Kurumu* söz konusu görevi yürütür.

Son olarak veri sorumlusuna ve veri işleyene ilişkin hükümler getirilmesinin Direktifin önemli yeniliklerinden biri olduğunun tekrar altı çizilmelidir. AB kanun koyucusu, 2008 Çerçeve Kararı ile getirmediği düzenlemelere, Direktifte yer vererek AB çapında veri sorumlusu ve işleyen makamlarının, belirli bir düzlemde ve yükümlülükler çatısı altında faaliyetlerini sürdürmelerini hedeflemektedir. Bu özellikle, kıta çapında yeknesaklığın sağlanması ve hesap verilebilirlik çıtasının artırılması bakımından önem arz eder.

A. Öngörülen Yükümlülükler

1. Tedbir Alma Yükümlülüğü ve Müşterek Veri Sorumluluğu

Direktifin 19. maddesinde, GDPR'la paralel bir düzenleme getirilerek veri sorumlusunun tedbir alma yükümlülüğü tanınmıştır. Buna göre, üye devletler veri işleme faaliyetlerinin Direktif ile uyumlu gerçekleşmesini sağlamak adına; veri sorumlusu yetkili makamın işlemenin doğası, kapsamı, bağlamı ve amaçları ile kişilerin temel hak ve özgürlükleri bakımından mevcut riskleri göz önünde bulundurarak uygun teknik ve organizasyonel tedbirleri almasını sağlamakla yükümlü kılınmışlardır. Ayrıca gerekli ise, bu tedbirler gözden geçirilmeli ve yenilenmelidir. Üye devletler bunun yanında, ilgili önlemleri içeren uygun bir veri koruma politikasını da ortaya koymalıdır.

Veri sorumlusu Direktifin 20. maddesi uyarınca, söz konusu önlemleri veri işleme faaliyetinin parçası haline getirmelidir. Veri sorumlusu, kişisel verilerin korunmasını hedef alarak işleme faaliyetini planlamakla (data protection by design) yükümlüdür. Tasarımdan itibaren veri koruması, veri işleme faaliyetinde kullanılacak herhangi bir sistemi (çoğunlukla veri kayıt sistemini) veya teknolojinin tasarlanma aşamasından itibaren, veri sorumlusunun her zaman aklında mahremiyet düşüncesi olması ve bu yönde bir sistematik yaklaşımı takip etmesi olarak tanımlanabilir.¹¹³

¹¹³ Lee A. Bygrave, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements* *Oslo Law Review*, Oslo, 2017, V. 4, No. 2, s. 114-116; Maria Grazia Porcedda,

Üye devletler ayrıca veri sorumlusu yetkili makamın, başlangıçtan itibaren her veri işleme faaliyetinde kişilerin mahremiyet haklarına saygı duymasını ve hukuki yükümlülüklerine uymasını sağlamalıdır. Bu yükümlülüğün (data protection by default) toplanan kişisel verilerin miktarı, yalnızca veri işleme faaliyetinin amaçları için gerekli olan verilerin işlenmesi, ne boyutlarda verinin işleneceği ve verilerin saklanma süresi ile bağlantılı olduğu ifade edilmektedir. Bu tedbirler, özellikle kişisel verilerin belirsiz sayıda ve statüdeki kişilerin erişimine açılmasını sağlamalıdır.¹¹⁴

Direktifin 21. maddesi ise müşterek veri sorumluluğuna ilişkin düzenlemeler getirmektedir. Veri sorumlusu yetkili makamın, veri işleme amaç ve araçlarını başka kurum ve kuruluşlar ile ortak şekilde kararlaştırabileceği düzenlendiğinden, GDPR'da olduğu gibi Direktifte ortak veri sorumlusu kavramı kendine yer bulmaktadır.

Anılan madde uyarınca, müşterek veri sorumlularının, özellikle veri ilgililerinin haklarını kullanması hususundaki yükümlülüklerini belirleyen bir anlaşmayı şeffaflıkla gerçekleştirmeleri gerekmektedir. Üye devletler, veri ilgililerinin gerektiğinde iletişime geçebilecekleri bir irtibat noktasını da muhakkak belirlemelilerdir. Bu noktada, üye devletler ortak veri sorumlularının tek bir irtibat noktası gibi hareket edebileceklerini de belirleyebilir.

2. Veri İşleyene İlişkin Yükümlülükler

22. madde uyarınca üye devletler, Direktifteki gereklilikleri yerine getirilebilecek ve kişilerin haklarının korunmasını sağlayacak teknik ve organizasyonel tedbirleri alabilecek veri işleyenlerle çalışmalıdırlar.

Veri işleyen ancak veri sorumlusunun talimatıyla hareket edebilir. Kişisel verileri işlemeye yetkili kişiler, gizlilik yükümlülüğüne uyacaklardır. Veri işleyen

"'Privacy by Design' in EU Law: Matching Privacy Protection Goals with the Essence of the Rights to Private Life and Data Protection", in: Manel Medina/Andreas Mitras/Kai Rannenberg/Erich Schweighofer/Nikolaos Tsouroulas (eds.), *Privacy Technologies and Policy, 6th Annual Privacy Forum, APF 2018, Barcelona, Spain, June 13-14, 2018, Revised Selected Papers*, Springer, Heidelberg, 2018, s. 183 vd.; Ann Bevitt/Peter Carey, "Data Security and Breach Notifications", in: Peter Carey (ed.), *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, Oxford, 2018, s. 95; Daniel Le Métayer, "Privacy by Design: A Matter of Choice", in: Serge Gutwirth/Yves Poulet/Paul de Hert (eds.), *Data Protection in a Profiled World*, Springer 2010, s. 323-324; George Danezis/José Domingo-Ferrer/Marit Hansen/Jaap-Henk Hoepman/Daniel Le Métayer/Rodica Tîrtea/Stefan Schiffner, *Privacy and Data Protection by Design - from policy to engineering*, European Union Agency for Network and Information Security (ENISA) 2015, s. 5-7; Paolo Balboni, "Let's not Forget about Data Protection by Design", (Çevrimiçi) <https://www.paolo-balboni.eu/index.php/2018/07/11/lets-not-forget-about-data-protection-by-design/> (Erişim Tarihi: 10.04.2019); GDPR Rec. 78; Directive 2016/680 Rec. 53.

¹¹⁴ Bevitt/Carey, s. 95; Carey, s. 41; Voigt/von dem Bussche, s. 242; Piotr Foitzik, "Privacy by Default in Online Services", (Çevrimiçi) <https://iapp.org/news/a/privacy-by-default-in-online-services/>, (Erişim Tarihi: 10.04.2019); Aurelia Tamò-Larrieux, *Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things, Law, Governance and Technology Series 40*, Springer, Heidelberg, 2018, s. 185.

ayrıca, veri sorumlusunun ilgili kişilerin haklarını kullanmaya yönelik tedbirlerine katkı sağlamalıdır.

Bunlar yanında veri işleyen, AB veya iç hukukta verilerin saklanması ilişkin bir düzenleme bulunmadığı sürece, yetkili makamın kararı üzerine işlemeye ilişkin hizmetlerin verilmesinin ardından tüm kişisel verileri silmeli veya veri sorumlusuna geri vermelidir. İşleyen, faaliyetlerinin yürütülmesinde Direktifteki gerekliliklere uyulduğunu ortaya koymak için gerekli tüm bilgileri veri sorumlusuna sağlayabilmelidir.

Son olarak, veri işleyen, veri sorumlusu adına işleme yapacak başka bir işleniyeni yetkilendirmek için, yukarıda sayılan tüm yükümlülüklerin sağlandığından emin olmalıdır. Bunun yanında, üye devletten bu konuya ilişkin özel veya genel bir yetkilendirmeye dayanılmalıdır.

3. Kayıt Tutma Yükümlülüğü ve Logging

Direktifin 24. maddesine göre üye devletler, veri sorumlusu yetkili makamlarının her türlü veri işleme faaliyetlerinde birtakım bilgileri kayıt etmelidirler. Veri sorumlusu ve veri işleyenler de Direktife uyum sağlamak için kendi sorumluluk alanlarında bulunan faaliyetlerde bu kayıtları tutmalıdır. Bu çerçevede, veri sorumlusu ve işleyen, denetleyici makamlar ile iş birliği yapmak ve bu kayıtları talep üzerine hazır bulundurmak zorundadır.¹¹⁵

Veri sorumlusunun kayıtlarında aşağıda sayılı tüm bu bilgilerin yer alması gerekir:

- a) Veri sorumlusunun ve varsa ortak veri sorumlusunun ve veri koruma görevlisinin kimliği ve iletişim bilgileri,
- b) Veri işlemenin amaçları,
- c) Üçüncü ülke veya uluslararası kuruluşlar da dâhil olmak üzere, verinin aktarıldığı veya aktarılacağı veri alıcısı kategorileri,
- d) Veri ilgisinin ve kişisel verileri tabi olduğu kategorilerin tanımı,
- e) Uygulanıyorsa, profil oluşturmada kullanıldığının bilgisi,
- f) Uygulanıyorsa, üçüncü bir ülkeye ve uluslararası kuruluşlara veri aktarımı kategorileri,
- g) Veri aktarımı ve verilerin ne amaçla işlendiği de dahi olmak üzere, veri işleme faaliyetinin hukuki dayanağına ilişkin gösterge,
- h) Mümkünse, farklı veri kategorilerinin silinmesi için planlanan süre,
- i) Mümkünse, 29. maddenin 1. fıkrası çerçevesinde alınan teknik ve organizasyonel tedbirlere ilişkin genel açıklamalar.

¹¹⁵ Directive 2016/680 Rec. 56.

Veri işleyenlerin veri sorumlusu adına gerçekleştirdiği faaliyetlerde aşağıdaki bilgilerin kayıtları tutulmalıdır:

- Veri işleyen veya işleyenler ile bu işleyenlerin hangi veri sorumlusu adına hareket ettikleri ve varsa veri koruma görevlisinin, kimliği ve iletişim bilgileri,
- Her bir veri sorumlusu adına gerçekleştirilen işleme faaliyeti kategorileri,
- İlgili hallerde, kişisel verilerin veri sorumlusunun açık talimatıyla bir üçüncü ülke veya uluslararası kuruluşa aktarıldığına ve alıcıların tarifine ilişkin bilgiler,
- Mümkünse, 29. maddenin 1. fıkrası çerçevesinde alınan teknik ve organizasyonel tedbirlere ilişkin genel açıklamalar.

Sayılan tüm bu bilgilerin yazılı olması gerekir. Bunun yanında, dijital formatta da bilgilerin sunulması mümkündür. Veri sorumlusu ve veri işleyenin, faaliyetlerinde söz konusu kayıtların tutulması öncelikle, bu kişilerin hukuk kurallarına ve Direktif hükümlerine tabi olarak veri işlemelerini sağlamaları adına oldukça önemlidir. Bunun yanında, hesap verilebilirliğin sağlanması bakımından kayıtların tutulması gerekir.

25. madde ise “Logging”e ilişkin hükmü içermektedir. Logging, gerçekleştirilen faaliyetler çerçevesinde meydana gelen olay ve hareketlerin kayıt altına alınması anlamına gelir. Özellikle bilgi yönetim sistemleri içerisinde bütünlüğü, gizliliği ve erişilebilirliği sağlamak açısından önemlidir.

Anılan madde uyarınca, üye devletler belirli faaliyetlerinde log kaydı tutmalıdır. Bunlar, verilerin otomatik olarak işlendiği; kişisel verilerin elde edilmesi, kaydedilmesi, değişiklik yapılması, danışma amacıyla kullanılması, aktarılması dâhil olmak üzere bir şekilde açıklanması, başka veriler ile birleştirilmesi ve silinmesi faaliyetleridir. Kişisel verilerin danışmaya konu edilmesi veya açıklanması edilmesi halinde, log kayıtları; bu işlemlerin gerekçesini, tarihini ve saatini ve mümkünse, kişisel verilerle ilgili danışılan veya ifşa eden kişinin kimliğini ve bu kişisel verilerin alıcılarının kimliğini tespit etmeyi mümkün kılacak bilgileri içermelidir. Madde 29 Çalışma Grubu, faaliyette bulunan kişinin kimlik bilgisinin yalnızca danışma ve ifşa edilme gibi sınırlı bir kapsamda değil, sayılan diğer bütün faaliyetler için de geçerli olmasını tavsiye etmektedir.¹¹⁶

Log kayıtları, yalnızca işlemenin hukuka uygunluğunu doğrulama, yetkili makamların kendi işlemlerini denetlemesi ve kişisel verilerin bütünlüğü ve güvenliğini sağlamak amacıyla ancak cezai soruşturma ve kovuşturmalar için tutulabilecektir. Kayıtlar, talep halinde denetleyici makamlara sunulmak üzere hazır tutulmalıdır.

¹¹⁶ WP29, Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680), s. 28

“Logging”, faaliyetlerdeki kötüye kullanımlarının tespit edilebilmesi bakımından, veri koruma izlemesi (data protection monitoring) ve veri işleme faaliyetlerinin kontrolü için son derece önemli bir araçtır.¹¹⁷ Madde 29 Çalışma Grubu’na göre, üye devletler kendi iç hukuklarında, log kayıtlarındaki gereklilikler konusunda, örneğin log kayıtlarının içeriği, teknik önlemler, öz denetim ve uyumluluğu yönünde düzenlemeler gerçekleştirmelidir.¹¹⁸ Bunun yanında Direktif, log kayıtlarının saklanması için belirli bir depolama süresi öngörmediğinden üye devletler, denetleyici makamların kayıtlar hakkındaki silinmesi ve gözden geçirmesi için gerekli makul bir süreyi, depolama süresi olarak belirlemelidir.¹¹⁹

AB kanun koyucusu, GDPR’da düzenlemediği “Logging” hususuna Direktifte yer vermiş olması dikkat çekicidir.¹²⁰ Ceza yargılaması sırasında ve kolluk alanlarında otomatik veri işleme sistemlerinin yoğun kullanılıp buna karşın işlemlere ilişkin kayıtların yeteri derecede tutulmaması, düzenlemenin nedenidir.

