MANAS Sosyal Araştırmalar Dergisi 2022 Cilt: 11 Sayı: 3
MANAS Journal of Social Studies 2022 Volume: 11 No: 3
ISSN: 1694-7215
Research Paper / Araştırma Makalesi

Türkiye'de Güvenlik Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi

Ömer ÖZKAYA[1] ve İbrahim TOPRAK[2]

Öz

Teknolojik gelişmeler, kişisel verilerin toplanması ve çeşitli yöntemlerle analiz edilmesine önemli ölçüde kolaylık sağlamaktadır. Bu durum kişinin özel hayatının gizliliğini ihlal eden bir etki yaratabilmektedir. Dolayısıyla kişisel verilerin korunması, her geçen gün daha çok önem kazanan bir insan hakkı meselesine dönüşmüştür. Tartışma alanı kişisel verilerin güvenlik faaliyetleri kapsamında işlenmesi olarak belirlenen bu çalışmanın amacı, kişisel verilerin güvenlik faaliyetleri kapsamında hangi yöntemlerle işlendiğini ortaya koyarak, bu yöntemlerin hak ihlaline yol açıp açmadığını mahkeme kararları ve ilgili mevzuat ekseninde analiz etmektir. Çalışmada öncelikle kişisel veri ve güvenlik kavramları açıklanarak kavramlar arasındaki ilişkiye değinilmiş, sonrasında ise kişisel verilerin başta ulusal güvenlik faaliyetleri olmak üzere hangi yöntemlerle işlendiği ele alınmıştır. Son olarak, açıklanan veri işleme yöntemlerinin meşru amaçlara dayanmaması halinde kişisel verilerin korunması hakkının ihlal edileceği tespit edilmiş, yasa koyucu tarafından kişisel verilerin güvenlik faaliyetleri kapsamında işlenmesini düzenleyen müstakil bir kanunun hazırlanması ve kullanılan her yöntemin muhakkak bir hukuki dayanağının bulunmasının hak ihlallerinin önüne geçebileceği önerilerinde bulunulmuştur.

Anahtar Kelimeler: Kişisel verilerin işlenmesi, Temel haklar ve özgürlükler, Güvenlik faaliyetleri.

Processing of Personal Data within the Scope of Security Activities in Turkey

Abstract

Technological advancements have made it easier to collect personal data and analyze it with various methods. This case can produce an effect that violates the privacy of the individual's private life. Hence, the protection of personal data has become a human rights issue that is gaining more essential day by day. The aim of this study, whose discussion area is the processing of personal data within the scope of security activities, is to reveal the methods by which personal data is processed within the scope of security activities and to analyze whether these methods lead to violations of rights in the axis of court decisions and relevant legislation. In the study, first of all, the concepts of personal data and security were explained, and the relationship between the concepts was mentioned. After that, the methods by which personal data are processed, especially for national security activities, were discussed. Finally, it has been determined that the right to protection of personal data will be violated if the disclosed data processing methods aren't based on legitimate purposes by us. It has been suggested that the legislator should legislate independent law regulating the processing of personal data within the scope of security activities and that the methods used should have a legal basis that could prevent rights violations.

Key Words: Processing of personal data, Fundamental rights and freedoms, Security activities.

Atıf İçin / Please Cite As:

Özkaya, Ö. ve Toprak, İ. (2022). Türkiye'de güvenlik faaliyetleri kapsamında kişisel verilerin işlenmesi. *Manas Sosyal Araştırmalar Dergisi, 11*(3), 1291-1305.

Geliş Tarihi / Received Date: 04.04.2022 **Kabul Tarihi / Accepted Date:** 03.06.2022

[1] Dr. Öğr. Üyesi - Polis Akademisi Güvenlik Bilimleri Enstitüsü, omerakademik@gmail.com
ORCID: 0000-0003-2302-5991
[2] Doktora Öğrencisi - İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, ibrahim.toprak@ogr.iu.edu.tr
ORCID: 0000-0002-8195-349X

Giriş

Sosyal ve toplumsal gelişim, insanlık var oldukça devam edecek olan bir süreçtir. Bu süreç, farklı zaman dilimlerinde; ateşin bulunması ve tekerleğin icadı ile başlamış, devletlerin doğuşu, iktidar mücadelelerinin varlığı ve dönüşümü, güvenlik ihtiyacının tanımlanması ve çeşitlenmesi, insan hakkı mücadeleleri, Sanayi Devrimi ve teknoloji toplumu gibi aşamalardan geçerek modern toplum ve devleti meydana getirmiştir. Günümüz şartlarında sosyal ve toplumsal gelişim süreçleri genel itibarıyla olumlu çıktılara sahip olmakla birlikte, ortaya çıkan her yeniliğin kişi hak ve özgürlükleri açısından belirli sonuçları olmaktadır. Modern devlet yapılarında kişi hak ve özgürlüklerini koruması ile onlara müdahale etmesi arasındaki denge güncel tartışmalara neden olmaktadır. Bu kapsamda kişi hak ve özgürlükleri çerçevesinde ele alınan kişisel verilerin korunması hakkı, güvenlik çalışmaları bağlamında güncel ve önemli bir tartışma alanı olarak karşımıza çıkmaktadır.

Kişiyi tanımlayan ya da belirli hale getirebilen her türlü bilgi olarak ifade edilen kişisel veri; teknolojinin gelişimiyle devletler tarafından kabul görmüş, kişi hak ve özgürlükleri ile doğrudan ilintili hale getirilerek koruma altına alınmıştır. Bilgiye erişimin gün geçtikçe kolay hale gelmesi aynı oranda kişisel verilerin gizliliğini ihlale yol açmaktadır. Bu nedenle kişisel verilerin korunması; mahremiyet hakkının, insan onurunun ve kişiliğin serbestçe geliştirmesi hakkının korunmasıdır (Akgül, 2014, s. 68) ve özel yaşamın gizliliği hakkı kapsamında güvence altına alınan bir insan hakkı meselesi olarak önemi giderek artmaktadır.

Toplum Sözleşmecilerin özgürlük-güvenlik ikilemini tartıştığı dünya düzeni; bireylerin doğrudan yaşam hakkıyla, yani hayatta kalabilmesiyle, ilgiliyken; günümüzde bu hakların yanı sıra özel hayatın gizliliği, ekonomik haklar, bilgi akışı, kişisel verileri de içine alacak şekilde kapsamlı bir hale gelmiştir (Ergil, 2001, s. 117-118). İşte tam da bu sebeplerle devletlerin özgürlüklere müdahale edip etmediği ya da ettiği durumlarda sınırlarının nasıl olması gerektiği tartışılmalıdır.

Bireylerin, kamu sektörü ve özel sektör alanlarında hizmet alabilmesi için günümüz şartlarında birçok verisinin elde edilmesi ve bu verilerin çeşitli yöntemlerle işlenmesi gerekmekte (Kılınç, 2012, s. 1092) ve neredeyse şart koşulmaktadır. Veri toplayan ve işleyen birimlere örnek olarak eğitim-sağlık-bankacılık-güvenlik hizmetlerini sunan kurum ve kuruluşlar gösterilebilir. Bu bakımdan birçok kurum ve kuruluş kişisel veri toplamakta ve bu verileri çeşitli yollarla işleyip saklamaktadır.

Günümüzde teknolojik gelişmelere bağlı olarak artan internet kullanımı, birçok suç türünün de doğmasına yol açmış; suçun önlenmesi, araştırılması, soruşturulması ve kovuşturulması aşamalarında kişisel verilerin işlenmesi kaçınılmaz bir hale gelmiştir. Bu durum güvenlik ve kişisel veri kavramlarının birlikte anılmasına, sınırlarının belirlenmesine hatta bu süreçlerde çeşitli yöntemlerle işlenen verilerin kişilerin özel hayatına saygı hakkının ihlal edilmesi riski sebebiyle güvenlik faaliyetleri kapsamında kişisel verilerin korunması gerekliliğini doğurmuştur (Sajfert ve Quintel, 2017, s. 2).

Çalışma kapsamında kişisel veri ve güvenlik kavramları açıklanarak aralarında ilişkiye değinilecek, daha sonra kişisel verilerin öncelikle ulusal güvenlik faaliyetleri olmak üzere önleyici kolluk faaliyetleri ve ceza muhakemesi işlemleri kapsamında hangi yöntemlerle işlendiği ele alınacak ve son olarak, açıklanan veri işleme yöntemlerinin kişisel verilerin korunması hakkına ihlale sebep olup olmadığı tartışılacaktır.

Genel Olarak Kişisel Veri ve Güvenlik Kavramı

Kişisel veri kavramı açıklanırken bu kavramı oluşturan kelimelerin ayrı açıklanması faydalı olacaktır. Bu noktada öncelikle "kişi" kavramı açıklanmalıdır. Çünkü bahse konu veri üzerinde hak sahipliği bulunmaktadır. Kişi kavramı*; "hukuken kendilerine değer verilen hak ve borçlara ehil olduğu hukuken tanınan kimseler"* (Şafak, 1992, s. 271) olarak tanımlanmakta olup gerçek veya tüzel kişi olarak ikiye ayrılmaktadır. Gerçek kişi insanı tanımlarken, tüzel kişi ise insan olmayan fakat hukukun bir tür kişilik atfettiği soyut varlıkları açıklamaktadır (Oğuzman vd., 2016, s. 2; Oğuzman ve Barlas, 2016, s. 174). Bu tanımlar ışığında kural olarak kişisel veri kavramındaki hukuki hak süjesinin yalnızca gerçek kişiler olduğu[3] ifade edilebilir.

Veri kavramı ise Türk Dil Kurumu Bilişim Terimleri Sözlüğünde genel olarak olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimi olarak

[3] Esasında kişisel veri kavramının sadece gerçek kişiler mi yoksa tüzel kişilerle birlikte mi ele alınacağı tartışılmaktadır. Tartışma için bkz: (Özkaya ve Toprak, 2022, s. 74).

tanımlanmaktadır (Türk Dil Kurumu, 2022). Köken itibarıyla Latince olan veri kavramı *"verilen bir şey"* anlamına da gelmektedir (Van Belle ve Ruiter, 2014, s. 28). Bu bağlamda bilişimle alakalı olan veri kavramı, kişisel veri perspektifinde, bir kelime, eşya, bilgi yahut rakamlardan oluşan bir kod dahi olabilir.

