

Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre Değerlendirilmesi

Evaluation of Exceptions Provided for Judicial and Preventive Purposes on Processing of Personal Data According to National and International Law

Arş. Gör. Baran KIZILIRMAK^(*)

Öz:

Çalışmada kişisel verilerin işlenmesine ilişkin güvence, sınırlama, ilke ve hakların; adli ve önleyici amaçlı faaliyetler bakımından nasıl daraltıldığı (istisna tutulduğu) incelenmektedir. Adli ve önleyici amaçla veri işlemede de sayılan güvence, sınırlama ilke ve hakların bir kısmı geçerlidir. Fakat bunlar özel hukuk ilişkilerinde olduğu kadar geniş boyutta sağlanmamaktadır. Uluslararası ve uluslararası mevzuattaki genel eğilim, adli ve önleyici amaçlı faaliyetlerin, kişisel verilerin işlenmesine ilişkin kuralların bir kısmından istisna tutulması; ulusal güvenlik amacıyla gerçekleştirilen istihbari faaliyetlerin ise tamamen istisna tutulması yönündedir. Ancak ikincisine ilişkin tartışmalar sürmektedir. Çalışmada, Türk hukuku ve literatüründeki eksiklik de gözetilerek hem 6698 sayılı Kişisel Verilerin Korunması Kanunu hem de konuya ilişkin önemli bazı uluslararası ve uluslararası hukuk metinleri incelenmiştir. Bunların adli ve önleyici amaçla kişisel veri işlemede istisnaların öngörülmesine ilişkin yaklaşımı değerlendirilmiştir. Bu güvence, sınırlama, ilke ve hakların her biri ayrı birer çalışma konusudur; bu çalışmada ana hatlarıyla üzerinde durulmakla yetinilmiş olup, konu çalışmanın kapsamını daha fazla genişletmemek amacıyla karşılaştırmalı hukuk disiplini altında incelenmemiştir.

Anahtar Kelimeler:

Kişisel Veri, Kolluk, Adli ve Önleyici Amaç, İstisna, 2016/680 Sayılı Direktif, GDPR, 108 no.lu Sözleşme.

Abstract:

In this study, how the safeguards, restrictions, principles and rights regarding the processing of personal data in judicial and preventive activities are restricted (excluded) is analyzed. Some of these safeguards, restrictions, principles and rights are also valid for data processing in judicial and preventive purposes. However, these are not ensured in a wide scale as in private law relations. General tendency in international and supranational regulations is excluding the judicial and preventive activities from

^(*) Kadir Has Üniversitesi, Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı,
E-posta: baran.kizilirmak@khas.edu.tr; Orcid Id: <https://orcid.org/0000-0001-9680-6727>.

Yayın Kuruluna Ulaştığı Tarih: 27.10.2019 / Kabul Tarihi: 13.11.2019.

some of the rules in personal data processing; while intelligence activities carried out for the purpose of national security are to be totally exempted. However, the debate on the latter continues. In this study, taking into account the lack in Turkish law and academic studies, both the Law on the Protection of Personal Data No. 6698 and some of the important international and supranational regulations relating to the topic are examined. Their approach in providing exceptions in personal data processing for judicial and preventive purposes was evaluated. Each of these safeguards, restrictions, principles and rights are subject to separate studies; in this study they are only evaluated superficially, also the issue hasn't been analyzed under comparative law discipline.

Keywords:

Personal Data, Law Enforcement Forces, Judicial and Preventive Purpose, Exception, Directive No: 2016/680, GVKT, Treaty No: 108.

I. Giriş

Teknolojideki gelişmeler, toplumsal yaşamın her alanında devasa boyutta veri elde etme, depolama ve onları değerlendirme olanağı doğurmuş, bu durum kişisel verilerin korunmasını günümüzün en çok tartışılan konularından biri olmasını sağlamıştır. Gerçekten bir yanda insanların kişisel verilerine ilişkin güvenlik beklentisi, diğer yanda ise *Big Data*'nın (Büyük Veri) ve sağladığı olanakların tartışıldığı günümüzde toplumsal yaşamın, devamlı olarak veri işleme faaliyeti üzerinden gelişmesi kişisel verilerin korunması konusunu son derece önemli kılmaktadır.

Yeni ve güncel bir konu olduğundan kişisel verilerin korunmasına ilişkin literatürde çok sayıda çalışma bulunmaktadır. Günümüzdeki hukuki çalışmalar konuyu çoğunlukla özel hukuk boyutuyla ele almakta; tartışmalar örneğin tüzel kişilerin gerçek kişilere ait kişisel verileri işleme usulü, güvenceler ve bu konudaki hak ve yükümlülükler üzerinde yoğunlaşmaktadır. Ancak kişisel verilerin işlenmesi bununla sınırlı değildir; devlet de yetkili merciler aracılığıyla kişisel veri işlemektedir. Konu yabancı hukuk literatüründe de son yıllarda gündeme getirilmekle birlikte; özel hukuk boyutunun aksine yetkili resmi mercilerin suçların önlenmesi, aydınlatılması, cezaların infazı gibi amaçlarla kişisel veri işlemesi hususunun üzerinde oldukça az durulmaktadır.

Bahsedilen amaçlarla kişisel veri elde edilmesini sağlayan yöntemlerin bir kısmı esasen başka bir hakka (genellikle özel yaşamın gizliliği) müdahalede bulunmaktadır. Dolayısıyla hukuk düzen-

lerindeki klasik yaklaşım, bu hak ekseninde söz konusu yöntemlerin uygulanmasını temel hak ve özgürlüklerin sınırlandırılması rejimine uygun olarak belirli güvencelere bağlamaktır. Örneğin, adli amaçla telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sonucunda elde edilen kişisel verileri de içeren kayıtların gizli tutulacağı; bunların bazı durumlarda ve belirli süre sonra yok edileceği (CMK m.137)¹ gibi hususlar bu tedbirle bağlantılı olarak düzenlenmiştir.² Bununla birlikte, günümüzde kişisel verilerin korunması hakkının özel yaşamın gizliliğinden ayrı bir hak olarak ortaya çıkması sonucunda; adli ve önleyici amaçlı yöntemler, ayrıca kişisel verilerin korunması hakkında doğan güvence ve sınırlamalara kavuşturulmaktadır.

Yetkili resmi mercilerce işlenen kişisel verilerin korunması, bireylerin temel hak ve özgürlüklerinin sağlanması açısından son derece önemlidir. Ancak konunun önemi bununla sınırlı değildir. Nitekim yukarıda belirtilen amaçlarla yetkili merciler arasında kişisel verilerin dolaşımı; diğer bir deyişle veri paylaşımı, madalyonun diğer yüzünü oluşturmakta olup, konuya ilişkin düzenlemeler bu dolaşımın ancak güçlü bir mekanizma kapsamında verilerin güvenliği korunarak sağlanmasını öngörmektedir.

Konunun Türkiye - AB ilişkileri bakımından da ayrı bir önemi haiz olduğu ifade edilmelidir. Türkiye'de 2016 yılında Kişisel Verilerin Korun-

¹ 04.12.2004 tarih ve 5271 s. Ceza Muhakemesi Kanunu, RG T.17.12.2004, S.25673.

² Ancak günümüzde kişisel veri elde edilmesini sağlayan pek çok yöntemde bu tür güvenceler dahi bulunmamaktadır.

ması Kanunu³ (KVKK) yürürlüğe girmiş olsa da, çalışmada da incelendiği üzere bu yeterli olmamıştır. Nitekim Avrupa Komisyonu'nun, Türkiye için hazırladığı son yıllardaki ilerleme raporlarında da kişisel verilerin korunması mevzuatının AB standartlarıyla uyumlu olmadığını vurgulamakta, bunun uyumlulaştırılması gerektiği ifade edilmektedir.⁴ Zira AB standartlarıyla uyumlu bir mevzuat, özellikle sınır aşan organize suçlulukla mücadelede işbirliği gibi amaçlarla (EUROPOL⁵ gibi örgütlerle operasyonel işbirliğinin kurulması vb.) kişisel verilerin ülke dışıyla paylaşılması da dahil olmak üzere, verilerin dolaşımı için temel koşuldur.⁶ Kısacası konuyu daha detaylıca düzen-

leyen, AB ile uyumlu bir mevzuatın hazırlanması AB tarafından beklenmektedir.

Biz de çalışmamızda esas olarak Türk hukukundaki AB ile uyum konusunda yapılan çalışmaları gözeterek, Birlik hukukuna ve bu konuda en önemli metin olan 2016/680 sayılı Direktif'e⁷ geniş yer ayırmış bulunmaktayız. 4 Mayıs 2016'da AB Resmi Gazetesi'nde yayımlanarak yürürlüğe giren ve 6 Mayıs 2018'e kadar üye devletlerin iç hukuklarında düzenleme yapması gereken⁸ bu Direktif, günümüzde konuyu düzenleyen en kapsamlı metin olmakla birlikte, geniş kapsamına ve önemli iddialarına karşın, ne yazık ki kanımızca yeterli değildir ve geliştirilmesi gerekmektedir. Ayrıca gerek akademik çalışmalarda gerekse uygulamada Genel Veri Koruma Tüzüğü'nün⁹

³ 24.03.2016 Tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu, RG T.07.04.2016, S.29677.

⁴ Avrupa Komisyonu'nun Türkiye 2018 İlerleme Raporu (Ing.), s.5, 41, 42. <https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-turkey-report.pdf> (çevrim içi), E.T. 20.10.2019, 13:30; 2016 İlerleme Raporu (Ing.), s.10, 22, 71, 78, 83, 85. https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2016/20161109_report_turkey.pdf (çevrim içi), E.T. 20.10.2019, 13:30; **DEVELİOĞLU, 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 Yayıncılık, İstanbul 2017, s.15.

⁵ 1999 yılında faaliyetlerine başlayan EUROPOL, AB üyesi devletler ile diğer devletler arasında veri alışverişinin sağlanmasında önemli bir işleve sahiptir. Türkiye ile EUROPOL arasında 2004 yılında kişisel verilerin paylaşımına olanak tanımayan bir işbirliği oluşturmuştur. 2018 İlerleme Raporu'nda da belirtildiği üzere, operasyonel bir işbirliği kurulamamasının nedeni Türkiye'nin bu konudaki mevzuatının AB standartlarıyla uyumlu olmamasıdır. Halbuki bu rapordan önce, yani 2016 yılında yürürlüğe giren KVKK'nin genel gerekçesinde, bu eksikliğe dikkat çekilerek KVKK'nin hazırlandığı belirtildiğinden, çıkarılan kanunun gerekli uyumu sağlayacağını düşünüldüğü anlaşılmaktadır. (KVKK genel gerekçesi, s.5. <https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf> (çevrim içi), E.T. 20.10.2019, 13:30).

Oysa sonraki tarihli ilerleme raporlarında açıkça EUROPOL ile operasyonel anlaşmanın, Türkiye'nin veri koruma koşulları nedeniyle tamamlanamadığını ve KVKK'nin, Avrupa standartlarıyla henüz uyumlu olmadığını belirtmektedir.

⁶ **PAJUNOJA, Lauri J.:** "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", *Univeristy of Helsinki - Faculty of Law*, Yayınlanmamış Yüksek Lisans Tezi, 2017, s.83.

⁷ Direktif'in tam adı: (Ing.): Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA; (Tr.): 2016/680 sayılı Gerçek Kişilere Ait Kişisel Verilerin Yetkili Merciler Tarafından Adli Suçların Önlenmesi, Araştırılması, Tespit Edilmesi veya Kovuşturulması ya da Mahkumiyetlerin İnfazı Amacıyla İşlenmesi ve bu Verilerin Serbest Dolaşımı Hakkında, 2008/977/JHA Çerçeve Kararı'nı İlgä Eden Direktif. Ks. 2016/680 sayılı Direktif. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG (çevrim içi), E.T. 20.10.2019, 13:30.

⁸ İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, *Avrupa Parlamentosu ve Konseyi'nin 2016/680 Sayılı ve 27 Nisan 2016 Tarihli Kişisel Verilerin Yetkili Otoritelerce Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması veya Cezaların İnfazı Amacıyla İşlenmesiyle İlgili Gerçek Kişilerin Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin ve 2008/977/JHA Sayılı Konsey Çerçeve Kararı'nı Yürürlükten Kaldıran Direktif Hakkında Bilgi Notu*, <https://itlaw.bilgi.edu.tr/media/2019/7/27/law-enforcement-directive-bilgi-notu.pdf>, s.3, 4, (çevrim içi), E.T. 20.10.2019, 13:30.

⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal data and on the free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation - GDPR), (Tr. GVKT), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL> (çevrim içi), E.T. 20.10.2019, 13:30.

(GVKT veya *Ing.* GDPR) gölgesinde kaldığını söylemek yanlış olmayacaktır. Bunun nedeni olarak Direktif'in düzenlediği alandaki gelişmelerin, GVKT'ye göre daha erken aşamada olduğu ve henüz olgunlaşmadığı ifade edilmektedir.¹⁰

Çalışmada öncelikle konuyla ilgili temel kavramlar açıklanmış; konunun özünü oluşturan amaca bağlılık ilkesi üzerinde durulmuştur. Ardından adli ve önleyici amaçlı faaliyetler ile istihbarat faaliyetleri arasındaki ilişki örneklerle ele alınmıştır. Konu açısından önem taşıyan Avrupa İnsan Hakları Sözleşmesi ve Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin (108 no.lu) Sözleşme'ye yer verildikten sonra günümüzdeki başlıca düzenleme sayılabilecek 2016/680 sayılı Direktif, konuya ışık tutması amacıyla bütünüyle ve fakat genel bir değerlendirmeye ele alınmış; son olarak KVKK hükümlerinin ne derece yeterli olduğu tartışılmıştır. İfade etmek gerekir ki, konunun kapsamı içinde kalan her bir alt başlık (örneğin, otel gibi konaklama tesislerinde kalanların kayıtlarındaki kişisel verilerin polis bilgisayar terminallerine aktarılması doğrultusunda, bu kişisel verilerin hangi sınırlamalar dahilinde nasıl işleneceği, veri sahiplerinin hakları vb. hususlar) esasen ayrı çalışmaların konusu olabilecektir. Dolayısıyla bu çalışmada, bu konudaki Türk hukuk literatüründeki eksikliği gözeterek genel bir değerlendirme yapmanın daha yararlı olacağı düşünülmüştür. Başka bir ifadeyle, yetkili resmi mercilerin adli ve önleyici amaçla kişisel veri işlerken, bu faaliyetlerin kendine has güvencelerinin yanında kişisel verilerin korunması bakımından da belirli sınırlamalara tabi tutulduğuna dikkat çekilmiştir. Bu doğrultuda söz konusu düzenlemelerde veri işlemeye yönelik temel ilkelere ne derece sadık kalındığı üzerinde durulmuş, bu amaçla 108 no.lu Sözleşme ve 2016/680 s. Direktif ile KVKK incelenmiş, Türk hukuk literatüründe (bağlayıcı olmadığından) pek önemsenmeyen bu Direktif'in başlangıç metni ve hükümlerindeki önemli kısımlar değerlendirilmiştir.

¹⁰ KÜZECİ, Elif: *Kişisel Verilerin Korunması*, 3. Baskı, Turhan Kitabevi Yayınları, Ankara 2019, s.197.

II. Kişisel Verilerin İşlenmesine İlişkin Temel Açıklamalar

A. Kavramlar

1. Veri

Türk Dil Kurumu veriyi¹¹ *“bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done”, “gözlem ve deneye dayalı araştırmanın sonuçları”* yahut *“bilgi, data”* olarak; bilgiyi ise *“insan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat”, “insan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf”* olarak tanımlamaktadır.¹² Veri sözcüğü, genellikle bilgi ile eş veya yakın anlamlı olarak kullanılmakla birlikte; kanımızca veri daha ziyade ham nitelikteki soyut varlığı; bilgi ise zihinsel süzgeçten geçerek anlamlandırılmış veriyi çağrıştırdığından; çalışmada konunun özü bakımından veri kavramı, 'bilgi'yi, de kapsayacak biçimde kullanılmaktadır.

2. Kişisel Veri

Kişisel veri gerek ulusal gerekse yabancı hukuk metinlerinde *“belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgi”* biçiminde tanımlanmaktadır. Buna göre, kişisel veriyi diğer verilerden ayırırken iki ölçüt kullanılmaktadır: 1- Verinin bir kişiye ilişkin olması; 2- Bu kişinin belirli ya da belirlenebilir nitelikte olması.¹³ Bu bağlamda kişinin adı ve soyadı, cep telefonu numarası, e-posta adresi, ev adresi, fotoğrafı, göz rengi, yurttaşı olduğu ülkenin kimlik numarası, öğrenci kimlik numarası, dernek ve sendika üyelikleri, kişisel bilgisayarında kullandığı IP adresi, parmak izi vb. kişisel verilerdir.¹⁴ Konuyla ilgili KVKK, GVKT (*Ing.* GDPR) gibi düzenlemelerde

¹¹ *Ing. data* sözcüğünü karşılamak üzere kullanılmaktadır.

¹² www.tdk.gov.tr (çevrim içi), E.T. 20.10.2019, 13:30.

¹³ KÜZECİ, a.g.e., s.9, 312; SERT, Şeyma: *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, Seçkin Yayıncılık, Ankara 2019, s.24.

¹⁴ Bir bilginin kişisel veri sayılması için nesnel nitelik taşımasının gerekmediği, örneğin iş yaşamındaki performansı gibi öznel bilgilerin de kişisel veri sayılabileceği ifade edilmektedir. Bkz.: DEVELİOĞLU, a.g.e., s.37.

yalnızca gerçek kişilere¹⁵ ait verilerin kişisel veri sayıldığı açıkça belirtilmektedir; ancak tüzel kişilerin de kişisel verilerin korunması kapsamında değerlendirilmesi gerekliliğine ilişkin öğretide görüş birliği bulunmamaktadır.^{16,17}

Önleyici ve adli amaçla kullanılan verilerin tamamı kişisel veri niteliğini haiz değildir. Örneğin kolluk, idari görevlerini yerine getirirken sıklıkla kişisel olmayan nitelikte veriler de toplamakta, bunları değerlendirmekte, yani işlemektedir. Söz gelimi, bir binada yangın çıkması tehlikesine karşılık binanın planlarının bulunulması konuya ilişkin veri niteliğinde olup, bir kişiye ilişkin olmadığından kişisel veri niteliğini haiz değildir.¹⁸

3. Veri İşleyen, Veri Sorumlusu ve İlgili Kişi (Veri Öznesi)

Kişisel Verileri Koruma Kanunu'nun 3. maddesine göre ilgili kişi (veri öznesi - Ing. *data subject*), "kişisel verisi işlenen gerçek kişiyi"; veri işleyen "veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi"; veri sorumlusu ise "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel

kişiyi"¹⁹ ifade etmektedir. Bu doğrultuda veri işleyen, veri sorumlusunun verdiği yetkiye dayanarak, onun adına, onun talimatları doğrultusunda veri işlemekte; veri sorumlusu ise veri işlemenin amacı ve işleme araçlarının temel bileşenleri gibi hususları belirlemektedir. Uygulamada özellikle geniş ve karmaşık yapılar ile elektronik iletişim ağlarında bu kişilerin aralarındaki ayrımı belirlemenin kimi zaman güç olduğu ifade edilmektedir.²⁰

Kamu kurum ve kuruluşları, kamu tüzel kişileri veri sorumlusu veya veri işleyen olabilirler. Bu, KVKK'nin Tanımlar başlıklı 3. maddesinde tüzel kişi ifadesi kullanılarak özel-kamu şeklinde bir ayırım yapılmamasından anlaşılmaktadır. Nitekim GVKT ve 2016/680 s. Direktif'te de kamu kurumlarının veri sorumlusu veya veri işleyen olabileceği açıkça belirlenmiştir. Bu tespit hukuki yükümlülüklerin belirlenmesi açısından önemlidir.

B. Kişisel Verilerin İşlenmesi ve Temel İlkeler

Kişisel verilerin işlenmesi, KVKK'nin tanımlar başlıklı 3. maddesine göre; kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder. Bu, sınırlandırıcı bir sayma olmayıp; verilerin silinmesi, yok edilmesi, başka şekilde elde edilebilir hale getirilmesi, sınıflandırılması gibi veriler üzerinde gerçekleştirilen

¹⁵ Kişilik gerçek ve tüzel kişilik ana başlıkları altında incelenir. Gerçek kişiler bakımından kişilik, Türk Medeni Kanunu'nun 28. maddesine göre sağ olarak doğmuş olmak kaydıyla, ana rahmine düşme anından başlar; dolayısıyla ceninin kişisel verileri de bu andan itibaren korunacaktır. Bkz.: DEVELİOĞLU, a.g.e., s.31.

¹⁶ AYM, Anayasa'nın lafzi yorumuyla hem gerçek hem de tüzel kişilerin kişisel verilerinin korunabileceğine işaret etmiştir: "(...) madde metninde kişisel verilerle ilgili olarak "herkes" tabirinin kullanılması dikkate alındığında, tüzel kişilere ilişkin verilerin de 20. madde kapsamında değerlendirilmesi gerekeceği açıktır." AYM, T.04.12.2014, E.2013/84, K.2014/183, RG T.13.03.2015, S.29294.

¹⁷ Tüzel kişilerin kişisel verilerin korunması kapsamında değerlendirilip değerlendirilemeyeceğine ilişkin tartışma için bkz.: SERT, a.g.e., s.29-31; TAŞTAN, Furkan Güven: *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 2. Baskı, On İki Levha Yayıncılık, İstanbul 2017, s.32-33.

¹⁸ YENİSEY, Feridun: *Kolluk Hukuku*, 2. Baskı, Beta Basım, İstanbul 2015, s.320.

¹⁹ AB hukuku düzenlemelerinde, aşağıda görüleceği üzere veri sorumlusu kavramı yerine Ing. *data controller*, yani veri kontrolörü terimi kullanılmaktadır. Ayrıca, hem GVKT hem de 2016/680 s. Direktif'te veri işlemeye yönelik bu tür işlemlerin amaç ve araçlarının Birlik veya üye devlet yasalarıyla belirlendiği durumlarda, veri sorumlusu veya onun belirlenmesine ilişkin spesifik koşulların] Birlik veya üye devlet yasaları tarafından sağlanabileceği belirtilmiştir.

²⁰ KÜZECİ, a.g.e., s.16, 319.

bu türden işlemlerin tümü veri işlemek anlamına gelmektedir.^{21,22} Benzer tanımlar yabancı hukuk düzenlerinde de yapılmaktadır.