Bu kayıtlar, cezai soruşturmalarda veri işlemenin hukuka uygunluğunun tespiti ve izinsiz veri işlemler açısından caydırıcılık içermesi adına,¹²¹ gerek yetkili makamın öz denetimini sağlamak gerekse de denetleyici makamların kayıtlara duyacağı gereksinimi gidermek bakımından önem taşımaktadır. Sözgelimi, bir kolluk görevlisinin otomatik veri işleme sistemine girip aile üyeleri veya komşuları hakkında arama yapması halinde, log kayıtlarının tutulması iç denetimde yetkili makamın ya da denetleyici makamın sorumluyu tespit etmesine olanak sağlayacaktır.¹²² Bununla birlikte, log kayıtlarının tutulmasının özellikle de eski otomatik veri işleme sistemleri açısından, masraflı ve teknik zorluklar içerdiği belirtilmektedir.¹²³ Ancak bu kayıtların, hukuki denetime sağlayacakları önemli katkılar göz önüne alındığında, kaydedilmesi yönünde bir düzenlemeye yer verildiği anlaşılmaktadır.

4. Veri Koruma Etki Değerlendirmesi ve Ön İstişare (Ön Denetim)

Direktif 27. maddesiyle, GDPR’da olduğu gibi, veri koruma etki değerlendirmesi (data protection impact assessment) ve 28. maddesi ile denetleyici makamla ön istişareye (prior consultation of the supervisory authority) ilişkin hükümler getirmektedir. Özellikle veri koruma etki değerlendirmesi ya da diğer bir ifadeyle mahremiyet etki değerlendirmesi (privacy impact assessment), AB

¹¹⁷ Bu yönde bkz: Sajfert/Quintel, s. 5.

¹¹⁸ WP29, Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680), s. 28.

¹¹⁹ WP29, Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680), s. 27-28.

¹²⁰ Bu yönde bkz: Sajfert/Quintel, s. 15.

¹²¹ WP29, Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680), s. 26.

¹²² The Information Commissioner’s Office (ICO), *Guide Law Enforcement Processing (Part III of the Bill)*, (Çevrimiçi) <https://www.pdpjournals.com/docs/887918.pdf>, 05/04/2018, s. 33 (Erişim Tarihi: 10.04.2019).

¹²³ Sajfert/Quintel, s. 15.

Hukuku açısından yeni bir kavram olmasına karşın dünyada önemli bir süredir kullanılmaktadır.¹²⁴

Veri koruma etki değerlendirmesi ana hatlarıyla; kişilerin verilerinin işlenmesinin temel hak ve özgürlüklerini ihlal etme riski yüksek olan durumlarda, faaliyetin hukuki gereksinimleri taşıyıp taşımadığının veri sorumlusu tarafından denetlenmesi ve gerekli önlemlerin gerçekleştirilmesidir.¹²⁵ Önleyici amaçlarla yürütülen kolluk faaliyetlerinde veya cezai soruşturmalarda, çok büyük ölçekte ve hassas nitelikte veriler işlenir. Bu nedenle veri koruma etki değerlendirmesi, Direktif özelinde ayrı bir önem ve değere sahiptir. Bu alt başlıkta ele alacağımız veri koruma etki değerlendirmesi ve ön istişare müesseseleri, Direktifin hassas konumu ve ilgili olduğu konu göz önünde bulundurulduğunda; kapsamında yürütülen faaliyetlerdeki ağır veri ihlali risklerine set çekme ve “ön denetim”i sağlaması bakımından Direktifin üzerinde durulması gereken konularından biridir.

Belirtmek gerekir ki, benzer bir mekanizmaya 95/46/EC sayılı Direktif ve 2008 Çerçeve Kararında da yer verilmekteydi. Ancak üye devletler tarafından, çok fazla idari yüke ve masrafa neden olduğu gerekçesi ile çeşitli eleştirilere konu olmuştu.¹²⁶ AB kanun koyucusu veri koruma etki değerlendirmesi ve sonrasında ön istişare müesseselerine yer vererek, eski sistemin dezavantajlarını ortadan kaldırmayı amaçlamaktadır. Yeni düzenlemenin de bu anlamda olumlu karşılandığını söylemek mümkündür.¹²⁷

Veri koruma değerlendirmesini unsurlarına ayırarak incelemek mümkündür:

1. **Risk Unsuru:** *Riskin olasılığı ve ciddiyeti; veri işlemenin niteliği, kapsamı, içeriği ve amaçları dikkate alınarak belirlenmelidir.* Veri işleme faaliyeti, kişilerin temel hak ve özgürlüklerini ihlal etme riskini yüksek derecede taşıyorsa, veri sorumlusunun veri etki değerlendirmesine başvurması gerekmektedir. Değerlendirmede özellikle riskin kaynağı, doğası, özgüllüğü ve

¹²⁴ David Wright/Paul de Hert, “Introduction to Privacy Assessment”, in: David Wright/Paul de Hert (eds.), *Privacy Impact Assessment*, Law, Governance and Technology Series 6, Springer, Heidelberg, 2012, s. 8.

¹²⁵ Paul de Hert, “A Human Rights Perspective on Privacy and Data Protection Impact Assessments”, in: David Wright/Paul de Hert (eds.), *Privacy Impact Assessment*, Law, Governance and Technology Series 6, Springer, Heidelberg 2012, s. 34; The Article 29 Working Party, “Guidelines on Data Protection Impact Assessment (DPIA)”, (Çevrimiçi), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, 04/04/2017, s. 19, (Erişim Tarihi: 10.04.2019); The Information Commissioner’s Office (ICO), Accountability and Governance: Data Protection Impact Assessments (DPIAs) (Çevrimiçi) <https://www.pdpjournals.com/docs/887901.pdf>, 22/03/2018, s. 19 (Erişim Tarihi: 10.04.2019).

¹²⁶ Françoise Gilbert, “EU General Data Protection Regulation: What Impact for Business Established Outside the European Union”, *Journal of Internet Law*, Mayıs 2016, s. 4 (akt: Develioğlu, s. 110).

¹²⁷ Gerrit Hornung, “A General Data Protection Regulation for Europe: Light and Shade in the Commission’s Draft of 25 January 2012”, *SCRIPTed*, 9, 2012, s. 77 (akt: Develioğlu, s. 110).

ciddiyeti göz önünde bulundurulmalıdır.¹²⁸ Riskler pek çok çeşitte karşımıza çıkabileceklerdir: Örneğin; ayrımcılığa neden olma, kimlik hırsızlıkları, maddi kayıplar, itibarın zedelenmesi, mesleki sırların ifşası, kişilerin hassas nitelikli verilerinin işlendiği durumlarda ortaya çıkabilecek ekonomik ve sosyal dezavantajlara yol açılması, istenmeyen sonuçlardan bazıları olarak sayılabilir.¹²⁹

2. **Zaman Unsuru:** *Veri koruma etki değerlendirmesi, veri işlemesinden önce gerçekleştirilmelidir.* Değerlendirmeye risklerin ortaya çıktığı ilk andan itibaren başlanmalıdır. Bu unsur veri sorumluların, tasarımdan itibaren veri koruması (data protection by design) ve başlangıçtan itibaren veri koruması (data protection by default) yükümlülükleri ile paralel olduğu söylenmelidir.¹³⁰
3. **Kişi Unsuru:** *Değerlendirmeyi veri sorumlusu yetkili makam gerçekleştirmelidir* (Direktif m. 27). Bu kısımda özellikle GDPR’da yer alan veri koruma görevlisine danışma hükmünün Direktifte yer almadığı göze çarpmaktadır. Uygulamada Direktifin bulunduğu alana ilişkin olarak, pratiklik ihtiyacını gidermek amacıyla bu hükme yer verilmediği düşünülebilir. Ancak kişilerin temel hak ve özgürlüklerinin sağlanması adına üye devletler daha yüksek bir standart belirlemelidir. Üye devletlerin, atadıkları veri koruma görevlisinin de değerlendirme sürecine katılımını sağlaması gerektiği kanaatindeyiz.
4. **İçerik Unsuru:** *Veri koruma etki değerlendirmesi, 27. maddede sayılan bilgileri mutlaka içermelidir.* Bu bilgiler; öngörülen faaliyetin genel tarifi, ilgili kişinin temel hak ve özgürlüklerine yönelik risklere ilişkin değerlendirme, risklere karşı öngörülen tedbirler ve veri korumasını sağlamak ve ortaya koymak için öngörülen mekanizmalardan oluşur.

Direktifin 28. maddesi ise ön istişare (prior consultation) kurumunu düzenler. Anılan madde uyarınca, üye devletler, veri sorumlusu veya veri işleyen yeni bir dosyalama sistemi oluşturacak veri işleme faaliyetinden önce denetleyici makamla istişare etmesini sağlamalıdır. Yeni bir dosyalama sistemini oluşturabilecek durumlar olarak; veri koruma etki değerlendirmesinin riski düşürmek için gerekli tedbirlerin alınmaması halinde veri işlemenin yüksek derecede risk içereceğine ilişkin raporları ve işleme faaliyetinde kullanılan özellikle yeni teknoloji, mekanizma veya usullerin kişilerin hak ve özgürlükleri açısından yüksek risk içermesi halleri sayılmıştır. Bu durumlarda veri sorumluları, denetleyici makama veri işleme faaliyetinin hukuki gerekliliklere uygunluğunu denetlemesi açısından kendi veri koruma etki değerlendirmesi raporunu ve talep halinde, makamın ken-

¹²⁸ GDPR Rec. 84.

¹²⁹ Directive 2016/680 Rec. 51; ICO, Accountability and Governance: Data Protection Impact Assessments (DPIAs), s. 39-41.

¹³⁰ WP29, “Guidelines on Data Protection Impact Assessment (DPIA), s. 14.

di değerlendirmesini yapabilmesi için gerekli birtakım ek bilgileri de sunmalıdır. Bu açıdan denetleyici makama sunulacak bilgilerin kapsamının GDPR'a göre daha sınırlı tutulduğu görülür.

Yapılan ön istişare sonucunda, denetleyici makamın veri işleminin Direktife aykırılık teşkil edeceğine ilişkin görüş bildirmesi ve özellikle, veri sorumlusunun riski tanımlayamamış veya alacağı tedbirler bakımından yetersiz kaldığı durumlarda; denetleyici makam, veri sorumlusu ve varsa, veri işleyene yazılı tavsiyesini bildirecektir. Denetleyici makam, yazılı tavsiyenin yanında Direktifin 47. maddesinde kendisine tanınan haklarını da kullanabilecektir. Buna göre denetleyici makam; veri sorumlusu ve veri işleyene uyarı verebilir, kişisel verilerin düzeltilmesini, silinmesini veya verilerin işlenmesini kısıtlanmasını emredebilir ya da son olarak, belirli ve geçici bir süre ile sınırlı olmak üzere veri işlemeyi yasaklayabilir.

Anılan maddede üye devletlerin iç hukuklarına ve yasama faaliyetlerine yönelik bir hüküm olarak, veri işleme faaliyetleri ile ilgili herhangi bir yasal düzenleme hazırlığı esnasında yine denetleyici makamlara danışılması ve görüşünün alınması gerektiği ifade edilmektedir. Bu durum, denetleyici makamların ülkele- rin bu hususlarda düzenleyici ve bağımsız bir otorite karakterine sahip olmalarından kaynaklanmaktadır.

Makamın bu anlamda, sahip olduğu ağır yaptırımlar ile veri sorumlusu ve işleyenleri hukuki düzlemde kalmaya iteceği söylenebilir. Bu alt başlıkta incelediğimiz, veri koruma etki değerlendirmesi ve ön istişare kurumları ile öncelikle veri sorumlusu kendi içerisinde öz denetimi gerçekleştirerek rapor- lama yapacak, daha sonrasında belirli risklerin halen var olması durumunda ise denetleyici makama yapılacak danışma ile tam anlamıyla bir ön denetim gerçekleşecektir. Ön denetimin iki aşamalı olması ve ikinci aşamada içerdiği yaptırım tehdidi bakımından, hem uygulamadaki ihtiyaçların göz önünde bulundurulduğu hem de Direktifin düzenlediği alan nedeniyle, kişilerin verileri- nin işlenmesinin temel hak ve özgürlük ihlallerine yol açma ihtimalinin yüksek olduğunun da değerlendirildiği görülmektedir. Sonuç olarak, yeni düzenlemeye ilişkin yapılan olumlu eleştirilere katılmakta ve bunun yerinde ve gerekli bir düzenleme olduğunu düşünmekteyiz.

B. Veri İşleme Güvenliği ve Bildirim Yükümlülüğü

Veri işleme güvenliği, Direktifin, GDPR'a oranla son derece ayrıntılı yer verilen ve üye devletlere son derece sıkı şartlar ile pek çok risk analizi ve durum kontrolü yapmasının amaçlandığı düzenlemelerinden biridir. Kavramı, veri işle- me sistemlerinin gizliliği, bütünlüğü ve kullanılabilirliğini korumayı amaçlayan ve bu amaçla, risk değerlendirmesine dayanan bir yaklaşımın benimsendiği, veri sorumluları ve veri işleyenlerin veri ilgililerine karşı bir sorumluluk alanı olarak

tanımlamak mümkündür.¹³¹ Direktif kapsamınca işlenecek veriler ve işleme faaliyetinin yaratabileceği riskler göz önünde bulundurulduğunda veri işleme güvenliğine verilmesi gereken önem ortaya çıkmaktadır.