"İsme bağlı veriler" veya "bireysel veriler" olarak da adlandırılan kişisel veriler (Kılınç, 2012, s. 1093), en genel tanımıyla, belirli veya belirlenebilir bir kişiyle ilgili olan her türlü veri (Aşıkoğlu, 2018, s. 5) olarak açıklanmaktadır. Örneğin adres bilgisi, sağlık bilgisi, pasaport bilgisi, telefon numarası, kişisel verilerdir. Kişinin doğduğu yerin, medeni durumunun, cinsiyetinin, parmak izinin, fotoğraflarının, tıbbi verilerinin, sosyal güvenlik bilgilerinin ve benzeri bilgilerinin kişisel veri kapsamında değerlendirildiği görülmektedir (Kılınç, 2012, s. 1101). Teknolojinin gelişmesiyle ihlal riski artan kişisel verilerin (Bilir, 2020, s. 308) korunması ihtiyacı da o denli artmış ve bu konuda ciddi tedbirler alınmasına sebep olmuştur. Dolayısıyla kişisel verilerin korunmasına ilişkin ilk çalışmaların 20. yüzyılın ikinci yarısında ortaya çıktığı ifade edilebilir (Hizarci, 2020, s. 19).

Bir bilginin kişisel veri olarak kabul edilmesi için bu bilginin kanıtlanmış olması veya güncel olması şart değildir (Turan Başara, 2020, s. 59). Kişisel veriler heterojen yapıda olup insanlarla ilgili verilerdir (Arınmış Uzun, 2021, s. 209). Kişisel verinin korunmasında kişinin doğrudan tanımlanmasının yanı sıra dolaylı olarak tanınmasına sebep olabilecek veriler de kişisel veri olarak tanımlanmaktadır (Kılınç, 2012, s. 1094). Kişisel veri, gerçek bir kişiye ilişkindir ve kişinin herhangi bir şekilde belirlenebilir olmasını sağlayan bilgiler bu kapsamdadır. Hangi verinin kişisel veri olduğu uluslararası belgelerde, anayasada ve kanunlarda tek tek sayılmamış, kişisel verilerin sınırına ilişkin genel ilkeler çerçevesine düzenlemeler yapılmıştır. Haliyle verinin bir kişiyle ilintili olması ve kimliğinin belirli olması veya belirlenebilir olması yeterlidir (Turan Başara, 2020, s. 59). Bu bakımdan kişisel veri kavramının hukuki düzenlemelerdeki tanımında kesin bir sınır konmaması (Henkoğlu, 2017, s. 50), başka bir ifadeyle tanımın açık uçlu bir şekilde yapılması, hak ve hürriyetlerinin korunması açısından kanaatimizce doğru bir yaklaşım olarak değerlendirilmektedir.

Kişisel veriler ele alındığında dikkat edilmesi ve açıklanması gereken bir diğer kavram ise hassas kişisel verilerdir. Hassas kişisel veriler bireyler ve devlet için önem taşımakta olup kişisel veri koruma kanunları ile özel olarak düzenlenip koruma altına alınan verilerdir. Çünkü bu tip veriler ırksal köken, sağlık verileri ya da siyasi görüş gibi bilgileri içermektedir (Kaya, 2011, s. 317). Avrupa Konseyi'nce hazırlanan 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin 6. maddesinde hassas veriler "özel veri kategorileri" olarak adlandırılarak *"...ırksal kökeni, siyasi düşünceleri, dini veya diğer inançları ortaya koyan kişisel veriler ile sağlık veya cinsel hayatla... ceza mahkumiyetiyle ilgili kişisel veriler..."* şeklinde sayılmıştır. Sözleşme kapsamında hassas kişisel verilerin neler olduğunun tek tek sayılmış olması bu konuda ortaya çıkabilecek uyuşmazlıkların çözümüne katkı sağlaması bakımından önem taşımaktadır.

Kişisel veri kavramı başlı başına açık uçlu bir kavram iken hassas kişisel veri kavramı ise sınırları belirli bir veri alanını ifade etmektedir. Hassas kişisel veriler, genel nitelikli kişisel verilere nazaran daha çok güvence altına alınması gereken verilerdir. Bu özenin sebebi hassas kişisel verilerin ortaya çıkması durumunda kişilik haklarının daha fazla zarar görme ihtimalinin bulunmasıdır. Bu nedenle hassas kişisel veriler, demokratik toplum düzeninin gerekleri ve ölçülülük ilkeleri gereği daha dikkate değer ve özenli bir şekilde ele alınmalıdır (Duman, 2020, s. 387).

Avrupa İnsan Hakları Mahkemesi içtihatları kişisel verilerin korunması hakkını özel hayatın gizliliği hakkı içerisinde değerlendirmektedir (Küzeci, 2020, s. 134). Bu kapsamda gerçekleşecek sınırlamalar ancak kanunla yapılması, sınırlamanın meşru bir amacının bulunması ve müdahalenin demokratik toplumda gerekli olması gerekir (Aydın, 2015, s. 82). Kişisel verilerin korunması hakkı, mutlak ve sınırsız bir hak değildir. Ancak yapılan sınırlandırma ile hakkın özüne dokunulamaz, sınırlandırma hukuka aykırı olamaz ve ölçülülük ilkesi çerçevesinde yapılabilir.

Dünyada veri kavramının her geçen gün daha fazla önem kazanmasıyla Türk hukukunda da çeşitli adımlar atılmıştır. Kişisel verilerin korunması anayasal bir hak olarak 2010 yılında güvence altına alınmıştır.[4] Daha önce kişisel veriler başta Türk Medeni Kanunu, Türk Ceza Kanunu ve Ceza Muhakemesi Kanunu'nda ve diğer mevzuatla koruma altına alınmış iken, 2016 yılında ise 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)[5] ile kişisel veriler müstakil bir kanun ile koruma altına alınmıştır. Bu doğrultuda kişisel veri kavramının tanımı ve kapsamı belirlenmiş, özel hayatın gizliliği ve korunması hakkı

[4] Türkiye Cumhuriyeti Anayasası, madde 20.
[5] 6698 sayılı Kişisel Verilerin Korunması Kanunu, 07.05.2016 tarih ve 29677 sayılı Resmi Gazete.

kapsamında devlet tarafından korunması gerekli görülen bir insan hakkı olarak Türk Hukukunda yerine almıştır.

Kişisel veri kavramının, hak sahipliği, niteliği ve hukuki dayanakları açıklandıktan sonra çalışma kapsamında ilişkili olduğu iddia edilen güvenlik kavramının da ayrıca açıklanması faydalı olacaktır. Güvenlik, ilk çağlarda insanın yalnızca hayatta kalabilmesi anlamına gelirken, zamanla korunmak için devlete olan ihtiyaca dönüşmüş (Öz Yıldız, 2019, s. 28) ve küreselleşmenin etkisiyle (Kartal, 2020, s. 54) çağdaş toplumlarda maddi-manevi hak ve özgürlükleri de kapsayan bir kavram halini almıştır (Çınar, 1997, s. 57). Toplumsal düzenin sağlanması amacıyla devlet tarafından alınan tüm tedbirleri içeren güvenlik kavramı (Çeçen, 2005, s. 115), özgürlük kavramı ile simbiyotik bir ilişki içindedir (Erdoğan, 2013, s. 23). Güvenlik kavramı bağlamında bahsedilen tedbirlerin insanın özgür bir biçimde yaşamasına imkân sağlayan sınırlandırmalar olduğu ön kabulü ile yola çıkıldığında; "*Özgürlük', ancak 'sınırlar' ile sağlanabilir*" (Özkaya, 2021: 108), söylemi bu ilişkiyi destekler niteliktedir. Başka bir ifadeyle özgürlük güvenliğin varlığının, güvenlikte özgürlüğün varlığının ön şartı durumundadır ve bunlardan birinin yokluğu diğerinin de yokluğunu ortaya çıkarır. Güvenlik, bireylerin kamusal alanda kendilerine ve mallarına karşı herhangi bir saldırıya, engellemeye ve tehdide maruz kalmadan yaşamlarını sürdürmelerine imkân sağlanmasıdır (Günday, 2013, s. 292; Öz Yıldız, 2019, s. 29). Teknolojik imkânların gelişmesi ile birlikte büyük boyutta kişisel verilerin toplanması kolay hale gelmiş ve yine aynı teknolojiyle birlikte kötü niyetli kişilerin eline geçme olasılığını da artırmıştır (Oğuz, 2018, s. 123). Dolayısıyla faillerin teknolojiye ve kişisel verilere olan ilgisi artmış ve bu alanda bilgili hale gelmişlerdir. Bu durumun bir sonucu olarak kolluk ve ceza adaleti birimlerinin bu suçlarla mücadelesi her zamankinden daha fazla önemli hale gelmiştir (Sajfert and Quintel, 2017, s. 21).

Mahremiyet hakkı ve özel yaşamın gizliliği ile doğrudan ilgili olan kişisel verilerin korunması hakkı, bir insan hakkı meselesidir. Bu bağlamda devletin hem negatif sorumlulukları hem de pozitif sorumlulukları bulunmaktadır. Bu kapsamda yer alan yükümlülükler devletin yürütme organına çeşitli sorumluluklar yükler ve bu haklara kimi zaman saygı gösterme ve müdahale etmeyerek kimi zaman da kişi özgürlükleri kapsamında korunması ile icra edilir (Acaray, 2021, s. 176-177). Bu noktada özellikle belirtmek gerekir ki kişisel verilerin korunmasıyla birlikte insanların özel hayatın gizliliği sağlanacak ve bu vesileyle insanın mahremiyetinin korunması sağlanacaktır (Kılınç, 2012, s. 1099).

Kişi hak ve özgürlüklerinin korunması ile kişilerin can ve mal emniyetinin sağlanması amacıyla çeşitli unsurlar aracılığıyla gerçekleştirilen güvenliği sağlama hali arasındaki ikilem şüphesiz ki kişisel veri ile güvenlik faaliyetlerini de kapsamaktadır. Bir başka deyişle vatandaşların özgür bir şekilde yaşayabilmeleri amacıyla kişisel verilerin analiz edilmesi ve işlenmesi günümüzde kaçınılmaz bir boyuta ulaşmıştır. Ancak bu işlemlerin yargı denetimde olması ve hukuki güvence altına alınması yalnızca kişileri değil onlara ait olan verileri de koruma altına alacaktır.