Kişisel verilerin işlenmesinde uyulması gereken birtakım ilkeler vardır. Bu ilkeler, kişisel veri işlemeyi gerektiren faaliyetlerin kendi niteliğinden doğan gerekliliklerin dışında, kişisel verilerin işlenmesinde uyulması gereken bazı kuralları belirlemektedir. *İlk olarak* veriler hukuka ve dürüstlük kurallarına uygun biçimde işlenmelidir. Hukuka uygunluk, yazılı ve yazılı olmayan hukuk kurallarının belirlediği yükümlülük ve ilkeleri ifade ederken; dürüstlük kuralına uygunluk veri sorumlusunun faaliyetlerinde ilgili kişilerin menfaatleri ile makul beklentilerini dikkate almasını ifade eder. *İkinci olarak* veriler gerçekte örtüşür biçimde doğru ve gerektiğinde güncel olarak tutulmalıdır. Bu ilkenin uygulanmasında hem veri sorumlusu ve işleyenin hem de veri sahibinin menfaati vardır. Zira güncel veya gerçek olmayan kişisel verilerin işlenmesi sonucunda yapılacak çıkarım doğru olmayacak; hem amaca ulaşılamamış hem de veri sahibinin hakları ihlal edilmiş olacaktır. *Üçüncü olarak* veriler belirli bir amaç dahilinde toplanmalı; toplandıkları amaca bağlı olarak, bununla sınırlı ve ölçülü biçimde işlenmelidir. Kişisel verilerin bir amaca yönelik olarak işlenmesi ve amaca bağlılık ilkesi, çalışma konumuzun özünü oluşturduğundan aşağıda daha detaylı açıklanacaktır.²³ *Dördüncü olarak*, veriler ilgili mevzuatta öngörülen veya işlendikleri amaç için gereken süre kadar tutulmalıdır. Kişisel verilerin işlenmesinin artık gereksiz olması; amaca ulaşılması yahut amacın ortadan kalkması gibi durumlarda söz konusu veriler somut olayın koşullarına göre silinmeli veya azaltılmalıdır.²⁴ *Beşinci olarak* kişisel verilerin işlenmesinde ölçülülük ilkesi dikkate alınmalıdır. Buna

göre kişisel veriler işleme amacına ulaşılacak kadar toplandıktan sonra amaca ulaşılması için daha azının yeterli olduğu görüldüğünde, veriler ‘azaltılmalıdır’. GVKT m.5/1-c’de bu ilke, verilerin “işlendikleri amaç için uygun, ilgili ve gerektiği kadarıyla sınırlı” şeklinde düzenlenmiştir.

Yukarıda belirtilen ilkelerin yanı sıra verilerin işlenmesinde şeffaflık ilkesi de kişisel verilerin işlenmesinde uygulanan ilkelerdendir. Şeffaflık ilkesi doğrultusunda kişisel verilerinin hangi amaçlarla, kimler tarafından, ne şekilde, ne kadar süre işleneceği/işlendiği hakkında ilgili kişi bilgilendirilmelidir. Bu, ilgili kişinin diğer haklarını etkili biçimde kullanabilmesinin ön koşuldur. İşin doğası gereği bildirim uygulanmadığı faaliyetlerde veri sorumluları gizliliği sağlamaya yönelik tedbirleri almalıdır.²⁷ Ayrıca, ilgili kişinin rızasının alınması da bir diğer önemli ilkedir. Rızanın geçerli olması için gerçekleştirilecek faaliyetin içeriği, amacı, süresi, verilerin kullanılacağı işler konusunda bilgilendirilmiş olması ve rızanın aydınlatılmış iradeye dayanması gerekir.²⁸ KVKK m.5’te kişinin açık rızası olmaksızın kişisel verile-

²⁵ Veri asgarileştirilmesi (İng. *data minimisation*) olarak da adlandırılan bu kavrama göre, yalnızca amaca ulaşılması için ihtiyaç olduğu kadar veri toplanmalıdır. Bu verilerin toplandıktan sonra amaca ulaşılması için daha azının yeterli olduğu görüldüğünde, veriler ‘azaltılmalıdır’. GVKT m.5/1-c’de bu ilke, verilerin “işlendikleri amaç için uygun, ilgili ve gerektiği kadarıyla sınırlı” şeklinde düzenlenmiştir.

²⁶ AŞIKOĞLU, Şehriban İpek: *Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri*, On İki Levha Yayıncılık, İstanbul 2018, s.75-77; KÜZECİ, a.g.e., s.200-216; ÖNGÜN AYÖZGER, Çiğdem: *Kişisel Verilerin Korunması Hukuku - Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil*, 2. Baskı, Beta Yayıncılık, İstanbul 2019, s.138-145; AKDAĞ, Türk Ceza Kanunu Kapsamında, s.71-79; SERT, a.g.e., s.75-91; TAŞTAN, a.g.e., 48-53; AKGÜL, Aydın: *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması - Personal Data Protection*, Beta Yayıncılık, İstanbul 2014, s.125-133; DEVELİOĞLU, a.g.e., s.47.

²⁷ SERT, a.g.e., s.91.

²⁸ AKDAĞ, Türk Ceza Kanunu Kapsamında, s.80-82; ÖNGÜN AYÖZGER, a.g.e., s.135, 150-151.

²¹ KÜZECİ, a.g.e., s.14-15.

²² AKDAĞ, Hale: *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, Adalet Yayınevi, Ankara 2013, s.71.

²³ Bkz. AŞ.: § III/C-1.

²⁴ Unutulma hakkı ile ilgili değerlendirmeler için bkz.: SERT, a.g.e., s.82-88.

rin işlenemeyeceği kuralı benimsenmiş, rızanın aranmayacağına kanunlarda açıkça öngörülmesi gibi durumlar istisna hükümler olarak aynı fıkarda *numerus clausus* biçimde sayılmıştır. İfade edilmelidir ki, çalışma konumuz olan adli ve önleyici amaçla kişisel verilerin işlenmesinde faaliyetlerin niteliği dolayısıyla ilgili kişinin rızasının çoğunlukla aranmaması doğaldır. Ancak Kanun'un 5. maddesinde kişisel verilerin işlenmesinde rıza koşulu bulunduğundan, rıza olmaksızın işleme ancak 5. maddenin 2. fıkrasında sayılan istisnai durumların birinin varlığı halinde mümkün olacaktır. Nitekim aşağıda görüleceği üzere, 28. maddede sayılan kısmen istisna tutulan durumlar da 5. maddenin uygulanmasını engellemektedir. Dolayısıyla KVKK hükümlerinden kısmen istisna tutulan faaliyetler hakkında da 5. madde hükmü uygulanacak ve verilerin işlenmesi için açık rıza yahut kanunda bunun gerekmediğinin açıkça belirtilmiş olması aranacaktır; aksi hâlde verilerin işlenmesi -kanunda bir değişiklik yapılmadıkça- mümkün görünmemektedir.

Kişisel verilerin işlenmesinde veri güvenliği ilkesinin de üzerinde durulması isabetli olacaktır. Veri güvenliği, kişisel verilerin korunmasından farklı olup; kişisel verilerin kaybolmasına, dağıtılmasına, değiştirilmesine, bozulmasına ve yok edilmesine, üçüncü kişilerin bilinçli veya bilinçsizce izinsiz erişimine karşı korunması için gerekli idari ve teknik tedbirlerin alınmasını gerektirir.²⁹ Ayrıca veri sorumlusunun gerekli sistem güvenliğini sağlamanın yanında, veri işleyen denetlenmesi de bu ilke kapsamında değerlendirilebilir.³⁰

Kişisel verilerin, amacı ne olursa olsun bir gün gerekebileceği düşüncesine dayanarak devamlı saklanması kabul edilemez. Bu durum kişinin maddi ve manevi bütünlüğünü, bireysel özerkliğini, kendini geliştirme³¹ ve verilerinin ka-

derini belirleme hakkını ihlal eder.³² Gerçekten, örneğin bir gün suç işlenebileceği düşüncesine dayanarak kişisel verilerin biriktirilmesi adeta bir *panoptikon* oluşturmaktır. Bu hâlde insanlar; davranış biçimleri, günlük rutinleri, alışkanlıkları vb.nin devamlı olarak gözetlendiğini bildiğinden toplumsal davranış kalıplarından sapmama eğilimi göstereceklerdir.³³

C. Kişisel Verilerin İşlenme Amacı ve Amaca Bağlılık İlkesi

1. Kavram

Kişisel verilerin işlenebilmesi bunların açık, belirli ve meşru amaçlarla elde edilmesini ve amaca bağlılık ilkesine uyulmasını; yani elde edildikleri amaç dışında kullanılmamalarını gerektirir. Verilerin sonraki işleme amaçları, baştaki elde edilmiş amacıyla uyumlu ve orantılı olmalı, veriler bu amaç dışında kullanılmamalıdır. Verilerin başlangıçta başka bir meşru amaç için elde edilmiş olmasına dayanarak bu yeni ve farklı bir amaçla işlenmesi bu ilkeyi ihlal edecektir.³⁴ Bu bağlamda veri sorumlusunun amaca ulaşmak için işleme konu edilecek kişisel verileri işlemenin gerçekten gerekli olup olmadığını da tespit etmesi gerekir.

Verilerin elde edilme amacının belirli ve açık olması, hukuki metinlerde (hem ilgili mevzuat, hem de sözleşmeler vb.) kişisel verilerin tam olarak hangi amaçlarla işleneceğinin net bir şekilde ifade edilmesini; muğlak ifadelerden kaçınılmasını gerektirir. Bu amaç, ilgililerin görebileceği ve anlayabileceği şekilde açıkça verilerin toplanmasından önce veya sırasında belirtilmelidir.

²⁹ ERDEM, Mustafa Ruhan: *Ceza Muhakemesinde, Organize Suçlulukla Mücadelede Gizli Soruşturma Tedbirleri*, Seçkin Yayıncılık, Ankara 2001, s.306 vd., 385; BAŞALP, Nilgün: *Kişisel Verilerin Korunması ve Saklanması*, Yetkin Yayınları, Ankara 2004, s.38.

³⁰ KIZILIRMAK, Baran: "Önleyici Amaçla Elde Edilen Verilerin Ceza Muhakemesinde Kullanılabilirliği", *İstanbul Üniversitesi Sosyal Bilimler Enstitüsü*, Yayınlanmamış Yüksek Lisans Tezi, 2018, s.184 d.n.; KÜZECİ, a.g.e., s.25.

³¹ *Handbook on Data Protection Law*, Luxembourg: Publications Office of the European Union, 2018, s.123. https://www.echr.coe.int/Documents/Handbook_data_protection_02ENG.pdf (çevrim içi), E.T. 20.10.2019, 13:30.

²⁹ AKGÜL, a.g.e., s.146; SERT, a.g.e., s.96; ÖNGÜN AYÖZGER, a.g.e., s.145-146.

³⁰ AKDAĞ, *Türk Ceza Kanunu Kapsamında*, s.82 vd.; SERT, a.g.e., s.95-97.

³¹ KÜZECİ, a.g.e., s.203.

Amacın meşru olmasından kasıt, verilerin elde edilmesindeki amacın yasal bir dayanağa sahip olması; bu kurallara ve ilkelere uyum içinde hareket edilmesi, amacı aşan faaliyetlerden kaçınılmasıdır.³⁵ Dolayısıyla yasal olmayan bir amaçla verilerin elde edilmesi mümkün değildir.

Kişisel verilerin elde edildikleri amaç doğrultusunda kullanılmalrı, bu faaliyetin hedeflerine ulaşmasının doğal koşuludur. Ancak bunun yanında ilgili kişilerin, verilerinin hangi amaçlarla işlendiğini bilmelerini de gerektirir. Zira rızasının arandığı durumlarda, ilgili kişi veri işleme amacını bilmesi halinde iradesini bilinçli olarak açıklayabilecektir. Bu koşul ilgili kişinin veriler üzerindeki denetimini gerçekleştirebilmesi için zaruridir.³⁶ Amacın değişmesi durumunda kişinin rızasına yeniden başvurulacaktır.³⁷ Ancak bu durum rızanın aranmadığı hallerde amacın serbestçe değiştirilebileceği anlamına gelmemektedir. Nitekim verilerin amaç dışı kullanımı keyfiyete, ölçsüzlüğe ve verilerin kontrolünün kaybedilmesine neden olabilecektir.

Amaç veri elde edilmeden önce belirlenmiş olmalı; veriler de elde edildikten sonra bu amaca aykırı biçimde kullanılmamalıdır.³⁸ Şayet elde edilen veriler başka amaçlarla kullanılacaksa, bu amacın verilerin elde edilmesindeki amaçla bağdaşması, ona aykırı olmaması gerekir.³⁹ Gerçekten, hem GVKT’de hem de 2016/680 s. Direktif’de kişisel verilerin *amaçlar dışında işlenmemesi* değil; *amaçlarla uyumlu olmayan şekilde işlenmemesi* gerektiği ifade edilmektedir.⁴⁰ Kanımızca bu, verilerin amaç dışında kullanılmasına göre daha esnek bir yaklaşım sağlamaktadır. Verilerin dar anlamda yalnızca ilk baştaki amaca sadık kalınarak değil, aynı zamanda o amaçla uyumlu olan, ona yakın ve meşru amaçlarla da

kullanılmasını mümkün kılmaktadır.⁴¹ Kanımızca bu uyumun ölçü ve sınırının iyi belirlenmesi, ilkenin özünü yitirmemesi için gereklidir.

Bir kişisel verinin o veriyi elde etmeye yetkili resmi mercilerden biri tarafından elde edilmiş olması, bu verinin başka amaçlarla da sınırsızca veya diğer merciler tarafından da kullanılabilceği anlamına gelmez. Bu durum, insan haklarına saygılı demokratik hukuk devleti olmanın gereğidir. Kişisel verilerin sırf elde edilmiş olmasına, bir bilginin sırf biliniyor olmasına dayanarak, bu verilerin tüm mercilerle paylaşılması; ölçsüz ve sınırsız biçimde kullanılması herkes hakkında her şeyi bilen otoriter bir devlet yapısına kapı aralar. Zira her an farklı yetkili merciler, kişilerle ilgili farklı bilgiler elde etmektedir. Bu bilgilerin tümünün toplanarak bir havuzda birleştirilmesi insan haklarına ve özgürlüklere saygılı bir devlette düşünülemez.⁴²

Açıklananlar doğrultusunda amaca bağlılık ilkesi önleyici amaçla elde edilen verilerin önleyici amaçla işlenmesini; suçları aydınlatma amacıyla elde edilenlerin adli amaçlar doğrultusunda işlenmesini gerektirir. Örneğin, polisin önleyici amaçlı ve istihbari yetkilerini düzenleyen PVSK⁴³ ek 7. maddesindeki faaliyetleriyle ilgili olarak 7. fıkrada *“Bu madde hükümlerine göre yürütülen faaliyetler çerçevesinde elde edilen kayıtlar, birinci fıkrada belirtilen amaçlar dışında kullanılamaz”* denilmek suretiyle amaca bağlılık ilkesine yer verilmiş; önleyici amaçla elde ettiği verilerin adli amaçla kullanılması yasaklanmıştır. Nitekim Yargıtay’ın içtihatları da söz konusu faaliyet aracılığıyla elde edilen verilerin delil olamayacağı yönündedir.⁴⁴

³⁵ KÜZECİ, a.g.e., s.203-204.

³⁶ KÜZECİ, a.g.e., s.206-207.

³⁷ SERT, a.g.e., s.78; TAŞTAN, a.g.e., s.51.

³⁸ AKDAĞ, Hale: “Türk Ceza Hukukunda Kişisel Verilerin Korunması İlkeleri”, Prof. Dr. Nevzat Toroslu’ya Armağan, C.1, Ankara, Ankara Üniversitesi Basımevi, 2015, s.32-34.

³⁹ AKDAĞ, Türk Ceza Kanunu Kapsamında, s.74.

⁴⁰ GVKT m.5/1-b & 2016/680 s. Direktif m.4/1-b.

⁴¹ KIZILIRMAK, a.g.e., s.186.

⁴² KIZILIRMAK, a.g.e., s.87.

⁴³ 2559 sayılı Polis Vazife ve Salahiyet Kanunu, RG T.14.07.1934, S.2751.

⁴⁴ YCGK, T.17.05.2011, E.2011/9-93, K.2011/95, www.kazanci.com, (çevrim içi), E.T. 20.10.2019, 13:30. Ancak bu verilerin başlangıç şüphesi kabul edilip, soruşturma başlatılabileceği yönünde içtihatları mevcuttur. Tartışmalar için bkz.: KIZILIRMAK, a.g.e., s.199 vd.

2. Faaliyetlerin Amaca Göre Sınıflandırılması

Yetkili resmi merciler, faaliyetlerini gerçekleştirirken kişisel verileri çeşitli amaçlar doğrultusunda işlemektedir. Örneğin suçların aydınlatılmasına yönelik adli nitelikli faaliyetlerde bulunulabileceği gibi, suç işlenmesini önlemeye yönelik işlemler de gerçekleştirilebilir. Bunun yanında kamu hizmetlerinin sağlanmasına yönelik çeşitli idari faaliyetlerde de kişisel veriler farklı (idari) amaçlarla işlenebilmektedir. Buna örnek olarak *e-devlet* kapsamında, Ulusal Yargı Ağı Projesi (UYAP), Merkezi Nüfus İdaresi Sistemi (MERNİS) gibi sistemler gösterilebilir.⁴⁵ Konumuz bakımından yalnızca adli ve önleyici amaçlı faaliyetlerde ‘amaç’ odaklı bir inceleme yapılacak, konuyla ilgisi bakımından istihbari faaliyetlere de yer verilecektir. En yalın ifadeyle, önleyici amaçlı faaliyetler suç öncesi aşamada suçların işlenmesinin önlenmesi amacıyla gerçekleştirilen ve idarenin görevine giren işleri; adli nitelikli faaliyetler ise suç sonrası aşamada, suçların aydınlatılması amacıyla, ceza muhakemesi kapsamında gerçekleştirilen ve adli mercilerin görevine giren işleri belirtir.

a. Adli Amaçlı Faaliyetler

Adli amaçlı faaliyetler bir suç işlendiğinin yetkili mercilerce öğrenilmesi üzerine başlayan, onu aydınlatmaya yönelik faaliyetlerdir. Ceza Muhakemesi Kanunu’nun⁴⁶ 160. maddesinde *ihbar veya başka bir suretle bir suçun işlendiği izlenimini veren hâli öğrenen C. savcısının hemen işin gerçeğini araştırmaya başlayacağı* düzenlenmiştir. Buna göre C. savcısı herhangi bir yoldan bir suç işlendiğine ilişkin ‘başlangıç şüphesini’ edindiğinde,⁴⁷ adli nitelik taşıyan araştırma faaliyetlerine başlayacaktır. Bu aşamadan itibaren adli merciler tarafından o suçu aydınlatmaya; yani işlenip işlenmediğini, işlendiyse kim(ler) tarafından, ne za-

man, nerede, ne şekilde, kime karşı işlendiğini vb. ortaya çıkarmak amacıyla gerçekleştirilecek faaliyetlerin tümü adli amaç taşımaktadır.⁴⁸ Öğretide bir yazarın deyişiyle bu şekilde basit (başlangıç) şüphenin öğrenilmesiyle birlikte kontak anahtarı çevrilecek ve adli yetkiler doğacaktır.⁴⁹ Bu noktadan itibaren adli merciler yetki sahibidir.^{50,51}

O halde adli amaçlı faaliyetlerden kasıt, bir suç işlendiğinin tespiti veya aydınlatılmasına yönelik yetkili merciler (C. savcısı, hakim veya mahkeme, kolluk) tarafından gerçekleştirilen işlemlerin tümüdür. Örneğin, olay yeri inceleme, tanık dinleme, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, arama ve el koyma, keşif, beden muayenesi bu kapsamda sayılabilir. Bu yöntemler aracılığıyla elde edilen kişisel veriler çalışmamızın konusunu oluşturmaktadır.

⁴⁸ KATOĞLU, Tuğrul: *Polis Vazife ve Salahiyet Kanunu ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun Tasarısı Hakkında Hukuki Görüş*, Türkiye Barolar Birliği Yayını, Ankara 2014, s.6, 19.

⁴⁹ YENİSEY, Feridun: “Tehlikeyi Önleyici Polis ve Adli Polis”, *Bavyera Polis Kanunu*, (Çev.: Feridun Yenisey), Asayiş Daire Başkanlığı, 2007, s.9.

⁵⁰ Hukukumuzda C. savcısı soruşturma evresinin ‘efendisi’ konumundadır. Kolluğun, (CMUK’tan ve Alman hukukundan farklı olarak) C. savcısının bilgisi ve talimatları olmaksızın soruşturma işlemleri yapabilmesi kural olarak mümkün değildir. Kanımızca PYSK ek m.6/18: “Polis, sanal ortamda işlenen suçlarda, yetkili Cumhuriyet başsavcılığının tespiti amacıyla, internet abonelerine ait kimlik bilgilerine ulaşmaya, sanal ortamda araştırma yapmaya yetkilidir” hükmü bu kuralın bir istisnasını oluşturmaktadır.

⁵¹ Öğretideki hakim görüşün aksine, biz mevcut hukuki düzenlemeler karşısında “basit şüpheyi yaratacak delillerin araştırılması” şeklinde gerçekleştirilen ve soruşturma evresine dahil edilmeyen “bilgi toplama” adı verilen bir “geçiş döneminin” de mümkün olmadığını düşünmekteyiz. Nitekim basit şüphe ya oluşmuştur ya da oluşmamıştır. Soruşturma, CMK m.158/6 uyarınca soruşturma yapılmasına yer olmadığına karar verilmedikçe, suç işlendiği izlenimi veren halin öğrenilmesi anında başlamış olacaktır. Türk hukukunun aksine Alman hukukunda (StPO §152/2) soruşturmanın başlatılmasında “somut dayanak noktalarının tespiti” aranmakta; bu doğrultuda başlangıç şüphesinin varlığını ortaya koymak amacıyla birtakım çalışmaların yapılabileceği ifade edilmektedir. Başlangıç şüphesinin tespiti amacıyla araştırma yapılmasına ilişkin tartışmalar için bkz.: KIZILIRMAK, a.g.e., s.13 vd.

⁴⁵ DAĞ, Güray: “Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması”, *Marmara Üniversitesi Sosyal Bilimler Enstitüsü*, Yayınlanmamış Doktora Tezi, 2011, s.126; KÜZECİ, a.g.e., s.449.

⁴⁶ 04.12.2004 tarih ve 5271 s. Ceza Muhakemesi Kanunu, RG T.17.12.2004, S.25673.

⁴⁷ CENTEL, Nur / ZAFER, Hamide: *Ceza Muhakemesi Hukuku*, 14. Baskı, Beta Yayıncılık, İstanbul 2017, s.88.

b. Önleyici Amaçlı Faaliyetler

Adli amaçlı faaliyetlerin kapsamının belirlenmesindeki kolaylığa karşılık, önleyici amaçlı faaliyetlerde “önlenmeye çalışılan nedir?” sorusunun yanıtı kolayca verilememektedir. Nitekim ceza ve ceza muhakemesi hukukunun çizgisinin giderek öne kayması, cezalandırılabilir alanın genişlemesi, ceza ve ceza muhakemesi hukuku yöntemlerinden belirli olgularla mücadele adına önleyici amaçla da yararlanılması ve ceza hukukunun *ultima ratio* özelliğinden taviz verilmesi bu sorunun yanıtını güçleştirmektedir.

Asıl olan suçların önlenmesi iken; zamanla devletlerin suç ve suçlulukla mücadele politikalarındaki değişime paralel olarak, bir zarar ihtimali olan tehlikenin önlenmesine kayma yaşanmış; hatta suç işleme tehlikesi dahi ortaya çıkmadan önce tehlike tehlikesinin önlenmesinden bahsedilir olmuştur.⁵² Özünde risk kavramına ve öğretide ifade edildiği şekilde ‘risk ceza hukukuna’ karşılık gelen bu durum, tehlikenin kaynağına müdahaleyi değil; riske neden olabilecek faktörlerin en başından ortadan kaldırılmasını amaçlar.⁵³ Bu eğilim eşitlik ilkesini, temel hak ve özgürlükleri gözetten bir hukuk devletinde hiçbir şekilde benimsenemez.