Veri işleme güvenliğinin, başlık altında saydığımız birçok yükümlülükle paralel ve onun tamamlayıcısı olduğu unutulmamalıdır. Bu çerçevede özellikle hassas nitelikte kişisel verilerin işlenmesi hallerinde veri sorumlusu, gerekli güvenliği sağlayacak yeterli teknik ve organizasyonel tedbirlerin alındığından emin olmalıdır. Direktifin 29. maddesi uyarınca, otomatik veri işleme faaliyetleri de dâhil olmak üzere, aşağıda sayılan risk analizlerinin yapılması gerekmektedir:

- a) Yetkisiz kişilerin kullanılan kişisel verilerin işlenmesi teçhizatlarına erişiminin olmaması (teçhizat erişim kontrolü),
- b) Veri ortamının yetkisiz kişilerce okunması, kopyalanması, değiştirilmesi veya kaldırılmasını önlenmiş olması (veri ortamı kontrolü),
- c) Kişisel verilerin sisteme yetkisiz kişilerin girişinin ve kayıtlı kişisel verilerin yetkisiz kişilerce incelenmesinin, değiştirilmesi ve silinmesinin önlenmiş olması (saklama kontrolü),
- d) Veri iletişim teçhizatı kullanan yetkisiz kişilerce otomatik işlem sistemlerinin kullanılmasının önlenmiş olması (kullanıcı kontrolü),
- e) Otomatik işleme sistemini kullanmaya yetkili kişilerin yalnızca erişim yetkilerinin kapsadığı kişisel verilere erişebilmelerini sağlanmış olması (veri erişim kontrolü),
- f) Veri iletişim teçhizatı kullanılarak kişisel verilerin aktarıldığı veya aktarılabileceği kurumları doğrulamanın ve tespit etmenin mümkün olması (iletişim kontrolü),
- g) Otomatik işleme sistemlerine hangi kişisel verilerin kaydedildiğini ve kişisel verilerin ne zaman ve kim tarafından kaydedildiğini doğrulamanın ve tespit etmenin mümkün olması (giriş kontrolü),
- h) Kişisel verilerin aktarılması veya veri ortamının taşınması sırasında kişisel verilerin yetkisiz kişilerce okunması, kopyalanması, değiştirilmesi veya silinmesinin önlenmiş olması (aktarım kontrolü),
- i) Kurulu sistemlerin, kesintiler halinde geri yüklenebilmesi (kurtarma),
- j) Sistemin işlevlerini yerine getirdiğinden, işlevlerindeki hataların bildiriliyor olması (güvenilirlik) ve sistemin hatalı çalışması nedeniyle toplanmış kişisel verilerin bozulmaması gerekir (bütünlük).

¹³¹ Paul Lambert, Understanding the New European Data Protection Rules, CRC Press, Boca Raton, 2017, s. 271; Handbook on European Data Protection Law: 2018 Edition, s. 131; European Union Agency for Network and Information Security (ENISA), Handbook on Security of Personal Data Processing, 2018, s. 6; GDPR Rec. 83.

İşleme güvenliğini sağlanamadığı durumlarda, veri sorumlusu ve veri işleyenlerin yükümlülükleri bir bildirim yükümlülüğüne dönüşmektedir. Direktif uyarınca, veri ihlali (personal data breach); aktararak, depolanarak veya başka şekillerle işlenen verilerin kazaen veya hukuka aykırı imhasına, kaybına, ifşasına veya ele geçirilmesine yol açılması şeklinde tanımlanmaktadır.

Direktifin 30. maddesi denetleyici makama yapılacak bildirimi, 31. maddesi ise veri ilgisine yapılacak bildirimi düzenlemektedir. GDPR'dan farksız olarak, veri sorumlusuna, kişilerin temel hak ve özgürlükleri bakımından düşük risk teşkil etmediği sürece, denetleyici makama ihlali derhal bildirme yükümlülüğü getirilmiştir. İhlal bildirimi, ihlalin varlığından haberdar olunmasından itibaren 72 saat içinde yapılmalıdır. Veri sorumlusu ayrıca bilgileri başka bir ülkenin yetkili makam veri sorumlusundan almış veya ona bizzat kendisi aktarmış ise bildirimin ayrıca söz konusu yetkili makama da yapılması gerekmektedir. Keza veri işleyen de ihlali öğrenir öğrenmez veri sorumlusunu bu durumdan haberdar etmelidir.

Denetim makamına ve ilgili hallerde üçüncü bir ülkenin yetkili makamına yapılacak bildirimde asgari olarak; mümkünse, ilgili kişi kategorileri ve veri kayıtlarının yaklaşık sayıları da dâhil olmak üzere ihlalin doğası, veri koruma görevlisi veya başka bir irtibat noktasının kimliği ile iletişim bilgileri, ihlalin muhtemel sonuçları ve zararlı etkilerini azaltmak üzere alınan tedbirler de dâhil olmak üzere, alınan veya alınması önerilen tedbirlere ilişkin bilgilerin yer alması gerektiği ifade edilmiştir.

İhlalin kişilerin temel hak ve özgürlüklerinin ihlaline yol açması bakımından yüksek risk taşıdığı durumlarda, Direktifin 31. maddesi uyarınca, veri sorumlusu ihlali gecikmeden ilgili kişiye bildirmelidir. Bildirimde açık ve sade bir dil kullanılmalıdır ve ihlalin niteliğini ve veri koruma görevlisinin kimliği ile iletişim bilgileri, ihlalin muhtemel sonuçları ve tedbirlere ilişkin yukarıda sayılan bilgileri içermelidir.

Buna karşılık, söz konusu yükümlülüğe istisna getirildiği görülmektedir. Veri şifreleme gibi, veriye izinsiz erişenlerin algılamasını engelleyecek uygun teknolojik ve organizasyonel önleyici tedbirler alınmış ise veri ilgisine bildirim yükümlülüğü yerine getirilmeyebilir. Aynı şekilde, ihlalin ardından yüksek riskin doğmasını engelleyecek tedbirler alınmışsa veya bildirimin yapılmasındaki zorluklar ile bildirimden doğacak menfaatler arasında aşırı orantısızlık var ise yükümlülük yerine getirilmeyebilir. Son durumda, veri sorumlusu bu durumu kamuoyuna bildirmeli ya da veri ilgililerin eşit derecede bilgilendirilebileceği benzer bir önlemi almalıdır.

C. Veri Koruma Görevlisi

Veri koruma görevlisi kavramı (data protection officer), 15 Aralık 2015'teki reform paketinin en önemli yeniliklerinden biridir.¹³² Nitekim Madde 29 Çalışma Grubu da veri koruma görevlisinin, yeni düzenlemenin odağında yer aldığını belirtmektedir.¹³³ Kısa ve öz bir tanım yapmak gerekirse: Veri koruma görevlisi, veri sorumlusunu bilgilendiren ve tavsiyelerde bulunan, kişisel verilerin işlenmesinin hukuka uygunluğunu takip eden alanında uzman ve bağımsız bir çalışandır.¹³⁴

Veri koruma görevlisi (Bundan sonra "VKG" olarak anılacaktır), GDPR'da bazı hallerde zorunlu tutulur. Bu hallerden, araştırma konumuzla ilgisi bulunanı ise veri işlemenin, ceza yargılamasındaki yargı makamları hariç, kamu kurum ve kuruluşları tarafından gerçekleştiriliyor olmasıdır. Kamu kurumları tarafından gerçekleştirilen veri işlemleri halinde bir VKG bulunmalıdır. Buna binaen, Direktifin 32. maddesi uyarınca, üye devletlerin veri koruma görevlisi atamaları zorunlu tutulmuştur. Ayrıca tek bir veri koruma görevlisi de örneğin, yetkili makamlar arasında paylaşılan kaynakların çok olması itibarıyla, organizasyon yapıları ve büyüklükleri dikkate alınarak birkaç üye devletin veri sorumluları tarafından müştereken atanabilir.¹³⁵

Direktifin 34. maddesine göre; veri sorumlusu ve çalışanlarını veri koruma yükümlülüklerine ilişkin olarak bilgilendirmek ve tavsiyelerde bulunmak, sürdürülen veri işleme faaliyetlerin veri sorumlusunun kişisel verilerin korunması politikalarına ve mevzuata uygunluğunu takip etmenin yanı sıra, faaliyetlerde yer alan çalışanlarının bilinçlendirmek ve eğitmek, VKG'nin başlıca görevlerinden biri olarak sayılabilir. Bunun yanında veri koruma görevlisi, talep halinde veri koruma etki değerlendirmesine ilişkin tavsiyelerde bulunmalı ve bu husustaki çalışmaları takip etmeli, denetleyici makam ile iş birliği yapmalı ve ön istişare mekanizması da dâhil olmak üzere, denetleyici makamın irtibat noktası olarak hareket etmeli ve gerektiğinde makama danışmalıdır.

VKG'nin veri koruma kurallarına uygunluktan şahsi bir sorumluluğunun bulunmadığını ifade etmek gerekir. Bu çerçevede, veri sorumlusu ve veri işleyenin sorumlulukları devam etmekte ve Üye devletlerin Direktife uyma yükümlülükleri

¹³² Bu yönde bkz. Jenai Nissim, "Accountability and the Role of the Data Protection Officer", in: Peter Carey (ed.), *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, Oxford, 2018, s. 226.

¹³³ The Article 29 Working Party, "Guidelines on Data Protection Officers ('DPOs')", (Çevrimiçi), https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf, 13/12/2016, s. 4, (Erişim Tarihi: 10.04.2019).

¹³⁴ Paul Lambert, *The Data Protection Officer: Profession, Rules and Role*, CRC Press, Boca Raton, 2017, s. 42-45; Nissim, s. 223; Voigt/von dem Bussche, s. 53.

¹³⁵ Directive 2016/680 Rec. 63.

sürmektedir. Bununla birlikte, VKG bu yükümlülükler kümesinin yerine getirilmesinde son derece önemli bir rol oynamaktadır.¹³⁶

KVKK ise VKG kavramına, mehzaz 95/46/EC sayılı Direktif ile paralel olarak, yer vermemiştir. Buna karşılık, KVKK'nın geçici 1. maddesinin 5. fıkrası, kanunun yayımından itibaren bir yıl içerisinde kamu kurum ve kuruluşlarında kanunun uygulanmasıyla ilgili koordinasyonu sağlamak üzere üst düzey bir yönetici belirlenmesini zorunlu kılmaktadır.

§ V. Veri Dolaşımına İlişkin Esaslar

Direktifin ilk bölümü, kişilerin temel hak ve özgürlüklerinin ve özellikle, kişisel verilerin korunması hakkının gerçekleştirilmesi ve bu anlamda kişilerin hakları ile veri işleme faaliyetinde bulunan kimselerin ödevlerinden oluşmaktaydı. Bu bölüm, daha önceki Çerçeve Kararın kapsamında bulunmayan ve bilhassa, kişisel veriler ve kişilik hakları boyutu konusunda hem ulusal ve uluslararası kamuoyunun hem de devletlerin farkındalık kazanması neticesinde yeni düzenlemenin başlıca konularından birini oluşturmaktadır. Öte yandan, Direktifin ilk maddesinde açıkça belirtilen ikinci boyutu ise AB içerisindeki yetkili makamlar arasındaki veri dolaşımını sağlamak, ceza yargılamalarında ve kolluk alanlarında iş birliğini arttırmaktır. Dolayısıyla, iki parçalı bu düzenlemenin 5. Bölümünde, 35 ve devamı maddelerinde düzenlenen “Üçüncü Ülkelere¹³⁷ veya Uluslararası Kuruluşlara Veri Aktarımı”, araştırma konumuzun temel taşlarından biridir.

Direktifin 35. maddesi veri aktarımına ilişkin esasları belirlemektedir. Aktarımın gerçekleşebilmesi için aşağıda sayılan tüm şartların karşılanması gerekir:

- a) Veri aktarımı Direktifin amaçları bakımından gerekli olmalıdır,
- b) Veriler üçüncü ülkedeki bir yetkili makam veri sorumlusuna veya uluslararası kuruluş aktarılmalıdır,
- c) Bir üye devletten aktarılan verilerin sonrasında başka bir uluslararası veri aktarımına konu edilmesi halinde, kamu güvenliğine yönelik acil ve ciddi tehditlerin engellenmesi için gerekli olması durumu hariç olarak, söz konusu üye devlet de bu faaliyeti kendi iç hukukundaki hükümler uyarınca onamalıdır. *Sözgelimi*, Alman yetkili makamı Amerikan yetkili makamına aktardığı verilerin, sonrasında; Brezilya yetkili makamına aktarılması ihtimalinde, ilk aktarımın gerçekleştiği üye devlet Alman makamının bu faaliyete izin vermesi gerekir.

¹³⁶ The Information Commissioner's Office (ICO), Data Protection Officers (Çevrimiçi) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/> (Erişim Tarihi: 10.04.2019); WP29, “Guidelines on Data Protection Officers ('DPOs')”, s. 24.

¹³⁷ Direktif bu konuyu açıklığa kavuşturmamış olsa da “üçüncü ülke” deyiminden, AB üyesi olmayan ülkeler anlaşılmalıdır. Ayrıca bu yönde bkz. Salami, s. 13.

- d) Avrupa Komisyonu'nun yeterlilik kararını kabul etmiş veya Direktif uyarınca sayılan diğer hallerin uygulama alanı bulmuş olması gerekir,
- e) Aktarmalı veri transferlerinde (onward transfer), ilk veri aktarımını yapan yetkili makamın veya o ülkedeki başka bir yetkili makamın özellikle fiilin ciddiyetini göz önünde bulundurarak söz konusu aktarıma onay vermiş olması gerekir.

GDPR'daki benzer hükümle karşılaştırıldığında, Direktifin ayrıca veri aktarımının sayılan amaçlar açısından gerekli olmasını ve aktarımın yetkili makamlar arasında gerçekleştirilmesini de aradığı görülür.¹³⁸ Ancak yalnızca sayılan şartların varlığı, üçüncü bir ülke veya uluslararası kuruluşa yapılacak veri aktarımlarını gerçekleştirebilmek için tek başına yeterli olmayacaktır. Bu şartların yanında veri aktarımı yapılacak ülke veya kuruluşun, "güvenli" olması aranır. Zira AB veri koruma modelindeki ana kural, sınır aşan veri dolaşımının serbestçe gerçekleştirilememesidir.¹³⁹ Bu noktada karşımıza, 95/46/EC sayılı Direktif ve GDPR'dan tanındık olan yeterli veri koruma seviyesi ve yeterlilik kararları kavramları çıkar.

İlk aşamada, Direktifin 36. maddesine göre aktarımın yapılacağı üçüncü ülke veya uluslararası kuruluşun "yeterlilik kararı" almış olması gerekir. Yeterlilik kavramından ne anlaşılması gerekeceği uzun süre gerek AB komisyonu gerekse de üye devletler bazında anlaşılammış, bu konuda somut kriterler koyulamamış ve sonuçta yalnızca az sayıda birtakım devlet yeterlilik kararı alabilmiştir.¹⁴⁰ Nihayet, yeterli koruma seviyesi (adequate level of protection) kavramının Avrupa Birliği Adalet Divanının (Divan) Schrems v. Digital Rights Ireland kararı¹⁴¹ ile açıklığa kavuşturulduğu görülmektedir.¹⁴²

Divana göre, üçüncü ülkeden elbette, AB hukuk düzeninde taahhüt edilen seviyedeki kadar yüksek bir koruma beklenmemelidir. Bununla birlikte, "yeterli koruma seviyesi" terimi, üçüncü ülkenin, kendi iç hukuku veya uluslararası yükümlülükleri nedeniyle, temel hak ve özgürlükleri ana hatlarıyla, AB Hukuku'nda 95 sayılı Direktif ile taahhüt edilen seviyeye eşdeğer bir korumayı sağlama gereği olarak anlaşılmalıdır.¹⁴³

¹³⁸ Sajfert/Quintel, s. 18.

