Savunma ve Güvenlik Araştırmaları Dergisi, 2(2): 123-142 (2025)

Basılı/Printed ISSN: **3023-5278**

SAVUNMA VE GÜVENLİK ARAŞTIRMALARI DERGİSİ

The Journal of Defence and Security Research

https://dergipark.org.tr/tr/pub/saga

Kişisel Verilerin Korunması Hakkına Yönelik Müdahale Oluşturan İstihbarat Faaliyetlerinin (Analiz ve Üretim) İncelenmesi

Examination of Intelligence Activities (Analysis and Production) That Constitute Interference with the Right to Protection of Personal Data

Alper Yasin ÖZÇELİK[1*]

[1]*Millî Savunma Üniversitesi, Alparslan Savunma Bilimleri ve Millî Güvenlik Enstitüsü, İstihbarat Çalışmaları Yüksek Lisans Öğrencisi, 06100 Çankaya/ANKARA*

Makale Bilgisi

Araştırma makalesi
Başvuru: 31.01.2025
Düzeltme: 30.06.2025
Kabul: 30.06.2025

Keywords

Intelligence Law
Personal Data
Data Privacy
Intelligence Analysis
Mass Surveillance

Anahtar Kelimeler

İstihbarat Hukuku
Kişisel Veriler
Veri Gizliliği
İstihbarat Analizi
Kitlesel Gözetim

Özet

Bilgi teknolojilerinin gelişmesi vesilesiyle eğitim, sağlık, güvenlik ve bankacılık gibi pek çok sektörde verilen hizmetin hızını, kalitesini ve kapsamını artırmak amacıyla milyonlarca insana ait veriler işlenmekte, analiz edilmekte veya saklanmaktadır. Bu veriler kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi kapsamaktadır. Bu sebeple üçüncü tarafa mensup odaklar tarafından ele geçirildiğinde telafisi zor mağduriyetler yaşanmaktadır. Bazı ülkelerde kanun koyucu, yaşanabilecek mağduriyetleri önlemek amacıyla, vatandaşlarına ait kişisel verilerin korunmasıyla ilgili yasal düzenlemeleri yürürlüğe koymuş; yasal altyapıyı oluşturduktan sonra kişisel verileri işleyecek resmi veya özel kurumları denetleyecek mekanizmaları devreye almış ve bu sayede kurumsal kapasiteyi arttırma yoluna gitmiştir ancak Millî güvenlik kapsamında yürütülen istihbarat faaliyetlerine karşı kişisel verilerin korunması talebi önümüze güvenlik-özgürlük dengesini çıkarmaktadır. Bu makale, istihbarat faaliyetlerinin kişisel verilerin korunması üzerindeki etkilerini inceleyerek Millî güvenliği riske atmadan bu verilerin korunmasına yönelik çözüm önerileri sunmayı amaçlamaktadır. Bu amaca giderken de Avrupa Birliği İnsan Hakları Sözleşmesi (AİHS), Avrupa Birliği Genel Veri Koruma Tüzüğü, Avrupa Birliği Adalet Divanı (ABAD) ve Avrupa İnsan Hakları Mahkemesi (AİHM) kararları incelenmiştir. Makalenin sonuç kısmında denetim, süre ve kapsam gibi hususların yasal düzenlemeyle netleştirilmesi şartıyla istihbarat faaliyetleri kapsamında kişisel verilerin toplanıp, işlenip, arşivlenebileceği belirtilmiştir.

Abstract

Personal data of millions are being processed, analyzed or stored in order to increase the speed, quality and scope of services provided in many sectors such as education, health, security thanks to rapid development of technology. This data includes all types of information relating to an identified person or may use to identify a person. Therefore, irreparable damage is may experience in case of seizing by third-party. In some countries, in order to prevent it, the legislator has put into legal regulations; then implement legal mechanisms to supervise official or private institutions that will process personal data, and thus has sought to increase institutional capacity. However, the demand for the protection of personal data against intelligence activities arise security and freedom dilemma. This article aims to examine the effects of intelligence activities on the protection of personal data and to offer suggestions for the protection without jeopardizing national security. Towards this goal, European Convention on Human Rights, the European Union General Data Protection Regulation, European Court of Justice (CJEU) and the decisions of the European Court of Human Rights (ECHR) were examined respectively. In the conclusion, it was stated that personal data can be collected, processed and archived within the scope of intelligence activities, only if the issues such as audition, duration and scope are clarified by legal regulation.

*Alper Yasin ÖZÇELİK, a.yasinozcelik@gmail.com

1. GİRİŞ

Bilişim dünyasında yaşanan hızlı ve kapsamlı değişiklikler yeni kavramların hayatımıza girmesine olanak sağlamıştır. Bu kavramlardan biri olan kişisel veriler; Kişisel Verilerin Korunması Kanunu Madde 3'e göre *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi",* özel nitelikli kişisel verilerse Madde 6'nın birinci fıkrasına göre; *"kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli verilerdir."* şeklinde tanımlanmaktadır (Kişisel Verilerin Korunması Kanunu, 2016).