Güvenlik Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi

Kişilerin güvenli bir ortamda yaşaması insan haklarının temel unsurları arasında yer almaktadır. Ancak unutulmamalıdır ki güvenlik ve insan hakları arasında ters orantılı bir ilişki vardır (Acaray, 2020, s. 37). Kanaatimizce güvenliğe dair tüm unsurların bireylerin temel hak ve özgürlüklerini sorunsuz bir şekilde kullanabilmeleri amacıyla var olması gerekmektedir. Kamu hizmetlerinde "kamu yararı" gözetilirken (Akyılmaz vd., 2021, s. 549-553; Gözler ve Kaplan, 2021, s. 477-478), kolluk faaliyetlerinde ise "kamu düzeninin" sağlanması ve hatta bozulduğunda yeniden tesis edilmesi esastır (Gözler ve Kaplan, 2021, s. 524; Akyılmaz vd., 2021, s. 577). Bu hususta idare, güvenliğin sağlanması amacıyla alacağı tedbir ve gerçekleştireceği eylemler açısından geniş yetkilere sahiptir. Ancak bu yetkilerin, bireysel hak ve özgürlük sınırlarını ihlal etmemesine özen gösterilmelidir. Bu nedenle devlet faaliyetleri sınırlandırılmaya mecburdur (Özkaya, 2021, s. 107-108).

Kişisel verilerin güvenlik faaliyetleri kapsamında işlenmesi çalışmanın temelini oluşturmaktadır. Bu anlamda açıklanması gereken en önemli husus ise kişisel verilerin idare tarafından hangi yöntemlerle işlendiğidir. Kişisel verilerin devlet tarafından hangi hallerde işlenebileceği istisna kapsamında birçok hukuki metinde düzenlenmiştir. Çalışma bağlamında ele alındığında ilgili mevzuat hükümleri kişisel verilerin istisnalar kapsamında millî savunma, millî güvenlik, kamu güvenliği, kamu düzeni, ekonomik güvenlik ile önleyici, koruyucu ve istihbarı faaliyetler gibi ülkenin genelini ilgilendiren önemli hususlarda ve ayrıca yargı makamlarınca soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak kişisel verilerin işlenebileceğini öngörmektedir.

Uluslararası ve ulusal hukuki metinler ile uygulamada güvenlik faaliyetleri kapsamında kişisel verilerin hangi yöntemlerle işlenebildiği hususları göz önünde bulundurularak konu; ulusal güvenlik faaliyetleri gereği veri işlenmesi, önleyici kolluk faaliyetleri kapsamında veri işlenmesi ve ceza muhakemesi işlemleri dâhilinde kişisel verilerin işlenmesi olarak üç alt başlıkta incelenecektir.

Ulusal Güvenlik Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi

Ulusal güvenlik kavramı devletin varlığını devam ettirmek amacıyla gerçekleştirmek zorunda kaldığı eylemlerinde kişi hak ve hürriyetlerine müdahalelerini meşrulaştırmasıdır. Devletin ülkeyi iç ve dış tehditlerden koruması ulusal güvenlik kapsamındadır (Kuloğlu, 2015, s. 16-17).

Ulusal güvenliğin sağlanmasında idarenin takdir yetkisi olabildiğince geniş kapsamda değerlendirilmektedir. Fakat bu takdir yetkisi, özgürlük ve güvenlik arasında dengeyi bozacak sınırları aşmamalıdır (Köksal, 2021, s. 1750). Anayasal düzen ve milli güvenliğin sağlanması amacıyla askeri, istihbarı ve kolluk faaliyetleri yürütülmektedir. Bu faaliyetlerin tehditler bağlamında değişmesi, gelişmesi ve çeşitlenmesi güvenlik faaliyetleri çerçevesinde kişisel verilerin işlenmesi ve özel hayatın gizliliğinin ihlaline yol açabilmektedir.

Bu noktada ulusal güvenliğin sağlanması amacıyla görevlendirilmiş ve yetkileri kanunlarla düzenlenmiş olan birimlerin bu amaçla gerçekleştirdiği faaliyetler olarak değerlendirilen istihbarı faaliyetler, ön alan araştırmaları ve güvenlik soruşturmalarının incelenmesi faydalı olacaktır.

İstihbarı Faaliyetler

Devletin iç ve dış güvenliği sağlamak amacıyla kullandığı birçok enstrüman vardır. Bunların başında ise istihbarat faaliyetleri gelmektedir (Öz Yıldız, 2019, s. 28). İstihbarat kavramı devlet güvenliğinin tesis edilmesi amacıyla genel risklerin hesaplanması ve bu riskleri en aza indirecek ya da ortadan kaldırabilecek seviyede gerekli bilgilerin bu alanda uzmanlaşmış birimlerce toplanması, bu verilerin işlenmesi ve analiz edilmesi sürecidir (Kuloğlu, 2015, s. 19; Öz Yıldız, 2019, s. 28). İstihbarı faaliyetler özü itibarıyla devletin varlığını devam ettirebilmesi amacına hizmet eder. Bu bakımdan devlete zarar vermesi muhtemel durumların önüne geçmek için ihtiyaç duyduğu ve ona fayda sağlayacak stratejik veriler elde edilir (Bayındır, 2016, s. 5). Tüm bu nedenlerle devletin milli güvenlik ve kamu düzenini sağlaması açısından istihbarat faaliyetleri vazgeçilmez bir unsurudur (Öz Yıldız, 2019, s. 34). İstihbarat faaliyetleri kapsamında kişisel veri elde etme ve verileri işleme; askeri istihbarat, dış güvenlik ve iç güvenlik istihbaratı şeklinde gerçekleşir (Yenisey, 2015, s. 373).

Yukarıda belirtilen şekillerde gerçekleştirilen istihbarı faaliyetler neticesinde kişisel veriler işlenmektedir. Ancak bu veriler ulusal güvenliğin tesisi amacıyla kullanılmaktadır. Bu amaçla suç işlenmesinin önlenmesi, terörizmle mücadele ve diğer ülkelerin casusluk faaliyetlerine karşı konulması gibi faaliyetlerde bulunulur (Can, 2021, s. 52; Kuloğlu, 2015, s. 36; Bayındır, 2016, s. 80; Öz Yıldız, 2019, s. 33-34).

İstihbarı faaliyetler devletin varlığının devamı ve güvenliğinin tesisi adına sürdürülmekte olan faaliyetlerdir. Ancak bu faaliyetlerin derinliği ile temel insan hakları arasındaki dengenin iyi kurulması gerekmektedir. Çünkü istihbarı amaçlarla bilgi edinme sürecinde devletin yasal sınır dahilinde hareket etmemesi, hukuk devleti anlayışıyla izahı mümkün olmayan hak ihlallerine neden olabilecektir. Başka bir ifade ile istihbarı faaliyetler ancak temel insan hakları çerçevesinde sınırlandırılmış olan yasal zeminde gerçekleştirilmelidir. Aksi halde hak ihlallerinin yaşanması kaçınılmazdır. Nitekim istihbarı faaliyetler çerçevesinde elde edilen kimi verilerin hak ihlallerine neden olduğu AİHM[6] kararlarına da yansımaktadır.

Kişisel verilerin işlenmesi kadar bu verilerin korunması da devletin görevleri arasında yer almaktadır. Yalnızca yargı makamlarınca istenebilecek ve yargı makamlarıyla paylaşılabilecek verilerin üçüncü kişi veya kurumlarla paylaşılması kişisel verilerin ihlali anlamına gelmektedir. Nitekim Türk Anayasa Mahkemesi'ne

[6] AİHM tarafından verilen *Rotaru v. Romanya* başvurusu doğrudan çalışmayla ilgilidir. Başvurucu, uzun zaman önce komünist rejimi eleştirdiği için hapis cezası almıştır. Bu doğrultuda başvurucu, Romanya İstihbarat Teşkilatı'nda kendisi hakkında asılsız ve aksini ispat edemeyeceği bilgilerin yer olduğu gerekçesiyle şikâyetçi olmuştur. Avrupa İnsan Hakları Mahkemesi (AİHM) ise kararında kişinin özel hayatına mahsus olan bilgilerin tutulması ve kullanılmasının yasalara uygun olmadığını değerlendirerek, Avrupa İnsan Hakları Sözleşme'nin (AİHS) 8. maddesinin ihlal edilmiş olduğuna karar vermiştir. Rotaru v. Romanya Kararı. (Çevrimiçi) https://www.echr.coe.int/Documents/FS_Data_TUR.pdf, (11.05.2021). Benzer kararlar için bkz. *Leander v. İsveç Başvurusu ve Amann v. İsviçre Başvurusu.*

2016 yılında yapılan bir bireysel başvuru[7] neticesinde Mahkeme, kişisel verilerin üçüncü kişilerle paylaşılması nedeniyle hak ihlali kararı vermiştir[8]. Mahkeme'nin de tespit ettiği üzere, devlet kişisel verilerin ancak kanunun kendisine tanıdığı çerçevede işlemeli ve paylaşmalıdır. Aksi halde bir hak ihlalinin ortaya çıkması kaçınılmaz olacaktır.

Ön Alan Araştırmaları

Doktrinde somut olarak suç şüphesinin oluşmadığı ancak suçun işlenmesinin önlenebileceği evre, ön alan olarak adlandırılmaktadır (Özbek vd., 2019, s. 151). Bir başka deyişle toplumda gelecekte meydana gelmesi muhtemel suçlar dolayısıyla oluşabilecek zararların önlenmesi (Yenisey, 2015, s. 347) amacı ön alan evresi temelini oluşturmaktadır. Bu evrede bilgi toplamak mümkündür ve kolluk yetkileri[9] bu kapsamda kişisel verileri toplama, saklama ve analiz etme yetkisine sahiptir (Yenisey ve Nuhoğlu, 2017, s. 283).

Ön alan evresi; kolluk faaliyetleri neticesinde suçun işlenmesinin önlenmesi ile ceza muhakemesi kapsamında suçun işlenmesinden sonra başlayan soruşturma evreleri arasında kalan hukuki bir alandır (Yenisey ve Nuhoğlu, 2017, s. 283). Ön alan evresinde kamu düzenini bozabilecek herhangi bir tehdit veya somut tehlike bulunmasa dahi kolluğun bu süreçte veri toplama, verileri işleme ve analiz etme yetkileri bulunmaktadır. Ön alan evresinde yapılan araştırmalar gizlidir ve elde edilen deliller yahut veriler istihbarı niteliktedir (Karabulut, 2014, s. 87; Özbek vd., 2019; Yenisey ve Nuhoğlu, 2017, s. 283-284). Kanaatimizce bu aşamada elde edilen veriler suçun ispatlanmasına fayda sağlayabileceği kadar öte yandan yalnızca niteliği itibari ile failinde lehine sonuçlar da doğurabilir.