¹³⁹ de Hert/Papakonstantinou, A First Analysis, s. 14.

¹⁴⁰ Bu yönde bkz. de Hert/Papakonstantinou, A First Analysis, s. 14.

¹⁴¹ ABAD, Maximillian Schrems v. Data Protection Commissioner and Digital Rights Ireland Ltd., C-362/14, 6 Ekim 2015.

¹⁴² Bu yönde bkz. Sajfert/Quintel, s. 18; Costanza Di Francesco Maesa, "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)", (Çevrimiçi) <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/>, Eurojus, 24/05/2016, (Erişim Tarihi: 10.04.2019); Salami, s. 13; Pajunoja, s. 63.

¹⁴³ Schrems v. Digital Rights Ireland, para. 73.

Bu bağlamda, yeterli seviye koruması değerlendirmesinin ilk bölümünde, özel hayata saygı hakkı çerçevesinde, kişisel verilerin korunması hakkının önemli bir rol oynayacağı söylenmelidir. İkincil olarak, şayet yeterli koruma seviyesi sağlanamaz ise çok sayıda kişinin haklarının ihlal edilip edilmeyeceği değerlendirmelidir. Divana göre bu durumda, yeterli seviyede koruma hükmünün katı yorumlanması gerektiğinden Avrupa Komisyonu'nun bu konudaki takdir yetkisi de sınırlı olmalıdır.¹⁴⁴

Ayrıca Direktife göre, uluslararası yükümlülükler yanında, Komisyon yeterli koruma seviyesini değerlendirirken, özellikle üçüncü ülkenin 1981 tarihli Kişisel Verilerin Otomatik İşlenmesine İlişkin Bireylerin Korunması Hakkındaki Sözleşme'ye taraf olup olmadığı ve söz konusu yükümlülükleri iç hukukuna aktarıp aktarmadığı da göz önünde bulundurulmalıdır. Bu konularda ayrıca Avrupa Veri Koruma Kurulu'ndan (European Data Protection Board)¹⁴⁵ görüş alınabilecektir.¹⁴⁶ Direktif uyarınca yeterlilik kararlarında ise Komisyon, periyodik bir gözden geçirme mekanizması sağlamalıdır. Bu periyodik gözden geçirme, söz konusu üçüncü ülke veya uluslararası kuruluşla istişare içinde yapılmalı ve üçüncü ülke veya uluslararası kuruluştaki ilgili tüm gelişmeler göz önünde bulundurulmalıdır.¹⁴⁷

Bununla birlikte, yeterlilik kararlarının alınamadığı bazı durumlarda da üçüncü ülke veya uluslararası kuruluşlara veri dolaşımının sağlanması mümkün olabilmektedir. AB kanun koyucusu Direktif bazında esneklik ve uygulanabilirliğinin artırılması için üç kademeli bir sistematığı benimsemektedir.¹⁴⁸

İlk aşamada, kişilik hakları yönünden uygun güvenceleri içeren veri aktarımları bulunur. Üçüncü ülke veya uluslararası kuruluş kişisel verilerin korunması hakkı bakımından bağlayıcı hukuki düzenlemelere sahipse¹⁴⁹ veya veri sorumlusu yetkili makam aktarım hakkındaki tüm koşulları değerlendirerek uygun güvence-

¹⁴⁴ Schrems v. Digital Rights Ireland, para. 78.

¹⁴⁵ Avrupa Veri Koruma Kurulu, GDPR'in 68 ve devamı maddeleri uyarınca kurulmuş, Avrupa Birliği genelinde veri koruma kurallarının uyumlu şekilde uygulanmasına katkıda bulunan ve AB'nin veri koruma makamları arasında iş birliğini teşvik eden bağımsız bir AB organıdır. Kurul, her üye devletin denetleyici makam başkanları ve Avrupa Veri Koruma Denetçisi veya temsilcilerinden oluşmaktadır. 95/46/EC sayılı Direktifin 29. maddesine dayanılarak kurulmuş Madde 29 Çalışma Grubu'nun yerini alan Kurul, AB veri koruma sisteminin merkezinde yer alacaktır.

¹⁴⁶ Directive 2016/680 Rec. 68.

¹⁴⁷ Directive 2016/680 Rec. 69.

¹⁴⁸ Sajfert/Quintel, s. 18-19; de Hert/Papakonstantinou, A First Analysis, s. 15.

¹⁴⁹ Söz konusu hukuki düzenlemeye örnek olarak, AB üyesi devletlerin polis ve cezai yargılama makamları ile ABD federal makamları arasında terörizm dâhil olmak üzere; suçların önlenmesi, soruşturulması, tespit edilmesi ve kovuşturulması amacıyla değiştirilen tüm kişisel verileri kapsayan ve bu konudaki genel ilkeleri koyması ile kapsamının genişliği bakımından "Şemsiye Anlaşma" (Umbrella Agreement) olarak adlandırılan uluslararası antlaşma gösterilebilir, bkz: "Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences", (Çevrimiçi) https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2016.336.01.0003.01.ENG&toc=OJ:L:2016:336:TOC 10/12/2016, (Erişim Tarihi: 10.04.2019).

lere sahip olduğu kanısına ulaşırsa veri aktarımı gerçekleşebilir (Direktif m. 46). Elbette, kişilik haklarına müdahale niteliği taşıyabilecek bu kararların, yalnızca veri sorumlusunun kişisel değerlendirmesine bırakılmasıyla yetinilmemelidir.

Direktif bu konuda veri sorumlusunu öncelikle, denetleyici makama söz konusu aktarımı bildirmekle yükümlü kılmış ve ayrıca bu faaliyetin, tarihi ve saati, aktarımın gerekçeleri ve alıcı yetkili makama ilişkin bilgileri içerecek şekilde belgelenmesini ve talep halinde, denetleyici makama sunmasını da hüküm altına almıştır. Hüküm vasıtasıyla, denetleyici makamın potansiyel hukuki denetimi için gereken bilgiler sunulması¹⁵⁰ ve bu sayede, kişilerin hakları daha güçlü şekilde korunması hedeflenmektedir. Ancak kişisel verilerin sınırlar arası aktarımlara konu olması halinde kişilerin, verilerinin hukuka aykırı kullanılması veya ifşa edilmesi hallerinde, haklarının korunmasının son derece güçleşeceği de açıktır. Bu gibi durumlarda, denetleyici makamların şikâyetleri takip etmeleri ve soruşturmaları yürütmeleri de yetki alanları dışında kalabilmektedir. Nitekim yeterli önleyici ve tazmin edici güçlerin yokluğunu ve ceza yargılamasında ve kolluk alanında kişisel verilerin korunması hususunda Birlik genelinde uyumluluğunun sağlanamadığını AB kanun koyucusu da kabul etmektedir.¹⁵¹ Yapılması gereken, üye devletlerdeki denetleyici makamlar ile üçüncü ülkelerdeki eşdeğer makamlar arasındaki bilgi alışverişini ve bu çerçevede iş birliği seviyesini arttırmak olmalıdır.¹⁵²

İkinci aşamada, Direktifin 38. maddesindeki özellikli durumların varlığı halinde veri aktarımı mümkün olabilmektedir. Veri aktarımının gerçekleştirilmesi aşağıda sayılı haller için gerekli olmalıdır:

- a) Veri ilgisinin veya başka bir kimsenin hayati menfaatlerinin korunması,
- b) Üye devlet hukukunun aktarıma izin verdiği hallerde, veri ilgisinin meşru menfaatinin korunması,
- c) Üye devlet veya üçüncü ülkenin kamu güvenliğine yönelik acil ve ciddi tehdidin önlenmesi,
- d) Direktifin belirlediği esas amaç (Direktif m. 1/f. 1) için bazı özel durumlarda,
- e) Direktifin belirlediği esas amaçlarla ilgili olarak, hukuki taleplerin oluşturulması, kullanılması veya savunulması için veri aktarımı gerekli olmalıdır.

Burada, (d) ve (e) bendinin uygulanmasında; yetkili makam, kamu yararı'nın gerçekleştirilmesinin veri ilgisinin temel hak ve özgürlükleri açısından bir dengesizlik yaratacağına karar verirse veri aktarımı gerçekleşmeyeceğinin belirtilmesi gerekir.

¹⁵⁰ Sajfert/Quintel, s. 19.

¹⁵¹ Directive 2016/680 Rec. 74; Ayrıca Direktifin 40. maddesi düzenlemenin efektif uygulanabilmesi adına üye devletler, AB Komisyonu, üçüncü ülkeler ve uluslararası kuruluşların, uluslararası iş birliği mekanizmaları getirmelerini ve karşılıklı yardımlaşmaları gerektiğini hüküm altında almaktadır.

¹⁵² Bu yönde bkz: Pajunoja, s. 62.

Yeterlilik kararının alınamadığı hallerde aktarımın gerçekleşmesi için ön-görülen üçüncü ve son aşama ise 39. maddesinde yer alan, Direktifin en yeni-likçi hükümlerinden “asimetrik veri aktarımı” düzenlemesidir.¹⁵³ Anılan madde uyarınca, üye devletin yetkili makamından yapılacak veri aktarımları bazı mün-ferit ve özel durumlarda; üçüncü ülke yetkili makamına değil, doğrudan üçüncü ülkede bulunan bir veri alıcısına yapılabilecektir. Böylece AB kanun koyucusu, m. 35/1-b’de düzenlenen, “*Veriler yetkili makam sıfatını haiz üçüncü ülkede-ki bir veri sorumlusuna veya uluslararası kuruluşu aktarılmalıdır.*” ilkesinden sapmaktadır.

Asimetrik veri aktarımının gerçekleşebilmesi için; aktarımın Direktifin be-lirlediği esas amaçlar için kesin surette gerekli olması, aktarımı gerçekleştiren yetkili makamın kamu yararı ile temel hak ve özgürlükler arasında makul denge bulunduğuna karar vermiş olması, üçüncü ülkedeki yetkili makama aktarım du-rumunda gecikmesinde sakıncalı bir halin bulunması, üçüncü ülke yetkili ma-kamının aktarım hususunda derhal bildirilmesi ve aktarımı gerçekleştiren yetkili makamın veri alıcısını veri işlemenin sınırlandırıldığı amaçlar hakkında bilgi-lendirmiş olması gerekir. Bu şartların tümünün karşılanmış olmasının yanında, aktarım faaliyetinde Direktifin diğer hükümlerine de uyulmalıdır.

Üç aşamayla sıralanan bu istisnalar dar yorumlanmalı kişisel verilerin sık, büyük ve yapısal transferlerine veya büyük ölçekli veri transferlerine izin verme-meli, ancak kesin surette gerekli olan verilerle sınırlı tutulmalıdır. Bu tür veri ak-tarımlarına ilişkin muhakkak dokümantasyon yapılmalı ve aktarımların hukuka uygunluğunu denetlemek için talep üzerine, denetleyici makama gerekli bilgiler sunulmalıdır.¹⁵⁴ Ancak bu şekilde, önemli boyutlarda yapılan veri aktarımlarında kişisel verilerin korunması hakkı fiiliyatta sağlanabilir.

§ VI. Direktifin Uygulanması Yönünde Üye Devletlerin Ulusal Hukukunda Atılmış Adımlar

Araştırma konumuzun odak noktasını oluşturan düzenleme, Direktif hük-münde olması bakımından üye devletler için doğrudan uygulanamaz ve iç hu-kuka aktarılmalıdır. Dolayısıyla ülkelerin mevzuatlarının da incelenmesi ve bu konudaki görüşlerimizin paylaşılması gereklidir. Belirtmeliyiz ki üye devletlerin bu yöndeki karnesinin pek parlak olmadığı, Almanya ve Avusturya haricindeki üye devletlerin, Direktifi iç hukuka aktarmaları için tanınan son süre olan Mayıs 2018 tarihine riayet etmedikleri ya bu sürenin geçmiş olduğu ya da ancak sürenin sonuna doğru bu konudaki düzenlemeleri yaptıkları görmekteyiz.¹⁵⁵

¹⁵³ Bu yönde bkz: Sajfert/Quintel, s. 19.

¹⁵⁴ Directive 2016/680 Rec. 72.

¹⁵⁵ Custers/Sears/Dechesne/Georgieva/Tani/van der Hof, s. 219.

Başlık altında AB'nin önemli ülkeleri Almanya, Fransa ve Brexit sürecinde bulunduğu AB ile ilgili hukuki ilişkileri son derece karmaşık hale gelen, bu bakımdan da değerlendirmeye muhtaç Birleşik Krallık'ın getirmiş olduğu düzenlemeleri konu edeceğiz.

A. Birleşik Krallık

1. Lordlar Kamarasının Direktif Hakkındaki Raporu

Lordlar Kamarasının AB seçilmiş komitesi (Lords Select Committees), AB veri koruma reform paketini, Birleşik Krallık'ın Brexit sonrası veri dolaşımının nasıl gerçekleşeceğini ve bu yönde belirlenmesi gereken veri koruma politikalarını 18 Temmuz 2017 tarihinde yayımladığı rapor ile değerlendirmiştir.¹⁵⁶ Birleşik Krallık öncelikle, Brexit sonrası da AB ile veri dolaşımına engelsiz ve kesintisiz devam etmek istemektedir. Raporda, Birleşik Krallık hükümetinin Brexit ve AB ile oluşturulacak yeni ortaklık hakkında ele aldığı metinde (White Paper) özellikle, AB, Üye Devletler ve İngiltere arasında veri transferinin istikrarını sağlamaya çalışacağı ifadesine vurgu yapılmaktadır. Zira Birleşik Krallık'ın uluslararası veri dolaşımı son derece ciddi boyutlara ulaşmıştır.¹⁵⁷

Lordlar Kamarası Direktife ilişkin yaptığı değerlendirmede, getirilen yeni düzenlemenin 2008 Çerçeve Kararının üye devletler arasındaki veri dolaşımına ilişkin sınırlı kapsamının aksine, hem uluslararası hem de ulusal düzeydeki veri işleme faaliyetlerini de içerdiği belirtmektedir. Bu durumun, komitenin daha önce yapmış olduğu; kolluk kuvvetlerinin ve yetkili makamların hangi verilerin ulusal veya uluslararası boyutta veri dolaşımına konu olacağını öngörememesinden kaynaklanan sorunların, Çerçeve Kararın sınırlı kapsamı nedeniyle meydana geldiği değerlendirmesini doğruladığı ifade edilmektedir.¹⁵⁸

Komite sonrasında, Direktifin uygulama alanına dikkat çekmektedir. Buna göre, Direktif AB Hukukunun sınırları dışındaki veri işleme faaliyetlerine, özellikle ulusal güvenliği ve güvenlik politikalarını etkileyen faaliyetlere uygulanamayacaktır. AB Antlaşmasının 5. Başlığının 2. Bölümünde düzenlenen, ortak dış ve güvenlik politikalarına ilişkin faaliyetlerin yürütülmesi sürecinde işlenen verilerin de Direktif kapsamı dışında olacağını belirtilmiştir.¹⁵⁹

Komite son olarak, Direktif uyarınca getirilen yenilik ve gelişmelere değinmektedir. Bu kısımda yukarıda belirtildiği gibi, yalnızca uluslararası veri dolaşımının değil aynı zamanda ulusal veri işleme faaliyetlerinin de kapsama alındığı-

¹⁵⁶ House of Lords, The European Union Committee, Brexit: the EU data protection package, (Çevrimiçi) <https://publications.parliament.uk/pa/ld201719/ldselect/lddeucom/7/7.pdf>, Authority of the House of Lords 18/07/2017, (Erişim Tarihi: 10.04.2019).