Suç öncesi alanda bir suçun işlendiğine dair şüphe henüz ortaya çıkmamıştır. Bu alanda kamu düzeni ve kamu güvenliği sağlanmaya, zararlar meydana gelmeden önlenmeye, tehlikelerin zarar haline gelmeden ortadan kaldırılmasına çalışılır. Devletler ulusal güvenliği, kamu düzeni ve güvenliğini sağlamak, suçlulukla mücadele etmek; bunun yanı sıra kamu hizmetlerinin yerine getirilmesinde stratejiler oluşturmak ve plan yapmak amacıyla kişisel ve kişisel olmayan verileri işler. Bu bağlamda suç öncesi alanda idari mercilerin suç işlenmesinin önlenmesi, caydırıcılık sağlanması veya suç önleme stratejilerinin oluşturulması gibi amaçlarla kişisel veriler toplanmakta ve kullanılmaktadır.

⁵² YENİSEY, *Kolluk Hukuku*, s.152.

⁵³ ERMAN, Barış: “Ceza Hukukunun Dönüşümü”, *YÜHFD (Prof. Dr. Duygun Yarsuvat’a Armağan)*, C.IX, S.2, 2012, s.456-459.

Önleyici tedbir kavramı esasen kamu düzeni ve güvenliği açısından zarar doğurucu etmenlerin önlenmesi, tehlike doğuranlarına -zarar haline gelmeden- tehlikenin kaynağına müdahale ederek ortadan kaldırılması için uygulanan yöntemleri ifade etmektedir. Çalışmamızda 2016/680 sayılı Direktif üzerinden değerlendirmelerde bulunduğumuzdan ve bu Direktif’te de “suçların önlenmesinden” söz edildiğinden; önleyici amaçlı faaliyet, içerik bakımından yalnızca suç işlenmesinin önlenmesini ifade etmek üzere kullanılmaktadır.⁵⁴

Bu doğrultuda suçların işlenmeden önlenmesi amacıyla kişisel verilerin işlenmesi önleyici amaçlı işlemdir. Önleyici kolluk faaliyetlerinde uygulanacak stratejileri belirlemek gibi amaçlarla veri işlenmesi ise daha ziyade istihbari faaliyet - istihbarat çarkı kapsamında değerlendirilir. Bunun tam olarak bir önleyici amaç olduğundan bahsetmek güçtür. Zira ikincisinde belirli yahut kolluğun bilgisi ve tecrübesinin yanında bilimsel yöntemlerin de yardımıyla belirlenebilecek bir suçun önlenmesinden ziyade, suçlulukla mücadele amacıyla gerçekleştirilen bir faaliyet söz konusudur. Bu, kamu düzeni ve güvenliğini korumaya yöneliktir. Kısacası, suç işlenmesinin önlenmesi amacıyla kişisel verilerin işlenmesi önleyici amaçlı bir faaliyet olsa da; suç öncesi alanda yetkili merciler tarafından gerçekleştirilen her işlem önleyici tedbir / önleyici amaçlı faaliyet olarak kabul edilemez. Pratikte uygulanan yöntemin tam olarak bir ‘önleyici tedbir’ veya ‘önleyici amaçla gerçekleştirilen faaliyet’ olup olmadığının tespiti önem arz etmektedir.

Açıklananları örneklendirmek gerekirse; hükümlülerin telefon görüşmelerinin dinlenmesi ve kayda alınması (CGİK⁵⁵ m.66/1) kişisel verilerin önleyici amaçla işlenmesidir. Yine, 5397 s.k. ile polise (PVSK ek m.7/2) ve jandarmaya (JTK⁵⁶

⁵⁴ Günümüzde çok sayıda farklı faaliyeti ifade etmek üzere kullanılan ‘önleyici tedbir’den ne anlaşılması gerektiği hk. bkz.: KIZILIRMAK, *a.g.e.*, s.40-41, 70-73.

⁵⁵ Jandarma Teşkilat, Görev ve Yetkileri Kanunu, 10.03.1983 tarih ve 2803 sayılı, RG T.10.03.1983, S.17985.

⁵⁶ 13.12.2004 tarih ve 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun, RG T.29.12.2004, S.25685.

ek m.5/1) tanınan telekomünikasyon yoluyla yapılan iletişimin denetlenmesi yetkisi de, istihbari nitelikli olmakla birlikte önleyici amaçlı bir faaliyettir. Zira, hükümde bu yetkinin yalnızca belirli suçların önlenmesi⁵⁷ amacıyla kullanılabileceği ve elde edilen verilerin de amaca bağlılık ilkesine uygun olarak önleme amacı dışında kullanılmaması⁵⁸ öngörülmüştür. Ancak PVSK ve JTK kapsamında tanınan bu yetkiler, önleyici amaçlı faaliyetler ile istihbari faaliyetlerin birleşmesinin bir görünümüdür. Bu soruna aşağıda istihbari faaliyetler başlığında değinilecektir.

1774 s. Kimlik Bildirme Kanunu'na göre, araç kiralama veya otelde konaklama gibi durumlarda kolluğun bilgisayar terminallerine kişisel veriler aktarılmaktadır. Bu veriler (çaydırcılık

da sağlamak suretiyle) önleme işlevinin yanı sıra, ileride işlenecek suçların aydınlatılmasında da kullanılmaktadır. Dolayısıyla bu şekilde işlenen veriler yalnızca önleme amacına hizmet etmektedir. Benzer bir durum PVSK m.5 uyarınca polisin belirli kişilerin parmak izi ve fotoğrafları bir sisteme kaydetmesinde de görülmektedir. Burada hem önleyici, hem de adli nedenlerle parmak izi ve fotoğraflar alınarak bir sisteme kaydedilmekte; üstelik bunların hangi amaçla alındığı (hüküm gereği) kaydedilmemektedir. Bir diğer benzer sorun, Toplantı ve Gösteri Yürüyüşleri Kanunu'nun 11. maddesinde bulunmaktadır. Burada henüz basit şüphenin dahi olmadığı suç öncesi alanda, polise toplantı ve gösteri yürüyüşlerinde ses ve görüntülü kayıt yapma yetkisi tanınmakta; bu kayıtların yalnızca adli amaçla kullanılabilmesi belirtilmektedir. Ayrıca burada elde edilen kişisel verilerin hangi merciler tarafından, ne kadar süre, ne şekilde; işlemeye tabi olup olmayacağı belirlenmemiştir.

Hukukumuzda yaygın biçimde uygulanan; öyle ki Yargıtay'ın görüntüler incelenmeden verilen mahkumiyet kararlarını hukuka aykırı gördüğü;⁵⁹ ancak bir yasal dayanağı bulunmayan MOBESE'ye de değinmek gerekir. MOBESE'ye entegre olan kapalı devre kameralar ile kişisel verilerin devamlı olarak toplandığına ve işlendiğine şüphe yoktur. MOBESE ile veri elde edilmesinin amacı konusunda öğretilerde yaygın biçimde temel amacın suçları önlemek; ikincil amacın işlenmiş suçların aydınlatılması olduğu belirtilmekte; nitekim uygulamada da genellikle bu yönde kullanılmaktadır.⁶⁰

⁵⁷ Bu kapsamda belirtilen suçlar: *CMK'nın casusluk suçları hariç, [mülga]250'nci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçlar ile bilişim suçlarıdır.* Ne var ki CMK'nın 250. maddesi, 02.07.2012 tarih ve 6352 sayılı kanunun 105. maddesi ile yürürlükten kaldırılmıştır. Günümüzde, 250. maddede yer alan suçlara yapılan atıf konusundaki boşluğu doldurmak amacıyla, 21.02.2014 tarih ve 6526 sayılı kanunla, TMK'ya geçici 14. madde eklenmiştir. Bu maddenin 6. fıkrası şu şekildedir: *"Mevzuatta Ceza Muhakemesi Kanununun mülga 250'nci maddesinin birinci fıkrası kapsamına giren suçlar ile Terörle Mücadele Kanununun 10'uncu maddesinin dördüncü fıkrası kapsamına giren suçlara yapılan atıflar, Türk Ceza Kanununda yer alan;*

a) Örgüt faaliyeti çerçevesinde işlenen uyuşturucu ve uyarıcı madde imal ve ticareti suçu veya suçtan kaynaklan malvarlığı değerini aklama suçu,
b) Haksız ekonomik çıkar sağlamak amacıyla kurulmuş bir örgütün faaliyeti çerçevesinde cebir ve tehdit uygulanarak işlenen suçlara,
c) İkinci Kitap Dördüncü Kısımın Dört, Beş, Altı ve Yedinci Bölümünde tanımlanan suçlara (305, 318, 319, 323, 324, 325 ve 332'nci maddeler hariç), yapılmış sayılır." Sonuç olarak, CMK m.250'de sayılan suçlara yapılan atıflar için günümüzde [19.10.2019] bu sayılan suçlar geçerlidir (Örgüt faaliyeti çerçevesinde işlenen uyuşturucu ve uyarıcı madde imal ve ticareti suçu veya suçtan kaynaklanan malvarlığı değerini aklama suçu; haksız ekonomik çıkar sağlamak amacıyla kurulmuş bir örgütün faaliyeti çerçevesinde cebir ve tehdit uygulanarak işlenen suçlar; (TCK m.305, 318, 319, 323, 324, 325, 332 ve casusluk suçları) haricinde, Devlet'in güvenliğine, anayasal düzene ve bu düzenin işleyişine, milli savunmaya ve devlet sırlarına karşı suçlar; bilişim suçları).

⁵⁸ PVSK ek m.7/7; JTK ek m.5/6.

⁵⁹ Örneğin: *"(...)adresleri gösterir kamera görüntüleri ve mobese görüntüleri araştırılıp incelendikten ve tanıkların dinlenmesinden sonra sanığın hukuki durumunun takdiri gerekir."* Y.13.CD., T.22.01.2015, E.2014/19442, K.2015/1604, www.kazanci.com (çevrim içi), E.T. 20.10.2019, 13:30.

⁶⁰ ÖZBEK, Veli Özer / DOĞAN, Koray / BACAŞIZ, Pınar / TEPE, İlker: *Ceza Muhakemesi Hukuku*, 10. Baskı, Seçkin Yayıncılık, Ankara 2017, s.172-173; ÖZKAN, Halid: *"MOBESE İzleme ve Kayıtlarının Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi"*, CHD, S.30, 2016, s.65; YENİSEY, Kolluk Hukuku, s.357; ŞEN, Ersan: *"Mobese ve Kamera Sistemi ile İzleme"*, Yorumluyorum 12, Seçkin Yayıncılık, Ankara 2016, s.119.

Yukarıda açıklanmaya çalışılan sorunları göz önünde bulundurarak ifade etmek gerekirse, hukukumuzda önleyici amaçla kişisel veri elde etmeye yönelik yöntemler yalnızca önleyici amaçla bağlantılı olarak kullanılmamaktadır. Genel eğilim bu verilerin başka alanlarda da değerlendirilmek istenmesi yönündedir. Henüz KVKK hükümlerine dahi değinmeksizin yukarıda belirtilen bu (ve diğer pek çok) yöntemde hem kişisel hem de kişisel olmayan verilerin işlenmesine yönelik düzenlemelerin eksik olduğunu ifade etmek gerekir. Bu yöntemlerde öncelikle amaç sorunu çözülmeli; verilerin tam olarak hangi meşru amaçlarla elde edileceği ve hangi amaçlarla kullanılacağı; hukuki belirlilik ilkesinin gereği olarak açık ve belirli biçimde düzenlenmelidir. Ardından, kişisel verilerin işlenmesine ilişkin diğer sorunlar olan veri işleyen belirlenmesi, verilerin tutulacağı süre, veri güvenliği vb. de kanunla açıkça belirtilmelidir. Nitekim Anayasa'nın 20. maddesinin 3. fıkrası⁶¹ (yeterli bir düzenleme olmasa dahi) kişisel veri işlemede amacın belirliliğinin önemini göstermektedir.

İfade edilmelidir ki, her ülkenin ceza adalet sistemi farklı olduğu gibi, idari merciler ile adli merciler arasındaki yetki bölüşümü de farklıdır. Bununla birlikte, suç işlenmesini önleyici faaliyetler ile adli faaliyetler arasındaki ayrım temelde burada belirtildiği şekildedir.⁶² Aşağıda incelenen yabancı hukuk metinleri bu doğrultuda değerlendirilmelidir.

c. İstihbari Faaliyetler

İstihbarat faaliyeti en basit ifadeyle, karar alıcılara sunulmak üzere toplanan ve değerlendirilen bilgilerin döngüsünü ifade eder. İstih-

⁶¹ Anayasa m.20/3: “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar (...)”.

⁶² Bununla birlikte, Türk hukukunda kolluk, adli ve idari kolluk şeklinde teşkilat bünyesinde ayrılmamıştır. Kolluğun esas görevi idari niteliklidir, bir suç ile karşılaştığında veya C. savcısının emirlerinin icrası kapsamında adli görevlerini yerine getirir.

barat çarkı da denilen bu kesintisiz döngüde, karar alıcıların amaçları doğrultusunda veriler toplanır, rafine edilir, sunulur ve bu bilgiler doğrultusunda yeni ihtiyaçlara yönelik yeni veriler toplanır.⁶³ Görüldüğü üzere istihbarat bir amaç değil, bir yöntemdir. Oysa önleyici amaçla veri elde edilmesinden söz ederken suç işlenmesinin önlenmesi **amacına** yönelik gerçekleştirilen faaliyetler kastedilmektedir; bu faaliyetlerdeki yöntem, somut olaya göre değişiklik gösterecektir.

İstihbarat genellikle iç güvenlik, dış güvenlik, askeri istihbarat gibi ayrımlara tabi tutulmaktadır. Devletler ulusal güvenliğine, anayasal düzenine, bağımsızlığına vb. tehdit oluşturan unsurları engellemek amacıyla veya suçla mücadele politikalarını belirlemek gibi amaçlarla bilgiye ihtiyaç duymakta; yani istihbarata başvurmaktadır. Dolayısıyla istihbari faaliyetler asıl olarak bir suç ile ilgili olmayıp, bu tehditleri yaratabilecek unsurlara yönelmektedir. Ne var ki, bunların bir kısmı aynı zamanda suç olarak düzenlendiğinden, istihbarat faaliyetleri ile önleyici amaçlı faaliyetler genellikle bu noktada (özellikle organize suçluluk noktasında) kesişmekte ve hatta iç içe geçmektedir. Nitekim, önleyici faaliyetleri yürütmekle görevli kolluğa istihbari yetkiler tanınması, kimi istihbarat kuruluşlarıysa operasyonel yetki tanınması bu ikisi arasındaki ayrımı silikleştirmektedir.⁶⁴

⁶³ ÖZDAĞ, Ümit: *İstihbarat Teorisi*, 4. Baskı, Kripto Kitaplar, Ankara 2010, s.371-372; TILISBIK, Niyazi / AKBAL, Özdemir: *Intelligence: İstihbarat ve Türkiye*, İkia Yayıncılık, Konya 2006, s.10 vd.

⁶⁴ Öğretide duvar ilkesi (Alm. *Trennungsgesetz*) olarak ifade edilen kavrama göre, “her şeyi bilen her şeyi yapmamalı, her şeyi yapan her şeyi bilmemelidir.” Yani, istihbarat kuruluşlarıyla operasyonel yetkiye sahip kuruluşların görev ve faaliyet alanı birbirinden ayrılmalıdır. Aksi durumda, *Gestapo* benzeri yapılar ortaya çıkabilir. Konuyla ilgili bkz.: EROĞLU, Fulya: “Örgütlü Suçlarda Yargılama Sistemi”, *Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü*, Yayınlanmamış Doktora Tezi, 2016, s.24 vd.; ÖZBEK, Veli Özer: *Organize Suçlulukla Mücadelede Kullanılan Gizli Görevlinin Görevin Gerektirdiği Suçlar Bakımından Cezalandırılabilirliği*, Yetkin Yayıncılık, Ankara 2003, s.70; VERVAELE, John: “Terrorism and Information Sharing Between the Intelligence and Law Enforcement Communities in the US and the Netherlands”, *Utrecht Law Review*, C.1, S.1, 2005, s.4, <http://doi.org/10.18352/ulr.1> (çevrim içi), E.T. 20.10.2019, 13:30.

Polis ve jandarmaya 5397 s.k. ile tanınan istihbari nitelikli önleyici amaçla telekomünikasyon yoluyla yapılan iletişimin denetlenmesi yetkisi tanınmıştır. Bu yetki MİT'e de tanınmakla birlikte polis ve jandarmanınkinden farklıdır: MİT'in yetkisine casusluk suçları da dahil edilmiştir; ayrıca MİT bu yetkilerini belirlenen suçların önlenmesi amacıyla değil, MİT Kanunu'nun⁶⁵ 4. maddesinde belirtilen görevlerine yönelik olarak istihbarat çalışmaları kapsamında kullanmaktadır. Bir başka ifadeyle, suçların önlenmesinden ziyade; istihbarat üretmeye yönelik olarak ulusal güvenliğin sağlanması amacıyla bu faaliyetleri gerçekleştirmekte ve MİT K.'de kendine tanınan diğer yetkileri kullanmaktadır. Nitekim MİT'in görevi belirli suçların önlenmesi değil; genel manada devletin güvenliğinin sağlanmasıdır. Ancak özellikle organize suçluluk gibi alanlarda önleyici amaçlı faaliyetler ile istihbari faaliyetler kesişmektedir. Aşağıda incelenenekte olan⁶⁶ Direktif'te bahsedilen ulusal güvenliğin sağlanması amacıyla yönelik kişisel veri işleme, özünde burada belirtildiği şekliyle bir gizli istihbarat faaliyetidir.

III. Konu Açısından Önemli Bazı Yabancı Hukuk Düzenlemeleri

2016/680 s. Direktif'in adli ve önleyici amaçla kişisel verilerin işlenmesini hangi boyutta sınırladığı ve ne gibi güvencelere bağlayarak hangi temel ilkelerin uygulanmasını öngördüğünü incelemeye önce, konuyu aydınlatmaya yarayacak başka hukuki metinlere de değinilecektir. Bu doğrultuda sırayla Avrupa İnsan Hakları Sözleşmesi ve Mahkeme'nin adli ve önleyici amaçla kişisel verilerin işlenmesine yaklaşımı ve Avrupa Konseyi bünyesindeki başlıca düzenleme olan 108 numaralı Sözleşme incelenecektir.

A. Avrupa İnsan Hakları Sözleşmesi

Avrupa İnsan Hakları Sözleşmesi'nin (ks. AİHS) 8. maddesinde özel yaşamın gizliliği hak-

kı düzenlenmiş olup, kişisel verilerin korunması hakkı da bu hak kapsamında değerlendirilmektedir. Bu doğrultuda 8. maddenin 2. fıkrasında düzenlenen hakkı sınırlama koşulları, kişisel verilerin korunması bakımından da geçerlidir.

AİHS, kişisel verilerin korunmasında Sözleşme'nin genel kapsamı ve uygulama alanı dışında bir belirleme yapmamakta, özel hukuk yahut kamu hukuku boyutu bakımından ayırmamaktadır. Örneğin adli amaçla kişisel verilerin işlenmesini de yine 8. maddede tanımlanan bu hak ve sınırlama ölçütleri bakımından ele almaktadır. Dolayısıyla, mutlak bir hak olmayan kişisel verilerin korunması da belirli koşullara uyulmak suretiyle sınırlanabilecek, Avrupa İnsan Hakları Mahkemesi'nin (AİHM veya Mahkeme) içtihatları doğrultusunda genel eğilim ve ilkeler belirlenecektir.⁶⁷ Ancak, Mahkeme her ne kadar içtihatlarında kişisel verilerin korunmasına ilişkin hukuki metinleri de gözetse dahi, görevinin AİHS'in 19. maddesi doğrultusunda taraf devletlerin taahhütlerini yerine getirmesini sağlamak olduğu; Sözleşme'nin kişisel verilerin korunmasına ilişkin detaylı bir ölçüt ortaya koymadığını akılda tutmak gerekir.

Adli ve önleyici amaçla kişisel verilerin işlenmesine ilişkin bazı AİHM kararlarına, konuya yaklaşımın görülebilmesi amacıyla yer verilecektir. İlk olarak Mahkeme, kişisel veriler de dahil olmak üzere kişinin haberleşmesinin gizliliğine müdahalede bulunan tedbirlerin uygulanmasında bir kanuni dayanak bulunmadığı durumlarda bu hakkın ihlal edildiğini tespit etmektedir.⁶⁸ Rotaru v. Romanya kararında AİHM, ulusal güvenliği sağlamak amacıyla birtakım gizli yöntemler aracılığıyla veri elde edilmesinin ve saklanması mümkün olduğunu; ancak bu yapılırken kötüye kullanımı engellemek amacıyla güven-

⁶⁵ 01.11.1983 tarih ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu (ks. MİT K.), RG T.03.11.1983, S.18210.

⁶⁶ Bkz. Aş. § IV/D-2, para.14.

⁶⁷ 108 no.lu Sözleşme AİHM'nin yargı yetkisi kapsamında olmasa da, Mahkeme 8. madde kapsamında hakkın ihlal edilip edilmediğini belirlerken 108 no.lu Sözleşme'de belirlenen temel ilkelerden yararlanmaktadır. *Handbook on Data Protection Law*, s.25.

⁶⁸ Satık v. Türkiye (no: 2), Başvuru no: 60999/00, 08.07.2008, para:57, www.hudoc.echr.coe.int (çevrim içi), E.T. 20.10.2019, 13:30.

celerini yanı sıra denetim mekanizmalarının da oluşturulması gerektiğini vurgulamıştır.⁶⁹ Amann v. İsviçre kararında “güvenlik gerekçesiyle” fişlenme olarak bilinen faaliyete ilişkin tespitlerinde Mahkeme, fişlemedeki bilgilerin kullanılması sonucunda kişinin ayrıca bir zorluğa düşmesinin aranmadığını (böyle bir zorluğa düşmüşse ve bu bir hak kaybına neden olmuşsa ayrıca değerlendirilecek şekilde), yalnızca bu şekilde ilgili kişinin verilerinin saklanması da özel yaşamın gizliliği, diğer insanlarla ilişki kurma ve geliştirme hakkına müdahale teşkil ettiğini ve ancak 2. fıkradaki *yasayla öngörülmüş olmak koşuluyla demokratik bir toplumda ulusal güvenlik, kamu güvenliği, düzenin korunması, suç işlenmesinin önlenmesi gibi* koşulların varlığı halinde gerçekleştirilebileceğini belirtmiştir.⁷⁰

B. Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin (108 no.lu) Sözleşme

28 Ocak 1981’de imzaya açılan Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin (108 no.lu) Avrupa Konseyi Sözleşmesi, bireyleri kişisel verilerin toplanması ve işlenmesinden doğabilecek kötüye kullanmalara karşı koruyan ve aynı zamanda kişisel verilerin sınır ötesi akışını düzenlemeyi amaçlayan ilk bağlayıcı uluslararası metindir.⁷¹

Sözleşme Avrupa Konseyi üyesi olmayan devletlerin de imzasına açılmıştır.⁷² Özellikle veri

dolaşımının sınır aşan özelliği düşünüldüğünde, kişisel verilerin korunmasının yalnızca bir devletin faaliyet alanında olmadığı gözetilerek, uluslararası nitelikte bağlayıcılığı bulunan bu Sözleşme hazırlanmıştır. Yine konunun önemi ve gelişimine paralel olarak Sözleşme’nin yenilenmesine yönelik çalışmalar doğrultusunda bir ek protokol (Council of Europe Treaty Series no. 223)⁷³ oluşturulmuştur.⁷⁴ Bu Protokol, Avrupa Konseyi Bakanlar Komitesi tarafından 18 Mayıs 2018’de kabul edilmiş; 19.10.2019 tarihi itibarıyla 34 devlet (31’i Avrupa Konseyi üyesi) tarafından imzalamış; fakat henüz yürürlüğe girmemiştir.⁷⁵ Türkiye ise henüz imzalamamıştır.⁷⁶

108 numaralı Sözleşme adli ve önleyici amaçla işlenen kişisel verilerin korunmasına, yaygın yaklaşıma uygun olarak birtakım istisnalar öngörmektedir. Sözleşme’nin asıl metninin istisnalar ve kısıtlamalar başlıklı 9. maddesinin ilk fıkrasında⁷⁷ “*İşbu maddede belirtilen sınırlar dışında, Sözleşmenin 5, 6 ve 8. maddeleri hükümlerine hiçbir istisna getirilemez*”; 2. fıkrasında; “*Taraf devletin kanunlarında öngörülmüş olması ve demokratik bir toplumda aşağıdaki hususların sağlanması için gerekli bir önlem oluşturması*

tions/full-list/-/conventions/treaty/108/signatures (çevrim içi), E.T. 20.10.2019, 13:30.