Bu kapsamda elde edilen verilerle mevcut teknolojik imkânların bir araya gelmesiyle özellikle örgütlü suçlar (Yenisey ve Nuhoğlu, 2017, s. 283-284) olmak üzere birçok suç ve yasadışı oluşumun bertaraf edilebilmesi gibi önemli faydalar elde edilmektedir. Örneğin göçmen kaçakçılığı ya da insan ticareti yapmak üzere hazırlıklara başlayan bir organizasyon henüz hazırlık aşamasında engellenebilir. Ön alan evresinin bu gibi faydalar sağlanırken kâr zarar analizi ilgili birimler tarafından doğru yapılmalıdır. Bir suç örgütünü sonlandırmak amacıyla yapılan ön alan çalışmalarında üçüncü kişilere ait haklar ihlal edilmemelidir.

Güvenlik Soruşturmaları

Kamu kurum ve kuruluşlarında göreve alacak kişilerin görevleri esnasında gizlilik dereceli bilgilere erişiminin uygunluğunun, ayrıca özellikle güvenlik faaliyetlerine ilişkin görevlerde yer alacak personelin değerlendirilmesi (Kuloğlu, 2015, s. 19), ulusal güvenlik açısından önem taşımaktadır. Milli güvenlik ve kamu düzeni açısından önemli olan kurumlardaki görevlere talip olan kişi hakkında göreve başlayacağı kurumun talebi doğrultusunda yetkili makamlar tarafından güvenlik soruşturması ve arşiv araştırması gerçekleştirilmekte ve yapılan araştırma neticesinde hazırlanan rapor doğrultusunda kurum bünyesinde oluşturulan komisyon ilgili kişinin göreve atamasının yapılıp yapılmayacağı konusunda karar vermektedir (Türkoğlu Üstün, 2021, s. 791). Güvenlik soruşturması ve arşiv araştırması sürecinde kişiye ait adli ve idari veriler, sağlık verileri gibi pek çok kişisel veriye erişilmektedir (Karabulut, 2014, s. 80).

Avrupa İnsan Hakları Mahkemesi (AİHM) *Leander v. İsveç Başvurusunda*[10] güvenlik soruşturmasına ilişkin yapılan değerlendirme nihayetinde işine son verilen kişiye ilişkin kararında, kişinin özel hayatına mahsus olan bilgilerin tutulması ve kullanılmasının yasalara uygun olmadığını değerlendirerek, Avrupa İnsan Hakları Sözleşme'nin (AİHS) 8. maddesinin ihlal edildiğine karar vermiştir.

Öte yandan güvenlik soruşturmasına ilişkin hak ihlali iddiaları Türkiye'de şikâyet konusu olmuş ve Anayasa Mahkemesi (AYM) kararlarına yansımıştır. AYM, güvenlik soruşturması ve arşiv araştırması kapsamında yapılan işlemlerde elde edilen verilerin kişisel veri niteliği taşıdığını ve bireylerin bu kapsamda kişisel verilerin korunmasını isteme hakkına sahip olduğunu belirtmektedir[11]. Kişisel verilerin işlenmesi konusunda *Fatih Saraman* başvurusu incelendiğinde; başvurucunun on sekiz yaşından evvel mahkûmiyetine konu olan adli sicil kaydı, güvenlik soruşturması işlemleri kapsamında talep eden idari makamla paylaşılmış ve güvenlik soruşturması olumsuz neticelenmiştir. AYM, yaptığı değerlendirme özel hayata saygı hakkının kanuna dayanma şartı bakımından eksik olması sebebiyle gerçekleştirilen bu işlemde hak ihlali bulunduğu

[7] Arif Ali Cangı Başvurusu: BN. 2016/4060, KT. 17/09/2020.
[8] Kararın detayı için bkz: (Özkaya & Toprak, 2022, s. 81).
[9] 2559 sayılı Kanun, Ek madde 7; 2803 sayılı Kanun madde 7, ek madde 5.
[10] *Leander v. İsveç Başvurusu,* (Çevrimiçi), https://www.echr.coe.int/Documents/FS_Data_TUR.pdf, (11.05.2021).
[11] Anayasa Mahkemesi, 19.02.2020 tarihli, E. 2018/163, K. 2020/13 sayılı kararı.

kararına hükmetmiştir.[12] Kişisel verilerin ihlali konulu Anayasa Mahkemesi kararları incelendiğinde; bu başvuru hakkında verilen karar önemli bir mihenk taşı olma özelliği taşımaktadır. Anayasa Mahkemesi de kararın bu özelliği nedeniyle gelecekte verdiği kararlarda sıklıkla bahse konu başvuruya atıf yapmıştır.

Önleyici Kolluk Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi

Güvenliğe dair önleyici faaliyetlerin esas amacı kamu düzeni ve güvenliğine olumsuz etki edecek unsurların tehlike arz edecek hale gelmeden engellenmesine ilişkin yöntemlerin uygulanmasıdır (Kızılırmak, 2019, s. 234). Bu kapsamda dikkat çeken husus kolluğa verilen yetkilerin mevzuatta yer alan birden çok düzenlemeyle tanımlanmış olmasıdır (Köksal, 2021, s. 1748). Kamu düzeninin sağlanması doğrudan toplumu ve idareyi ilgilendiren bir husustur. Dolayısıyla bu alanda yetkili birimlerin görev, yetki ve bu bağlamda kullanılan yöntemlerin kodifiye edilerek genel bir kolluk mevzuatının oluşturulması hem kişi hak ve özgürlüklerinin tesis edilmesi noktasında hem de çalışma bağlamında ele alınan kişisel verilerin korunması hususunda önem taşımaktadır. Önleyici kolluk faaliyetleri kapsamında başvurulan yöntemler kimlik sorma ve kimlik tespiti, parmak izi, yüz tanıma sistemleri, elektronik gözetim sistemleri, telekomünikasyon yoluyla iletişimin denetlenmesi, teknik araçlarla izleme ve banka hesaplarının incelenmesi olarak sayılabilir.[13]

Kimlik sorma, çalışma kapsamında ele alınacak ilk önleyici kolluk faaliyetidir. Kimlik sorma ve kimlik tespiti işlemleri yalnızca kanunda belirtilen hallerde gerçekleştirilebilecek bir kişisel veri toplama ve işleme yöntemidir (Yenisey, 2015, s. 77). Bu sebeple görevli polislerin bu işlemi yaparken geçerli bir sebebinin olması önem taşımaktadır. Kimlik sorma uygulaması yalnızca ilgili kanunla verilen yetkiler kapsamında gerçekleşebilir. 2559 sayılı Polis Vazife ve Salahiyetleri Kanunu (PVSK) polise bu yetkiyi tanımaktadır. Kanun'un belirlediği hallerde makul şüphe doğrultusunda kimlik sorulan kişinin kimliğini ibraz etmesi gerekir. Aksi halde kişi kimlik tespiti amacıyla görevli polis tarafından tutulur, durum Cumhuriyet Savcısına iletilir ve alınan talimatlar doğrultusunda gerekli işlem yapılır. Alınan talimatlar doğrultusunda kişinin açık kimliği anlaşılıncaya kadar kişi gözaltına alınabilir[14] ya da ülke nüfusuna kayıtlı olmadığı anlaşılan kişilerin fotoğrafı çekilir ve parmak izi alınarak bu bilgiler kaydedilir.[15] Yukarıda açıklanan nedenlerle polis, suçun tespiti noktasında takdir yetkisini kullanabilmektedir (Atlı, 2019, s. 12). Ancak bu suça müdahalesinin hak ihlaline yol açmaması önem taşımaktadır.

Çalışma bağlamındaki bir diğer yöntem parmak izi alınması ve bu kayıtların kaydedilmesidir.[16] Bilim ve teknolojik imkânların gelişmesiyle biyometrik verilerin kullanımında gözle görülür bir artış yaşanmaktadır (Kaya, 2011, s. 332). Parmak izi, retinal örnek, yüz şekli, ses, el yazılı imza, yürüyüş tipi vb. veriler biyometrik veri olarak kabul edilmektedir (Walker, 2012, s. 197-199). Biyometrik veriler, özel nitelikli kişisel veri olduğundan[17] bu verilerin güvenlik faaliyetleri kapsamında işlenmesi kaçınılmaz olmaktadır. Bu durumun en bariz sebebi ise parmak izi gibi eşsiz –kişiye özel- verilerin suçla mücadelede olayların aydınlatılmasına büyük fayda sağlamasıdır. Yine de biyometrik verilerin kişisel veri olmasından hareketle; alınması, kaydedilmesi, paylaşılması ve saklanması hususlarında kanuna uygun hareket etmek ve kamu yararı ile kişisel çıkarlar arasında adil bir dengenin sağlanması[18] gerekmektedir.

Yüz tanıma teknolojisi de yine güvenlik faaliyetleri kapsamında sıklıkla başvurulan yöntemlerden birisidir. Parmak izi gibi kişiye özel olan yüz yapısı özel nitelikli kişisel verilerdendir. Yüz tanıma teknolojisinde, kişinin kimliğini tespit etmek veya doğrulamak için insan yüzlerinin yapısal analizini yapan ve benzerlikler doğrultusunda belirli sonuçlar ortaya koyan yazılımlar kullanılmaktadır. Bu sayede suçun önlenmesi ve adli işlemleri gerçekleştiği süreçte bu teknolojiden yararlanılmaktadır (Interpol-I, 2020, s. 2).

Yüz tanıma teknolojisinin sağladığı faydaların yanı sıra en önemli dezavantajı yaşlanma, cerrahi operasyon, makyaj, uyuşturucu kullanımı ve çeşitli sebeplerle yüz bölgesine verilen zararlar dolayısıyla

[12] Fatih Saraman Başvurusu, BN. 2014/7256, KT. 27.02.2019.
[13] Bahsedilen önleyici faaliyet yöntemlerinin tamamı bu başlık altında incelenecek olup ayrı başlıklandırma yapılmayacaktır. Detaylı bilgi için bkz. (Can, 2021:147-180).
[14] 2559 sayılı Kanun, madde 4/A-9.
[15] 2559 sayılı Kanun, madde 4/A-11.
[16] 2559 sayılı Kanun, madde 5.
[17] 6698 sayılı Kanun madde 6.
[18] Parmak izi kayıtlarının saklanma sürelerine ilişkin ortaya çıkan uyuşmazlıklar AİHM kararlarına da konu olmuş, Mahkeme; *S. ve Marper v. Birleşik Krallık Başvurusunda* parmak izi kayıtlarının veri tabanlarında belirsiz bir süre ile saklanmasının adil bir denge sağlamaması sebebiyle hak ihlaline sebep olduğu kararını vermiştir. Benzer karar için bkz. *M.K. v. Fransa Başvurusu.*

önleyici kolluk faaliyetlerinde ve soruşturma işlemlerinde kimi zaman istenilen faydayı sağlamamasıdır. Her ne kadar parmak izi gibi eşsiz olsa da onun aksine bozulma ihtimali bulunmaktadır (Interpol-I, 2020, s. 2). Bu dezavantajın en net örneği çocuklardır. Çocukların yüz yapısı kısa sürede değişip parmak izi değişmediğinden yüz tanıma teknolojisinden faydalanılması uzun süreler mümkün değildir. Bahse konu örnekten yola çıkıldığında ise bu denli değişken bir verinin saklama sürelerinin de aynı oranda kısa olması gerektiği söylenebilir (Can, 2021, s. 156).