¹⁵⁷ House of Lords, s. 3.

¹⁵⁸ House of Lords, s. 14.

¹⁵⁹ House of Lords, s. 15.

nı, veri ilgililerine yönelik güncellenmiş bilgilendirme ve veriye erişim hakları tanındığını belirtmektedir. Bununla birlikte, veri sorumlularının, uygun güvenlik seviyesini sağlamak ve işlemin Direktif ile uyumlu olduğundan emin olmak için uygun teknik ve organizasyonel önlemleri almakla yükümlü olduğu ve veri işleminin (ex-ante) bu şekilde gerçekleştirilmesi gerektiği (data protection by desing) belirtilmektedir. Nihayet komite, veri ilgililerinin doğrudan yetkili makamlardan verilerinin silinmesini talep edebileceğini, veri sorumlularının kişisel verilerin korunması hakkı ihlallerinde bildirim yükümlülüğü bulunduğunu belirtmekte ve üye devletlere, veri koruma görevlisi atama zorunluluğu getirildiği de Direktifin yenilikleri kapsamında saymaktadır.¹⁶⁰

Komite değerlendirmelerinin sonuç ve tavsiye kısmında, kesintisiz veri dolaşımını sağlamanın en etkili yolunun Direktifin 36. maddesi uyarınca yeterlilik kararlarının alınması olduğunu ve böylece, Birleşik Krallık'ın AB ile eşdeğer veri koruma standartlarını içerdiğini doğrulaması gerektiğini ifade etmiştir. Bu konuda ICO (Information Commissioner's Office) yetkilisinin görüşü de AB ile Birleşik Krallık arasındaki veri dolaşımının son derece bütünleştiği (entegre) olduğu ve bu nedenle yeterlilik kararına mutlaka ihtiyaç olduğu yönündedir.¹⁶¹

Ancak yeterlilik kararlarının ancak üçüncü ülkeler tarafından alınabilecek olması nedeniyle, bu kararların AB'den çıkış sürecinde alınmasında birtakım sorunlar ortaya çıkabilecektir. Bu noktada komitenin önerisi, çıkış sürecinde veri paylaşımını ve dolaşımını sürekliliğini sağlayacak geçiş düzenlemelerinin yapılmasıdır. Zira bu tür geçiş düzenlemelerinin bulunmaması durumunda, kolluk alanında veri paylaşımı için daha önce uygulanmış herhangi bir seçeneğin bulunmaması, Birleşik Krallık hükümetini, AB üyesi devletler arasında; ceza yargılamasında ve kolluk alanındaki iş birliğini sürdürme konusunda endişelendirmektedir.¹⁶²

2. Veri Koruma Kanunu (Data Protection Act 2018)

Birleşik Krallık, GDPR ve Direktif'e ilişkin düzenlemeleri içeren Veri Koruma Kanunu, *Data Protection Act*'ı (DPA) 23 Mayıs 2018 tarihli Kraliyet onayı ile kabul etmiştir.¹⁶³ Birleşik Krallık'ın üçüncü nesil temel veri koruma düzenlemesi olan DPA'nın birinci kısmında, kişisel verilere ve kişisel verilerin korunması hakkına ilişkin bir girizgâh yapılmıştır. İkinci kısımda, kişisel verilerin; kamu ve özel sektör tarafından işlenmesi, üçüncü kısımda ise ceza yargılamasında ve kolluk faaliyeti amaçlarıyla işlenmesi ve dördüncü kısımda, istihbarat teşkilatları tarafından işlenmesi halinde uygulanacak hükümlere yer verilmiştir. DPA'nın altıncı

¹⁶⁰ House of Lords, s. 16.

¹⁶¹ House of Lords, s. 50.

¹⁶² House of Lords, s. 51.

¹⁶³ UK Legislation, Data Protection Act 2018 ("DPA") (Çevrimiçi) http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf (Erişim Tarihi: 10.04.2019).

bölümü, denetleyici makam ICO'nun rolünü, işlevini, görevlerini ve yetkilerini hüküm altına almakta ve yedinci ve son kısmı ise tamamlayıcı ve nihai maddeleri (supplementary and final provisions) içerir.

Konumuz bakımından önem arz eden bölüm elbette, kanunun üçüncü bölümünde yer alan ve kolluk ile ceza yargılamasında veri işleme faaliyetlerini düzenleyen kısımdır. Kısım, toplamda 6 bölümden ve 53 hükümden meydana gelir. Direktifle paralel olarak, birinci bölüm kapsam ve tanım hükümlerinden oluşur. İkinci bölümde ilkelere yer verilir. Üçüncü bölüm veri ilgililerinin haklarını, dördüncü bölüm veri sorumlusu ve veri işleyene ilişkin hükümleri, beşinci bölüm veri aktarımını ve son bölüm, tamamlayıcı hükümleri düzenler.

Kişisel veriye ilişkin altı temel ilke belirleyen DPA, elli altı kurumu da bu ilkeye uyarak veri işlemeye yetkili makam olarak saymaktadır.¹⁶⁴ İlkeler Direktiften herhangi bir farklılık içermez. Bununla birlikte, GDPR'da yer verilen şeffaflık ilkesine Direktifte de DPA'da da yer verilmemiştir. Bu ilkenin gizli yürütülmesi gereken soruşturma ve bu soruşturmada yürütülen teknikler açısından sakınca doğurabileceği belirtilmiştir. Burada özellikle Regulation of Investigatory Powers Act 2000 (RIPA) ya da Investigatory Powers Act 2016 (IPA) çerçevesinde yürütülecek veri işleme faaliyetlerine dikkat çekilmiştir.¹⁶⁵ Hassas nitelikli veri işleme hususunda ise düzenleme kapsamında yürütülecek faaliyetlerin büyük ölçüde bu nitelikte verileri konu edeceği belirtilerek,¹⁶⁶ veri işleminde sekizinci ekte belirtilen şartlardan birinin varlığı veya veri ilgisinin rızası gerekmektedir. Rızaya dayanılarak yürütülecek veri işleme faaliyetinin büyük ölçüde, veri ilgisine verilebilecek zararlardan koruma amacıyla veri işlenmesi halinde ortaya çıkabileceği düşünülebilir.

Veri ilgililerinin hakları ve veri sorumluların yükümlülükleri bakımından GDPR'dan herhangi bir temel fark içermeyen düzenlemede, Direktifin 5. maddesi ile üye devletlerin takdir alanına bırakılan verilerin silinmesi veya periyodik olarak gözden geçirilmesi için gereken süreyi ise bir ay olarak belirtilmiştir.¹⁶⁷ Veri güvenliği ilkesi ile faaliyetler yürütülürken yapılabilecek izinsiz işlemleri engellemeyi amaçlayan DPA,¹⁶⁸ veri güvenliğinin ihlal edildiği faaliyetlerde aktörler arasındaki iletişime ilişkin hükmü de içermektedir.¹⁶⁹

¹⁶⁴ DPA, Schedule 7; Department for Digital, Culture, Media and Sport (DCMS)/Home Office, Data Protection Bill: Explanatory Notes (Çevrimiçi) <https://publications.parliament.uk/pa/bills/cbill/2017-2019/0153/en/18153-EN.pdf>, para. 175 (Erişim Tarihi: 10.04.2019).

¹⁶⁵ DCMS/Home Office, para. 183.

¹⁶⁶ The Information Commissioner's Office (ICO), Guide to Law Enforcement Processing (Part 3 of the Bill) (Çevrimiçi) <https://www.pdpjournals.com/docs/887918.pdf>, s. 5, (Erişim Tarihi: 10.04.2019).

¹⁶⁷ DPA Art. 54; ICO, Guide to Law Enforcement Processing, s. 22.

¹⁶⁸ DPA Art. 66; DCMS/Home Office, para. 224-225.

¹⁶⁹ DPA Art. 67-68; ICO, Guide to Law Enforcement Processing, s. 42-45.

Veri koruma görevlisi kavramının da Direktif ile getirilen yeniliklerden biri olduğuna dikkat çekilmiştir.¹⁷⁰ Burada özellikle veri sorumlularının müşterek tek bir VKG atayabildiği ifade edilmiş,¹⁷¹ örneğin kolluk güçleri için bir bölgenin tamamında görev yapacak bir VKG belirleyebileceği belirtilmiştir.¹⁷² Veri dolaşımı konusunda ise Direktifin bilhassa tüm üye devletlerde uyumlu bir düzenleme oluşturmayı hedeflediği de göz önünde bulundurulduğunda, herhangi temel bir farklılığa yer verilmediği görülmektedir.

Son olarak, tamamlayıcı hükümlerde yer alan düzenlemeye göre de Devlet Bakanının (Minister of the Crown) ulusal güvenliğin sağlanması için gereklilik bulunması halinde, veri ilgililerinin bilgilenme, erişim, silme, düzeltme, veri ihlalini öğrenme gibi temel haklarını kısıtlayabileceği ve bu konuda kısıtlama yetkisi verebileceği düzenlenmiştir.¹⁷³ Bu yetkinin kullanılması son derece sıkı şartlara bağlı da olsa, temel kazanımları bir çırpıda hiçe sayma riskini de barındırır. Birleşik Krallık'ın bu konudaki geçmiş karnesinin pek parlak olmadığı ve benzer bir durumun RIPA ile 11 Eylül sonrası yaşandığı hatırlanmalı, bu tehlikeye dikkat çekilmelidir.

B. Almanya- Federal Veri Koruma Kanunu (Bundesdatenschutzgesetz)

Yukarıda da belirttiğimiz üzere, Almanya gerek GDPR gerekse de Direktife ilişkin iç hukukunda düzenlemeyi ilk yapan ve yeni bir veri koruma mevzuatına geçen ilk ülkelerden biridir. 30 Haziran 2017 tarihli yeni düzenleme, Almanya'nın ikinci nesil ana veri koruma düzenlemesidir (*Bundesdatenschutzgesetz*) ve selefinden 20 yıl sonra kabul edilmiştir.¹⁷⁴

Kanun dört kısımdan oluşur; birinci kısım, tüm veri işleme faaliyetlerine uygulanacak genel hükümleri düzenler, ikinci kısım GDPR, üçüncü kısım ise Direktifi iç hukuka aktaran maddelere (*Datenschutz-Anpassungs Und Umsetzungs-gesetz EU*) yer verir. Son kısımda ise Alman kanun koyucusu, GDPR ve Direktifin kapsamı dışında kalan veri koruma faaliyetlerine uygulanacak hükümlere düzenlemiştir.

İlk bölümünde kapsam, tanım ve ilke maddelerini içeren üçüncü kısım, sonrasındaki ilk hükümde hassas nitelikte kişisel verilerin işleme şartlarını düzenlemektedir. Maddeye göre, hassas veriler ancak katı surette gerekli ise ve uygun önlemler alınmış ise işlemenin konusu haline getirilebilecektir.¹⁷⁵

¹⁷⁰ Department for Digital, Culture, Media and Sport (DCMS)/Home Office, para. 227-228.

¹⁷¹ DPA Art. 69; ICO, Guide to Law Enforcement Processing, s. 40.

¹⁷² DCMS/Home Office, para. 227

¹⁷³ DPA Art. 79.

¹⁷⁴ Christian Ludwig Geminn, "The New Federal Data Protection Act - Implementation of the GDPR in Germany", *Blog Droit Européen*, E-conference: National Adaptations of the GDPR, Haziran 2018, (Çevrimiçi) <https://blogdroiteuropeen.files.wordpress.com/2018/06/christian-1.pdf>, s. 1, (Erişim Tarihi: 10.04.2019).

¹⁷⁵ Bundesdatenschutzgesetz (BDSG-neu), Art. 48.

Bunun yanında BDSG, Direktifin veri işleme güvenliği hükmü ile uyumlu şekilde, uygun önlem oluşturabilecek önlemleri de saymaktadır. Veri güvenliği veya veri koruma izlemesi için özel gereklilikler getirilmesi, verilerin ilgili olup olmadığı ve silinme açısından gözden geçirilmesi gereken özel zaman sınırları tanınması, işleme faaliyetlerine katılan personelin farkındalığını arttırmaya yönelik tedbirler, kişisel verilere erişim ile ilgili kısıtlamalar, bu verilerin ayrı olarak işlenmesi, kişisel verilerin maskelenmesi (*pseudonymization*), veri şifreleme ve son olarak, başka amaçlarla veri aktarımı veya işleme yapılması durumunda yasal işlemlerin sağlanması için özel davranış kuralları getirilmesi şeklinde sayılmıştır. Sayılan tedbirlerin, Direktif ve GDPR’ın da böyle bir hükmü içermemesi itibarıyla, kamu kurumlarınca yapılacak hassas veri işleminde rehber niteliği taşıyabileceği kanaatindeyiz.