⁷³ Protocol Amending the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, 2018 [Sözleşme 108+olarak da anılmaktadır], <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/09000016808ac918> (çevrim içi), E.T. 20.10.2019, 13:30.

⁷⁴ Güncel gelişmeler doğrultusunda 1987 yılında Sözleşme’ye yönelik bir tavsiye kararı kabul edilmiştir. R 87 (15) tavsiye kararı, polisin veri işleme ve veri paylaşımına ilişkin belirlemeler içermektedir. Bu konudaki değerlendirmeler için bkz.: **BOSTANCI BOZBAYINDIR, Gülşah**: “Avrupa Birliği Ceza Hukuku’nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler”, *GSÜHFD*, C.2, 2018, s.60 vd.

⁷⁵ **KÜZECİ, a.g.e.**, s.126-131.

⁷⁶ <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures> (çevrim içi), E.T. 20.10.2019, 13:30.

⁷⁷ Resmi çeviridir: <https://www2.tbmm.gov.tr/d26/1/1-0320.pdf> (çevrim içi), E.T. 20.10.2019, 13:30.

⁶⁹ Rotaru v. Romanya, Başvuru no: 28341/95, 04.05.2000, para: 59, www.hudoc.echr.coe.int (çevrim içi), E.T. 20.10.2019, 13:30.

⁷⁰ Amann v. İsviçre, Başvuru no: 27798/95, 16.02.2000, para: 66 vd., www.hudoc.echr.coe.int (çevrim içi), E.T. 20.10.2019, 13:30.

⁷¹ <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> (çevrim içi), E.T. 20.10.2019, 13:30.

⁷² Türkiye 108 no.lu Sözleşme’yi 1981 yılında imzalamış olsa da, iç hukukunda yürürlüğe koyması 1 Eylül 2016’yi bulmuştur. Zira Sözleşme’nin 4. maddesinden doğan yükümlülüğünü ancak 6698 s. KVKK’yı çıkararak yerine getirmiştir. Bu bakımdan Avrupa Konseyi ülkeleri arasında en son onaylayan ve yürürlüğe koyan ülkedir. Bkz.: <https://www.coe.int/en/web/conven>

halinde işbu Sözleşmenin 5, 6 ve 8. maddelerine istisna getirilebilir: a- Devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi; b- İlgili kişinin veya başkasının hak ve özgürlüklerinin korunması” hükümleri yer almaktadır.

Sözleşme'nin beşinci maddesinde kişisel verilerin hukuka ve dürüstlük kurallarına uygun elde edilmesi; belirli ve meşru amaçlar için tutulması ve bu amaçlarla uyumlu kullanılması; yeterli, gerekli ve aşırı olmaksızın tutulduğu amaçlar doğrultusunda kullanılması; doğru ve gerektiğinde güncel olarak tutulması; ilgili kişilerin kimliğinin belirlenmesine izin verdiği hallerde, saklandıkları amaca göre gerektiğinden daha uzun bir süre tutulmaması gerektiği düzenlenmiştir. Altıncı maddede, özel nitelikteki kişisel verilerin ulusal hukuk, uygun güvenceleri öngörmediği müddetçe otomatik olarak işlenmemesi gerektiğini düzenlenmekte, bunun mahkumiyet hükümleri için de geçerli olduğu özel olarak belirtilmektedir. Sekizinci maddede ise ilgili kişinin, yetkili resmi mercilerce işlenen kişisel verilerinin denetimine, bilgi edinmesi ve benzerine ilişkin hak ve güvenceler düzenlenmiştir.

Bu doğrultuda, Sözleşme'nin yukarıda belirtilen 9. maddesi uyarınca açıklanan güvence ve haklar kural; sınırlanması istisnaidir. Bu istisnalar devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi olarak belirlenmiştir. Yine ilgili kişinin veya başkasının hak ve özgürlüklerinin korunması amacıyla da bu güvence ve haklar sınırlanabilecektir. Sözleşme'nin asıl metninde istisna sayılan hallere adli amaçla kişisel verilerin işlenmesinin dahil edilmediği görülmektedir.

Sözleşme'ye aradan geçen yaklaşık 37 yılın ardından güncel gelişmeleri de dikkate alarak yenilikler getiren Protokol'ün kapsamına ise kişisel verilerin işlendiği -birtakım istisnalar olsa da- ulusal güvenlik gerekçeleri de dahil tüm faaliyet alanlarının girdiği belirtilmiştir.⁷⁸

⁷⁸ <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223> (çevrim içi), E.T. 20.10.2019, 13:30.

Sözleşme'nin asıl metnindeki istisnalar ve kısıtlamalar başlıklı 9. maddesi, Protokol ile değiştirilerek 11. madde olarak düzenlenmiştir. On birinci maddenin ilk fıkrasına göre;⁷⁹ “m.5/4,⁸⁰ m.7/2,⁸¹ m.8/1,⁸² ve m.9⁸³ hükümleri dışındaki, bu bölümde yer alan hükümlere⁸⁴ istisna getirilemeyeceği düzenlenmiştir. Madde 5/4, 7/2, 8/1, ve 9 hükümlerine getirilecek istisnalar ise ancak yasayla öngörülmesi, temel hak ve özgürlüklerin özüne saygı göstererek demokratik bir toplumda gerekli ve ölçülü olmak kaydıyla; **a-** ulusal güvenliğinin, savunmanın, kamu güvenliğinin, devletin önemli ekonomik ve mali çıkarlarının korunması, yargının tarafsızlığı ve bağımsızlığı veya adli suçların önlenmesi, soruşturulması ve kovuşturulması ile cezai mahkumiyetlerin infazı ve kamu yararına ilişkin diğer önemli görevlerin icrası; **b-** ilgili kişinin korunması veya başkalarının başta ifade özgürlüğü olmak üzere hak ve temel özgürlüklerinin korunması amaçlarıyla mümkündür.”

⁷⁹ Buradaki çeviriler resmi olmayıp, yazar tarafından yapılmıştır.

⁸⁰ Madde 5/4'te Kişisel verilerin işlenmesine ilişkin amaçla bağlılık, doğruluk ve gerektiğinde güncellik gibi yukarıda Sözleşme'nin asıl metninde beşinci madde kapsamında belirtilen ilkeler yer almaktadır.

⁸¹ Madde 7/2 kişisel verilerin ihlali durumunda denetleyici kurum ve taraf devletin yükümlülüğüne ilişkindir.

⁸² Madde 8/1'de şeffaflık ilkesi doğrultusunda veri sorumlusunun ilgili kişiyi, kişisel verilerinin işlenme amacı gibi konularda bilgilendirme yükümlülüğü düzenlenmektedir.

⁸³ Madde 9 ilgili kişinin bilgi edinme gibi haklarını düzenlenmektedir.

⁸⁴ Bu bölümde [Chapter II - Basic principles for the protection of personal data (Tr. Kişisel verilerin korunmasına ilişkin temel ilkeler)] yer alan diğer hükümlerden bazıları şöyledir: 5. maddenin 4. fıkrası dışındaki hükümlerinde; kişisel verilerin işlenmesinde ölçülülük ilkesine uyulacağı, kişisel veri işlemenin hukuka uygun olması, yasayla öngörülmüş meşru bir temele dayanarak veya gerekli şekilde aydınlatılması koşuluyla ilgili kişinin izin vermesi halinde mümkün olduğu düzenlenmiştir. 6. maddede özel nitelikteki kişisel verilerin ancak Sözleşme'de öngörülen hükümler doğrultusunda yasayla öngörüldüğü ve gerekli güvencelerin sağlandığı hallerde işlenebileceği belirtilmektedir. Madde 7/1'de veri sorumlusu ve işleyenin gerekli güvenlik tedbirlerini sağlaması gerekliliği düzenlenmiştir. 10. Maddede ise taraf devletlerin ek yükümlülükleri düzenlenmiştir.

On birinci maddenin konuyla ilgili üçüncü fıkrasında ulusal güvenlik ve savunmaya ilişkin ek istisnalar öngörülmüştür: *“Bu maddenin 1. fıkrasında öngörülen istisnalara ek olarak, ulusal güvenlik ve savunma amacıyla işleme faaliyetlerine istinaden Taraflar, yasayla öngörmek ve yalnızca bu amacı gerçekleştirmek için demokratik bir toplumda gerekli ve ölçülü olmak kaydıyla m.4/3,⁸⁵ m.14/5⁸⁶ ve 6, m.15/2-a,b,c,d⁸⁷ hükümlerine istisnalar getirilebilir. Bu, ulusal güvenlik ve savunma amaçlı işleme faaliyetlerinin ilgili Tarafın yerel mevzuatı uyarınca bağımsız ve etkili bir inceleme ve denetime tabi olması koşuluna halel getirmez.”*

Protokol ile değiştirilen Sözleşme’ye göre, kişisel verilerin korunmasına ilişkin temel ilkeler başlıklı bölümde (Chapter II) birtakım hükümlere (ulusal güvenlik vb. amaçlarla dahi) hiçbir koşulda istisna tanınmamaktadır. Buna karşılık, yukarıda belirtilen m.5/4’te sayılan birtakım ilkeler, m.7/2’de öngörülen verilerin ihlali durumundaki yükümlülükler, m.8/1’de yer verilen bilgilendirme yükümlülüğü ve m.9’da belirtilen ilgili kişinin hakları belirli istisnalara tabi tutulabilecektir. Yani, belirli koşullara uyulmak suretiyle, Sözleşme’nin yeni 11. maddesinde belirlenen adli ve önleyici kişisel verilerin işlenmesi durumunda, kişisel verilerin korunmasına ilişkin kurallardan m.5/4, m.7/2, m.8/1 ve m.9 hükümleri istisna tutularak, taraf devletler tarafından uygulanmayabilecektir. Bu sayılan hükümlere ancak yasayla öngörülmeye, temel hak ve özgürlüklerin özüne saygı göstererek demokratik bir toplumda gerekli ve ölçülü olma koşuluna bağlı olarak istisnalar tanınabilecektir. Ayrıca bu istisnalar ancak belirli faaliyet alanları için kabul edilmiştir. Bu faaliyetler ulusal güvenlik, savunma, suçların önlenmesi, kovuşturulması veya mahkumiyet hükümlerinin infazı gibi hususlardır.

⁸⁵ Madde 4/3, taraf devletlerin Sözleşme’de öngörülen Sözleşme Komitesi’nin Sözleşme’nin etkililiğine ilişkin değerlendirme yapmasına izin verme ve bu faaliyete katkıda bulunma yükümlülüğünü düzenlemektedir.

⁸⁶ Madde 14/5 ve 6 hükümleri, taraf devletlerin yetkili denetleyici kuruma kişisel veri aktarımına ilişkin bilgi sağlama yükümlülüğünü düzenlemektedir.

⁸⁷ Madde 15/2-a,b,c,d hükümleri, taraf devletlerin Sözleşme’ye uyumu ve denetimi sağlamak üzere oluşturduğu organlarının görevlerini düzenlemektedir.

Protokol’de istisna tanınabilecek faaliyetler belirlenirken, ulusal güvenliğin sağlanması, suçların önlenmesi, kovuşturulması gibi amaçlar yan yana sıralanmıştır. Bunun nedeni kanımızca metnin uluslararası bir sözleşme olmasıdır. Bu amaçlar arasında istisnanın kapsamına ilişkin olarak, konunun önemi ve boyutu doğrultusunda yapılacak ayırım ulusal hukuka bırakılmaktadır. Zira her ülkenin hukuk sisteminde adli, önleyici ve istihbari faaliyetlerin işleyişi farklı olduğundan, bu hükümde öngörülen istisna tutmaya ilişkin temel belirlemeler doğrultusunda düzenlenecek spesifik kurallar ulusal hukukta şekillenecektir.

Bununla birlikte, hükmün üçüncü fıkrasında ulusal güvenlik ve savunma amacıyla kişisel verilerin işlenmesi, ayrıca bir istisnaya daha tabi tutulmuştur. Bu istisna doğrultusunda yukarıdaki dipnotta yer verilen (m.4/3, 14/5 ve 6, m.15/2-a,b,c,d) kurallar ulusal güvenlik ve savunma amacıyla gerçekleştirilen faaliyetlerde uygulanmayacaktır. Diğer bir deyişle, taraf devletlerin Sözleşme’de öngörülen Sözleşme Komitesi’nin Sözleşme’nin etkililiğine ilişkin değerlendirme yapmasına izin verme ve bu faaliyete katkıda bulunma yükümlülüğünü düzenleyen hüküm; yetkili denetleyici kuruma kişisel veri aktarımına ilişkin bilgi sağlama yükümlülüğünü düzenleyen hüküm ve Sözleşme’ye uyumu ve denetimi sağlamak üzere oluşturduğu organlarının görevlerini düzenleyen hükümler; ulusal güvenlik ve savunma amacıyla gerçekleştirilen kişisel verilerin korunmasından istisna tutulabilecektir.

Özellikle ulusal güvenlik ve savunma amacıyla gerçekleştirilen istihbari faaliyetlerin yerine getirilmesi ve işleyişine ilişkin olan bu hükümlerin istisna tutulması; taraf devletlerin bu konudaki bilgi ve istihbaratı paylaşmak istememesi doğrultusunda anlaşılabilir. Bu hükümde belirlenen istisnaların uygulanabilmesi; ancak yasayla öngörülmesi ve yalnızca ulusal güvenlik ve savunma amaçlarını gerçekleştirmek için demokratik bir toplumda gerekli ve ölçülü olması koşuluna tabi kılınmıştır. Yine, gerek Sözleşme gerekse Protokol bakımından istisna tutulan hü-

kümlerin dar yorumlanması gerektiği ve kıyas yoluyla genişletilemeyeceği⁸⁸ unutulmamalıdır.

C. 2016/680 Sayılı AB Direktifi'nde Kişisel Verilerin Adli ve Önleyici Amaçla İşlenmesine İlişkin Düzenlemeler

1. Genel Olarak

AB hukukunda kişisel verilerin adli ve önleyici amaçla işlenmesine dair düzenlemeler,⁸⁹ 2016/680 sayılı Direktif'ten önce farklı hukuki metinlerde ele alınmaktaydı.⁹⁰ 2016/680 sayılı Direktif, kendinden önce yürürlükte bulunan 2008/977/JHA sayılı çerçeve kararını ilga ederek yerini almıştır. Yine, 2016/680 s. Direktif'ten ve 2016/679 s. Genel Veri Koruma Tüzüğü'nden önce, 95/46/EC s. Direktif hem kamu hem de özel hukuk alanında uygulama alanına sahip olsa da, ceza hukukuna ilişkin adli amaçlı işbirliği ile kolluk işbirliğinde uygulanmamaktaydı.⁹¹

Direktif 8 Nisan 2016'da Bakanlar Konseyi'nde kabul edilmiş, 5 Mayıs 2016'da Resmî Gazete'de yayımlanmış; fakat üye devletlerin mevzuat uyumlarının sağlanması amacıyla Mayıs, 2018'de yürürlüğe gireceği kararlaştırılmıştır.⁹² 2016/680 sayılı Direktif, kendinden önce var olan çerçeve kararların eksiklerini gidermek, AB genelinde yeknesak ve uyumlu bir düzenleme getirerek bireylere eşit düzeyde koruma

sağlama amacıyla düzenlenmiştir. 'Kolluk faaliyetleri ve adli işbirliği' alanında kişisel verilerin işlenmesi diğer alanlardan farklı olduğundan, GVKT'nin aksine bu alan (tüzük yerine) bir direktif ile düzenlenmiş ve ülkelere ulusal hukukları doğrultusunda düzenleme yapabilme esnekliğini bırakılmıştır.^{93,94} Bu faaliyetlerin niteliği dolayısıyla Direktif'te, örneğin Tüzük'ten farklı olarak kişilerin verilere erişebilme hakkı sınırlandırılmış, ilgilinin rızasının temel koşul olması gibi birtakım ilkeler dahil edilmemiş, istisnalar faaliyetlerin niteliğine uygun olarak düzenlenmiştir. Direktif'te temel olarak suçları önleme, araştırma, tespit etme ve mahkumiyetlerin infazını sağlamaya yönelik kamusal menfaatler ile gerçek kişilerin kişisel verilerinin işlenmesine karşı korunmasındaki menfaatlerin dengelenmeye çalışıldığını söylemek yanlış olmayacaktır.⁹⁵

⁸⁸ GÖZLER, Kemal: *Hukuka Giriş*, 14. Baskı, Ekin Basım Yayın Dağıtım, Bursa 2017, s.317 vd..

⁸⁹ Diğer düzenlemelerin yanında, AB Temel Haklar Şartı'nın 8. maddesinde, 7. maddesinde düzenlenen özel yaşamın gizliliğine ilişkin haktan bağımsız olarak, herkesin kişisel verilerin korunması hakkına sahip olduğu düzenlenmiştir. Hükme göre, bu tür kişisel veriler ancak özellikle belirtilen amaçlar doğrultusunda ilgili kişinin rızası veya yasayla belirlenen diğer meşru temele dayanarak adil bir şekilde işlenebilir. Herkes kendisiyle ilgili toplanan verilere erişme ve düzeltilmesini sağlama hakkına sahiptir. Bu kurallara uyulmasının bağımsız bir otorite tarafından denetlenmesi öngörülmüştür.

⁹⁰ Konuyla ilgili değerlendirmeler için bkz.: BOSTANCI BOZBAYINDIR, a.g.e., s.66-69.

⁹¹ PAJUNOJA, a.g.e., s.8.

⁹² <https://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-law-enforcement/> (çevrim içi), E.T. 20.10.2019, 13:30.

⁹³ Avrupa Birliği'nin İşleyişi Hakkında Antlaşma - Madde 288: "(1) Tüzükler genel uygulama alanına sahiptir. Bütünüyle bağlayıcıdır ve tüm üye devletlerde doğrudan uygulanır. (2) Direktifler, muhatap alınan her üye devleti, ulaştırılması gerekli sonuçları itibarıyla bağlar, şekil ve yöntem seçimini ise ulusal otoritelere bırakır." Yani, Direktifler üye devletler için bağlayıcı olmakla birlikte, ulaştırılmak istenen sonuca uygun olarak düzenleme yapma yetkisi üye devletlere aittir. AB üye devletleri arasındaki uyumu sağlamak açısından tüzükler, direktiflere göre daha etkilidir. CARUANA, Mireille M.: "The reform of the EU data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement", *International Review of Law, Computers & Technology*, 2017, s.4, <http://dx.doi.org/10.1080/13600869.2017.1370224> (çevrim içi), E.T. 20.10.2019, 13:30.

⁹⁴ Bu esneklik her ne kadar ülkelerin kendi adli yapısı ve polis uygulamaları dolayısıyla anlaşılabilir olsa da, üye devletler arasında farklı uygulamaların oluşmasına neden olabilecektir. Bu farklılıklar Direktif'in getirmek istediği yeknesaklık ve veri güvenliği açısından sorun oluşturabilecektir. BOSTANCI BOZBAYINDIR, a.g.e., s.90-91.

⁹⁵ BOSTANCI BOZBAYINDIR, a.g.e., s.69-71; AKINTUNDE, 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", s.2, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2912449 (çevrim içi), E.T. 20.10.2019, 13:30.

Direktif ile hem kişisel verilerin işlenmesini korumak hem de veri dolaşımını güvence altına alarak, kolluk faaliyetlerinde ve adli işbirliğinin güçlendirilmesi amaçlanmaktadır. Bu açıdan sanıldığı aksine kişisel verilerin dolaşımının sınırlandırılması değil; tam tersine belirli standartlar dahilinde veri paylaşımının artırılması hedeflenmektedir.⁹⁶ Bu doğrultuda gerçek kişilerin kişisel verilerinin; suçları önlemeye, araştırmaya, tespit etmeye ve cezaların infazını sağlamaya yetkili resmi merciler tarafından işlenmesinde yüksek düzeyde koruma sağlanması ve bu korumada bir yeknesaklık oluşturarak verilerin dolaşımının belirli güvence ve koşullara bağlanarak kolaylaştırılması hedeflenmektedir.

Direktif'in kişisel verilerin korunmasında yeterli güvenceyi gerçekten sağlayıp sağlamadığını söylemek için henüz erken bir aşamada olduğumuzu belirtmek gerekir.⁹⁷ Bunda şüphesiz, AB üyesi devletlerin Direktif'i iç hukuklarına aktarırken yaşayacakları farklılıklardan doğan güçlüklerin de etkisi vardır. En baştan ifade etmek gerekir ki, Direktif'in geniş bir uygulama alanına sahip olduğu izlenimi oluşturmaya karşın aslında pek çok açıdan sınırlı bir alana sahip olduğu eleştirisi sıklıkla dile getirilmektedir. Yine de, ulusal hukuktaki uygulamalar ile yargısal faaliyetlerin kapsam içine alınması ve bu konuda güncel teknolojiyle uyumlu bir şekilde hazırlanan Direktif'in kişisel verilerin işlenmesinde temel koruma mekanizmalarını getirmesi önemli bir kazanım olarak değerlendirilmektedir.⁹⁸

Son olarak ifade etmek gerekir ki, Direktif adli ve önleyici amaçlarla kişisel verilerin işlenmesi faaliyetlerine uygulanmak üzere hazırlanmıştır. Buna karşılık GVKT ise AB içerisinde kişisel verileri işlenen gerçek kişilerin korunmasına ilişkin genel kuralları öngörmektedir. Direktif'te

belirtilen amaçlar dışındaki veri işlemlerine GVKT uygulanacaktır. Bu ikisi arasında -faaliyetlerin niteliği gözetilerek- bir ayırım yapılması isabetli bir yaklaşımdır. Zira, GVKT tarafından tanınan haklar, Direktif'te belirtilen faaliyetler bakımından aynen uygulanacak olsa idi, ceza soruşturmalarının gerçekleştirilmesi fiilen imkansız hale gelebilirdi.⁹⁹

2. Direktif'in Başlangıç Metni'ndeki Konuya İlişkin Belirlemeler

Yukarıda ifade edildiği üzere Direktif adli suçların önlenmesi, araştırılması, tespit edilmesi veya kovuşturulması ya da mahkumiyetlerin infazı amacıyla kişisel verilerin yetkili mercilerce işlenmesini ve bu verilerin serbest dolaşımını düzenleyen AB hukukundaki başlıca kaynaktır. Direktif'in başlangıç metni ise konuya ilişkin AB kurumlarının genel değerlendirme ve gerekçelerini yansıtmakta, Direktif hükümlerini açıklamaktadır. Buradaki önemli hususların ortaya konulması, devletlerin belirtilen amaçlarla kişisel verileri işlemesine ilişkin güncel yaklaşımın ve değişimin anlaşılmasını sağlayacaktır. Bu doğrultuda Direktif'in başlangıç bildirisindeki konu bakımından önemli kısımlar aşağıda ele alınmakta ve değerlendirilmekte / yorumlanmaktadır.