Elektronik gözetim sistemleri de önleyici kolluk faaliyetlerinin vazgeçilmez yöntemlerinden biridir. Günümüzde kamusal alanların belirli noktalarına elektronik gözetim sistemleri kurularak kişilerin suç işlemesinin önüne geçileceği, bir başka deyişle caydırıcılık yaratılacağı, fikri hâkimdir (Özbek vd., 2019, s. 176; Karabulut, 2014, s. 94). Bu açıdan değerlendirildiğinde suçun önlenmesi temel amaç olduğundan elektronik gözetim sistemleri önleyici kolluk faaliyetleri kapsamındadır. Ancak bu noktada dikkat edilmesi gereken husus bu gözetim sistemlerinin kullanımının amaca uygun olmasıdır.[19] Gözetim sisteminin amacı dışında süreklilik arz edecek şekilde var olması; kişisel verilere erişilmesi ve verilerin işlenmesi kişilerin özel hayatının gizliliğinin ihlali anlamına gelecektir (Can, 2021, s. 156).

Gözetim sistemleri güvenlik faaliyetleri konusunda ihtiyaca göre uyarlanmaktadır. Bu uyarlamaların en bilinen örneklerinden biri plaka tanıma sistemleridir. Bu sistem ile belirli noktalardan geçen araçların plakaları sorgulanmakta böylece trafik kuralı ihlal eden şahıslardan suça karışmış kişilere kadar pek çok kişi tespit edilebilmektedir (Yenisey, 2015, s. 330). Bu yöntemle sorgulanmak amacıyla pek çok plaka verisi toplanmakta olup bahse konu verilerin saklanması ve korunması hususlarında kişisel verilerin ihlali hususlarına azami önem gösterilmelidir.

Ceza Muhakemesi İşlemleri Kapsamında Kişisel Verilerin İşlenmesi

Bir suçun işlenip işlenmediği; işlenmiş ise suçun aydınlatılması ve faillerinin ortaya çıkarılması ve bu suçun yaptırımının ne olacağı şeklindeki bir dizi adli nitelikli faaliyet ceza muhakemesi işlemleri kapsamındadır (Öztürk vd., 2021, s. 7). Ceza muhakemesi kapsamında yürütülen birtakım işlemler doğrudan güvenlik faaliyetleri ile ilgili olduğunda bu süreçte kişisel verilerin işlendiğini söylemek mümkündür. Çünkü suçun meydana geliş biçimi, faillerin tespiti ancak belirli araştırmaların yapılması, dolayısıyla kişisel verilerin işlenmesi, ile mümkündür. Hali hazırda birçok uluslararası metin ve KVKK kapsamında bu işlemler istisna kapsamında yer aldığından[20] adli merciiler bu işlemlerini ilgili mevzuatta belirtilen kuralları takip ederek gerçekleştirmektedir.

Ceza muhakemesi kapsamında ele alınacak ilk kişisel veri işleme yöntemi fiziki kimliğin tespitidir. Fizik kimliği tespit edilirken kişinin biyometrik verileri ve/veya fotoğraflarından yararlanılmaktadır (Can, 2021, s. 180). Fizik kimliğinin tespiti amacıyla ilgili mevzuat[21] gereği şüpheli veya sanığın fotoğrafı çekilebilir, parmak izi alınabilir, ses ve görüntüleri kaydedilebilir. Yapılan soruşturma neticesinde kovuşturmaya yer olmadığı kararı ile beraat ve ceza verilmesine yer olmadığı kararının kesinleşmesi hallerinde bahse konu veriler Cumhuriyet Savcısı huzurunda yok edilip yapılan bu işlem tutanağa bağlanmaktadır ki bu uygulama veri koruma hukukuna uyarlık teşkil eder. Bu tür işlemlerin yapılmasında ilgili mevzuatın dışına çıkmak hukuka aykırılık oluşturur.

Beden muayenesi, vücuttan örnek alınması ve moleküler genetik inceleme kişisel verilerin işlenebildiği bir diğer ceza muhakemesi işlemidir. Olay akabinde yapılan inceleme veya yapılan beden muayenesinin ardından vücuttan alınan örnekler üzerinde moleküler genetik inceleme yapılmaktadır (Ünver ve Hakeri, 2019, s. 619). Genellikle parmak izinin alınması şeklinde uygulanan bu yöntem ile ayrıca saç teli, tükürük gibi kişiye özel DNA örnekleri elde edilmekte ve bu veriler suçla mücadele sürecinde kullanılmaktadır (Temizsoy Bayram, 2018, s. 93).

DNA örnekleri; cinayet vakaları başta olmak üzere özellikler kayıp şahısların bulunması ile kimliği belirsiz cesetlerin kimliklendirilmesi işlemlerinde hayati öneme sahiptir. Kayıp vakalarında, kayıp şahsın yakınlarından 5237 sayılı Ceza Muhakemesi Kanunu (CMK) kapsamında alınan DNA örnekleri, kimliği belirsiz cesedin beden muayenesinde elde edilen/edilebilen veriler ile karşılaştırılıp, kimliği belirsiz cesedin kimliklendirilebilmesi sağlanmaktadır. Bu kapsamda kimliği belirsiz kişilerin kimlik tespitinin yapılabilmesi

[19] Amacına uygun olarak kullanılmayan kamera görüntülerinin özel hayatın gizliliğinin ihlali konulu AİHM Kararı hakkında bkz. *Peck v. Birleşik Krallık Başvurusu.*
[20] KVKK, madde 28/1-ç.
[21] 5271 sayılı Ceza Muhakemesi Kanunu, madde 81.

amacıyla Interpol tarafından uluslararası bir veri tabanı oluşturulmuş[22] ve konuya verilen önem ortaya konulmuştur. Bahse konu projede yer alan biyometrik verilerin depolanmasında DNA sahiplerinin rızasının alınacağı ve depolamada kişisel bilgilerin (ad, soyad, ulusal kimlik no vb.) yerine alfanümerik kodlama kullanılacağı belirtilmiş bu sayede kişisel verilerin korunması ilkelerine de azami ölçüde dikkat edilmiştir.

İletişimin denetlenmesi yöntemi, hem suçların önlenmesinde[23] hem de ceza muhakemesi faaliyetleri[24] çerçevesinde meydana gelen suçlarında aydınlatılması ve faillerinin yakalanması sürecinde yaygın olarak kullanılmaktadır (Şahin, 2007, s. 1097). İletişimin denetlenmesi, araya elektromanyetik bir araç dâhil etmek yoluyla gerçekleştirilen her türlü haberleşmenin (iletişimin) gizli olarak dinlenmesi, tespiti, bu sayede elde edilen bilgilerin kaydedilmesi ve değerlendirilmesi şeklinde gerçekleşir (Öztürk ve Erdem, 2008, s. 637). Bu yöntem ile amaç her ne kadar suç ve suçluyla mücadele kapsamında kamu düzeninin sağlanması olsa da kişilerin özel hayatına ve haberleşme gizliliğine müdahale niteliğindedir. Dolayısıyla devlet kişi hak ve hürriyetlerine saygı duymalı ihlalden kaçınmalıdır (Sözüer, 1997, s. 71; Yokuş Sevük, 2006, s. 54; Şahin, 2007, s. 1109).

İletişimin denetlenmesi, yukarıda belirtilen sebeplerle suçla ve suçluyla mücadele yöntemlerinden biridir. Ancak sebepleri itibarıyla adli nitelikli bir olay olarak değerlendirilemeyecek olan bir çocuğun kaybolması durumu sonuçları itibarıyla adli nitelikli bir olaya dönüşebileceğinden iletişimin denetlenmesi yöntemine başvurulabilir. 2017 yılında 680 sayılı Kanun Hükmünde Kararname ile PVSK'ya eklenen ilgili hüküm[25] gereği gecikmesinde sakınca bulunan hallerde çocuğun yüksek yararı gereği en az zararla bulunabilmesi amacıyla kolluk sulh ceza hâkimi veya mülki idare amirinin emriyle iletişimin denetlenmesi yoluna başvurulabilmektedir.

İletişimin denetlenmesi konusu AİHM kararlarına da konu olmuştur. *Malone v Birleşik Krallık*[26] kararında, başvurucu suç eşyasını bulundurma suçu sebebiyle yargılanmış ve beraat etmiştir. Daha sonra kişinin telefonları Metropolitan Polis Teşkilatı'nca dinlenmiş, denetlenmiş ve kaydedilmiştir. AİHM'nin değerlendirmesinde; iletişimin denetlenmesi konusunda iç hukukta kolluk ve adli makamlara yetki veren bir kuralı olmalıdır. Bahse konu başvuruda haberleşmelerinin dinlenmesi ve telefonunun izlenmesine ilişkin kayıtların polise verilmesi yasalara uygun olmadığından Sözleşme'nin 8. maddesinin ihlal edildiğine karar verilmiştir. Dolayısıyla bu yöntemin kullanımının bağımsız ve tarafsız mekanizmalar tarafından denetlenmesinin standart hale getirilmesi (Köksal, 2021, s. 1754) başta özel hayatın gizliliği ve kişisel verilerin korunmasını isteme hakkının korunmasına önemli bir katkı sağlayacaktır.

Adli bilişim uygulamaları da kişisel verilerin yoğun olarak işlendiği ve saklandığı bir süreçtir. Genel itibarıyla hukuk ve bilişim biliminin sentezi olarak kabul edilen adli bilişim; güvenlik faaliyetlerinin hemen her aşamasında delillerin tespiti, analizi ve korunması ya da delil niteliğini kaybetme ihtimali olan bozulmuş veya değişikliğe uğramış verilerin düzeltilmesinde kullanılır. Böylece adli bilişim, güvenlik faaliyetlerinde ilgili makamlara destek olur ve suçların aydınlatılmasına fayda sağlar (Turan, 2021, s. 94; Arıcı, 2018, s. 23-24).