BDSG, 51. maddesinde, veri ilgisinin rızası ile veri işlenebileceğini şayet bu veri hassas nitelikte ise açık rıza aranacağını düzenlemiştir. Oysa daha önceki değerlendirmelerimizde belirttiğimiz üzere rıza, kişisel verilerin kolluk faaliyetleri esnasında ve ceza yargılamasında işlenmesinde bir hukuka uygunluk nedeni oluşturamaz; veri işleminin dayanağı olarak gösterilemez. Zira rızanın varlığı, veri işleminin suçun önlenmesi, cezanın infazı, kamu güvenliğinin sağlanması gibi somut, belirli ve subjektif kıstas ve amaçları ortadan kaldırmamalıdır. Esas unsur, bu gibi durumların kanunlarda belirtilmesi ve faaliyetlerin bu amaca uygunluğunun sağlanması olmalıdır. Rıza gibi sonradan geri alınabilecek ve varlığı ile kurumların, düzenlemenin amaçlarını ve belirlilik ilkesini hiçe sayması ihtimalini doğuracak bir hukuka uygunluk nedeni kabul edilmemelidir.

Düzenleme, veri ilgililerinin hakları ve veri sorumlularının yükümlülükleri bahsinde Direktif ile çok büyük ölçüde paralellikler içermekte ve herhangi bir temel farklılığı barındırmamaktadır. Ana hatları itibarıyla incelediğimiz BDSG, özellikle Almanya’nın ilk kollukta ve ceza yargılamasındaki veri işleme faaliyetlerine dair ilk düzenlemesi olması bakımından ulusal bazda öncü ve genel çerçevede Direktif ile yeknesaklığı sağlamayı başarmış bir hukuki metin olarak değerlendirilebilir.

C. Fransa- Veri Koruma Kanunu (Loi Informatique et Libertés)

Fransa 1978 tarihinde yürürlüğe giren ilk veri koruma kanunu, Loi Informatique et Libertés (LIL) ile dünyada bu alanda ilk ulusal düzenlemeyi gerçekleştiren ülkelerden biriydi.¹⁷⁶ Ancak üye devletlere iç hukukuna aktarılması için tanınan son süre Mayıs 2018’i geçirmiş, ana veri koruma düzenlemesini 20 Haziran 2018; Fransız Veri Koruma Otoritesi CNIL’e ilişkin kararnamayı 1 Ağustos 2018, Fransız mevzuatının GDPR’a uyumluluğunu hedefleyen yönetmeliği ise 12 Aralık 2018 tarihi ile tamamlayabilmiş ve bu konudaki geçmiş başarılı karnesi aksine, hareket etmekte geç kalmıştır.

¹⁷⁶ Custers/Sears/Dechesne/Georgieva/Tani/van der Hof, s. 137.

LIL, toplamda 14 bölüm ve 72 hükümden oluşmakta ve Direktife ilişkin düzenlemeye on üçüncü bölümde yer vermektedir.¹⁷⁷ Kanunun ilgili bölümüne değinmeden önce, düzenlemenin dördüncü bölümünde yer alan, otomatik veri işlemesi öncesinde gerçekleştirilmesi gereken prosedürlere değinmek gerekir.

Kanunun 26. maddesi uyarınca, devlet, savunma veya kamu güvenliğinin sağlanması ile ilgili olarak veya suçların önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması veya cezai hükümlerin veya güvenlik önlemlerinin uygulanması amacıyla veri işlenebilmesi yetkili bakan ya da bakanların emri, CNIL'in gerekçeli ve yayınlanmış bir görüşünün ardından gerçekleştirilebilir.¹⁷⁸ Dolayısıyla söz konusu "önceden yetkilendirme ilkesi", Direktifin iç hukuka aktarıldığı hükümler için de geçerlidir. Ancak LIL'in Direktif ile ilgili bölümünde yer alan 70-3 maddesi bu konuda bir istisna getirmiş ve yetkili makamlar tarafından cezai suçların önlenmesi ve tespiti amacıyla kullanılan kişisel verilerin işlenmesi, konunun soruşturulması ve kovuşturulması veya kamu güvenliğine yönelik tehditlere karşı koruma ve bu tür tehditlerin önlenmesi dâhil olmak üzere, cezai yaptırımların uygulanması amacıyla veri işlemesi halinde 26. maddedeki ilgili şartın sağlanacağını hüküm altına almıştır. Maddenin özellikle hassas veriler bakımından da herhangi bir ayırım yapmaksızın, kişilere Fransız Hukukunda uzun süredir tanınan bu korumayı kaldırmış olması kaygı vericidir. Bunun yanında kanun, CNIL'e *varsayılan* yetkiyi geri çekme imkânı tanınmamakta, idari para cezası uygulama yetkisini de vermemektedir.¹⁷⁹ Buna karşılık, düzenlemenin Direktifin kendine has tabiatını koruduğu savunulmuştur.¹⁸⁰

Öte yandan, Fransız kanun koyucusu 70-4 hükmü ile temel hak ve özgürlükler açısından yüksek derecede risk içeren veri işleme faaliyetlerinde başvurulacak veri koruma etki değerlendirmesinin CNIL'e sunulması ve görüşünün alınması şeklindeki hükmü ihdas ederek, bu noktada olumlu ve ilerici bir düzenlemeye de yer vermektedir. LIL'in ilgili hükümleri incelenmeye devam edildiğinde Direktifin çekirdeğini oluşturan veri ilgilileri hakları ve veri sorumlusu yükümlülükleri hususunda herhangi temel bir farklılığa yer vermediği görülür. Bununla birlikte, kişilerin bilgilendirme ve erişim haklarının daha geniş bir kapsamı içermesi ve doğrudan kullanılabilmesi

¹⁷⁷ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ("LIL"), (Çevrimiçi) <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT00000886460#LEGIARTI000037088717>, (Erişim Tarihi: 18.04.2019).

¹⁷⁸ Bununla birlikte CNIL'in, özellikle "kamu güvenliği" kavramının neleri kapsadığının belirsiz olduğu görüşünde olduğu belirtilmelidir. Bkz: Commission Nationale de l'Informatique et des Libertés (CNIL), "Délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978", (Çevrimiçi) https://www.cnil.fr/sites/default/files/atoms/files/projet_davis_cnil.pdf, s. 31, (Erişim Tarihi: 18.04.2019).

¹⁷⁹ LIL, Art. 45.

¹⁸⁰ Olivia Tambou, "Que retenir du projet de loi relative à la protection des données personnelles ? Partie II: L'amélioration relative du régime des traitements pénaux par la transposition de la directive n°2016/680" (Çevrimiçi) <https://www.village-justice.com/articles/que-retenir-projet-loi-relatif-protection-des-donnees-personnelles-partie,28175.html>, (Erişim Tarihi: 18.04.2019).

ulusal hukuk ve Birlik hukuku bakımından bir ilerleme olarak görülmelidir. Ayrıca getirilen 70-23 hükmü uyarınca, kişilerin; bilgi alma, erişim, düzeltme ve silme hakkı ile ilgili olarak, bu talep hakkın kötüye kullanılması için yapılmadığı ve dayanaksız olmadığı sürece, kişiye iletilen ilişkili bilgilerin uygun bir biçimde ve ücretsiz sunulmasının düzenlenmiş olması da kişi hakları bakımından olumlu bir gelişmedir.¹⁸¹

Veri sorumlusunun yükümlülükler bakımından ise Alman düzenlemesinde açıklamalarımıza paralel şekilde, hassas (özel) nitelikteki kişisel verilerin işlenmesi durumunda alınması gereken uygun önlemler örneklem şeklinde sayılmaktadır. Bunlar, yetkisiz kişilerin işleme için kullanılan araçlara, otomatik veri işleme sistemlerine ve veri dosyalarına erişiminin, veri ortamının yetkisiz bir şekilde okunması, kopyalanması, değiştirilmesi veya silinmesinin engellenmesi; otomatik işleme sistemlerine hangi kişisel verilerin ne zaman ve kimin tarafından girildiğinin ve kişisel verilerin hangi aşamada aktarıma konu edildiğinin tespit edilebilmesi, kesinti durumunda sistemin geri yüklenebilmesi ve sistemin fonksiyonlarının çalıştığından, işletim hatalarının bildirildiğinden ve kaydedilen kişisel verilerin sistem arızası nedeniyle bozulmamasıdır.¹⁸² Ayrıca log kayıtları da veri işlemenin gerekçesini, gerçekleştirildiği tarih ve saati ve veri işleme faaliyetinde danışılan kimselerin CNIL tarafından belirlenmesi için tutulacaktır.

Uygulama alanı bakımından ise on üçüncü bölümün son hükmü gereği, kişisel verilerin yargı makamlarının karar içeriğinde veya dosya kapsamında bulunması durumunda LIL'in ilgili hükümlerinin değil, Fransız Ceza Muhakemesi Kanunu hükümlerinin uygulanacağı belirtilmelidir.¹⁸³

Esasında belirli gelişmeleri de barındıran ancak temel eksikler de içeren bu düzenlemeye ilişkin değerlendirmelerimizi, CNIL'in eleştirilerine yer vererek son vermek yerinde olacaktır. CNIL, tasarıya ilişkin sunmuş olduğu görüşte; veri işlemenin hukuka uygunluğu koşulları altında işleme güvenliği ilkesinin oluşturulmaması göz önüne alındığında, tasarının belirli açılardan eksik olduğunu düşünmektedir. CNIL, raporunda; veri sorumlusunun niteliği, müşterek veri sorumlusu kavramının yokluğu, hassas verilerin işlenmesine ilişkin herhangi bir şartın düzenlenmemiş oluşu, veri ilgisinin haklarının kullanmasını kolaylaştırma yükümlülüğü ve veri koruma ilkelerinin hüküm altına alınmamasını, son derece önemli ve ivedilikle giderilmesi gereken eksikler olarak belirlemiştir.¹⁸⁴ CNIL'in

¹⁸¹ Bu yönde bkz: Commission Nationale de l'Informatique et des Libertés (CNIL), "Délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978", s. 37; Tambou, "Que retenir du projet de loi relative à la protection des données personnelles ? Partie II: L'amélioration relative du régime des traitements pénaux par la transposition de la directive n°2016/680".

¹⁸² LIL, Art. 70-13.

¹⁸³ LIL, Art. 70-24.

¹⁸⁴ CNIL, "Délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978", s. 32.

raporunu yayımladığı 30 Kasım 2017 tarihinden günümüze halen bu konudaki adımların atılmamış olması, düzenlemeyi eksik bırakmaktadır. Bu anlamda, ne yazık ki LIL'in, en azından bu haliyle, kişilerin hak ve özgürlüklerine ilişkin yeterli güvenceyi sağlamaktan uzak olduğu söylenebilir.

§ VII. Türk Hukukunda Ceza Yargılamasında ve Kolluk Teşkilatı Tarafından İşlenen Kişisel Verilere Uygulanan Hükümler

Ülkemizde henüz bu konuda özel bir düzenleme bulunmamaktadır. KVKK incelendiğinde de, Kanunun açıkça bu alanı kapsam dışında bıraktığı görülür.¹⁸⁵ KVKK'nın 28. maddesiyle kişisel verilerin; (i) kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında ve (ii) soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi halleri, KVKK'nın kapsamı dışında bırakılmıştır.

Kişisel verilerin suç öncesi alanda, toplanabileceği bazı hallere, örneğin parmak izi ve fotoğraf kaydı alma (PVSK m. 5), toplantı ve gösteri yürüyüşlerinde ses ve görüntüleri kaydetme (Toplantı ve Gösteri Yürüyüşleri Kanunu m. 11) gibi hallere kanunlarda özel olarak ve polisin genel istihbarat yetkisine de PVSK ek m. 7 ile yer verildiğini görmekteyiz.¹⁸⁶ Kolluğun kişisel verileri işleyebileceği hallere ilişkin düzenlemeler bulunmaktayken, ki ek 7. maddedeki gibi bu haller çok geniş ve belirsiz de olabilirken, bu verilerin işlenmesine ilişkin ilke, kural ve standartlar hiçbir düzenleme ile öngörülmuş değildir. Tam da Direktifin konusunu oluşturan ve KVKK kapsam dışında bırakılan, her gün kamu kurumlarının MOBESE (Mobil Elektronik Sistem Entegrasyonu) gibi uygulamalarıyla geniş çapta veri işleme ilkelerini ihlal ettiği bu alandaki boşluk bir an evvel giderilmelidir.

Yine bu konudaki güncel tartışmalardan, MOBESE uygulamasının herhangi bir yasal dayanağının bulunmadığı hatırlatılmalıdır. Dolayısıyla MOBESE üzerinden elde edilen kişisel verilerin işlenmesi, saklanması ve herhangi bir soruşturmada ya da kovuşturmada delil olarak kullanılması hukuka aykırı olacak, buradan elde edilen delillerin hukuka aykırı delil olarak sınıflandırılması ve yargılamada kullanılmaması gerekecektir. MOBESE şayet caydırıcı, önleyici bir tedbir olarak öngörülmüşse yalnızca bu amaç için kullanılmalı ve suç sonrası alanda, yargılamaalarda ispat aracı olarak kabul edilmemelidir.¹⁸⁷

¹⁸⁵ Börekçi, s. 103.

¹⁸⁶ Baran Kızılırmak, *Önleyici Amaçla Elde Edilen Verilerin Ceza Muhakemesinde Kullanılabilirliği*, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2018, s. 98 - 148.

¹⁸⁷ Bu yönde bkz. Kızılırmak, s. 269 vd.

Bildiğimiz kadarıyla İçişleri Bakanlığı bünyesinde bu konuda bir çalışma yapılmaktadır. Ancak duyumdan öteye geçmeyen bu bilginin bilimsel olma iddiasında olan bir makalede yer alması doğru değildir. Oysa beklenen (ki son yıllarda ülkemizde gerçekleştiğini pek görmemekteyiz) konunun uzmanlarının ve tüm paydaşlarının çağırıldığı komisyonlar tarafından bu tür çalışmaların yapılması, bunların kamuoyuna sunulması, olumlu ve olumsuz görüşler alındıktan sonra metne son halinin verilip yasama meclisine sunulmasıdır. Demokratik bir ülkede beklenen ve olması gereken hukuki düzenleme yapma tekniği budur.