7. paragrafta cezai konularda üye devletlerin kolluk ve adli mercileri arasındaki işbirliğinin güçlendirilmesinin ancak bunların işlediği kişisel verilerin korunmasına ilişkin yüksek seviyede güvence sağlayan bir mekanizma oluşturulmasıyla sağlanabileceği belirtilmiştir.

11. paragrafta 680 s. Direktif'in yalnızca yargı mercileri veya kolluk gibi resmi mercileri değil, aynı zamanda kamusal yetki veya kamu

⁹⁶ DE HERT, Paul / PAPAKONSTANTINO, Vagelis: "The New Police and Criminal Justice Data Protection Directive", *New Journal of European Criminal Law*, 2016, s.11 <https://journals.sagepub.com/doi/abs/10.1177/203228441600700102> (çevrim içi), E.T. 20.10.2019, 13:30.

⁹⁷ PAJUNOJA, a.g.e., s.84.

⁹⁸ BOSTANCI BOZBAYINDIR, a.g.e., s.75.

⁹⁹ 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)", <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/> (çevrim içi), E.T. 20.10.2019, 13:30; BOSTANCI BOZBAYINDIR, a.g.e., s.92.

gücü kullanmakla yetkilendirilmiş diğer organ, kuruluş ve benzerini de kapsadığı ifade edilmiştir. Buna örnek olarak özel güvenlik kuruluşları verilebilir. Günümüzde güvenlik hizmetlerinde resmi kolluğun yanında, özel güvenlik hizmetlerinden yararlanılır olmuştur.¹⁰⁰

12. paragrafta üye devletlerin yetkili mercileri adli suçların önlenmesi, araştırılması, tespiti, kovuşturulması, kamu güvenliğinin tehlikeye düşmesinin önlenmesi gibi amaçlar dışındaki amaçlarla yetkilendirdiği durumlarda 2016/680 s. Direktif'in değil, GVKT'nin uygulanacağı belirtilmiştir.

14. paragrafa göre Direktif AB hukukunun uygulama alanına girmeyen faaliyetlere uygulanamayacağından, ülkelerin ulusal güvenliğinin sağlanması gibi faaliyetlerde bulunan kuruluş ve birimlerin işlediği kişisel verilerde uygulama alanına sahip değildir. Üye devletlerin AB Antlaşması'nın 2. bölümünün 5. başlığında yer alan ortak dış ve güvenlik politikasına¹⁰¹ ilişkin faaliyetleri de 680 sayılı Direktif kapsamında değildir. Ulusal güvenliğin sağlanması amaçlı faaliyetler ile kastedilen aslında, bu amaçla çalışan gizli istihbarat teşkilatlarının faaliyetleridir. Nitekim Direktif'te istihbari amaçla kişisel veri işlenmesi ayrıca düzenlenmemiştir. Dikkat edilmelidir ki açıklamada istihbari faaliyetin kapsam dışı bırakılmasının nedeni olarak, bu faaliyetin özellikleri ve niteliği değil; AB hukukunun uygulama alanı dışında kalması gösterilmektedir.

Ancak ulusal güvenliğin sağlanması amaçlı faaliyetlerin, her ne kadar başlangıç metninde Di-

¹⁰⁰ Bu ihtiyacın artması doğrultusunda, İçişleri Bakanlığının verilerine göre Türkiye'de 2011 yılında 147 bin olan özel güvenlik personeli sayısı 2017 yılında 284 bine çıkarak, EGM'nin 261 bin olan personel sayısını geçmiştir. http://www.cumhuriyet.com.tr/haber/siyaset/809844/Ozel_guvenlik_ordusu.html, (çevrim içi), E.T. 20.10.2019, 13:30.

¹⁰¹ Günümüzde AB bu alanda genel yönlendirici ilkeleri, AB'nin kendisinin gerçekleştireceği eylemleri ve tutumu belirleyecek kararlar alabilecektir. Ancak bu kararlar yasama tasarrufu niteliğinde değildir. **BAYKAL, Sanem / GÖÇMEN, İlke**: "Avrupa Birliği Hukukunun Kaynakları Bakımından Normlar Hiyerarşisi", *Prof. Dr. Erdal Onar'a Armağan*, Ankara Üniversitesi Basımevi, Ankara 2013, s.330-331.

rektif'in kapsamı dışında olduğu belirtilmişse de, Avrupa Birliği Adalet Divanı'nın (ABAD) içtihatları¹⁰² doğrultusunda ve AB'nin sınır aşan suçlarla mücadelede işbirliğinin sağlanması amacıyla¹⁰³ Direktif'in kapsamına dahil edilmek üzere, taslak metindeki *ulusal güvenliğin kapsam dışında olduğu ibaresinin* çıkarıldığı ifade edilmektedir.¹⁰⁴ Gerçekten Direktif'in kapsamının belirlendiği 2. maddede -aşağıda da üzerinde durulacağı üzere-¹⁰⁵ kişisel verilerin AB hukukunun uygulama alanı dışındaki faaliyetlerde veya Birlik kurum, organ, ofis ve ajansları tarafından işlenmesinde Direktif'in uygulanmayacağı düzenlenmiştir. Bir diğer deyişle, Direktif'in 2. maddesine 'ulusal güvenlik' atfı taslak metinden çıkarılarak Direktif metnine alınmamış; ancak başlangıç metni 14. paragrafta ifade edilmiştir.¹⁰⁶ 2. maddedeki saymanın tahdidi olduğuna şüphe yoktur. Ne var ki, ulusal güvenlik her üye devletin kendi sorumluluğunda olup, başlangıç metninde de belirttiği üzere bu amaçla gerçekleştirilen faaliyetler, örneğin gizli istihbarat çalışmaları AB hukukunun kapsamının dışında kalmaktadır. Zira AB Antlaşması'nın 4. maddesine göre "*Birlik, ülke bütünlüğünün teminat altına alınması, kamu düzeninin muhafaza edilmesi ve ulusal güvenliğin korunması da dahil, devletin temel işlevlerine saygı gösterir. Özellikle ulusal güvenlik, her üye devletin kendi sorumluluğunda kalmaya devam eder*". **Dolayısıyla, kanaatimizce ulusal güvenliğin Direktif'in kapsamının belir-**

¹⁰² ABAD kimi kararlarında, üye devletlerin iç ve dış güvenliğini sağlamak kendi sorumluluklarına dahil olsa da, konunun sırf ülke güvenliğini ilgilendirdiğine ilişkin bir kararın Birlik hukukunun uygulanmayacağı sonucunu doğurmadığına işaret etmiştir. (Ör: ZZ v. *Secretary of State for the Home Department*, C- 300/11, 04.06.2013, para.38, <http://curia.europa.eu/juris/document/document.jsf?jsessionid=870159A2FFC979074A8A0B5EDB72FEE8?text=&docid=137981&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7955409> (çevrim içi), E.T. 20.10.2019, 13:30), **CARUANA, a.g.e.**, s.8-9.

¹⁰³ Nitekim Direktif'in yalnızca kişisel verilerin işlenmesine güvenceler getirmekle sınırlı kalmayıp, aynı zamanda yetkili merciler arasında veri dolaşımını da kolaylaştırdığını akıld tutmak gerekir.

¹⁰⁴ **BOSTANCI BOZBAYINDIR, a.g.e.**, s.72.

¹⁰⁵ Bkz. Aş. § IV/D-3, Birinci ve ikinci madde.

¹⁰⁶ **CARUANA, a.g.e.**, s.8.

lendiği 2. maddede açıkça zikredilmesine gerek yoktur; bu faaliyetler Direktif'in kapsamı dışında bırakılmıştır. Fakat bu kez de bir başka husus belirsizliğe neden olmaktadır. Direktif'in 12 ve devamı maddelerinde ilgili kişinin kişisel verilerinin korunmasına ilişkin hakları düzenlenirken buna getirilebilecek sınırlamalarda ulusal güvenlik gerekçesine açıkça yer verilmiştir. Bir başka ifadeyle, kişisel verilerin işlenmesine ilişkin ilkelerde veya Direktif'in kapsamının belirlendiği ana hükümlerde ulusal güvenlik ifadesi zikredilmemiş; fakat ilgili kişinin hakları bölümünde bu hakların kamu güvenliğinin korunması ve birkaç başka sebebin yanı sıra, ulusal güvenlik gerekçesiyle de sınırlanabileceği açıkça düzenlenmiştir. Buradaki açık belirlemenin karşıt anlamından hareketle; kişisel verilerin işlenmesindeki temel ilkelerde yahut Direktif'in genel kapsamına ilişkin hükümlerde ulusal güvenlik gerekçesinin belirtilmemiş olması, ulusal güvenlik faaliyetlerinin Direktif'in kapsamına dahil olduğu anlamına mı gelmektedir? Kanımızca, her halükârda ulusal güvenliğin Birlik hukukunun uygulama alanı dışında kalması sebebiyle Direktif hükümlerinin uygulanmayacağı sonucuna ulaşılmaktadır. AB hukukunun dışında kalan bu alana Direktif hükümlerinin uygulanması ancak, söz konusu faaliyetin bir yönüyle AB hukukunu ilgilendirmesi yahut herhangi bir şekilde Direktif'in kapsamına giren faaliyetlerden biriyle ilişki içerisinde gerçekleştirilmesi halinde mümkündür.

Direktif'in birinci maddesinde belirtilen, "... kamu güvenliğine yönelik tehditlerin önlenmesi için uygulanan tedbirler ve sağlanan güvenceler de dahil olmak üzere..." hükmü göz önünde alındığında bir başka sorunla daha karşılaşmaktadır. Nitekim ulusal güvenlik kavramı ile kamu güvenliği kavramları birbirine yakındır. Özünde farklı kavramlar olmalarına karşın, uygulamada sık sık iç içe geçebilmektedirler. O halde, bir kişisel veri işleme faaliyetinin Direktif'in kapsamı içinde mi, yoksa dışında mı değerlendirileceği uygulamada sorun yaratabilecektir. Nitekim, öğretilerde de bu husus eleştirilmekte ve devletlerin genellikle bu muğlaklık sayesinde faaliyetlerinin ulusal güvenliğe ilişkin olduğunu ileri sürerek

Direktif'in kapsamı dışındaymışçasına hareket ettiği belirtilmektedir.¹⁰⁷

17. paragrafta Direktif'in yalnızca gerçek kişilere uygulanacağı belirtilmiştir. Dolayısıyla tüzel kişiler, kişisel verilerin korunması bakımından kapsam dışında bırakılmıştır.

20. paragrafta Direktif'in üye devletleri, ulusal hukuklarında ceza muhakemesine ilişkin olarak, özellikle adli süreçte tutulan kayıtlarda veya mahkemelerin hükümlerinde kayda geçen kişisel verilerin, mahkeme veya diğer yargı organlarının işlenmesine ilişkin faaliyet ve usullerini belirlemekten alıkoymayacağı düzenlenmiştir. Gerçekten bu konuda, aşağıda görüleceği üzere ulusal hukukta düzenleme yapabilme serbestisi tanınmaktadır.

25. paragrafa göre; tüm üye devletler Interpol'e üyedir. Interpol yapısı gereği kişisel verileri alır, depolar, yetkili mercilerle paylaşır. Bu işbirliğinin kuvvetlendirilmesi önemlidir. Interpol'e delege gönderen ülkeler de vardır. Dolayısıyla bu faaliyetlerde Direktif'in özellikle verilerin uluslararası paylaşımına ilişkin kuralları uygulanır.

26. paragrafta kişisel verilerin işlenmesine dair hukuka ve dürüstlük kurallarına uygunluk, yalnızca yasal olarak belirlenen amaçlar doğrultusunda işleme bağlı olma, şeffaflık gibi ilkeler belirtilmiştir. Fakat örneğin şeffaflık ilkesinin gizli soruşturma yöntemlerinin uygulanmasını engellemeyeceği ifade edilmiştir.

29. paragrafta kişisel verilerin belirli, açık ve meşru amaçlarla işlenebileceği vurgulanmıştır. Elde edilen bir kişisel veri aynı veya başka bir merci tarafından yine bu Direktif'te belirtilen (fakat toplama amacından farklı olan) amaçlarla işlendiyse, bu işlemeye ancak yasal düzenlemelerce izin verilmiş, gerekli ve ikinci amaç bakımından orantılıysa izin verilir.

30. paragrafta verilerin doğruluğu ilkesine vurgu yapılmakta ve örneğin adli işlemlerde kişisel veri içeren ifadelerin öznel değerlendirmelere dayandığının altı çizilmektedir.

¹⁰⁷ BOSTANCI BOZBAYINDIR, a.g.e., s.75.

31. paragrafta kişisel verilerin işlenmesinde önemli bir ayırım yapılmasının gerekliliğini belirtmektedir. Buna göre Direktif'teki amaçlar doğrultusunda kişisel verilerin işlenmesi, kişinin hukuki statüsüne bağlı olarak değişiklik göstermektedir. Dolayısıyla kişisel verilerin; şüpheli / sanık, suç ortağı, mahkum, mağdur ve suçtan zarar gören, tanık gibi açık kategorilere ayrılarak işlenmesi mümkün olduğunca sağlanmalıdır. Bu ayırımın yapılması AİHS m.6'da belirtilen suçsuzluk karinesini ihlal etmemelidir.

34. paragrafta Direktif'in kurallarının, burada belirtilen amaçlar doğrultusunda kişisel verilerin bu Direktif'e tabi olmayan bir alıcıya iletilmesine de uygulanacağını belirtmektedir. Bu, yukarıda da açıklandığı üzere Türkiye ile AB arasındaki kişisel veri dolaşımı ve adli işbirliği açısından önemlidir.

35. paragrafta kişisel verilerin **bu Direktif'te belirtilen amaçlarla söz konusu yetkili merciler tarafından** işlenmesinin meşru olması için, işlemin kamu yararı doğrultusunda gerçekleştirilen bu görev için gerekli olması gerektiği belirtilmektedir.

39. paragrafta veri sahibinin kişisel verilerle ilgili haklarını kullanabilmesini sağlamak amacıyla, veri sorumlusunun (*data controller*) ilgili kişiyle (*data subject*) ilgili tüm bilgileri kolayca erişilebilir hale getirmesi, açık ve anlaşılır bir dil kullanarak anlaşılmasını kolay kılması gerekliliği üzerinde durulmuştur. Ayrıca bu bilgiler, çocuklar gibi savunmasız kişilerin ihtiyaçlarına göre uyarlanmalıdır. Kişiler, verilerini mümkünse ücretsiz olarak alabilmelidir. Doğrudan §39'da yer almamakla birlikte bir örnekle açıklamak gerekirse, veri sahibi kendisiyle ilgili işlenen kişisel verileri -bir istisna tanınmış olmadıkça- kolluk mercilerinden talep edebilir. Bu doğrultuda kolluk, ilgili kişinin kimliğini tespit ettikten sonra, ona hukuki dayanak noktalarını da göstererek, açık dille bir açıklama yapmalıdır.¹⁰⁸

¹⁰⁸ Council of Europe Directorate General of Human Rights and Rule of Law, *Consultative Committee of the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data - Practical Guide on the Use of Personal Data in the Police Sector*, T-PD(2018)01, Strasbourg, 15.02.2018,

42. paragrafta ilgili kişiye en azından veri sorumlusunun kimliği, işlemin varlığı ve amaçları, şikayette bulunma hakkı ile verilerin düzeltilmesi ve silinmesini isteme hakkı konusunda bilgi verilmesi gerektiği ifade edilmiştir.

43. paragrafta göre gerçek kişi, kendisiyle ilgili toplanan kişisel verilere kolayca ve makul aralıklarla erişebilme, işlemin varlığı ve meşruluğu konusunda bilgi edinebilme hakkına sahip olmalıdır. Bu doğrultuda kişisel verilerinin hangi amaçlarla işlendiğini bilme hakkı tanınmalıdır. §43'e göre üye devletler belirli güvenceler doğrultusunda kimi durumlarda bu erişimi engelleyebilecekse de §44, bu erişimin reddedildiğine ilişkin bilgilendirmenin yazılı olarak somut ve hukuki gerekçelerle yapılması gerektiğini belirtmektedir.

47. paragrafta göre gerçek kişiler kendileriyle ilgili yanlış tutulan kişisel verilerin düzeltilmesini isteme hakkına sahip olmalıysa da; bu örneğin bir tanık beyanının değiştirilmesi anlamına gelmemelidir. Yanlış tutulan veya kişisel değerlendirmeler dolayısıyla yanlış bilgiler içeren kişisel veri kayıtları, son derece önemli sorunlara yol açabilmektedir. Özellikle istihbarat faaliyetinin gizli niteliği, çoğunlukla ikincil kaynaklardan veri elde edilmesi ve bunların doğrulanamaması durumları düşünüldüğünde, ilgili kişilerin bu verileri mümkün olduğunca denetleyebilmesi ve yanlış bilgilerin silinmesi imkanının tanınması önem taşır.¹⁰⁹

48. paragrafta veri sorumlusunun, ilgili kişinin verilere erişimini, düzeltilmesini, silinmesini vb. reddettiğinde, kişinin bu kararın hukukiliğini denetlemesi için ulusal denetim makamına başvurma hakkı olması gerekliliği ifade edilmiştir.

<https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5> (çevrim içi), E.T. 20.10.2019, 13:30.

¹⁰⁹ Özellikle gizli nitelikli bilgi elde etme yöntemlerinin doğru olmayan bilgiler üzerinden gerçekleştirilebileceği eleştirisi için bkz.: AKSOY, Muammer: "Güvenlik Soruşturması" Denilen Hukuksal Sapıklığın, MİT Raporlarındaki Korkunç Yanlış ve Yalanlar Işığında Değerlendirilmesi", *Bahri Savcı'ya Armağan, Mülkiyeliler Birliği Vakfı Yayınları - 7, Maya Matbaacılık, Ankara 1988, passim.*

49. paragrafa göre kişisel verilerin bir ceza soruşturma veya kovuşturması kapsamında işlenmesi durumunda, üye devletler ulusal mevzuata uygun olarak kişilerin bilgi edinme, verilerin düzeltilmesini ve silinmesini isteme hakkını kullanabilmesi olanağını tanımalıdır. Bu, ilgili faaliyetin gerçekleşmesini engellemediği sürece, şeffaflık ilkesi bakımından son derece önemli bir güvence olarak karşımıza çıkmaktadır.

56. paragrafa göre Direktif'e uyumun gösterilebilmesi amacıyla, veri sorumlusu veya işleyicisi, kendi sorumluluğu altındaki tüm işlem faaliyet kategorileriyle ilgili kayıtları tutmalıdır. Bunlar denetimde gösterilebilmek amacıyla verileri hazır etmeli ve denetim kuruluşuyla işbirliği içinde çalışmalıdır.

59. paragrafa göre ilgili kişilerin hak ve özgürlüklerinin etkili bir şekilde korunmasını sağlamak amacıyla veri sorumlusu veya işleyicisi, belirli durumlarda verileri işlemeyen önce denetim otoritesine danışmalıdır. Bu özellikle özel nitelikli kişisel verilerin işlenmesi bakımından son derece önemlidir. Direktif'in taslağına ilişkin Veri Koruma Çalışma Grubu, polis ve adli mercilerin işlediği kişisel verilerin hassasiyeti dikkate alındığında, önceden bu denetleyici organa danışılmasının kural haline gelmesini önermiştir.¹¹⁰ 95/46/EC sayılı Direktif'in 20. maddesinde de, hak ve özgürlükler açısından özel risk taşıma olasılığı bulunan hallerde, devletlere ön denetimde bulunma yükümlülüğü getirilmiştir. Ne var ki, hangi işlemlerin özel risk taşıyabileceği Direktif'te belirtilmediğinden bunları belirleme görevi devletlere bırakılmıştır.¹¹¹

¹¹⁰ Article 29 Data Protection Working Party, Opinion 03/2015 on the Draft Directive on the Protection of Individuals With Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, 3211/15/EN, WP 233, 01.12.2015, s.11-12, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640460 (çevrim içi), E.T. 20.10.2019, 13:30., ÖNGÜN AYÖZGER, a.g.e., s.32.

¹¹¹ AKGÜL, a.g.e., s.135.

64. paragrafta verilerin dolaşımına ilişkin bir güvence öngörmektedir. Buna göre üye devletler kişisel verileri bu Direktif'teki amaçlar ve güvenceler doğrultusunda üçüncü bir ülkeye veya uluslararası kuruluşa aktarırken bu aktarımın gerçekten gerekli olduğunu ve aktarılan merciin Direktif'te yetkili sayılanlardan olduğunu tespit etmelidir.

65. paragrafa göre kişisel verilerin bir üye devletten üçüncü ülkelere veya uluslararası kuruluşlara aktarılması, böyle bir aktarım kuralı olarak, verinin elde edildiği Üye Devletin yetki vermesi halinde yapılmalıdır.

66. paragraf uyarınca Türkiye'nin AB ile uyumlu bir mevzuata sahip olmasının önemi anlaşılmaktadır. Buna göre Avrupa Komisyonu bir üçüncü ülkenin veri koruma mevzuatının yeterli düzeyde koruma sağlayıp sağlamadığını tespiti edebilmelidir. Ülkenin yeterli düzeyde korumaya sahip olması halinde, üye devletin ayrıca yetkilendirmesi zorunlu olmadıkça bu tür veri aktarımları için ayrıca bir yetkilendirmeye gerek olmamalıdır.

67. paragrafa göre üçüncü ülkeler özellikle verinin bir veya birkaç belirli sektörde işlendiği durumlarda, Birlik içinde sağlanan ile eşdeğer yeterli düzeyde koruma sağlayacak garantiler sunmalıdır. Bunun yanında §68'e göre üçüncü ülkelerin uluslararası veya bölgesel kuruluşlarla işbirliğinden doğan yükümlülükleri de dikkate alınmalıdır.

75. paragrafta üye devletlerde, görevlerini tam bağımsızlıkla yerine getirebilen denetleyici otoritelerin kurulması, kişisel verilerinin işlenmesi konusunda gerçek kişilerin korunmasının temel bir bileşeni olduğu belirtilmiştir. Üye devletler GVKT uyarınca oluşturulmuş denetleyici kuruluşlarını bu direktifin uygulanması bakımından da yetkilendirebilirler.

İfade etmek gerekir ki, Direktif'in başlangıç metninde kişisel verilerin üçüncü ülkelerle paylaşımına ilişkin başka önemli hususlara da dikkat çekilmektedir. Örneğin 72. paragrafta kişisel verilerin aktarılacağı ülkede yeterli veri koruma mekanizması yoksa bu transferin ancak önemli bir suçun önlenmesi, acil bir ihtiyacın giderilmesi gibi

sınırlı durumlarda söz konusu olabileceği belirtilmektedir. Ancak bu konudaki değerlendirmemizi açıklananlarla sınırlamamız, çalışma konumuzunu aşma kaygısını gözeterek isabetli olacaktır.