Bilgi teknolojileri, yapay zekâ, büyük veri, doğal dil işleme ve makine öğrenmesi gibi alanlardaki gelişmeler neticesinde kişisel verilerin işlenmesi ve analizi kolaylaşmış, bu sayede bireylerin davranışlarıyla ilgili geleceğe yönelik tahminlerde bulunma imkânı ortaya çıkmıştır. Teknolojinin getirdiği kolaylıklar her ne kadar ilk başta olumlu bir gelişme olarak görünse bile olası veri ihlallerinde vatandaşların mağduriyetine sebep olmakta, kişisel verilerin korunması hakkını vatandaşların mahremiyetlerini güvence altına almak ve teknolojinin kötüye kullanımını engellemek açısından modern toplumların temel meselelerinden biri hâline gelmektedir.

Dijital medyanın yaygınlaşmasıyla birlikte birden fazla kaynaktan yararlanarak kişilerin ilgi alanları, arkadaşlıkları, seyahatleri ve istekleri hakkındaki verileri kullanmak suretiyle örüntü bularak detaylı bir profil oluşturabilecek kapasiteye ulaşılmıştır. Bu gelişmelerin yasal sonuçları teknolojinin, yasal düzenlemelerden çok daha hızlı ilerlemesi sebebiyle hâlâ tam olarak ön görülmemiştir. Mahkemeler, teknolojik gelişmelerin sebep olduğu etkileri incelemekte; ayrıca polis ve savcılar, soruşturma veya kovuşturma aşamasında bu araçlardan daha da fazla yararlanmaktadır (Cole, 2013, s. 96).

İstihbarat kurumları, Millî güvenliği sağlama amacıyla terörle mücadele, organize suçlarla başa çıkma ve benzeri kritik görevleri yerine getirmek için veri toplama, analiz etme ve bilgi üretme süreçlerinde geniş yetkilere sahiptir. Örnek vermek gerekirse Federal Almanya Cumhuriyeti Anayasası Madde 87'ye göre devletin çıkarlarına, şiddet eylemleriyle zarar vermek isteyenlere karşı federal sınır muhafızlarını, polis istihbarat birimlerini ve haber alma servislerini görevlendirmiştir (Federal Almanya Cumhuriyeti Anayasası, 1949).

Almanya örneğine benzer şekilde İtalya'da 2007 yılında kabul edilen Bilgi Güvenliği ve İstihbarat Yasasında istihbarat servislerine, anayasal düzene karşı işlenecek suçlara, kamu düzenini ve ulusal güvenliği tehdit eden unsurlara, casusluk faaliyetlerine karşı bilgi toplamak, tespit etmek ve önlemek yetkisi verilmiştir. Bu görev sorumluluklara ek olarak belirli durumlarda gizli bilgileri mahkemeye sunmama yetkisine sahiptirler (Bilgi Güvenliği ve İstihbarat Yasası, 2007).

Ancak bu yetkilerin kapsamı, özel hayatın gizliliğinin korunmasına yönelik endişelere sebep olacak niteliktedir. Büyük ölçekli veri toplama neticesinde elde edilen verilerin analizi ve işlenmesi şüpheli şahıslarla beraber masum insanların da verilerinin ele geçirilmesiyle sonuçlanabilir. Bu tarz olumsuz

durumlar vatandaşların devlete karşı olan güvenini sarsacak nitelikte olup hukuk devleti ilkesine zarar verecek potansiyele sahiptir. Hukukun üstünlüğünün geçerli olduğu demokratik devletler, millî güvenlik kapsamında gerçekleştirdiği istihbarat faaliyetleri sonucunda kendilerine yönelik tehditleri tespit edip önlerken aynı anda vatandaşlarının özel hayatının gizliliğini korumakla mükelleftir. Demokratik devletler, hukukun üstünlüğünü esas alıp, millî güvenlik amacıyla yürüttükleri istihbarat faaliyetleri sayesinde kendilerine yönelik tehditleri tespit edip önlemekle ve aynı zamanda vatandaşlarının özel hayatının gizliliğini de korumakla yükümlüdür.