Ülkemizde KVKK'nın ve ilgili diğer mevzuatın yürürlüğe girmesi son derece olumlu, önemli ve ileri bir adımdır. Ancak bu yetersizdir; zira kişisel verilerin korunmasına ilişkin ilke ve kurallar, kurumlar ve bireyler tarafından benimsenip uygulanmadıktan sonra tek başına hukuk düzenleme yapmak tek başına yetersiz kalacaktır. Bu kurumlara belki de yapılacak ihlallerin boyutu en yüksek derecede olabilecek, kolluk güçleri ve adliye teşkilatı da dâhildir. Bu yapıların KVKK'ya tabi olmamaları yapıları ve işlevleri gereği anlaşılabilir bir durumdur, ancak bu kuralızsızlık anlamına gelmemelidir; zira bu peşinden hukuksuzluğu getirir. Dolayısıyla bu kurumların da kişisel veri tutmaları ve işlemleri hukuk normlarına bağlı olmalıdır. İşte bu normlar için AB Hukukunun gelişmeleri ve yukarıda incelemeye çalıştığımız Direktif örnek ve esas alınmalı ve bu doğrultuda zaman kaybetmeden bir kanun çıkarılmalıdır.

Sonuç

Gelecekteki sosyo-politik gelişmeleri tahmin etme zorluğu ve teknolojinin nasıl gelişeceğinin belirsizliği, kişiliğimiz ve kişisel verilerimizin güvenliği hakkındaki kaygılarımızı giderilemez kılıyor. Modern toplumların sınırsız ve merkezi olmayan bilişim teknolojilerine daha fazla bağımlı olmaya başladığı göz önüne alındığında, hayatımızın önemli bir bölümünü kaplayan siber alan; organize suçlular, bilgisayar korsanları, yasadışı faaliyetler, terörist ağların oluşumu ve sürekliliği için kolay bir hedef haline gelmektedir.¹⁸⁸

Elbette yalnızca bilişim suçları değil, aynı zamanda fiziksel alanda işlenen “geleneksel” suçlar da veri işleme dosyalarının konusunu oluşturur. Bu anlamda sıfatı ister şüpheli, sanık veya suçlu ister mağdur, suçtan zarar gören isterse de tanık olsun, yargılamanın tüm sükelerinin kişisel verileri; ceza yargılamasına ve kolluk faaliyetine konu edilmekte ve toplumun her biri ferdi temel hak ve özgürlüklerine yapılacak müdahalelere maruz kalabilmektedir.

Direktif, bu alanda ortaya çıkan temel iki değeri, kişilik hakları ile kamu güvenliğini esas alır ve aralarında adil ve makul bir denge kurmayı amaçlar. Çer-

¹⁸⁸ Anthony Minnaar, “Cybercrime, Cyberattacks, and Problems of Implementing Organizational Cybersecurity”, in: John A. Eterno/Arvind Verma/Aiedeo Mintie Das/Dilip K. Das, (eds.), *Global Issues in Contemporary Policing*, CRC Press, Boca Raton, 2017, s. 122.

çeve Karar ile kıyaslandığında, yerel veri işleme faaliyetlerinin dâhil edilerek Direktifin çok daha geniş bir kapsamı içermesi; detaylı bir veri işlemesi ilkeleri düzenlemesinin bulunması, kişilerin haklarını arayabilecekleri güçlü mekanizmaların öngörülmüş olması ve veri sorumlusu yetkili makamların daha geniş bir sorumluluk yüküne tabi tutulması bu amaçla paralel değişikliklerdir. Direktif bu açıdan, Bilişim Çağındaki ceza yargılamasına ve kolluk faaliyetlerine açık, kapsamlı ve ileriye dönük bir dizi kural içermektedir.

Öte yandan, düzenlemenin birtakım sorunlu alanları da bulunur: Tanınan kimi güvencelerin üye devletlerin iç hukuklarında getirebilecekleri geniş istisnalarının yer alması ve bunların uygulanmasına ilişkin genel ve muğlak terimlerin kullanılması; veri işlenmesinde hukuka uygunluk nedeni olarak yalnızca amaçlar doğrultusunda veri işleminin gösterilmesi, amaçlar dışında yapılacak veri işleme faaliyetlerine GDPR uygulanacağı için ceza yargılamasında ve kolluk makamlarında yaşanabilecek yasal belirsizlik ve direktif hükmünde bir normatif enstrüman ile düzenleme getirildiğinden, Çerçeve Karar döneminde kadar olmasa da halen ortaya çıkması kuvvetle muhtemel ülkeler arası veri koruma rejimleri arasındaki önemli farklar, Direktifin eleştiriye açık yönleri arasında sayılabilir. Tüm bu tespitlerimiz ışığında, bir taraftan ceza yargılamasının ve kolluk alanının ihtiyaçlarının göz önünde bulundurularak, faaliyetlerde esnek veri işlemesi ve dolaşımının sağlanırken yüksek gizlilik ve veri koruma standartlarına ulaşmak ve üye devletlerin veri koruma mevzuatında bu alana ilişkin uyumluluğu sağlamak, 2016/680 sayılı Direktifin getiriliş amacı olarak özetlenebilir.

Bu makaleyi yazmakta ve Direktifi incelememizdeki temel motivasyonumuz, ülkemizde bu alanda herhangi bir düzenlemenin bulunmamasıydı. Ülkemizde kolluk ve ceza yargılamasında makamlar, kişilerin verilerini yoğun biçimde işlemekte iken, bu kişisel verilerin işlenmesine dair herhangi bir düzenleme ne yazık ki bulunmaz. Ülkemizde de yukarıda belirtmiş olduğumuz yöntemle ve kapsamda bir an önce bu konuda adım atılmalı, bu alandaki yasal boşluk giderilerek, hukuka aykırı eylem ve işlemlere bir an önce son verilmesinin sağlanmalıdır.

Kaynakça

Kitap ve Makaleler

- Alonso Blas Diana, “First Pillar and Third Pillar: Need for a Common Approach on Data Protection?”, in: Serge Gutwirth/Yves Poullet/Paul de Hert/Cecile de Terwangne/Sjaak Nouwt (eds.), *Reinventing Data Protection?*, Springer, Heidelberg, 2009, s. 225-238.
- Ayözger Öngün A. Çiğdem, *Kişisel Verilerin Korunması Hukuku: Elektronik Haberleşme Sektörüne İlişkin Düzenlemeler Dahil*, Beta, İstanbul, 2019.
- Bajovic Vanja, “Criminal Proceedings in Cyberspace: The Challenge of Digital Era”, in: Emilio C. Viano (ed.), *Cybercrime, Organized Crime, and Societal Responses: International Approaches*, Springer, Heidelberg, 2017, s. 87-102.
- Balboni Paolo, “Let’s not Forget about Data Protection by Design”, (Çevrimiçi) <https://www.paolobalboni.eu/index.php/2018/07/11/lets-not-forget-about-data-protection-by-design/> (Erişim Tarihi: 10.04.2019).
- Balboni Paolo, “Personal Data Protection and the Use of Information to Fight Online Terrorist Propaganda Recruitment and Radicalization: Part III”, (Çevrimiçi), <https://www.paolobalboni.eu/index.php/2019/02/10/personal-data-protection-and-the-use-of-information-to-fight-online-terrorist-propaganda-recruitment-and-radicalization-part-iii/> (Erişim Tarihi: 01.04.2019).
- Bevitt Ann/ Carey Peter, “Data Security and Breach Notifications”, in: Peter Carey (ed.), *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, Oxford, 2018, s. 88-104.
- Blasi Casagran Cristina, *Global Data Protection in the Field of Law Enforcement: An EU Perspective*, Routledge Research in EU Law, Routledge, Oxford, 2016.
- Boehm Franziska, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-Level*, Springer, Heidelberg, 2011.
- Bosco Francesca/Creemers Niklas/Ferraris Valeria/Guagnin Daniel/Koops Bert-Jaap, “Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities”, in: Serge Gutwirth/Ronald Leenes/Paul de Hert (eds.), *Reforming European Data Protection Law*, Law, Governance and Technology Series 20, Springer, Heidelberg, 2015, s. 3-34.
- Bostancı Bozbayındır Gülşah, “Avrupa Birliği Ceza Hukuku’nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler”, *GSÜHFD*, Beta, İstanbul, 2018/2, s. 51-103.
- Böreği Eşref Barış, *Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu*, Yayımlanmamış Yüksek Lisans Tezi, Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2019.
- Bygrave Lee A., “Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling”, *Computer Law & Security Review: The International Journal of Technology Law and Practice*, Elsevier, London, 2001, V. 17, I. 1, s. 17-24.

- Bygrave Lee A., “Data Protection by Design and by Default: Deciphering the EU’s Legislative Requirements”, *Oslo Law Review*, Oslo, 2017, V. 4, No. 2, s. 105-120.
- Carey Peter, “Data Protection Principles”, in: Peter Carey (ed.), *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, Oxford, 2018, s. 32-41.
- Cole Simon, *Suspect Identities: A History of Fingerprinting and Criminal Identification*, Harvard University Press, Cambridge, 2002.
- Custers Bart/Sears Alan M./Dechesne Francien/Georgieva Ilina/Tani Tommaso/van der Hof Simone, *EU Personal Data Protection in Policy and Practice*, Information Technology and Law Series Volume 29, Springer, Heidelberg, 2019.
- de Hert Paul/Papakonstantinou, Vagelis, “The Data Protection Framework Decision of 27 November 2008 regarding Police and Judicial Cooperation in Criminal Matters - A Modest Achievement However not the Improvement Some Have Hoped for”, *Computer Law & Security Review: The International Journal of Technology Law and Practice*, Elsevier, London, 2009, V. 25, I. 5, s. 403-414. (Not The Improvement Some Have Hoped For).
- de Hert Paul/Papakonstantinou Vagelis, “Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency”, *I/S: A Journal of Law and Policy for the Information Society*, V. 9., I. 2, s. 271-324. (Three Scenarios).
- de Hert Paul/Sajfert Juraj, “Police, Privacy and Data Protection from a Comparative Legal Perspective” in: Monica den Boer (ed.), *Comparative Policing from a Legal Perspective*, Edward Elgar Publishing, Cheltenham, 2018, s. 306-328.
- de Hert Paul, “A Human Rights Perspective on Privacy and Data Protection Impact Assessments”, in: David Wright/Paul de Hert (eds.), *Privacy Impact Assessment*, Law, Governance and Technology Series 6, Springer, Heidelberg, 2012, s. 33-76.
- de Hert Paul/Dimitrova Diana, “The Right of Access Under the Police Directive: Small Steps Forward”, in: Manel Medina/Andreas Mitrakas/Kai Rannenberg/Erich Schweighofer/Nikolaos Tsouroulas (eds.), *Privacy Technologies and Policy, 6th Annual Privacy Forum, APF 2018, Barcelona, Spain, June 13-14, 2018, Revised Selected Papers*, Springer, Heidelberg, 2018, s. 111-130.
- Dehon Estelle/Carey Peter, “Fair, Lawful and Transparent Processing”, in: Peter Carey (ed.), *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, Oxford, 2018, s. 42-65.
- Develioğlu Hüseyin Murat, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha, İstanbul, 2017.
- Di Francesco Maesa Costanza, “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)”, (Çevrimiçi) <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/>, Eurojus, 24/05/2016, (Erişim Tarihi: 10.04.2019).

- Dülger Murat Volkan, Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi, İstanbul, 2019.
- Erman Ragıp Barış, “Ceza yargılamasında Yargı Sisteminde DNA Örnekleri ve Profilleri - S. ve Marper - Birleşik Krallık Davası”, *Fasikül Hukuk Dergisi*, Seçkin, Ankara, 2010, C. 2, S. 10, s. 20-23.
- Foitzik Piotr, “Privacy by Default in Online Services”, (Çevrimiçi) <https://iapp.org/news/a/privacy-by-default-in-online-services/>, (Erişim Tarihi: 10.04.2019).
- Foucault Michel, Özne ve İktidar, Seçme Yazılar 2, (Çev: Işık Ergüden-Osman Akınhay), 4. Bası, Ayrıntı, İstanbul, 2014.
- Geminn Christian Ludwig, “The New Federal Data Protection Act - Implementation of the GDPR in Germany”, *Blog Droit Européen*, E-conférence: National Adaptations of the GDPR, Haziran 2018, (Çevrimiçi) <https://blogdroiteuropeen.files.wordpress.com/2018/06/christian-l.pdf>, (Erişim Tarihi: 10.04.2019).
- Giddens Anthony, The Nation-State and Violence: Volume Two of a Contemporary Critique of Historical Materialism, Polity Press, Cambridge, 1985.
- Gilbert Francoise, “EU General Data Protection Regulation: What Impact for Business Established Outside the European Union”, *Journal of Internet Law*, Mayıs 2016.
- González Fuster Gloria, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Law, Governance and Technology Series 16, Springer, Heidelberg, 2014.
- Grazia Porcedda Maria, “Privacy by Design” in: Manel Medina/Andreas Mitrakas/Kai Rannenberg/Erich Schweighofer/Nikolaos Tsouroulas (eds.), *Privacy Technologies and Policy, 6th Annual Privacy Forum, APF 2018, Barcelona, Spain, June 13-14, 2018, Revised Selected Papers*, Springer, Heidelberg, 2018, s. 183-205.
- Greenwald Glenn, No Place to Hide, Penguin Books, London, 2014.
- Gutiérrez Zarza Ángeles, Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe, Springer, Heidelberg, 2015.
- Handbook on European Data Protection Law: 2018 Edition, Publications Office of the European Union, Luxembourg, 2018.
- Hijmans Hielke / Raab Charles D., “Ethical Dimensions of the GDPR” in: Mark Cole/Franziska Boehm (eds.), *Commentary on the General Data Protection Regulation*, Edward Elgar, Cheltenham, 2019, Forthcoming, (Çevrimiçi) <https://ssrn.com/abstract=3222677>, (Erişim Tarihi: 10.04.2019).
- Hijmans Hielke, The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU, Springer, Heidelberg, 2016.
- Hornung Gerrit, “A General Data Protection Regulation for Europe: Light and Shade in the Commission’s Draft of 25 January 2012”, *SCRIPTed*, 9, 2012.
- Hustinx Peter, “The Role of Data Protection Authorities”, in: Serge Gutwirth, Yves Poullet, Paul de Hert, Cecile de Terwangne, Sjaak Nouwt (eds.), *Reinventing Data Protection?*, Springer, Heidelberg, 2009, s. 131-139.