80. paragrafta Direktif'in aynı zamanda ulusal mahkeme ve diğer yargı organlarının faaliyetlerine de uygulandığı hatırlatılmaktadır. Ancak, bağımsız denetim organının yetkilerinin, mahkemelerin bağımsızlıklarına hanel getirmemek adına, yargısal görevlerini yerine getirirken uygulanmaması gerektiği belirtilmektedir. Bunun yalnızca davalardaki yargısal faaliyetlerle sınırlı tutulması gerektiği, yargıçların ulusal hukukla bağlı olduğu diğer hususlara uygulanmaması gerektiği ifade edilmektedir. Ayrıca C. savcılıkları gibi diğer bağımsız yargısal mercilerin de, yargısal faaliyetlerde bulunurken bu yaklaşımın benimsenmesi gerektiği belirtilmektedir.¹¹² Bunun yanında, her halükarda mahkeme ve diğer bağımsız yargı mercilerinin bu Direktif ile uyumlulukları, AB Temel Haklar Şartı m.8/3¹¹³ uyarınca denetime tabidir.

3. Direktif'in İçeriği

2016/680 s. Direktif on bölümden oluşmaktadır. İlk bölümde (m.1-3) genel hükümler, ikinci bölümde (m.4-11) ilkeler, üçüncü bölümde (12-18) ilgili kişinin (veri öznesi) hakları düzenlenmektedir. Dördüncü bölümde (m.19-34) veri sorumlusu ve işleyene ilişkin hükümler, beşinci bölümde (m.35-40) kişisel verilerin üçüncü ülke ve uluslararası kuruluşlara aktarılmasına ilişkin hükümler yer almaktadır. Altıncı bölümde (m.41-49) bağımsız denetim organlarına; yedinci bölümde (m.50-51) işbirliğine; sekizinci bölümde (m.52-57) çözüm yolları [Ing. *remedy*], sorumluluk ve cezalara; dokuzuncu bölümde (m.58) uygulama anlaşmalarına ve onuncu bölümde (m.59-65) son hükümlere yer verilmektedir.

¹¹² C. savcılarının Türk hukukunda bir yargı mercii olup olmadığı aşağıda değerlendirilmiştir. Kanımızca kimi yabancı ülke hukuklarındaki yaklaşımdan farklı olarak Türk hukukunda C. savcılıkları bir yargı mercii değildir. Bkz. Aş.: Ş V/C.

¹¹³ Kişisel Verilerin Korunması kenar başlıklı Madde 8 (3): "Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecaktır."

Direktif'in **birinci maddesinde Yetkili merciler tarafından gerçek kişilerin kişisel verilerinin; kamu güvenliğine yönelik tehditlerin önlenmesi için uygulanan tedbirler ve sağlanan güvenceler de dahil olmak üzere, adli suçların önlenmesi, araştırılması, tespiti veya kovuşturulması ya da ceza mahkumiyetlerinin infazı amacıyla işlenmesine yönelik kuralların** bu Direktif'te belirlendiği öngörülmüştür. Maddede ayrıca, üye devletlerin kişilerin bu konudaki temel hak ve özgürlüklerini güvence altına almasını vurgulamış; söz konusu verilerin AB içerisindeki yetkili merciler tarafından değişimini Birlik veya üye devlet hukukunun gerektirmesi ve bunun yasaklanmamış olması koşuluna bağlamıştır. Yine Direktif hükümlerinin iç hukukta daha yüksek seviyede koruma sağlayan bir mevzuat oluşturulmasına engel olmayacağı bu maddede belirtilmiştir. Ancak özellikle yeknesak bir uygulama getirerek verilerin güvenceli paylaşımını artırmayı hedefleyen Direktif'in, farklı ülkelerin daha yüksek standartlı koruma sağlaması sonucunda bu paylaşımın ket vurulabileceği eleştirisi getirilmektedir.¹¹⁴

İkinci maddede Direktif'in kapsamı belirtilirken, kişisel verilerin tamamen veya kısmen otomatik yollarla işlenmesi ve otomatik araçlar dışında bir dosyalama sisteminin parçasını oluşturan veya oluşturması amaçlanan araçlarla işlenmesi halinde uygulanacağı öngörülmüştür. Dolayısıyla, bu koşulu sağlamadığından, yalnızca manuel olarak gerçekleştirilen polis bir kimseyi durdurarak üstünü araması gibi yöntemlerin Direktif'in kapsamı dışında kaldığı; ancak bu suretle elde edilen kişisel verilerin kaydedildiği veya mevcut dosyalarla ilişkilendirildiği hallerde Direktif'in uygulama alanına gireceği ifade edilmektedir.¹¹⁵

¹¹⁴ BOSTANCI BOZBAYINDIR, *a.g.e.*, s.94.

¹¹⁵ BÄCKER, Matthias / HORNUNG, Gerrit: "Data Processing by Police and Criminal Justice Authorities in Europe - The Influence of the Commission's Draft on the National Police Laws and Laws of Criminal Procedure", *Computer Law & Security Review*, C.28, S.6, 2012, s.630, https://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IWR/Hornung/Baecker_Hornung_CLSR_2012_627_fulltext.pdf (çevrim içi), E.T. 20.10.2019, 13:30; BOSTANCI BOZBAYINDIR, *a.g.e.*, s.73.

İkinci maddenin üçüncü fıkrasında Direktif'in AB hukukunun uygulama alanı dışındaki faaliyetlerde veya Birlik kurum, organ, ofis ve ajansları tarafından işlenmesinde Direktif hükümlerinin uygulanmayacağı belirlenmiştir. Bu hükme göre Direktif'in uygulama alanı oldukça sınırlandırılmıştır. Örneğin EUROPOL, EUROJUST, OLAF, Schengen Information System (SIS) vb.nin faaliyetleri Direktif tarafından düzenlenmemektedir; bunlar kişisel verilerin korunmasına ilişkin kendi özel düzenlemeleri ile yetinmeye devam edeceklerdir.¹¹⁷ Bu noktada, yukarıdaki açıklamaların ve ifade edildiği şekilde ulusal güvenliğin Direktif'in kapsamı dışında, kamu güvenliğinin ise kapsamın içinde olmasının yarattığı sorunlara ilişkin değerlendirmeleri göz önünde bulundurmakta yarar vardır.¹¹⁸

Tanımlar başlıklı **üçüncü maddede yetkili merciden** anlaşılması gerekenin kamu güvenliğine yönelik tehlikelerin önlenmesi için uygulanan tedbirler ve güvenceler de dahil olmak üzere, adli suçların önlenmesi, araştırılması, tespiti veya kovuşturulması ya da ceza mahkumiyetlerinin infazı konusunda yetki sahibi olan resmi otoriteyi veya bu sayılan amaçlar doğrultusunda üye devlet tarafından kamusal yetki ve kamu gücü kullanmakla yetkilendirilmiş herhangi bir organ veya kuruluşu ifade ettiği açıklanmıştır. Buna göre örneğin, özel güvenlik görevlilerinin faaliyetleri doğrultusunda işlediği kişisel veriler de Direktif kapsamındadır.

Kişisel verilerin işlenmesine ilişkin ilkeler başlıklı **dördüncü maddede** üye devletlerin, kişisel verilerin hukuka uygun ve adil bir şekilde işlenmesini; belirli, açık ve meşru amaçlarla elde edilmesini ve bu amaçlarla uyumsuz biçimde işlenmemesini; işlendikleri amaçlarla ilgili olarak yeterli, ilgili olmasını ve aşırı olmamasını sağlamakla yükümlü olduğu düzenlenmiştir. Söz konusu veriler doğru ve gerektiğinde güncel tutulmalı; işledikleri amaçlar göz önüne alınarak, hatalı olanların silinmesini veya düzeltilmesini

sağlamak için tüm makul adımlar atılmalıdır. Veriler, ilgili kişilerin kimliğinin belirlenmesine izin verecek hallerde, işlendikleri amaca göre gerektiğinden daha uzun bir süre tutulmamalıdır. Diğer bir deyişle, verilerin işlendikleri amaç doğrultusunda artık anonimleştirilmesi veya silinmesi mümkün olduğunda, bu yola başvurulmalıdır. Hükme göre üye devletler, bu verilere yetkilendirilmemiş veya yasadışı erişimlere karşı, uygun teknik veya yapısal önlemleri alarak; kazara kayıp, imha veya hasar olasılıklarına karşı koruma gibi uygun tedbirleri almalıdır.

Kişisel verilerin toplandığı amaç dışında (Direktif'in birinci maddesinde belirtilen amaçlardan biri olmak kaydıyla) aynı veya başka bir veri sorumlusu tarafından işlenmesi ancak belirli koşulların varlığı halinde mümkündür (m. 4/2). Bu koşullar; veri sorumlusunun Birlik veya ülke hukuku gereği bu verileri böyle bir amaçla işlemeye yetkili olması ve bu verileri Birlik veya ülke hukukunca diğer amaçla da işlemenin gerekli ve ölçülü olmasıdır. Hükümde bu ikisi ve bağlayıcı ile bağlandığından bunların kümülatif koşullar olarak anlaşılması gerekir.

Direktif'in **altıncı maddesinde**, daha önceki veri koruma rejiminde olmayan kişisel veri sahiplerinin farklı kategorilere ayrılması öngörülmüştür. Buna göre, bir kişinin suç işlediğine veya işlemek üzere olduğuna inanmak için ciddi nedenler bulunanlar bir gruba (a); bir suçtan mahkum olanlar bir gruba (b); işlenmiş veya işleneceğine inanmak için belirli olguların bulunduğu suçların (potansiyel) mağdurları bir diğer gruba (c); ve tanık olarak dinlenebilecek veya kovuşturmaya bilgi sağlayabilecek kişiler ile ilk iki gruptaki kişilerle bağlantılı veya ortak olan diğer kişiler ayrı bir gruba (d) ayrılmıştır. Bu hükmün uygulanmasında, bir suç işlendiği gerekçesiyle başlayan soruşturmanın doğrusal akışı boyunca, veri sahibinin hukuki konumu ve hakları da; veri sorumlusunun hukuki yükümlülükleri de değişecektir. Bir görüşe göre, bu ayırım ilk bakışta olumlu gibi görünse de; adli sürecin ilerleyen aşamalarındaki kişilerin kişisel verilerin korunması standartlarının düşmesine yol açaca-

¹¹⁶ BOSTANCI BOZBAYINDIR, *a.g.e.*, s.75.

¹¹⁷ HERT / PAKONSTANTINOU, *a.g.e.*, s.10-11.

¹¹⁸ Bkz. Yuk. § IV/D-2, paragraf 14.

ğından ayrımcı bir yaklaşımdır.¹¹⁹ Kanımızca böyle bir çıkarımda bulunmak için henüz erkendir; uygulamanın dikkatle gözlemlenmesi gerekir.

Yedinci maddede, üye devletlerin kişisel verilerin mümkün olduğunca kişisel değerlendirmelerden ayrılmasını sağlamaları gerektiği vurgulanmıştır. Bunun yanında yetkili merciler doğru veya güncel olmayan, eksik verilerin kullanıma sunulmamasını / bulundurulmamasını¹²⁰ ve aktarılmamasını sağlamalıdır. Bu amaçla yetkili merciler mümkün mertebe verilerin güncelliğini ve doğruluğunu verilerin bulundurulmasından ve aktarılmasından önce denetlemelidir. Bir kişisel verinin aktarımdan sonra hatalı vb. olduğu anlaşılırsa, alıcının konu hakkında gecikmeksizin bilgilendirilmesi gerekmektedir. Ayrıca bu durumda kişisel verinin düzeltilmesi, silinmesi veya işlemenin m.16'ya göre sınırlandırılması gerekmektedir.

Sekizinci maddede Direktif kapsamındaki kişisel veri işlemeyi düzenleyen üye devlet mevzuatının; en azından verilerin işlenmesi ile ulaşılabilecek hedefi, işlemde geçirilecek kişisel verileri ve işlemenin amaçlarını belirtmesi gerektiği düzenlenmiştir. Yine hükmün ilk fıkrasında verilerin yalnızca belirtilen amaçların gerçekleştirilmesi için gerekli olduğunda işlenmesi öngörülmektedir.

Dokuzuncu madde kişisel verilerin işlenmesinde özel durumları düzenlemektedir. Buna göre, kişisel verilerin yetkili mercilerce birinci maddede belirtilen amaçlar doğrultusunda elde edilmesine karşın, burada belirtilen amaçlar dışında işlenmesi kural olarak yasaktır. Ancak yetkili mercilerce bu amaçlar dışında kişisel verilerin

işlenmesi AB veya üye devlet hukuku tarafından izin verilmiş olması koşuluyla ve bu faaliyet Birlik hukukunun kapsamının dışında olmadıkça GVKT (GDPR) hükümlerine göre işlenebilecektir.¹²¹

Onuncu maddeye göre etnik köken, siyasi görüş, dini veya felsefi inanç, sendika üyeliği gibi özel nitelikteki kişisel verilerin işlenmesi ancak bu işlemenin gerçekten gerekli olması, ilgili kişinin hak ve özgürlükleri bakımından gerekli güvencelerin sağlanması ve AB ve üye devlet hukuku tarafından izin verilmiş olması; ilgili kişinin veya başka bir gerçek kişinin yaşamsal menfaatlerini korumak amacıyla ya da bu verilerin, veri sahibi tarafından açıkça alenileştirilmesi halinde mümkündür.

On birinci maddede, üye devletlerin kişisel verileri otomatik işleme tabi tutarak karar alması ve profillemeye¹²² gibi faaliyetlerde bulunmasına karşı birtakım güvenceler getirilmiştir. Buna göre veri sahibini olumsuz şekilde etkileyen bir durum yaratan yahut onu ciddi şekilde etkileyen profillemeye gibi işlemler Birlik veya üye devlet hukukunda izin verilmedikçe ve bu kişilerin hak ve özgürlükleri güvence altına alınmadıkça yapılamayacaktır. Ayrıca söz konusu işleme tabi tutulacak verilerin onuncu maddedekilerden olması halinde bu faaliyet hak ve özgürlüklere yönelik uygun güvenceler oluşturulmadıkça ve meşru menfaat uygun biçimde sağlanmadıkça yasaklanmıştır. Özel nitelikli kişisel veriler esas alınarak profillemeye işlemi ayrımcılığa neden olarsa, bu faaliyetin gerçekleştirilmesi açıkça yasaklanmıştır.

Genel olarak ifade etmek gerekirse, Direktif'te kişisel verilerin yetkili resmi merciler tarafından adli suçların önlenmesi, araştırılması,

¹¹⁹ AKINTUNDE, a.g.e., s.4.

¹²⁰ Kullanıma sunulma / bulundurma kavramı, İngilizce metindeki *make available*; Fransızca metindeki *mettre à disposition*; ve Almanca metindeki *Bereitstellung* sözcüklerinin karşılığında kullanılmış olup, kanımızca bunu "verilerin ilgili kişi ve mercilerin erişimine hazır halde bulundurmak" şeklinde anlamak mümkündür. İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü tarafından yapılan çeviride de bu kavram, "erişilebilir kılma" olarak alınmıştır. Bkz.: <https://itlaw.bilgi.edu.tr/media/2019/7/29/law-enforcement-directive-turkce.pdf> (çevrim içi), E.T. 20.10.2019, 13:30.

¹²¹ Benzer durum kamu yararı doğrultusunda arşivleme, bilimsel veya tarihi araştırma veya istatistiksel amaçlarla işlemede de söz konusudur (m.9/2).

¹²² Profillemeye, herhangi bir otomatik veri işleme usulüne göre, gerçek bir kişiye ait kişisel verilerinden belirli kişilik özelliklerini değerlendirilerek; özellikle kişinin işyerindeki performansı, ekonomik durumu, sağlığı, kişisel tercihleri ve ilgi alanları, güvenilirliği, davranış biçimi, konum veya hareketlerinin tahmin edilebilmesidir. (GVKT m.4/4; 2016/680 sayılı Direktif m.3/4).

tespit edilmesi veya kovuşturulması ya da ceza mahkumiyetlerinin infazı amacıyla işlenmesine birtakım sınırlamalar, temel hak ve özgürlükler açısından güvenceler getirilmektedir. Buna göre kişisel veriler açık, belirli ve meşru amaçlar doğrultusunda amaçla bağlantılı olarak; adil; ölçülü; veri asgarileştirmesine uygun biçimde; verilerin doğruluğunun ve güncelliğini denetlenerek işlenmekte ve bu doğrultuda yetkili merciler arasında paylaşılabilir.

Direktifin **on iki vd. maddelerinde** ilgili kişilerin hakları düzenlenmektedir. Konumuzun kapsamı dışına çıkmamak adına, yalnızca bu hakların hangi hallerde sınırlanabileceğine değinilecek, hakların içeriğine girilmeyecektir. **On ikinci madde**, veri sorumlusunun şeffaflık ilkesi doğrultusundaki bazı yükümlülüklerini düzenlemektedir.

On üçüncü madde, ilgili kişiye sağlanacak bilgileri düzenlemektedir. Buna göre ilgili kişiye veri sorumlusunun kimliğinin, verilerin işlenmesinin amacının ve yasal gerekçesinin, verilerin ne kadar süre saklanabileceğinin vb. bilgilerin sunulması öngörülmüştür. Bununla birlikte, maddenin üçüncü fıkrasına göre üye devletler, bu bilgilerin bazılarının (ikinci fıkrada öngörülenler) ilgili kişiye sağlanmasını geciktirme; sınırlama ve bundan kaçınma amacıyla yasal düzenleme yapabilir. Ancak bunun için böyle bir işlemin ilgili kişinin temel hakları ve meşru menfaatlerini gözeterek demokratik bir toplumda gerekli ve ölçülü olması ve belirli amaçlara hizmet etmesi gerekmektedir. Bu amaçlar sınırlı sayma yoluyla şöyle belirlenmiştir: **a- resmi veya yasal araştırmaları, soruşturmaları veya prosedürleri engellemeyi önlemek; b- adli suçların önlenmesini, tespit edilmesini, soruşturulmasını veya kovuşturulmasını ya da cezai mahkumiyetlerin infazını etkilemeyi engellemek; c- kamu güvenliğini korumak; d- ulusal güvenliği korumak; e- başkalarının hak ve özgürlüklerini korumak.** Dördüncü fıkrada ise üye devletlerin, tamamen veya kısmen 3. fıkrada belirtilen hususların kapsamına girebilecek veri işleme kategorilerini belirlemek için yasal düzenlemeler yapabileceği düzenlen-

miştir. Buna göre örneğin hakkında soruşturma yapılmakta olan bir kişiye, soruşturmayı etkilemesini engellemek gibi amaçlarla, kişisel veri işlemeye dair bazı bilgilerin verilmemesi üye devletin bu konuda yasal düzenleme yapmasıyla mümkün olabilecektir.

On dördüncü madde de yine şeffaflık ilkesi doğrultusunda, ilgili kişinin bilgi edinme hakkını düzenlemektedir. Buna göre, kişisel verilerinin işlenmesinin amacını ve yasal dayanağını, kişisel verilerinin olduğu kategori gibi bilgileri edinebilecektir.

On beşinci maddeye göre üye devletler, ilgili kişinin temel hakları ve meşru menfaatlerini gözeterek demokratik bir toplumda gerekli ve ölçülü olduğu müddetçe ilgili kişinin erişim hakkını tamamen veya kısmen kısıtlayan yasal düzenlemeleri belirlenen amaçlar doğrultusunda yapabilecektir. Bu amaçlar, 13. maddede belirtilen amaçlarla (suçların tespiti, önlenmesi, ulusal güvenlik vb.) aynıdır. Erişimin kısıtlanması veya reddedilmesi halinde ilgili kişiye gecikmeksizin bilgi verilmesi gerektiği; ancak bundan da belirtilen amaçları engelleyeceği durumlarda itiraz hakkı hatırlatılmak suretiyle kaçınılabileceği hüküm altına alınmıştır.

On altıncı maddede unutulma hakkı bağlamındaki kişisel verilerin düzeltilmesi ve silinmesi hakları ile işlenmesinin kısıtlanması düzenlenmektedir. Maddenin üçüncü fıkrasına göre bir kişisel verinin, ilgili kişinin itiraz etmesine karşın doğruluğu veya yanlışlığının henüz tespit edilememesi halinde¹²³ yahut bu verinin delil olarak saklanması gerektiği hallerde, silinmesi yerine işlenmesinin kısıtlanması veri sorumlusu tarafından sağlanır.

On sekizinci maddede, üye devletlerin madde 13, m.14 ve m.16'daki hakların kullanılması amacıyla; kişisel verilerin yargısal kararlarda, kayıtlarda (duruşma tutanaklarında) veya soruşturma ve kovuşturma evrelerindeki işlem dosyalarında tutulduğu hallerde ulusal hukukun

¹²³ Bu halde, veri işleminin kısıtlanmasına son verileceği zaman önce ilgili kişi bilgilendirilir (fıkra 3, 2. cümle).

uygulanmasını öngörebileceği düzenlenmiştir.¹²⁴ Üye devletler, ilgili kişinin temel hakları ve meşru menfaatlerini gözetererek demokratik bir toplumda gerekli ve ölçülü olduğu müddetçe ilgili kişinin bilgilendirilmesini tamamen veya kısmen kısıtlayan yasal düzenlemeleri belirlenen amaçlar doğrultusunda yapabilecektir. Bu amaçlar 13. maddede belirtilen amaçlarla (suçların tespiti, önlenmesi, ulusal güvenlik vb.) aynıdır. Madde- nin beşinci fıkrasına göre veri sorumluları yanlış kişisel verilerin düzeltilmesini, bu verilerin kaynaklandığı yetkili otoriteye bildirmelidir. Altıncı fıkraya göre düzeltilen, silinen veya işlenmesi kısıtlanan kişisel verilerin alıcıları da veri sorumlusu tarafından bilgilendirilecek ve bu doğrultuda hareket edeceklerdir.^{125,126}

IV. 6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Verilerin Adli ve Önleyici Amaçla İşlenmesi

A. Kanundaki İstisnalar

Anayasa'nın 20. maddesinin 3. fıkrası doğrultusunda¹²⁷ hazırlanan 6698 s. Kişisel Verilerin

¹²⁴ Direktif'in 13. maddesinde ilgili kişinin bilgilendirilmesi, 14. maddesinde bilgi edinmeye ilişkin haklar, 16. maddesinde ise kişisel verilerin düzeltilmesi veya silinmesi ve veri işlemenin sınırlandırılması hakkı düzenlenmektedir.

¹²⁵ Çalışma konumuzun kapsamını aşma kaygısıyla Direktif hükümlerinin değerlendirilmesi bu kadarla sınırlı tutulmuştur. Bu nedenle veri sorumlusunun ve işleyeninin yükümlülüklerine, veri güvenliğine, bağımsız denetim organına ilişkin hükümlere, verilerin üçüncü ülkeler ve uluslararası kuruluşlarla paylaşılmasına vs. değinilmeyecektir.

¹²⁶ Direktif'in 19 vd. maddeleri ise çalışma konumuzun kapsamının dışında kaldığından üzerinde durulmayacaktır. Bu hükümlerle ilgili genel bir değerlendirme için bkz.: BOSTANCI BOZBAYINDIR, a.g.e., s.80-89.

¹²⁷ AY m.20/3: "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

Korunması Kanunu, 07.04.2016 Tarihli Resmi Gazete'de yayımı tarihinde, bazı hükümleri ise 6 ay sonra yürürlüğe girmiştir. Kanun'un kapsamı, 2. maddede, "(...) kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır" şeklinde belirlenmiştir. Kanun, kişisel verilerin korunmasına ilişkin dünyadaki gelişmelere paralel olarak güvenceleri, hakları; kişisel verilerin işlenmesine getirilen sınırlamaları ve temel ilkeleri düzenlemektedir. Ancak yukarıda belirtildiği üzere AB mevzuatının gerisinde bir kanundur.¹²⁸

Kanun'da belirtilen hak ve yükümlülükler ile güvencelerin, temel ilkelerin ve veri işlemeye ilişkin sınırlamaların bir kısmının veya tamamının bazı faaliyetler söz konusu olduğunda uygulanmayacağı 28. maddede düzenlenmiştir.¹²⁹

¹²⁸ Bkz. Yuk. § II.