Kişisel verilerin korunması amacıyla hazırlanan AB Genel Veri Koruma Tüzüğü; devlet tarafından yürütülen istihbarat faaliyetlerinin kişisel verilerin korunması hakkına bazı durumlarda müdahale etmesine izin vermektedir. Bu makale kapsamında incelenen Avrupa İnsan Hakları Sözleşmesinde, (AİHS) ilgili tüzüğün aksine hazırlandığı dönemde kişisel veri kavramı henüz oluşmadığı için bu konuyla ilgili doğrudan bir düzenleme bulunmamaktadır. Ancak ilerleyen süreçle beraber, Avrupa İnsan Hakları Mahkemesi'nin içtihatları sayesinde, AİHS'nin 8. maddesinde düzenlenen özel hayatın korunması hakkı, kişisel verilerin korunmasıyla da ilişkilendirilmiş ve bu alan kısmen güvence altına alınmıştır. Bu çalışmada bahse konu içtihatlarla da ilgili bilgi verilecektir.

Bu çalışmanın amacı; istihbarat faaliyetlerini engellemeyecek şekilde vatandaşlara ait kişisel verilerin korunmasına yönelik çözüm önerileri getirmektir. İstihbarat faaliyeti tanımı çok kapsamlı olduğundan dolayı sadece analiz ve üretim aşamalarında toplanan kişisel verilerin korunmasına yönelik öneriler belirtilmiştir. Bu çalışmanın hipotezi; istihbarat çalışmaları kapsamında gerçekleştirilen faaliyetler esnasında kişisel verilerin; süre, kapsam ve denetime tabi olma şartıyla belirli kurum veya kurumlar vasıtasıyla toplanmalı düşüncesine dayanmaktadır.

Bu çalışmada ilk adım olarak kişisel verilerin Avrupa İnsan Hakları Sözleşmesi (AİHS), Avrupa Birliği Genel Veri Koruma Tüzüğü (GDRP), Avrupa Birliği Adalet Divanı (ABAD) ve Avrupa İnsan Hakları Mahkemesi (AİHM) kararlarındaki yeri ve korunması için öngörülen düzenlemeler incelenmiş, meselenin hukuki çerçevesi ve doktrini belirlenmiştir. İkinci adımda istihbarat faaliyetleri çerçevesinde gerçekleştirilen analiz ve üretim aşamaları incelenmiş, bu aşamalar esnasında kişisel verilerin işlenme yöntemleri ve kullanılan teknikler hakkında genel bir bilgilendirme yapılmıştır. Sonuç kısmında konuyla ilgili değerlendirme ve öneriler okuyucunun dikkatine sunulmuştur.

2. KİŞİSEL VERİLERİN KORUNMASINDA AVRUPA BİRLİĞİ YAKLAŞIMI

Bu bölümde Avrupa Birliği İnsan Hakları Sözleşmesi, AB Genel Veri Koruma Tüzüğü, AB Adalet Divanı ve AİHM tarafından verilen üç adet hak ihlali kararı, ele alınmış; kişisel veri tanımı, hangi verilerin kişisel veri kapsamına girdiği, kişisel verilerin nasıl korunduğu ve koruma aşamasında oluşturulan denetim mekanizmalarının doktrindeki yeri incelenmiştir.

2.1 Avrupa İnsan Hakları Sözleşmesi

Ülkemizin de kurucu üyeleri arasında yer aldığı Avrupa Konseyi tarafından hazırlanan ve 4 Kasım 1950'de Roma'da imzalanıp 3 Eylül 1953'te yürürlüğe giren İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi (AİHS), kişisel verilerle ilgili doğrudan bir ifade veya düzenleme içermemektedir. Ancak, Avrupa İnsan Hakları Mahkemesi zaman içinde oluşturduğu içtihatlarla kişisel verileri korumaya almıştır (Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, 2019, s. 18).

Bu çalışmanın giriş bölümünde de belirtildiği üzere; hazırlandığı dönemde kişisel veri kavramı henüz olmadığı için AİHS'te kişisel verilerin korunmasına doğrudan yer verilmemiştir. Ancak AİHM'in zaman içinde oluşturduğu içtihatlarla kişisel verilerin korunması hakkı, özel hayatın gizliliği kapsamında değerlendirilmiştir (AİHM, Guide on Article 8 of the European Convention on Human Rights, 2024).

AİHS'nin 8. maddesinde; herkesin özel hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahip olduğu belirtilmiştir. Ancak bu hakka kamu otoritesinin müdahalesinin, ancak müdahalenin yasayla öngörülmüş olması ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ekonomik refah, düzenin korunması, suç işlenmesinin önlenmesi, sağlık, ahlak ve başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda gündeme gelebileceği ifade edilmiştir (Avrupa İnsan Hakları Sözleşmesi, 1950).