- Kızılırmak Baran, *Önleyici Amaçla Elde Edilen Verilerin Ceza Muhakemesinde Kullanılabilirliği*, Yayınlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2018.
- Kierkegaard Sylvia/Waters Nigel/Greenleaf Graham/Bygrave Lee A./Lloyd Ian/Saxby Stephen, “30 Years on - The Review of the Council of Europe Data Protection Convention 108”, *Computer Law & Security Review*, Elsevier, 2011, V. 27 I. 3, s. 223-231.
- Küzeci Elif, *Kişisel Verilerin Korunması*, 3. Bası, Turhan Kitabevi, Ankara, 2019.
- Lambert Paul, *Understanding the New European Data Protection Rules*, CRC Press, Boca Raton, 2017.
- Lambert Paul, *The Data Protection Officer: Profession, Rules and Role*, CRC Press, Boca Raton, 2017.
- Le Métayer Daniel, “Privacy by Design: A Matter of Choice”, in: Serge Gutwirth, Yves Poullet, Paul de Hert (eds.), *Data Protection in a Profiled World*, Springer, Heidelberg, 2010, s. 323-332.
- Leiser Marc, “The Law Enforcement Directive: The ‘Forgotten Directive’s Delicate Interplay with the GDPR”, *Avrupa ve Türk Hukukunda Kişisel Verilerin Korunmasına İlişkin Güncel Sorunlar Sempozyumu*, Yeditepe Üniversitesi, 9 Aralık 2018.
- Lynskey Orla, *The Foundations of EU Data Protection Law*, Oxford Studies in European Law, Oxford University Press, Oxford, 2015.
- Lyon David, “Surveillance, Power, and Everyday Life”, in: Danny Quah/Chrisanthi Avgerou/Robin Mansell/Roger Silverstone (eds.), *The Oxford Handbook of Information and Communication Technologies*, Oxford University Press, Oxford, 2007, s. 449-473.
- Marquenie Thomas, “The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework”, *Computer Law and Security Review: The International Journal of Technology Law and Practice*, Elsevier, London, 2017, V. 33, I. 3, s. 324-340.
- Minnaar Anthony, “Cybercrime, Cyberattacks, and Problems of Implementing Organizational Cybersecurity”, in: John A. Eterno/Arvind Verma/Aiedeo Mintie Das/Dilip K. Das, (eds.), *Global Issues in Contemporary Policing*, CRC Press, Boca Raton, 2017, s. 121-138.
- Nino Michele, “The Protection of Personal Data in the Fight Against Terrorism: New Perspectives of Pnr European Union Instruments in the Light of the Treaty of Lisbon” *Utrecht Law Review*, Utrecht, 2010, Vol. 6, No. 1, s. 62-85.
- Nissim Jenai, “Accountability and the Role of the Data Protection Officer”, in: Peter Carey (ed.), *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, Oxford, 2018, s. 223-239.
- Pajunoja Lauri, *The Data Protection Directive on Police Matters 2016/680 Protects Privacy - The Evolution of EU’s Data Protection Law and Its Compatibility with the Right to Privacy*, Yayınlanmamış Yüksek Lisans Tezi, University of Helsinki, Helsinki, 2017.

- Reding Viviane, “The European Data Protection Framework for the Twenty-First Century”, *International Data Privacy Law*, Oxford Academic, Oxford, 2012, V. 2, I. 3, s. 119-129.
- Reding Viviane, “Privacy Matters - Why the EU Needs New Personal Data Protection Rules”, EU Commission, (Çevrimiçi) http://europa.eu/rapid/press-release_SPE-ECH-10-700_en.htm?locale=en (Erişim Tarihi: 01.04.2019).
- Sajfert Juraj/Quintel Teresa, “Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities”, in: Mark Cole/Franziska Boehm (eds.), *GDPR Commentary*, Edward, Elgar Publishing, Cheltenham, 2019, Forthcoming, (Çevrimiçi) <https://ssrn.com/abstract=3285873>, (Erişim Tarihi: 01.04.2019).
- Salami Emmanuel, “The Impact of Directive (EU) 2016/680 on 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 on the Existing Privacy Regime” (Çevrimiçi) <http://dx.doi.org/10.2139/ssrn.2912449>, (Erişim Tarihi: 10.04.2019).
- Tambou Olivia, “Que retenir du projet de loi relative à la protection des données personnelles ? Partie II: L’amélioration relative du régime des traitements pénaux par la transposition de la directive n°2016/680” (Çevrimiçi) <https://www.village-justice.com/articles/que-retenir-projet-loi-relatif-protection-des-donnees-personnelles-partie,28175.html>, (Erişim Tarihi: 18.04.2019).
- Tamò-Larrieux Aurelia, *Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things*, Law, Governance and Technology Series 40, Springer, Heidelberg, 2018.
- Taylor Roger, “No Privacy without Transparency” in: Ronald Leenes/Rosamunde van Brakel/Serge Gutwirth/Paul De Hert (eds.), *Data Protection and Privacy: The Age of Intelligent Machines*, Computers, Privacy and Data Protection Series, V. 10, Hart Publishing, Oxford, 2017, s. 63-88.
- Voigt Paul/von dem Bussche Axel, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, Heidelberg, 2017.
- Weigend Thomas, “Information Society and Penal Law: General Report”, *Revue Internationale de Droit Penal*, 2013/1-2 (V. 84).
- Wright David/de Hert Paul, “Introduction to Privacy Assessment”, in: David Wright/Paul de Hert (eds.), *Privacy Impact Assessment*, Law, Governance and Technology Series 6, Springer, Heidelberg, 2012, s. 3-32.
- Zouave Erik/Schroers Jessica, “You’ve been Measured, You’ve been Weighed and You’ve been Found Suspicious: Biometrics and Data Protection in Criminal Justice Processing” in: Ronald Leenes/Rosamunde van Brakel/Serge Gutwirth/Paul De Hert (eds.), *Data Protection and Privacy: The Internet of Bodies*, Computers, Privacy and Data Protection Series, V. 11, Hart Publishing, Oxford, 2018, s. 1-20.

Belge, Görüş, Araştırma ve Raporlar

Anti-Phishing Working Group (APWG), “Unifying the Global Response to Cybercrime”, (Çevrimiçi) <https://www.antiphishing.org/resources/apwg-reports/> (Erişim Tarihi: 01.04.2019).

Cannataci Joseph / Caruana Mireille, Report: Recommendation R (87) 15 - Twenty-Five Years Down the Line, Council of Europe 2013.

Commission Nationale de l’Informatique et des Libertés (CNIL), “Délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d’adaptation au droit de l’Union européenne de la loi n°78-17 du janvier 1978”, (Çevrimiçi) https://www.cnil.fr/sites/default/files/atoms/files/projet_davis_cnil.pdf, (Erişim Tarihi: 18.04.2019).

Commission Nationale de l’Informatique et des Libertés (CNIL), “Délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d’adaptation au droit de l’Union européenne de la loi n°78-17 du janvier 1978”

Convention for The Protection of Individuals with Regard to Automatic Processing of Personal Data. (Çevrimiçi) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>, (Erişim Tarihi: 10.04.2019).

Council Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters, (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977>, (Erişim Tarihi: 01.04.2019).

Danezis George/Domingo-Ferrer Josep/Hansen Marit/Hoepman Jaap-Henk/Le Métayer Daniel/Tirtea, Rodica/Schiffner, Stefan, Privacy and Data Protection by Design - from policy to engineering, European Union Agency for Network and Information Security (ENISA) 2015.

de Hert Paul/Bellanova Rocco, Data Protection in the Area of Freedom, Security and Justice: A System Still to be Fully Developed?, European Parliament, (Çevrimiçi) [http://www.europarl.europa.eu/RegData/etudes/note/join/2009/410692/IPOL_LIBE_NT\(2009\)410692_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/note/join/2009/410692/IPOL_LIBE_NT(2009)410692_EN.pdf), Mart 2009.

Department for Digital, Culture, Media and Sport (DCMS) / Home Office, Data Protection Bill: Explanatory Notes (Çevrimiçi) <https://publications.parliament.uk/pa/bills/cbill/2017-2019/0153/en/18153-EN.pdf>, Erişim Tarihi: 10.04.2019).

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 (Çevrimiçi) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG (Erişim Tarihi: 01.04.2019).

European Commission, “Communication from the Commission to the European Parliament and the Council: Overview of Information Management in the Area of Freedom, Security and Justice”, (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0385&from=EN>, 20/7/2010, (Erişim Tarihi: 01.04.2019).

- European Commission, “Safeguarding Privacy in a Connected World a European Data Protection Framework for the 21st Century”, (Çevrimiçi) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF>, 25/1/2012, (Erişim Tarihi: 10.04.2019).
- European Commission, Proposal for a Directive of the European Parliament and of the Council on the Protection of Individual 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, (Çevrimiçi) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF>, (Erişim Tarihi: 01.04.2019) (Avrupa Komisyonu Tasarısı).
- European Data Protection Supervisor (EDPS), “Opinion of the European Data Protection Supervisor for a Directive of the European Parliament and of the Council regarding the European Investigation Order in Criminal Matters”, (Çevrimiçi) [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010XX1229\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010XX1229(01)), 29/12/2010, (Erişim Tarihi: 10.04.2019).
- European Union Agency for Network and Information Security (ENISA), Handbook on Security of Personal Data Processing, 2018.
- House of Lords, The European Union Committee, Brexit: the EU data protection package, (Çevrimiçi) <https://publications.parliament.uk/pa/ld201719/ldselect/ldcom/7/7.pdf>, Authority of the House of Lords18/07/2017, (Erişim Tarihi: 10.04.2019).
- Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, (Çevrimiçi) <https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler>, (Erişim Tarihi: 10.04.2019).
- Recommendation R (87) 15 of the Committee of Ministers to Member States Regulating the use of Personal Data in the Police Sector, (Çevrimiçi) <https://rm.coe.int/168062dfd4>, (Erişim Tarihi: 01.04.2019).
- Statewatch, Implementing the “principle of availability”: The European Criminal Records Information System, The European Police Records Index System, The Information Exchange Platform for Law Enforcement Authorities, (Çevrimiçi) <http://www.statewatch.org/analyses/no-145-ecri-epris-ixp.pdf> (Erişim Tarihi: 10.04.2019).
- Statewatch, The Directive on Data Protection and Law Enforcement: A Missed Opportunity?, (Çevrimiçi) <https://www.statewatch.org/analyses/no-176-leas-data%20protection.pdf> (Erişim Tarihi: 10.04.2019).
- TBMM Başkanlığı, “Kişisel Verilerin Otomatik İşlenme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı”, (Çevrimiçi) <https://www.tbmm.gov.tr/d24/1/1-0966.pdf>, 1/8/2014, (Erişim Tarihi: 01.04.2019).
- The Article 29 Working Party, “Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679”, (Çevrimiçi) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, 06/02/2018, (Erişim Tarihi: 10.04.2019).

- The Article 29 Working Party, “Guidelines on Data Protection Impact Assessment (DPIA)”, (Çevrimiçi), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, 04/04/2017, s. 19, (Erişim Tarihi: 10.04.2019).
- The Article 29 Working Party, “Guidelines on Data Protection Officers (‘DPOs’)”, (Çevrimiçi), https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf, 13/12/2016, s. 4, (Erişim Tarihi: 10.04.2019).
- The Article 29 Working Party, “Guidelines on Transparency Under Regulation 2016/679”, (Çevrimiçi), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227, 22/08/2018, (Erişim Tarihi: 10.04.2019).
- The Article 29 Working Party, “Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector”, (Çevrimiçi) <https://www.pdpjournals.com/docs/88168.pdf>, 27/02/2014, (Erişim Tarihi: 10.04.2019).
- The Article 29 Working Party, “Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680)”, (Çevrimiçi) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178, 29/11/2017, (Erişim Tarihi: 10.04.2019).
- The Article 29 Working Party, “The Future of Privacy”, (Çevrimiçi) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf, 01/12/2009, s. 26, (Erişim Tarihi: 10.04.2019).
- The Council of Europe (CoE), Practical Guide on the use of Personal Data in the Police Sector (Çevrimiçi) <https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5>, (Erişim Tarihi: 10.04.2019).
- The Information Commissioner’s Office (ICO), Accountability and Governance: Data Protection Impact Assessments (DPIAs) (Çevrimiçi) <https://www.pdpjournals.com/docs/887901.pdf>, 22/03/2018, s. 19 (Erişim Tarihi: 10.04.2019).
- The Information Commissioner’s Office (ICO), Data Protection Officers (Çevrimiçi) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/> (Erişim Tarihi: 10.04.2019).
- The Information Commissioner’s Office (ICO), Guide Law Enforcement Processing (Part III of the Bill), (Çevrimiçi) <https://www.pdpjournals.com/docs/887918.pdf>, 05/04/2018, (Erişim Tarihi: 10.04.2019).
- The Information Commissioner’s Office (ICO), Guide to Law Enforcement Processing (Part 3 of the Bill) (Çevrimiçi) <https://www.pdpjournals.com/docs/887918.pdf>, (Erişim Tarihi: 10.04.2019).
- The Information Commissioner’s Office (ICO), Guide to the General Data Protection Regulation (GDPR), (Çevrimiçi) <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>, (Erişim Tarihi: 10.04.2019).
- The Organization for Economic Cooperation and Development (OECD), “The OECD Privacy Framework” s. 15-16, (Çevrimiçi) https://www.oecd.org/internet/ieconomy/oecd_privacy_framework.pdf (Erişim Tarihi: 10.04.2019).

The Organization for Security and Co-operation in Europe (OSCE), Guidebook on Democratic Policing, (Çevrimiçi) <https://www.osce.org/secretariat/23804?download=true> (Erişim Tarihi: 01.04.2019).

UK Government Department for Digital, Culture, Media and Sport (DCMS) / University of Portsmouth, “Cyber Security Breaches Survey 2019”, (Çevrimiçi) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/791940/Cyber_Security_Breaches_Survey_2019_-_Main_Report.PDF (Erişim Tarihi: 01.04.2019).

UK Legislation, Data Protection Act 2018 (“DPA”) (Çevrimiçi) http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf (Erişim Tarihi: 10.04.2019).

Kararlar

ABAD, Maximillian Schrems v. Data Protection Commissioner and Digital Rights Ireland Ltd., C-362/14, 6 Ekim 2015.

AİHM, Liberty ve Diğerleri v. Birleşik Krallık, Başvuru no: 58243/00, 1 Ekim 2008.

AİHM, Rotaru v. Romanya, Başvuru no: 28341/95, 4 Mayıs 2000.

AİHM, S. ve Marper v. Birleşik Krallık, Başvuru no: 30562/04, 30566/04, 4 Aralık 2008.