¹²⁹ "MADDE 28- (1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz: a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi. b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi. c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi. ç) Kişisel verilerin millî savunmayı, millî güvenliği, 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 işlenmesi. d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi. (2) Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10'uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11'inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16'ncı maddeleri aşağıdaki hâllerde uygulanmaz: a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya

İstisnalar kenar başlıklı bu hükmün ilk fıkrasında Kanun hükümlerinden tamamen istisna tutulan, yani Kanun'un hiçbir hükmünün uygulanmayacağı haller belirlenmiştir. Konumuzla ilgili olan bu faaliyetler: (ç) ve (d) bentlerinde şu şekilde belirtilmiştir: “**ç**) *Kişisel verilerin millî savunmayı, millî güvenliği, 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 işlenmesi.* **d**) *Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.*”

Bununla birlikte, Kanun'un bazı hükümlerinin uygulanmayacağı, geri kalanların ise uygulanacağını belirttiği, yani kısmen istisna tuttuğu konumuzla ilgili faaliyetler ise 28. maddenin 2. fıkrasında “**a**) *Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması*” şeklinde belirtilmiştir.

B. İstisna Sayılmanın Sonuçları

Yirmi sekizinci maddenin ilk fıkrası uyarınca KVKK hükümlerinden tamamen istisna tutulmuş olmak, yalnızca KVKK hükümlerinin uygulanmayacağı anlamına gelmektedir.¹³⁰ Bu faaliyetler

suç soruşturması için gerekli olması. b) ilgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi. c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurum niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturma için gerekli olması. ç) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.”.

¹³⁰ KVKK hükümlerinin uygulanmadığı bu alanlarda, TCK'de düzenlenen Özel Hayata ve Hayatın Gizli Alanına Karşı Suçların kamu görevlisi tarafından, görevin verdiği yetki kötüye kullanılmak suretiyle (m. 137/1-a) işlenmesi haline ilişkin olarak, kamu görevlilerinin görevinin gereklerini belirlemeye yönelik davranış normlarında boşluk olduğu eleştirisi için bkz.: BÖREKÇİ, Eşref Barış: “Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu”, *Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü*, Yayınlanmamış Yüksek Lisans Tezi, 2019, s.112.

KVKK dışındaki diğer hukuk kurallarının öngördüğü sınırlamalara ve genel ilkelere tabi olacaktır. Dolayısıyla örneğin istihbari faaliyetlerin KVKK'da öngörülen sınırlamaların dışında tutulmuş olması, bu alana ilişkin kişisel verilerin sınırsız ve ölçsüz biçimde işlenebileceği anlamına gelmemektedir.

Maddenin 2. fıkrasında sınırlı sayma yoluyla yalnızca belirli hükümlerin ilgili faaliyetlerde uygulanmayacağı düzenlenmiştir. Bunlar; *veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10'uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11'inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16'ncı maddeleridir*. Dolayısıyla bu hükümler haricindeki KVKK'nin tüm hükümleri sayılan faaliyetler için de uygulanabilecektir.

O halde KVKK hükümlerinden kısmen istisna tutulan faaliyetlere, ilgili kişisel veriler bakımından Kanun'un 4. maddesinde düzenlenen kişisel verilerin hukuka ve dürüstlük kurallarına uygun; doğru ve gerektiğinde güncel biçimde; belirli, meşru ve açık amaçlarla; amaçla bağlı, sınırlı ve ölçülü olarak; gerekli ve sınırlandırılmış süre için işlenmesi zorunluluğu geçerlidir. Yine 5. maddede belirtilen kişinin açık rızası ile yahut rızanın aranmadığının kanunda açıkça öngörülmesi halinde işlenebileceği hükmü de kısmen istisna tutulan faaliyetlerde uygulanabilecektir. Bununla birlikte 6. maddede belirtilen özel nitelikli kişisel verilerin işlenmesine ilişkin kurallarda, ilgilinin açık rızası olmaksızın işlemenin mümkün olmadığı belirtilmiştir. Bu durumda, m.28/2-a uyarınca “bir suç soruşturması için gerekli” olduğunda, kişinin özel nitelikli kişisel verisi, onun açık rızası olmaksızın işlenemeyecek midir? Bunun gibi sorular aşağıda tartışılacaktır.

Kısmen istisna tutulan hallerde, Kanun'un 7. maddesi uyarınca kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin hükümlerin de uygulanabileceği anlaşılmaktadır. Yine, 8. ve 9. maddelerde düzenlenen verilerin aktarılmasına ilişkin kurallar da uygulama alanına sahip olacaktır.

Kanun'un 10. maddesinde düzenlenen veri sorumlusunun aydınlatma yükümlülüğünün kısmen istisna tutulan faaliyetlerde uygulanmayacağı belirtilmiştir. Bu, söz konusu faaliyetlerin niteliği düşünüldüğünde anlaşılabilir bir durumdur. Nitekim, bir suç soruşturması kapsamında yahut suçun önlenmesi amacıyla gerçekleştirilen faaliyetlerde "kişisel veri toplamanın yöntemi"nin açıklanması faaliyetin gerçekleştirilmesini engelleyebilecektir. Ancak 10. maddenin alt bentlerinde sayılan yükümlülüklerin hiçbirinin uygulanmayacağına belirtilmesi, yukarıda açıklanan 2016/680 s. Direktif'in paralel düzenlemeleri (m.12 vd.) ile uyumsuzdur.¹³¹

Kısmen istisna tutulan faaliyetlere KVKK'nin 11. maddesinin 1. fıkrasının (ğ) bendinde yer alan zararın giderilmesini talep hakkı hariç, aynı maddede düzenlenen diğer haklar uygulanacaktır. Gerçekten, ilgili kişinin *verileri işlenmişse buna ilişkin bilgi talep etmesi* bazı "suç işlenmesinin önlenmesi için gerekli" faaliyetlerle bağdaşmayabilir, zira bu faaliyetler gizli nitelikte olabilir. Ancak yine de Kanun'un ilgili kişinin haklarına ilişkin sınırlama yaklaşımının, 2016/680 s. Direktif ile uyumlu olduğu söylenemez.

Kanun'un veri güvenliğine ilişkin hükümleri kısmen istisna tutulan hallerde de uygulanacaktır. Veri güvenliğinin sağlanması, izinsiz erişimlerin engellenmesi hem veri işleyen ve sorumlusunun menfaatleri açısından, hem de ilgili kişinin hakları açısından önemlidir. Bu isabetli bir yaklaşım olsa da, kanımızca tamamen istisna tutulan hallerde de veri güvenliği ilkesinin benimsendiğinin açıkça düzenlenmesi gerekirdi.

Kısmen istisna tutulan faaliyetlerde, Kanun'un 13 ilâ 15. maddeleri arasında düzenlenen veri sorumlusuna başvuru, kurula şikayet ve buna ilişkin usul ve esaslara ilişkin hükümler uygulanacaktır. 16. maddede düzenlenmekte olan veri sorumluları siciline ilişkin hüküm ise uygulanamayacaktır. Kanun'un 17 vd. hükümleri suçlar ve kabahatlere, 19 vd. hükümleri ise Kişisel Verileri Koruma Kurumu ve teşkilatına ayrılmıştır.

¹³¹ Bkz. Yuk.: § IV/D-3.

Açıklananlara ek olarak, 28. maddenin 2. fıkrasında kısmen istisna tutulan faaliyet alanlarında *Kanun'un amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla* bazı hükümlerin uygulanmasının sınırlandırıldığı belirtilmektedir. Dolayısıyla her ne kadar belirli ilke ve hakların bu faaliyetlerde uygulanmayacağı belirtilmiş olsa da, bu sınırlama kanunun amacına ve kişisel veri işlemenin temel ilkelerine aykırı olmayacaktır. Örneğin kişisel verilerin işlenmesinde ölçülülük, amaca bağlılık ilkesi gibi pek çok ilke her halükarda uygulanmalıdır. Bununla birlikte, kanunda kısmen ve tamamen istisna tutulan hallere ilişkin sınırlamalar; hangi hak, güvence, ilke ve sınırlamaların uygulanıp, hangilerinin uygulanmayacağına ilişkin düzenlemelerin 2016/680 s. Direktif ile uyum içerisinde olduğunu söylemek güçtür. Yapılması gereken, bu konudaki en güncel uluslararası (108 s. Sözleşme [hatta 108+esas alınarak])¹³² ve uluslararası (AB hukuku bk., 2016/680 s. Direktif) hukuki metinler doğrultusunda KVKK hükümlerinin yeniden düzenlenmesidir.¹³³ Söz konusu hukuki metinler -her ne kadar yukarıda açıklanan nedenlerle yetersiz olmakla eleştirilse de- bu yaklaşım, çağın gereklerine uygun hareket edilmesini sağlayacaktır.

C. Kanun'un Tamamen ve Kısmen İstisna Ayrımındaki Belirsizlik

Yukarıda belirtildiği üzere KVKK'nin 28. maddesinin ilk fıkrasında "*ç) Kişisel verilerin millî savunmayı, millî güvenliği, 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 işlenmesi; d) kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi*" durumları tamamen istisna tutulmuş; ikinci fıkrasında, "*a) Kişisel veri işlemenin suç işlenmesinin önlenme-*

¹³² Bkz. Yuk. § IV/B.

¹³³ 2016/680 sayılı Direktif'te sayılan yöntemler açısından kişisel verilerin korunmasına ilişkin ayrım ve düzenlemelerin Türk hukukunda da benimsenmesi gerektiğine ilişkin: BÖREKÇİ, a.g.e., s.116.

si veya suç soruşturması için gerekli olması” durumu kısmen istisna tutulmuştur. Kanun’un lafzında önleyici ve adli amaçlı faaliyetlerde tamamen ile kısmen istisna tutmaya ilişkin bir belirsizlik olduğu görülmektedir. O halde uygulamada hangi faaliyetlerin KVKK hükümlerinin uygulanmasından tamamen, hangilerinin kısmen istisna tutulduğunun tespit edilmesi son derece önemlidir. Bunun belirlenmesi, örneğin PVSK ek m.7/6 uyarınca gerçekleştirilen önleyici amaçlı teknik araçlarla izleme kapsamında işlenen kişisel veriler hakkında verilerin silinmesi, yok edilmesi yahut anonim hale getirilmesi işlemlerinin uygulanabilip uygulanamayacağı¹³⁴ gibi tespitlerin yapılmasını sağlayacaktır.

İlk olarak önleyici amaçlı faaliyetler üzerinden değerlendirmek gerekirse; Kanun’da milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak yetkili mercilerin gerçekleştirdiği önleyici, koruyucu ve istihbari faaliyetler tamamen istisna tutulmuştur. Kişisel veri işleminin suç işlenmesinin önlenmesi için gerekli olması ise kısmen istisna tutulmuştur. Kanun koyucunun ‘önlemeye’ yönelik bu ayrımı bilinçli olarak yapıp yapmadığının; bu ayrım ile hangi faaliyetleri tamamen, hangi faaliyetleri kısmen istisna tuttuğunun incelenmesi gerekir.

Birinci halde; milli güvenlik, kamu güvenliği gibi gerekçelerle gerçekleştirilen önleyici ve istihbari faaliyetlerden söz edilmektedir. Bunun *suç işlenmesinin önlenmesine* göre daha makro düzeyde, ulusal güvenliğe ilişkin faaliyetleri işaret ettiği düşünülebilir. Yukarıda önleyici amaçlı faaliyetler ile istihbari faaliyetlerin yakınlaşmasından; 5397 s.k. ile jandarmaya ve polise tanınan önleyici amaçlı istihbari yetkilerden söz edilmişti.¹³⁵ Polis ve jandarmanın söz konusu yetkisinde organize suçlardan bazılarının, devletin güvenliğine, anayasal düzene ve bu düzenin işleyişine, milli

savunmaya ve devlet sırlarına karşı suçlar olduğu göz önünde bulundurulduğunda; bu faaliyetlerin kamu güvenliğinin korunmasına hizmet edecek büyüklükte önleyici nitelik taşıdığı düşünülebilir. Bununla birlikte MİT’in gerçekleştirdiği -5397 s.k. ile kendisine tanınan yetki de dahil olmak üzere¹³⁶ istihbarat faaliyetlerinin ulusal güvenliğe yönelik olduğu ve bu doğrultuda tamamen istisna tutulduğu anlaşılmaktadır. Gerçekten, madde gerekçesi¹³⁷ de bu görüşümüzü destekler niteliktedir:¹³⁸ “(...) **Milli İstihbarat Teşkilatı ile diğer istihbarat birimlerinin milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik faaliyetler kapsamında işlediği veriler Kanun kapsamı dışında tutulmaktadır. Aynı şekilde belirtilen amaçlarla, suç gelirlerinin aklanması, terörizmin finansmanının önlenmesi ve mali suçların araştırılması konusunda; yetkili birim tarafından yürütülen faaliyetler kapsamında işlenen veriler de bu istisna kapsamındadır (...)**”. Gerekçe bağlayıcı olmasa da, diğer istihbarat birimleri ile polis ve jandarmaya da tanınan istihbari yetkilerin kastedildiği düşünülebilir. Bunun yanında Mali Suçları Araştırma Kurulu’nun (MASAK), m.28/1 uyarınca “ekonomik güvenliği sağlamaya yönelik” faaliyetleri kapsamında kişisel veri işleminin de tamamen istisna tutulduğu anlaşılmaktadır. Kısmen istisnaların sayıldığı 2. fıkranın (a) bendinde ise “**kişisel verileri işleminin suç işlenmesinin önlenmesi, için gerekli olması**” hali düzenlenmiştir. Birinci fıkrada belirtilen önleyici faaliyetler dışında kalan suç işlenmesini önleyici işlemler, 2. fıkra kapsamında düşünülebilir. Bunun içeriğine ancak ulusal güvenlik veya kamu düzeni ve güvenliğiyle ilgili olmayan, suçların önlenmesi gibidir. Ne var ki, bu belirlemeye rağmen maddenin 1. fıkrasındaki önleyici faaliyetler kavramı ile, 2. fıkrasındaki suç işlenmesinin önlenmesi kavramları yine de birbirine karışabilecektir. Nitekim uygulamada hangi önleyici faaliyetin kamu düzenini koruma-

¹³⁴ Bu, KVKK m.7 uyarınca kısmen istisna tutulan hallerde uygulanan; fakat tamamen istisna tutulan hallerde uygulanmayan bir güvencedir. Bunun gibi, kısmen ve tamamen istisna tutulan haller arasındaki farklar da bu belirlemenin yapılmasını gerektirmektedir.

¹³⁵ Bkz. Yuk. § III/C-2-b,c.

¹³⁶ Bkz. Yuk. § III/C-2-c.

¹³⁷ <https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf>, s.16-17, (çevrim içi), E.T. 20.10.2019, 13:30.

¹³⁸ Aşağıda belirtilen 2014 tasarısındaki ayrım da bu görüşümüzü desteklemektedir.

ya¹³⁹ yönelik olduğunun; hangisinin olmadığını *apriori* olarak kategorik biçimde belirlenmesi son derece güçtür.

Adli amaçlarla kişisel veri işlenmesini gerektiren faaliyetlerin hangilerinin tamamen, hangilerinin kısmen istisna tutulduğunun ayırımı ise çok daha güçtür. Zira, 28. maddenin 1. fıkrasında kişisel verilerin *soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi* tamamen istisna tutulmuş; 2. fıkrasında ise *suç soruşturması için gerekli olması* kısmen istisna tutulmuştur. Sorun, iki hükümde de yer alan *soruşturma* ifadesinden doğmaktadır. Buna karşılık, 2. fıkrada belirtilmeyen kovuşturma evresi ve ceza muhakemesinde yargılama ve infaz işlemlerinde kişisel verilerin işlenmesi 1. fıkra kapsamında açıkça zikredilmiştir. Dolayısıyla bu faaliyetlerin tamamen istisna tutulduğu düşünülebilir. Yine de, yargı makamları veya infaz mercilerinin kovuşturma evresi ve infaz aşamasında kişisel verileri işlenmesinin tamamen istisna tutulmasının 2016/680 s. Direktif bakımından uyumlu bir yaklaşım olmadığını akılda tutmak gerekir.

Kanunun açık hükmü doğrultusunda “*suç soruşturması için gerekli olanlar*” dışındaki *soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından* yürütülen faaliyetlerin tamamen istisna tutulduğunu kabul etmek gerekmektedir. Sorun, yargı makamı veya infaz mercii sayılmayan; ancak suç soruşturmasında kişisel veri işleyen merciler açısından doğmaktadır. O halde, böyle bir mercii olup olmadığının, varsa nasıl değerlendirileceğinin tespiti gerekir. Türk hukukunda soruşturmayı başlatmak ve yürütmekle görevli merci C. Savcılıklarıdır. Bilindiği üzere, soruşturma evresinde C. savcısı, emrindeki adli kolluk vasıtasıyla delilleri toplayacaktır. Burada delil değeri taşıyan kişisel verilerin de suç soruşturması kapsamında elde edilmesinin ve saklanmasının gerektiği açıktır. Bu durum ikinci fıkradaki ifadeye uyuyor gibi görünmektedir. Ancak ilk fıkrada da soruşturma işlemlerinde kişisel verilerin işlenmesinden söz edilmektedir. İlk fıkra hükmünde

¹³⁹ Maddede yalnızca ulusal güvenliğin korunmasından değil, kamu düzeni ve güvenliğinin korunmasından da bahsedildiğine dikkat edilmelidir.

aynı zamanda kişisel verilerin “yargı makamları veya infaz mercileri tarafından işleme[sinden]” söz edilmektedir. Acaba birinci fıkrada C. Savcısının yaptığı işlemler mi dışarıda bırakılmıştır? Bu konuda madde gerekçesi hükmün tekrarıyla ibaret olduğundan, yol gösterici nitelikte değildir. O halde yapılabilecek tek şey, C. savcısının bir yargı veya infaz mercii olup olmadığının belirlenmesidir.

Tartışmanın özü C. savcısının suç soruşturması kapsamındaki yetkileri olduğundan, infaz mercii sayılıp sayılmadığının değerlendirilmesine gerek yoktur. Anayasa’nın 9. maddesinde “*Yargı yetkisi, Türk Milleti adına bağımsız ve tarafsız mahkemelerde kullanılır*” geçmektedir. CMK’nın 112. maddesinde de, “*(...) yetkili yargı mercii hemen tutuklama kararı verebilir*” hükmü yer almaktadır. C. savcısının tutuklama kararı veremeyeceği düşünüldüğünde, burada yargı merciiinden kastedilenin mahkemeler olduğu anlaşılmaktadır. Bu örneklerin çoğaltılması mümkündür. Nitekim C. Savcısı, bir yargı makamı değil; toplumsal iddia makamını işgal eden süjüdür.¹⁴⁰ Dolayısıyla C. savcısının soruşturma evresindeki suç soruşturması faaliyetlerinin KVKK’da 1. fıkra değil; 2. fıkra kapsamında ele alındığı, yani kısmen istisna tutulduğu sonucuna varılmaktadır. Bununla birlikte infaz veya yargı makamlarının soruşturma işlemlerinde kişisel veri işlenmesini gerektiren faaliyetlerin de tamamen istisna tutulduğunu akılda tutmak gerekir. O halde C. Savcılığı tarafından soruşturma evresinde kişisel veri işleme faaliyeti, KVKK’nin yukarıda belirtilen¹⁴¹ sınırlama rejimine uygun olarak yerine getirilmelidir.

Bilindiği üzere KVKK yasalaşmadan önce 2008 ve 2014 yıllarında başka yasa tasarıları hazırlanmış idi. Bu doğrultuda bu tasarıların da incelenerek, istisnaların belirlenmesinde nasıl bir yaklaşımın benimsendiği üzerine düşünmek tartışmaya ışık tutacaktır. İlk olarak, 2014 tasarısında¹⁴² istisnalar 24. maddede düzenlenmiş ve

¹⁴⁰ CENTEL / ZAFER, *a.g.e.*, s.113.

¹⁴¹ Bkz. Yuk. § IV/B.

¹⁴² 03.11.2014 tarihinde Adalet Bakanlığınca hazırlanarak meclise sunulmuş ve fakat kadük hale gelmiştir. Kişisel Verilerin Korunması Kanun Tasarısı (2014) <http://www2.tbmm.gov.tr/d24/1/1-1009.pdf> (çevrim içi), E.T. 20.10.2019, 13:30.

tamamen ve kısmen istisna tutulan haller ayrılmıştır. Yirmi dördüncü maddenin ilk fıkrasının (ç) bendinde tamamen istisna tutulan hallerde PVSK, JTK ve MİT K.'nin isimleri açıkça zikredilmiş, *bu kanunların istihbari faaliyetlere ilişkin hükümleri çerçevesinde kişisel verilerin işlenmesinden* söz edilmiş, önleyici amaçtan bahsedilmemiştir. Nitekim, söz konusu maddenin gerekçesinde de, “2559 sayılı Kanun, 2803 sayılı Kanun, 2937 sayılı Kanunun sadece istihbari faaliyetlere ilişkin hükümleri çerçevesinde kişisel verilerin işlenmesi hali kanunun kapsamı dışında tutulmaktadır. Bununla birlikte, bu kanunların, istihbari faaliyete ilişkin hükümleri dışında kalan hususların Kanun kapsamında kaldığı açıktır. Örneğin bu kanunların pasaport, trafik ve personel gibi konulara ilişkin hükümlerindeki genel düzenlemelere istinaden yapılacak işlemler bakımından Kanun hükümleri geçerli olacaktır” ifadesi geçmektedir. Dolayısıyla önleyici amaçlı da olmayan kolluk faaliyetleri bakımından Kanun hükümleri uygulama alanı bulacaktır.

Kısacası 2014 tasarısının önleyici amaçla kişisel veri işlemeye ilişkin KVKK'dan temel farkı; tamamen istisna tutulan hallerle ilişkin faaliyetlerin düzenlendiği kanunlarının adlarının açıkça sayılmasıdır. Bu nedenle istihbari nitelikte olmayan veya ulusal güvenliği, kamu düzenini korumaya yönelik olmayan önleyici faaliyetlerden hangilerinin hangi istisna başlığında değerlendirileceği sorusu yine net bir biçimde yanıtlanamamaktadır. Kanımızca, KVKK'nin mevcut lafzı karşısında bu şekildeki faaliyetlerin kısmen istisna tutulduğu sonucuna varılmaktadır. Ancak, bu belirlemenin açıkça yapılması, muğlaklığın giderilmesi açısından isabetli olacaktır.

2014 tasarısında adli suçların soruşturulması, kovuşturulması veya mahkumiyet hükümlerinin infazına ilişkin olarak, maddenin 3. fıkrasında; “Soruşturma, kovuşturma, yargılama ve infaz mercileri tarafından kişisel verilerin işlenmesinde ve korunmasında ilgili kanun hükümleri uygulanır. İlgili kanunlarda hüküm bulunmayan hallerde, 9'uncu, 10'uncu ve 15'inci maddeleri hariç olmak üzere, bu Kanun hükümleri uygu-

lanır” denilmekte ve gerekçesinde de bu ifade tekrar edilmektedir. Kısacası, bu faaliyetler bütünüyle kısmen istisna tutulmaktadır. Oysa KVKK'da bu hususta ikili bir ayırım yapılmış idi. Tasarıdaki bu hüküm, konuya yaklaşım açısından önem taşısa da; KVKK'nin mevcut düzenlemesindeki belirsizliği izah etmemektedir.