Adli bilişim sistemleri kapsamlı bir terimdir ve içerisinde birçok projeyi barındırmaktadır. Bu projeler ise çalışma bağlamında kişisel verilerin işlenmesiyle doğrudan ilgilidir. Bunlardan ilki "Genel Bilgi Toplama" yaygın kullanım adı GBT olan sistemdir. Sistem ile kolluk tarafından haklarında aranma, yakalama, tutuklama, yurt dışına çıkma yasağı olan şahısların kaydı tutulmaktadır. Ayrıca yakalanmamış olsa dahi suç işlemiş kişilerden haklarında kovuşturma yürütülen kişilerin de bilgileri sistemde yer almaktadır (Çiçek, 2013, s. 45). GBT sisteminde bulunan kayıtlar ilgili yönerge kapsamında belirlenen usul ve esaslara göre tutulmaktadır.[27]

[22] Detaylı bilgi için bkz. I-Familia Projesi. Interpol-II: https://www.interpol.int/How-we-work/Forensics/I-Familia. (18.06.2021).
[23] 2559 sayılı Kanun, Ek madde 7.
[24] 5237 sayılı Kanun, madde 135.
[25] 2559 sayılı Kanun, madde 13/A.
[26] *Malone v. Birleşik Krallık* Kararı. (Çevrimiçi) https://www.echr.coe.int/Documents/FS_Data_TUR.pdf, (11.05.2021). Benzer kararlar için bkz. *Kruslin v. Fransa Başvurusu, Kopp v. İsviçre Başvurusu, Taylor-Sabori v. Birleşik Krallık Başvurusu, Roman Zakharov v. Rusya Başvurusu,*
[27] Bahse konu yönerge hizmete özel olup açık kaynak erişimi bulunmamaktadır. Bu sebeple yalnızca ilgili yönerge kapsamında erişilebilecek bilgilere tarafımızca yer verilmemiştir. Detaylı bilgi için bkz. (Çiçek, 2013, s. 45). Ayrıca bahse konu Yönergenin yayımlanmamış olması, kişiler açısından öngörme ve çeşitli hukuki güvenceler açısından tartışmalıdır (Köksal, 2021, s. 1774).

GBT sisteminde yer alan veriler suçla aktif mücadele işlemleri dışında güvenlik soruşturması ve arşiv araştırması işlemlerinde de kullanılmaktadır (Can, 2021, s. 182). Esas olarak bu süreçte hukuki ihtilaflar doğmakta ve kişiler ilgili makamlara bu konularda yaşadıkları hak ihlallerinden dolayı başvuruda bulunmaktadırlar.

GBT sistemi ile ilgili en önemli soru işaretlerinden birisi verilerin ne kadar süre ile saklanacağıdır. GBT kayıtlarına dair işlemler ilgili yönerge kapsamında yürütülmektedir. Yönerge'nin 9/b maddesi kapsamındaki suçlarda, şahıs yakalansa dahi kaydı silinmemekte şahsın yakalanmış olması kaydın saklanmasına engel teşkil etmemektedir. Ancak diğer madde kapsamında suçlardan yakalanan şahısların işlemleri tamamlandıktan sonra GBT kaydının silinmesi gerekmektedir. Ayrıca şahıslar kayıtlarının tetkiki ve silinmesi amacıyla ilgili makama dilekçe ile başvurabilmektedir (Çiçek, 2013, s. 45-46).

GBT kayıtlarının silinmesi ve buna dair işlemlerin zamanında yapılması kişilerin haklarına ilişkin ihlallerin yaşamaması açısından önem taşımaktadır. Çünkü işlemleri tamamlandığı halde kayıtları silinmemiş bir şahıs kolluk kuvvetleri tarafından sehven de olsa yeniden yakalanabilir ve ihmali bir davranışın sonucunda kişi hürriyetinden yoksun kılma suçu oluşabilir. Ayrıca kayıtların silinmemesi veya buna dair işlemlerin zamanında yapılmaması diğer hakların kullanılması noktasında da sorunlar çıkarabilir. Nitekim Türk Anayasa Mahkemesine yapılan bireysel başvurularda bu tür mağduriyetlerin yaşandığı görülmektedir[28]. Anayasa Mahkemesine gelen davada[29] özetle; başvurucu terör örgütüne yardım suçundan gözaltına almış, hakkında kamu davası açılmış, dava sonucunda davanın kesin hükme bağlanmasının ertelenmesine karar verilmiştir. Başvurucunun talebi üzerine İçişleri Bakanlığınca GBT kaydı da iptal edilmiştir. Daha sonra ceza infaz kurumu şoförlüğü için başvuruda bulunan başvurucu, Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü'nden adli sicil kaydı ve adli sicil arşiv kaydı belgesinde adli sicil ve arşiv kaydının olmadığına dair belge almıştır. Bu belgeye rağmen başvurucu, işe alım komisyonu tarafından söz konusu yargılamaya ilişkin eylemi bakımından işe uygun bulunmayarak göreve başlatılmamıştır. Yaşanan bu gelişmeler çerçevesinde Anayasa Mahkemesi gerekli incelemeleri yaparak elde edilen bilgilerin belirli bir sürede silinmesi ya da bu yönde izlenecek usul eksikliğinden yola çıkarak hak ihlali gerçekleştiği kararını vermiştir.

Adli bilişim kapsamında yer alan bir diğer sistem "Ulusal Yargı Ağı Projesi" yaygın kullanım adıyla UYAP'tır. Bu sistem, birçok alanda gerçekleştirilen yapısal reformların bir parçası olarak ortaya çıkmıştır. Temel amacı uzun süren yargı işlemlerinin otomasyon sistemi ile daha hızlı ilerlemesi ve kurumlar arası faaliyetlerde koordinasyonun sağlanmasıdır (Sarı, 2021, s. 145; Can, 2021, s. 196). UYAP sistemi, MERNİS[30] ve POL-NET ile entegre bir şekilde hizmet sunmakta olup bu projelerin kullanımı esnasında kişisel verilere erişim ve onların işlenmesi söz konusu olabilmektedir.

Polis Bilgi Sistemi (POL-NET) ise ülke genelinde görev yapan emniyet birimleri arasında işlemlerin hızlı ve güvenilir bir şekilde gerçekleşmesini sağlayan bir altyapı sistemidir (Sarı, 2021, s. 102). POL-NET sayesinde emniyet birimlerinin görev alanına giren adli ve idari işlemler gerçekleştirilmektedir. Yukarıda bahsedildiği üzere UYAP ile entegrasyon yapılmış olması adli işlemlerin seri bir şekilde ilerlemesine imkân tanımaktadır. Alt uygulamalar ile kolluğun soruşturma evresinde olayla bağlantısı olan şahısların ifadelerini alması, fezleke hazırlamasına imkân tanımaktadır. Bu sayede kolluk; kişilerin sosyal güvenlik kurumu bilgileri, kimlik numaraları, mobil iletişim bilgileri, ikamet adresleri gibi kişisel veri niteliğinde bilgilerine erişim sağlayabilmektedir. Ayrıca projeler arası entegre ile kolluk, haklarında yakalama ve tutuklama kaydı olan şahısları sorgulayabilmekte bu sistemlerde kişisel veriler bulunabilmektedir (Çam, 2015, s. 73-74).

POL-NET bünyesinde bulunan birçok farklı proje sayesinde emniyet birimleri delil, parmak izi, balistik inceleme raporları gibi soruşturmanın seyrine olumlu etki sağlayacak dokümanlarına kısa süre içinde elektronik ortamda erişebilmektedir (Çam, 2015, s. 93-97). Böylesi bir imkân şüphesiz ki maddi gerçeğin kısa sürede ortaya çıkarılmasına önemli katkı sağlamaktadır.

Adli bilişim projeleri kapsamında yer verilebilecek bir diğer proje ise TÜBİTAK tarafından geliştirilen Balistika projesidir. Bu proje ile balistik iz ve görüntüler analiz edilmekte ve ait olduğu ateşli silahlarla eşleştirilebilmektedir. Balistika'nın belki de en önemli özelliği incelemeler ve olaylar arası analizler yaparak

[28] Örneğin; Süleyman Akif Nazlıgül Başvurusu, BN. 2018/31982, KT. 15.06.2021.
[29] Turgut Duman Başvurusu, BN. 2014/15365, KT. 29.05.2019.
[30] Merkezi Nüfus İdaresi Sistemi (MERNİS) fiziki ortamda bulunan nüfus kayıtlarının dijital ortama aktarılması ve merkezi bir yapıda tutulmasını sağlayan bir projedir. Detaylı bilgi için bkz. (Çevrimiçi) https://nvi.gov.tr/mernis.

bu sonuçları gerçek kişilerle ilişkilendirilebilmesidir.[31] Bu özelliği itibarıyla kişisel verilere erişimi olan bu projede veri koruma hukukuna dikkat edilmesi gerekliliği unutulmamalıdır.

Sonuç ve Öneriler

Teknolojinin bu denli geliştiği ve suç türlerinin her geçen gün yöntem değiştirdiği bir ortamda güvenlik faaliyetleri kapsamında bilgi teknolojilerinin kullanımı bir ihtiyaç haline dönüşmüştür. Ayrıca iç ve dış tehditlerin fiziki olmasının yanı sıra siber saldırılar gibi bilişim boyutunda olduğu bir dönemde milli güvenlik ve kamu düzeninin sağlanması hususlarında kişisel verilerin işlenmesi ve bu veriler üzerinden stratejiler üretilmesi elzemdir. Bu noktada dikkat edilmesi gereken husus kişisel verilerin işlenmesinde uluslararası düzeyde kabul gören ilkelere riayet edilip edilmediğidir. Asıl olan kişisel verilerin meşru amaçlar doğrultusunda işlenmesi ve hangi şekillerde işlediğinin ilgilisine ve yargı makamlarına açıklanabilir olmasıdır.