Son olarak konuya ışık tutması amacıyla 2008 tasarısına da değinilecektir.¹⁴³ Bu tasarıda yalnızca kısmen istisna tutulan hallerle yer verilmiştir. Tasarının 22. maddesine göre, “(a) milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi veya bu amaçla yapılan istihbari faaliyetlerin yürütülmesi; (b) kamu düzeninin korunması ve suç işlenmesinin önlenmesi; (c) suçun önlenmesi için gerekli olması, suç veya meslek ahlak kurallarını ihlal eden eylemlerin soruşturulması veya kovuşturulması” durumları kısmen istisna tutulmuştur. Burada istihbari faaliyetler ile kamu düzeninin korunması ve suçların önlenmesinin ayrı ayrı ele alındığı görülmektedir. Özellikle KVKK'da milli güvenliği, milli savunmayı, kamu düzeni ve kamu güvenliğini aynı bentte sayarak bu amaçla gerçekleştirilen önleyici, koruyucu ve istihbari faaliyetlerin aynı bentte sayılmasındansa, ayrı ayrı ele alınması (bağlanan hukuki sonuçtan bağımsız olarak) daha isabetli bir yaklaşımdır. Zira kamu düzeni ve kamu güvenliği ile ulusal güvenlik farklı kavramlardır. Aynı cümlede yer verilmesi, bu doğrultularda gerçekleştirilen faaliyetlerin de sanki aynı amaca hizmet ediyor gibi algılanmasına neden olmaktadır. 2008 tasarısında ayrıca, suç işlenmesinin önlenmesi de, suçların soruşturulması ve kovuşturulması da kısmen istisna tutulmuştur.

Bütün bu açıklamalar, ne yazık ki kanundaki belirsizliği tam olarak gidermeyi sağlamamaktadır. Yine de önleyici ve istihbari faaliyetlere ilişkin KVKK açısından yapılabilecek **temel çıkarım şudur:** ağırlıklı olarak milli güvenliği ve milli savunmayı, kamu güvenliğini ve kamu düzenini sağlama, suçları önleme gibi amaçlarla istihbari yetkiler kullanan mercilerin bu yöndeki kişisel

¹⁴³ Kişisel Verilerin Korunması Kanun Tasarısı (2008), <https://www2.tbmm.gov.tr/d23/1/1-0576.pdf> (çevrim içi), E.T. 20.10.2019, 13:30.

veri işleme faaliyetleri tamamen istisna tutulmuş;¹⁴⁴ buna karşılık, istihbari nitelik taşımayan ve yalnızca münferit suçların önlenmesine yönelik olan, kamu düzeni ve güvenliğini sağlama boyutunda olmayan kişisel verilerin işlendiği faaliyetler kısmen istisna tutulmuştur. Tekrar ifade edilmelidir ki bu, pratikteki belirsizliği giderme amacı taşıyan zorlama bir yorumdur. Yapılması gereken, kanun koyucu tarafından belirsizliğin giderilmesidir.

Bununla birlikte adli amaçlı yöntemler açısından sorun, kanunun lafzı nedeniyle kolayca çözülememektedir. Böylesi önemli bir konuda açık ve belirsizlikten uzak bir düzenleme yapılmadıkça adeta sözcüklerle oynayarak anlama ulaşma çabası içinde bulunulacaktır. Kanun'un mevcut düzenleniş itibarıyla C. Savcısının soruşturma evresi kapsamında işlediği kişisel verilerin kısmen; yargı veya infaz mercileri tarafından soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak işlenen kişisel verilerinse tamamen istisna tutulduğu sonucuna ulaşılmaktadır.

Açıklamalar doğrultusunda bazı kolluk yetkilerinin KVKK bakımından tamamen mi kısmen mi istisna tutulduğunun incelenmesi isabetli olacaktır. İlk olarak, polisin PVSK m.5 uyarınca parmak izi ve fotoğraf veri tabanı oluşturma yetkisine ilişkin olarak, maddenin 6. fıkrasında *"Bu sistemde yer alan bilgiler, kimlik tespiti, suçun önlenmesi veya yürütülmekte olan soruşturma ve kovuşturma kapsamında (...) kullanılabilir"* denildiğinden; kanımızca suç 2. fıkrada yer alan kısmen istisna tutulan hükümler arasındadır. Zira bu, ulusal güvenliğe veya kamu düzeni ve güvenliğine yönelik bir faaliyet niteliği taşımaktadır. Buna karşılık yukarıda polis ve jandarmanın 5397 s.k. doğrultusunda sahip olduğu istihbari yetkiler her ne kadar önleyici amaçlı olsa da; ör. PVSK ek m.7'de açıkça *Anayasal düzene ve genel güvenliğe dair önleyici ve koruyucu tedbirleri almak* şeklinde açıkça ifade edildiğinden, KVKK m.28/1-ç uyarınca tamamen istisna tutulmaktadır.

¹⁴⁴ (ç) bendindeki bu istisnanın kapsamının uygulama çok sayıda insan hakkı ihlali doğuracağı ifade edilmektedir. Bkz.: ÖNGÜN AYÖZGER, a.g.e., s.34.

Polisin kişisel veri işlediği bir diğer yöntem, polisin toplantı ve gösteri yürüyüşlerinde kayıt yapması konusunu düzenleyen TGYK¹⁴⁵ m.11'de hükmüdür. Bu yetki kapsamında elde edilen veriler, hükmün 2. fıkrasındaki *"... elde edilen kayıt ve görüntüler, şüphelilerin ve suç delillerinin tespiti dışında başka bir amaçla kullanılamaz"* ifadesi doğrultusunda, C. savcısı tarafından soruşturma evresinde kullanılması halinde kısmen istisna tutulan haller kapsamında ele alınabilecektir.

Suçların aydınlatılabilmesi, önlenmesi gibi amaçlarla yetkili merciler tarafından ilgili kişilerin verilerinin işlenmesi doğaldır; fakat suçla ilgisi olmayan bireylerin kişisel verilerinin korunmasına dikkat edilmelidir.¹⁴⁶ Nitekim İstanbul Bölge Adliye Mahkemesi bir kararında *"Yargısal organlara tanınan istisna, ancak uyumsuzluğun tarafları açısından geçerli olabilir. Anayasa'nın 20/3. maddesine göre aynı zamanda temel haklardan olan kişisel verilerin korunmasını isteme hakkı, 6698 Sayılı Yasanın 28/1-d maddesinin geniş yorumlanması ile daraltılamaz"* demek suretiyle konuyla ilgisi olmayan üçüncü kişilerin kişisel verilerinin korunmasının buradaki istisnalar gerekçe gösterilerek sınırlanamayacağını belirtmiştir.¹⁴⁷

Kanımızca suçların soruşturulması, kovuşturulması veya önlenmesi amacıyla kişisel verilerin işlenmesinde belirli güvencelerin tanınması, temel ilkelerin uygulanması ve ilgili kişiye kimi hakların tanınması gerekmektedir. Bunun sınırını, yürütülen faaliyetin niteliği gözetilerek, bu faaliyeti engellememesi ve amacını tehlikeye düşürmemesi oluşturmalıdır. Bu faaliyetlerin tümünü en başından kişisel verilerin korunması hakkının sağladığı güvencelerden yoksun kılmak, temel hak ve özgürlüklere saygılı hukuk devletlerinde olmaması gereken bir tutumdur. Nitekim, yukarıda açıklanan uluslararası ve uluslararası hukuktaki genel eğilim de bu yöndedir.

¹⁴⁵ 06.10.1983 tarih ve 2911 sayılı Toplantı ve Gösteri Yürüyüşleri Kanunu, RG T.08.10.1983, S.18185.

¹⁴⁶ AKGÜL, a.g.e., s.29.

¹⁴⁷ İstanbul BAM, 23.HD., T.31.03.2017, E.2017/596, K.2017/527, www.kazanci.com (çevrim içi), E.T. 20.10.2019, 13:30.

Ayrıca, açıklanmaya çalışıldığı üzere, KVKK'daki istisnaların belirlenmesine ilişkin hükümlerin birbirine son derece yakın anlamlar ifade ettiği ve belirsizliklere yol açtığı gözetilerek, bu muğlaklığı giderecek bir yasal düzenleme yapılması isabetli olacaktır. Her halükarda, gerek kısmen gerekse tamamen istisna tutulan bu hükümlerin dar yorumlanması gerekir.

V. Sonuç

Kişisel verilerin korunması hakkının, özel yaşamın gizliliğinden ayrı bir hak olarak ele alınması, yeni tartışmaları beraberinde getirmiştir. Bunun yanı sıra, pek çok farklı güvence ve ilkenin de kabul edilmesini sağlamıştır. Genellikle özel hukuk ilişkileri boyutuyla üzerinde durulmakla birlikte, devletin de özellikle adli ve önleyici amaçla kişisel veri işlediği; üstelik bunu yaparken kişisel verilerin korunması hakkından doğan belirli sınırlamalara tabi olduğu genellikle gözden kaçmaktadır. Devlet tarafından gerçekleştirilen adli ve önleyici amaçlı faaliyetlerin niteliği itibarıyla bu hak kapsamında sağlanan güvenceler, ilkeler, haklar ve sınırlamalar diğer kişilerin kişisel veri işlemesindeki kadar geniş kapsamlı değildir. Bu nedenle yetkili resmi mercilerce gerçekleştirilen belirli faaliyetler kişisel verilerin korunmasına ilişkin kurallardan tamamen veya kısmen istisna tutulmaktadır.

Çalışmanın esas amacı, yabancı ülke hukukundaki başlıca düzenlemeleri detaylıca inceleyerek, Türk hukukuna ışık tutmak olmuştur. Nitekim oldukça güncel olan bu konu Türk hukuk literatüründe pek az çalışılmış olmakla birlikte; yabancı hukuk literatüründe de genellikle göz ardı edilmektedir.

AİHS, kişisel verilerin korunmasına ilişkin detaylı kriterler koymasa da, "living instrument" / yaşayan belge olmasının getirisi olarak AİHM içtihatlarıyla hakka müdahalenin sınırları şekillenmektedir. Bunun yanında 108 numaralı Sözleşme her ne kadar eski olsa da, ek protokol ile konunun dünyadaki gelişmeler doğrultusunda yeniden gündeme gelmesi isabetli olmuştur. Ek protokolü imzalayan devletlerin sayısının her

geçen gün artması umut vericidir. GVKT ile 680 sayılı Direktif'in oluşturulması gerek resmi mercilere gerekse özel kişilere karşı kişisel verilerin korunması hakkının önemini göstermektedir. Bununla birlikte özellikle resmi mercilerin suçların önlenmesi, aydınlatılması veya ulusal güvenlik gibi amaçlarla kişisel veri işlemesinin de bu haktan doğan belirli güvence ve sınırlamalara tabi tutulması, kişisel verilerin korunmasının özel yaşamın gizliliğinden ayrı bir hak olarak ortaya çıktığının somut göstergelerindedir. Ancak hem resmi mercilerin söz konusu amaçlarla kişisel veri işlemesinin de sınırlanabileceği düşüncesinin oldukça yeni olması itibarıyla hem de bir yandan AB üyesi devletlerin ulusal güvenlik ve egemenlik kaygıları ile kolluk faaliyetlerinin ulusal yönünün ağır bastığı; bir yandansa AB bütünlüğünün uluslararası yöndeki gelişimi düşünüldüğünde, gelecekte söz konusu düzenlemelerde daha fazla ilerleme kat edileceği söylenebilir.

KVKK hükümlerinin, 108 no.lu (özellikle 108+) Avrupa Konseyi Sözleşmesi ve 2016/680 sayılı AB Direktifi hükümleriyle karşılaştırıldığında pek çok açıdan yetersiz olduğu görülmektedir. Kanun'un özellikle 28. maddesinde düzenlenen istisna hükümlerindeki ikili yaklaşım son derece belirsizdir. Bu nedenle kolluğun gerçekleştirdiği hangi faaliyetlere kişisel verilerin korunmasına ilişkin kuralların uygulanacağı, hangilerine uygulanmayacağı net bir biçimde tespit edilememektedir. Yapılması gereken bu konuyu açıklığa kavuşturacak, belirsizlikten uzak bir yasal düzenlemedir. Ayrıca yasal düzenleme yapılırken, çalışmamızda yer yer vurguladığımız güncel yabancı kaynakların yaklaşımından da yararlanması, Örneğin 2016/680 sayılı AB Direktifi'ndeki gibi kişisel verilerin işlenmesinde şüpheli / sanık, suç ortağı, mahkum, mağdur ve suçtan zarar gören, tanık gibi kategorilerin belirlenmesi isabetli olacaktır. Başlıca güncel yabancı hukuk metinlerinden yararlanması, veri kavramının oldukça önemli olduğu günümüzde çağın yakalanmasında bir nebze rol oynayacaktır.

Kaynakça¹⁴⁸**Kitaplar**

- AKDAĞ, Hale:** *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, Adalet Yayınevi, Ankara 2013.
- AKGÜL, Aydın:** *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması - Personal Data Protection*, Beta Yayıncılık, İstanbul 2014.
- AŞIKOĞLU, Şehriban İpek:** *Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri*, On İki Levha Yayıncılık, İstanbul 2018.
- BASAĞALP, Nilgün:** *Kişisel Verilerin Korunması ve Saklanması*, Yetkin Yayınları, Ankara 2004.
- CENDEL, Nur / ZAFER, Hamide:** *Ceza Muhakemesi Hukuku*, 14. Baskı, Beta Yayıncılık, İstanbul 2017.
- DEVELİOĞLU, 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 Yayıncılık, İstanbul 2017.
- ERDEM, Mustafa Ruhan:** *Ceza Muhakemesinde, Organize Suçlulukla Mücadelede Gizli Soruşturma Tedbirleri*, Seçkin Yayıncılık, Ankara 2001.
- GÖZLER, Kemal:** *Hukuka Giriş*, 14. Baskı, Ekin Basım Yayın Dağıtım, Bursa 2017.
- Handbook on Data Protection Law**, Luxembourg: Publications Office of the European Union, 2018, https://www.echr.coe.int/Documents/Handbook_data_protection_02ENG.pdf.
- KATOĞLU, Tuğrul:** *Polis Vazife ve Salahiyet Kanunu ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun Tasarısı Hakkında Hukuki Görüş*, Türkiye Barolar Birliği Yayını, Ankara 2014.
- KÜZECİ, Elif:** *Kişisel Verilerin Korunması*, 3. Baskı, Turhan Kitabevi Yayınları, Ankara 2019.
- ÖNGÜN AYÖZGER, Çiğdem:** *Kişisel Verilerin Korunması Hukuku - Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil*, 2. Baskı, Beta Yayıncılık, İstanbul 2019.
- ÖZBEK, Veli Özer / DOĞAN, Koray / BACAĞSIZ, Pınar / TEPE, İlker:** *Ceza Muhakemesi Hukuku*, 10. Baskı, Seçkin Yayıncılık, Ankara 2017.

ÖZBEK, Veli Özer: *Organize Suçlulukla Mücadelede Kullanılan Gizli Görevlinin Görevin Gerektirdiği Suçlar Bakımından Cezalandırılabilirliği*, Yetkin Yayıncılık, Ankara 2003.

ÖZDAĞ, Ümit: *İstihbarat Teorisi*, 4. Baskı, Kripto Kitaplar, Ankara 2010.

SERT, Şeyma: *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, Seçkin Yayıncılık, Ankara 2019.

TAŞTAN, Furkan Güven: *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 2. Baskı, On İki Levha Yayıncılık, İstanbul 2017.

TILISBIK, Niyazi / AKBAL, Özdemir: *Intelligence: İstihbarat ve Türkiye*, İkia Yayıncılık, Konya 2006.

YENİSEY, Feridun: *Kolluk Hukuku*, 2. Baskı, Beta Basım, İstanbul 2015.

Makale ve Tezler

- AKDAĞ, Hale:** "Türk Ceza Hukukunda Kişisel Verilerin Korunması İlkeleri", *Prof. Dr. Nevzat Toroslu'ya Armağan*, C.1, Ankara, Ankara Üniversitesi Basımevi, 2015, s.27-48.
- AKINTUNDE, 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", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2912449.
- AKSOY, Muammer:** "Güvenlik Soruşturması" Denilen Hukuksal Sapıklığın, MİT Raporlarındaki Korkunç Yanlış ve Yalanlar Işığında Değerlendirilmesi", *Bahri Savcı'ya Armağan, Mülkiyeliler Birliği Vakfı Yayınları - 7*, Maya Matbaacılık, Ankara 1988, s.69-164.
- BÄCKER, Matthias / HORNUNG, Gerrit:** "Data Processing by Police and Criminal Justice Authorities in Europe - The Influence of the Commission's Draft on the National Police Laws and Laws of Criminal Procedure", *Computer Law & Security Review*, C.28, S.6, 2012, s.627-633, https://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IWR/Hornung/Baecker_Hornung_CLSR_2012_627_fulltext.pdf.
- BAYKAL, Sanem / GÖÇMEN, İlke:** "Avrupa Birliği Hukukunun Kaynakları Bakımından Normlar Hiyerarşisi", *Prof. Dr. Erdal Onar'a Armağan*, Ankara Üniversitesi Basımevi, Ankara 2013, s.317-365.

¹⁴⁸ Çalışmada yer verilen tüm çevrim içi kaynakların güncelliğinin son kontrol edilme tarihi 20.10.2019, saat 13:30'dur.

- BOSTANCI BOZBAYINDIR, Gülşah:** “Avrupa Birliği Ceza Hukuku’nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler”, *GSÜHFD*, C.2, 2018, s.51-104.
- BÖREKÇİ, Eşref Barış:** “Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu”, *Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü*, Yayınlanmamış Yüksek Lisans Tezi, 2019.
- CARUANA, Mireille M.:** “The reform of the EU data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement”, *International Review of Law, Computers & Technology*, 2017, s.4, <http://dx.doi.org/10.1080/13600869.2017.1370224>.
- DAĞ, Güray:** “Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması”, *Marmara Üniversitesi Sosyal Bilimler Enstitüsü*, Yayınlanmamış Doktora Tezi, 2011.
- DE HERT, Paul / PAPAKONSTANTINOU, Vagelis:** “The New Police and Criminal Justice Data Protection Directive”, *New Journal of European Criminal Law*, 2016, s.7-19, <https://journals.sagepub.com/doi/abs/10.1177/203228441600700102>.
- 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)”, <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/>.
- ERMAN, Barış:** “Ceza Hukukunun Dönüşümü”, *YÜHFD (Prof. Dr. Duygun Yarsuvat’a Armağan)*, C.IX, S.2, 2012, s.447-480.
- EROĞLU, Fulya:** “Örgütlü Suçlarda Yargılama Sistemi”, *Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü*, Yayınlanmamış Doktora Tezi, 2016.
- KIZILIRMAK, Baran:** “Önleyici Amaçla Elde Edilen Verilerin Ceza Muhakemesinde Kullanılabilirliği”, *İstanbul Üniversitesi Sosyal Bilimler Enstitüsü*, Yayınlanmamış Yüksek Lisans Tezi, 2018.
- ÖZKAN, Halid:** “MOBESE İzleme ve Kayıtlarının Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi”, *CHD*, S.30, 2016, s.63-103.
- PAJUNOJA, Lauri J.:** “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”, *Univeristy of Helsinki - Faculty of Law*, Yayınlanmamış Yüksek Lisans Tezi, 2017, <https://helda.helsinki.fi/bitstream/handle/10138/181500/HU%20Masters%20thesis%20Pajunoja.pdf?sequence=2&isAllowed=y>.
- ŞEN, Ersan:** “Mobese ve Kamera Sistemi ile İzleme”, *Yorumluyorum 12*, Seçkin Yayıncılık, Ankara 2016, s.119-122.
- VERVAELE, John:** “Terrorism and Information Sharing Between the Intelligence and Law Enforcement Communities in the US and the Netherlands”, *Utrecht Law Review*, C.1, S.1, 2005, s.1-27, <http://doi.org/10.18352/ulr.1>.
- YENİSEY, Feridun:** “Tehlikeyi Önleyici Polis ve Adli Polis”, *Bavyera Polis Kanunu*, (Çev.: Feridun Yeni-sey), Asayiş Daire Başkanlığı, 2007.

Çevrim içi Kaynaklar

- 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun Gerekçesi, <https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf>.
- Article 29 Data Protection Working Party, Opinion 03/2015 on the Draft Directive on the Protection of Individuals With Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, 3211/15/EN, WP 233, 01.12.2015, s.11-12, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640460.
- Avrupa Komisyonu’nun Türkiye 2016 İlerleme Raporu (Ing.) https://ec.europa.eu/neighborhood-enlargement/sites/near/files/pdf/key_documents/2016/20161109_report_turkey.pdf.
- Avrupa Komisyonu’nun Türkiye 2018 İlerleme Raporu (Ing.), <https://ec.europa.eu/neighborhood-enlargement/sites/near/files/20180417-turkey-report.pdf>.
- Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [108 numaralı Sözleşme], <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>.
- Council of Europe Committee of Ministers, Recommendation Rec 87 15 to memberstates regulating the use of personal data in the police sector, 17.07.1987, <https://rm.coe.int/168062dfd4>.

Council of Europe Directorate General of Human Rights and Rule of Law, *Consultative Committee of the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data - Practical Guide on the Use of Personal Data in the Police Sector*, T-PD(2018)01, Strasbourg, 15.02.2018, <https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5>.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA [ks. 2016/680 sayılı Direktif], https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv-%3A0J.L_.2016.119.01.0089.01.ENG.

<https://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-law-enforcement>.

İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, *Suçların Önlenmesi, soruşturulması, Ortaya Çıkarılması veya Kovuşturulması ya da Cezaların İnfazı Amacıyla Yetkili Makamlarca Kişisel Verilerin İşlenmesine İlişkin Olarak Gerçek Kişilerin Korunması ve Bu Verilerin Serbest Dolaşımı ile İlgili, 2008/977/Aİİ sayılı Konsey Çerçeve Kararı Yerine Geçen 27 Nisan 2016 tarihli (AB) 2016/680 SAYILI AVRUPA PARLAMENTOSU ve KONSEY DİREKTİFİ* (Türkçe Çevirisi), <https://itlaw.bilgi.edu.tr/media/2019/7/29/law-enforcement-directive-turkce.pdf>.

İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, *Avrupa Parlamentosu ve Konseyi'nin 2016/680 Sayılı ve 27 Nisan 2016 Tarihli Kişisel Verilerin Yetkili Otoritelerce Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması veya Cezaların İnfazı Amacıyla İşlenmesiyle İlgili Gerçek Kişilerin Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin ve 2008/977/JHA Sayılı Konsey Çerçeve Kararı'nı Yürürlükten Kaldıran Direktif Hakkında Bilgi Notu*, <https://itlaw.bilgi.edu.tr/media/2019/7/27/law-enforcement-directive-bilgi-notu.pdf>.

Kişisel Verilerin Korunması Kanun Tasarısı (2008), <https://www2.tbmm.gov.tr/d23/1/1-0576.pdf>.

Kişisel Verilerin Korunması Kanun Tasarısı (2014) <http://www2.tbmm.gov.tr/d24/1/1-1009.pdf>.

Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme'yi Uygun Bulma Kanunu, <https://www2.tbmm.gov.tr/d26/1/1-0320.pdf>.

Protocol Amending the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/09000016808ac918>.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal data and on the free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation - GDPR), (Tr. GVKT), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL>.

www.hudoc.echr.coe.int.

www.kazanci.com.

www.tdk.gov.tr.