Özel hayatın gizliliği ile ilişkilendirilen kişisel verilerin korunması hakkı, uluslararası ve ulusal hukukta kendisine yer edinmiş bir hak olarak karşımıza çıkmaktadır. Güvenlik faaliyetleri kapsamında bazı yöntemler hukuki metinler tarafından istisnai kapsamda değerlendirilmiş olsa da bu faaliyetlerinin yürütülmesi sırasında kişi hak ve özgürlüklerinin ihlal edilmesi durumları ortaya çıkabilir. Zaten Anayasa Mahkemesi ve AİHM kararları göstermektedir ki kolluk faaliyetleri kapsamında kişisel verilerin işlenmesinde hak ihlalleri yaşanabilmektedir. İlerleyen dönemlerde kolluk faaliyetleri çerçevesinde kişisel verilerin işlenmesi, depolanması ve paylaşılmasına ilişkin çeşitlenmesi muhtemel yeni teknolojiler çerçevesinde insan hakları ve güvenlik arasındaki çatışmanın devam edeceği tarafımızca değerlendirilmektedir. Başka bir ifadeyle teknolojik gelişmelerin hızla ilerlemesi, güvenlik ve insan hakları arasında var olan çatışmanın ilerleyen dönemlerde daha da artması anlamına gelmektedir. Bu bakımdan yasama organının istisnalar kapsamında yer alan hususların korunmasına ilişkin müstakil bir yasal düzenleme yapmasının ve güncel gelişmeler çerçevesinde mevzuatı güncellemesinin, hakkın kullanımı ve korunması açısından isabetli olacağı değerlendirilmektedir.

Kişisel verilerin işlenmesinde; veriye erişim yetkisi bulunan kişilerin ilgili mevzuat tarafından belirlenen ilkelere riayet edilmesi önem taşımaktadır. Öte yandan kamu kurum ve kuruluşlarınca kişisel verilerin işlenmesine, kaydedilmesine ve analiz edilmesine yarayan her sisteme ilişkin mevzuatta müstakil düzenlemeler yapılmasının da yine hakkın kullanımı ve korunması açısından gerekli olduğu değerlendirilmektedir. Bu noktada kişisel verilerle iştigal olan her birimde görevli personele en temelde hukuk devleti, insan hakları gibi eğitim konularının yanı sıra kişisel verilerin korunması konusunda da nitelikli eğitimler verilmelidir. Eğitimlerde teori ve pratik bir arada olmalı teorik bilgiler somut olaylarla birleştirilmelidir.

Son olarak çalışma kapsamında ele alınan kişisel verilerin meşru amaçlar doğrultusunda çeşitli adli bilişim sistemleri aracılığıyla işlenmesi konusu üzerinde durulmalıdır. Bu sistemler kamu düzeninin sağlanması, adalet hizmetlerinin etkili bir şekilde yürütülmesi açısından önemlidir. Ancak insan faktörü göz önünde bulundurularak sıkı denetime tabi olmalıdır. Bu denetimler herhangi bir sorunun varlığı akabinde değil, düzenli olarak gerçekleştirilmeli ve mümkün olduğunca teknolojik imkânlardan faydalanılmalıdır. Denetimlerde şekli unsurlarla birlikte esasa dair incelemeler de yapılmalı, özellikle kişisel verilerin işlenmesinde uyulması gereken ilkelere göre hareket edilip edilmediği kontrol edilmelidir. Bu sayede kişisel verilerin, ilgili personel karşısında korunma potansiyeli artacak ve hak ihlalleri de en aza indirilebilecektir.

Etik Beyan

"Türkiye'de Güvenlik Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi" başlıklı çalışmanın yazım sürecinde bilimsel kurallara, etik ve alıntı kurallarına uyulmuş; toplanan veriler üzerinde herhangi bir tahrifat yapılmamış ve bu çalışma herhangi başka bir akademik yayın ortamına değerlendirme için gönderilmemiştir. Bu araştırma doküman incelemesine dayalı olarak yapıldığından etik kurul kararı zorunluluğu bulunmamaktadır.

Kaynakça

Acaray, D. (2020). 21. yüzyılda insan hakları ve güvenlik. İçinde Özkaya Ö. (Edt.) *Farklı açılımlarla insan hakları ve güvenlik*. Ankara: Adalet Yayınevi.

[31] Detaylı bilgi için bkz. (Çevrimiçi) https://uzay.tubitak.gov.tr/tr/urunlerimiz/balistika-0. (19.06.2021).

Acaray, D. (2021). Anayasa mahkemesi kararları ışığında Türkiye'de insan haklarının korunmasında polisin rolü. *Ombudsman Akademik*, *7*(14), 171-197.

AİHM tematik bilgi notu – kişisel verilerin korunması. Erişim adresi: https://www.echr.coe.int/Documents/FS_Data_TUR.pdf. E.T.11.05.2021.

Akgül, A. (2014). *Danıştay ve Avrupa İnsan Hakları Mahkemesi kararları ışığında kişisel verilerin korunması* (1. Baskı). İstanbul: Beta Yayıncılık.

Akyılmaz, B., Sezginer M. ve Kaya, C. (2021). *Türk idare hukuku* (14. Baskı). Ankara: Savaş Yayınevi.

Arıcı, H. Y. (2018). *Adli bilişim.* Ankara: Seçkin Yayıncılık.

Arınmış Uzun, S. (2021). Türkiye'de kişisel verilerin korunması ve vatandaş algısının ölçülmesi. *Bilişim Teknolojileri Dergisi*, *14*(3), 207-221.

Aşıkoğlu Şehriban, İ. (2018). *Avrupa Birliği ve Türk hukukunda kişisel verilerin korunması ve büyük veri*. İstanbul: On İki Levha Yayıncılık.

Atlı, T. (2019). Kişisel verilerin önleyici, koruyucu ve istihbarı faaliyetler amacıyla işlenmesi. *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi, 2*(1), 4-22.

Aydın, S. E. (2015). *AİHM içtihatları bağlamında kişisel verilerin kaydedilmesi suçu* (1. Baskı). İstanbul: On İki Levha Yayıncılık.

Bayırdır, Z. (2016). *Özel hayatın korunması çerçevesinde istihbarat faaliyetleri* (Yüksek Lisans Tezi). Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Bilir, F. (2020) 6698 sayılı Kişisel Verilerin Korunması Kanunu'na ilişkin değerlendirme ve internet çağında kişisel verilerin korunması. *Anayasa Yargısı Dergisi*, *37*(2), 305-342.

Can, N. (2021). *Kolluk ve adli makamlar tarafından işlenen kişisel verilerin korunması* (1. Basım). İstanbul: On İki Levha Yayıncılık.

Çam, A. R. (2015). *Adli kolluk ve bilişim*. İstanbul: On İki Levha Yayıncılık.

Çeçen, A. (2005). Türkiye'nin güvenliği. İçinde Güngörmüş Kona G. (Der.) *Uluslararası çatışma alanları ve Türkiye'nin güvenliği*, İstanbul: Okumuş Adam Yayınları.

Çınar, B. (1997). *Devlet güvenliği, istihbarat ve terör*, Ankara: SAM Yayınları.

Çiçek, İ. (2013). GBT (genel bilgi toplama) kayıtlarının silinmesi. *Terazi Hukuk Dergisi, 8*(88), 44-48.

Duman, Ö. (2020). Kişisel verilerin korunmasını isteme hakkına ilişkin anayasal güvenceler ve ilkeler. *Anayasa Yargısı Dergisi, 37(2),* 357-401.

Erdoğan, M. (2013). Anayasal-demokratik bir rejimde özgürlük ve güvenlik. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, 12(24),* 21-29.

Ergil, D. (2001). Güvenlik ve özgürlükler: siyaset felsefesi açısından. İnsan Hakları ve Güvenlik. *Türkiye Barolar Birliği.*

Gözler, K. ve Kaplan, G. (2021). *İdare hukuku dersleri.* Bursa: Ekin Basın Yayın Dağıtım.

Günday, M. (2013). *İdare hukuku.* Ankara: İmaj Yayınevi.

Henkoğlu, T. (2017). Kişisel verileriniz ne kadar güvende? Bilgi güvenliği kapsamında bir değerlendirme. *Arşiv Dünyası Dergisi*, *17-18,* 46-56.

Hizarci, E. (2020). 6698 *sayılı kişisel verilerin korunması kanununun AB veri koruma hukuku ışığında değerlendirilmesi*. Ankara: Yetkin Yayınları.

Interpol-I. Erişim adresi: https://www.interpol.int/How-we-work/Forensics/Facial-Recognition. E.T.11.05.2021.

Interpol-II. Erişim adresi: https://www.interpol.int/How-we-work/Forensics/I-Familia. E.T. 18.06.2021.

Karabulut, R. (2014). *Kişisel verilerin korunması ve kolluk hizmetleri* (Yüksek Lisans Tezi). Dicle Üniversitesi Sosyal Bilimler Enstitüsü, Diyarbakır.

Kartal, Ç. (2020). Küreselleşmenin güvenlik parametrelerine etkileri ve bireye yönelmiş güvenlik: insan güvenliği. İçinde Özkaya, Ö. (Edt.) *Farklı açılımlarıyla insan hakları ve güvenlik*. Ankara: Adalet Yayınevi.

Kaya, C. (2011). Avrupa Birliği Veri Koruma Direktifi ekseninde hassas (kişisel) veriler ve işlenmesi. *Journal of Istanbul University Law Faculty*, *69*(1-2), 317-334.

Kılınç, D. (2012). Anayasal bir hak olarak kişisel verilerin korunması. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, *61*(3), 1089-1169.

Kızılırmak, B. (2019). Kişisel verilerin işlenmesinde adli ve önleyici amaçla öngörülen istisnaların ulusal ve uluslararası hukuka göre değerlendirilmesi. *Kadir Has Üniversitesi Hukuk Fakültesi Dergisi*, *7*(2), 225,261.

Köksal, T. D. (2021) Bilgi toplamaya yönelik istihbari kolluk faaliyetine insan hakları perspektifinden bakış. *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi*, *20*(2), 1745-1798.

Kuloğlu, G. (2015). *İç güvenlik istihbaratı ve kolluk*. İstanbul: Beta Yayınevi.

Küzeci, E. (2020). *Kişisel verilerin korunması* (4. Baskı). İstanbul: On İki Levha Yayıncılık.

Oğuz, S. (2018). Kişisel verilerin korunması hukukunun genel ilkeleri. *BEYDER, 13*(2), 121-138.

Oğuzman, K. ve Barlas, N. (2016). *Medeni hukuk*. İstanbul: Vedat Kitapçılık.

Oğuzman, K., Seliçi, Ö., ve Oktay Özdemir, S. (2016). *Kişiler hukuku.* İstanbul: Filiz Kitapevi.

Öz Yıldız, S. (2019). Yeni güvenlik paradigması ekseninde istihbarat ve propaganda savaşları. İçinde M. Imıl (Edt.). *Propaganda ve algı yönetimi.* Ankara: Orion Kitabevi.

Özbek, V. Ö., Doğan, K. ve Bacaksız, P. (2019). *Ceza muhakemesi hukuku* (12. Baskı). Ankara: Seçkin Yayıncılık.

Özkaya, Ö. (2021). Hukuk devletinin bir gereği olarak idarenin denetlenmesi: yargı denetimi. İçinde (Edt.) Kızılboğa Özaslan R. *Kamuda denetim türleri (*ss. 107-158.) (1. Baskı). Ankara: Adalet Yayınevi,

Özkaya, Ö. ve Toprak, İ. (2022). Anayasa Mahkemesi kararları ışığında bir insan hakkı olarak kişisel verilerin korunması. *Sayıştay Dergisi, 33*(124), 71-99.
Öztürk, B. ve Erdem, M. R. (2008). *Uygulamalı ceza muhakemesi hukuku* (12. Baskı). Ankara: Seçkin Yayıncılık.
Öztürk, B., Töngür, A. R. ve Çetintürk, E. (2021). *Ceza ve muhakeme hukukunun temel kavramları II* (1. Baskı). Ankara: Polis Akademisi Yayınları.
Sajfert, J. ve Quintel, T. (2017). Data protection directive (eu) 2016/680 for police and criminal justice authorities. Available at SSRN: https://ssrn.com/abstract=3285873
Sarı, Ö. K. (2021). *İdare hukuku bağlamında e-devlet dönüşümü ve UYAP*. Ankara: Adalet Yayınevi.
Sözüer, A. (1997). Türkiye'de karşılaştırmalı hukukta telefon, teleks, faks ve benzeri araçlarla yapılan özel haberleşmenin bir ceza yargılaması önlemi olarak denetlenmesi. *İÜHFM*, *55*(3), 65-110.
Şafak, A. (1992). *Hukuk terimleri sözlüğü* (1. Baskı). Ankara: Rehber Yayıncılık.
Şahin, C. (2007). Telekomünikasyon yoluyla iletişimin denetlenmesi Yargıtay kararları çerçevesinde bir değerlendirme. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, *11*(1), 1095-1112.
T.C. İçişleri Bakanlığı, MERNİS. Erişim adresi: https://nvi.gov.tr/mernis. E.T. 21.10.2021.
Temizsoy Bayram, N. (2018). *Ceza muhakemesi hukukunda moleküler genetik inceleme ve elde edilen verilerin delil olarak kullanılması* (Yüksek Lisans Tezi). İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.
Turan Başara, G. (2020) Kişisel veri işleme sözleşmesi. *Uyuşmazlık Mahkemesi Dergisi, 8*(16), 57-90.
Turan, M. (2021). *Bilişim hukuku* (5. Baskı)/ Ankara: Seçkin Yayıncılık.
TÜBİTAK. Erişim adresi: https://uzay.tubitak.gov.tr/tr/urunlerimiz/balistika-0. E.T. 19.06.2021.
Türk Dil Kurumu bilişim terimleri sözlüğü. Erişim adresi: https://sozluk.gov.tr/ E.T. 30.05.2022.
Türkoğlu Üstün, K. (2021). Güvenlik soruşturmalarında kişisel verilerin korunması. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, *25*(2), 787-837.
Ünver, Y. ve Hakeri, H. (2019). *Ceza muhakemesi hukuku* C. 1 (15. Baskı). Ankara: Adalet Yayınevi.
Van Belle, G. ve Ruiter, L. (2014). Data and law: beyond the sweat of the brow: who owns published data? and what ıs data? *Journal of Significance*, *11*, 28-31.
Walker, D. R. (2012). Biometric technology in law enforcement. *Neurosurgery, 71*(2), 197-200.
Yenisey, F. (2015). *Kolluk hukuku* (2. Baskı). İstanbul: Beta Yayıncılık.
Yenisey, F. ve Nuhoğlu, A. (2017). *Ceza muhakemesi hukuku.* Ankara: Seçkin Yayınları.
Yokuş Sevük, H. (2006). Kolluk tarafından suçun işlenmesini önlenmesine yönelik yapılan iletişimin denetlenmesine ilişkin değerlendirmeler. *TBB Dergisi*, *67,* 41-56.

ANAYASA MAHKEMESİ KARARLARI

Fatih Saraman Başvurusu, BN. 2014/7256, KT. 27.02.2019.
Turgut Duman Başvurusu, BN. 2014/15365, KT. 29.05.2019.
Arif Ali Cangı Başvurusu: BN. 2016/4060, KT. 17.09/2020.
Süleyman Akif Nazlıgül Başvurusu, BN. 2018/31982, KT. 15.06.2021.

AİHM KARARLARI

Rotaru v. Romanya Kararı, BN. 28341/95, T. 04.05.2000.
Leander v. İsveç Başvurusu, BN. 9248/81, T. 26.03.1987.
Amann v. İsviçre Başvurusu, BN. 27798/95, T. 16.02.2000.
Malone v. Birleşik Krallık Kararı, BN. 8691/79, T. 02.08.1984.
Kruslin v. Fransa Başvurusu, BN. 11801/85, T. 24.04.1990.
Kopp v. İsviçre Başvurusu, BN.23224/94, T. 25.3.1998.
Taylor-Sabori v. Birleşik Krallık Başvurusu, BN. 47114/99, T. 22.01.2003.
Roman Zakharov v. Rusya Başvurusu, BN. 47143/06, T. 04/12/2015.
S. ve Marper v. Birleşik Krallık Başvurusu, BN. 30562/04, T. 04.12.2008
M.K. v. Fransa Başvurusu, BN.19522/09, T. 18.07.2013
Peck v. Birleşik Krallık Başvurusu, BN. 44647/98, T. 28.04. 2003.

EXTENDED ABSTRACT

"Personal data", which refers to all kinds of data related to an identified or identifiable person, is collected in all areas of life in nowadays statues. With the processing of personal data, the accessing to information becomes easier, but the risk of disclosure of the privacy of personal data arises at the same time. In this point, it is also vital to make sure the security of the data in the processing and storage of personal data. To provide the security of data, it is important to detect the officers who process this data, and to determine their authorities and responsibilities. In the study, an evaluation will be made in terms of security activities for the processing of personal data.

Personal data such as place of birth, marital status, gender, fingerprint, social security information, medical data, photographs of individuals are processed within the scope of law enforcement activities. In

2010, the Turkish constitutional law on the protection of personal data was amended. After this constitutional amendment, the Law on Protection of Personal Data No. 6698 was enacted in 2016. In this way, the legal basis for the protection of personal data has been strengthened. These regulations regarding personal data are important in terms of ensuring the confidentiality of people's private life and, on this occasion, protecting human privacy and personality. The main thing in law enforcement activities is to ensure public order. However, while maintaining public order, interference with the fundamental rights and freedoms of individuals is expected to be minimal.

There is an inversely proportional relationship between security and human rights. In our opinion, all elements of security should exist in order for individuals to enjoy their fundamental rights and freedoms without any problems. While "public interest" is taken into consideration in public services, "public order" should be ensured in law enforcement activities. In addition, it is essential to re-establish it when public order is disturbed. In this regard, the administration has wide powers in terms of precautions and actions to be taken to provide security. However, authority must be taken that these powers do not violate individual rights and freedoms. For this reason, state authority has to be limited.

Personal data can be used for national defense, national security, public security, public order, economic security and preventive, and intelligence activities. There are also exceptions for using it. In addition to these, it can be processed in important matters that concern the whole country, as well as in investigation, prosecution, trial, or execution proceedings by the judicial authorities. Personal data within the scope of law enforcement activities are handled in the following three categories: data processing as required by national security activities, data processing within the scope of preventive law enforcement activities, and personal data processing within criminal proceedings.

Within the framework of national security activities personal data can be considered within the scope of national security as intelligence activities, investigations and security investigations are activities.

Preventive law enforcement activities include the following methods: asking for identity and identification, fingerprinting, facial recognition systems, electronic surveillance systems, monitoring communication via telecommunication, monitoring by technical and examining bank accounts.

It is possible to say that personal data is processed in some transactions carried out within the scope of criminal procedure. Because the way of the crime occurs and the perpetrators might be found out can only be possible with certain researches and processing of personal data. The first personal data processing method to be considered within the scope of criminal procedure is the determination of physical identity. While determining the physical identity, the biometric data and photographs of the person are used. Physical examination, taking samples from the body and molecular genetic analysis are another criminal procedure that personal data can be processed. The method of monitoring of communication is widely used both in the prevention of crimes and in the process of finding out the crimes that occur within the framework of criminal procedure activities and catching the perpetrators. Forensic applications are also a process in which personal data is intensively processed and stored.

Forensic informatics, which is generally accepted as the synthesis of law and information science, is used in almost every stage of security activities. The aim is to identify, analyze and preserve evidence. It is also used to correct corrupted or altered data that may lose its evidential quality. GBT is a security information system. Thanks to the system, the law enforcement can keep records of individuals who are prohibited to go abroad being searched, arrested, detained. In addition, even if they have been caught, the information of the people who have been prosecuted is also included in the system. The records in the GBT system are kept in accordance with the procedures and principles determined within the scope of the relevant directive. Another system within the scope of forensic informatics is UYAP (National Judiciary Informatics System). This system is made as a part of structural reforms carried out in many areas. Its main purpose is to ensure that the long-lasting judicial proceedings proceed faster with the automation system and to ensure coordination in inter-institutional activities. The UYAP system provides services in an integrated manner with MERNİS and POLNET. During the use of these projects, personal data may be accessed and processed. Another project that can be included within the scope of forensic informatics projects is the "Balistika" project developed by TUBITAK. With this project, ballistic traces and images are analyzed, so firearms can be determined for belonging to them. Perhaps the most important feature of Balistika is the ability to associate the results with real people by making investigations and analyzes

between events. Due to this feature, it should not be forgotten in this project, the project should obey the law about data security.

It is important that the persons authorized to access the data regarding the processing of personal data comply with the ethical rules and principles. On the other hand, regulations regarding the processing, recording and analysis of personal data should be made according to each institution specifically. This is necessary for the use and protection of the right. Forensic information systems are important in terms of ensuring public order and effective execution of justice services. However, it should be subject to rigid auditing, considering the human factor. These inspections should be carried out regularly, not after the existence of any problems. In addition, technological opportunities should be utilized as much as possible.