Bu çerçeve kapsamında AİHM'in dinamik yorum yöntemi kullanarak geliştirdiği ve karar verdiği davaların bazıları aşağıda sıralanmıştır:

- Centrum för Rättvisa v. İsveç kararı (Başvuru No. 35252/08, 25 Mayıs 2021)
- Ekimdzhiev ve Diğerleri v. Bulgaristan kararı (Başvuru No 70078/12, 11 Ocak 2022)
- Szabo ve Vissy v. Macaristan kararı (Başvuru numarası 37138/14, 12 Ocak 2016)

Bu kararların özünde, kişisel verilerin korunmasının, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesiyle güvence altına alınan özel hayata ve aile hayatına saygı hakkının tam anlamıyla yaşanabilmesi ve ayrıca kişisel verilerin kamuya açık olması, 8. madde kapsamındaki korumayı ortadan kaldırmayacağı anlayışı yatmaktadır (Guide on Article 8 of the European Convention on Human Rights, 2024).

Bu anlayış çerçevesinde, belirli bir kişi hakkında veri derlendiğinde, işlendiğinde ya da bu veriler normalde öngörülemeyecek bir kapsamda veya şekilde kamuya açıklandığında, özel hayata saygı hakkının devreye gireceği aşikârdır. Bu tür kişisel veri kullanımlarını, 8. maddedeki güvencelere aykırı düşmeyecek şekilde önleyecek uygun yasal güvencelerin iç hukukta yer alması, birey açısından faydalı olacaktır. AİHM'in dinamik yorum yöntemiyle geliştirdiği içtihatların detaylarına bu çalışmanın ilgili bölümünde yer verilecektir. Bir sonraki kısımda AB Genel Veri Koruma Tüzüğü ve ABAD kararları çerçevesinde kişisel verilerin korunmasına yönelik doktrin okuyucunun dikkatine sunulacaktır.

2.2 Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ve AB Adalet Divanı Kararları (ABAD-CJEU)

4 Mayıs 2016 tarihli Avrupa Birliği (AB) Resmî Gazetesi'nde yayımlanan ve 25 Mayıs 2018 tarihinde uygulanmaya başlayan (AB) 2016/679 sayılı AB Genel Veri Koruma Tüzüğü (GDPR) kapsamında kişisel verileri işlenen kişilerin hakları, veri işleme faaliyetinde bulunanların sorumlulukları, kurallara uyum sağlama usulleri belirtilmiş ve kurallara uymayanlar hakkında uygulanacak yaptırımlar öngörülmüştür (Avrupa Birliği Başkanlığı, 2023).

Tüzüğün tanımlar kısmını anlatan (Article 4) bölümünde kişisel veri tanımı, kişisel verilerin işlenmesi faaliyeti, profilleme ve takma ad kullanımı gibi tanımlar yapılmıştır. İlgili bölüme göre kişisel veri; bir bireyi doğrudan veya dolaylı olarak tanımlayabilecek her türlü bilgi olarak kabul edilmekte olup, isim, kimlik numarası, konum bilgileri, çevrimiçi tanımlayıcılar (IP adresi gibi) ve fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya sosyal kimliğe ilişkin bilgiler kişisel veri kapsamına girmektedir (AB Genel Veri Koruma Tüzüğü, 2016).

Tüzükte kişisel verilerin işlenmesi faaliyetini; kişisel veriler veya kişisel veri kümeleri üzerinde otomatik yollarla ya da manuel olarak gerçekleştirilen, verilerin toplanması, kaydedilmesi, düzenlenmesi, yapılandırılması, saklanması, uyarlanması veya değiştirilmesi, geri alınması, danışılması, kullanılması, aktarılması, yayılması veya başka bir şekilde erişime açılması, hizalanması veya birleştirilmesi, sınırlandırılması, silinmesi veya yok edilmesi gibi her türlü işlem veya işlem dizisini ifade eder (AB Genel Veri Koruma Tüzüğü, 2016).

Kişisel verileri kullanarak yapılan profilleme işlemi; kişisel verilerin otomatik yollarla işlenmesi yoluyla, belirli bir gerçek kişiye ilişkin kişisel yönlerin değerlendirilmesini içeren her türlü işlem olarak tanımlanmıştır. Bu işlem sayesinde ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışı, konumu veya hareketleri ile ilgili analizler yapmak veya tahminlerde bulunulabilir (AB Genel Veri Koruma Tüzüğü, 2016).

Takma ad kullanımı; kişisel verilerin, ek bilgiler olmadan belirli bir veri sahibine atfedilemeyecek şekilde işlenmesi anlamına gelir. Ancak, bu ek bilgilerin ayrı tutulması gerekmekte olup kişisel verilerin belirli veya belirlenebilir bir gerçek kişiye atfedilmesini önlemek için teknik ve kurumsal önlemlere tabi olmalıdır. İlgili tüzüğün kişisel verilerin korunması ve orantılılık ilkesini kapsayan 4. maddesine göre; kişisel verilerin işlenmesi insanlığa hizmet edecek şekilde gerçekleştirilmelidir. Ancak kişisel verilerin korunması hakkı mutlak bir hak değildir; bu sebeple toplumdaki işlevi ile diğer temel haklara göre dengelenmeli ve orantılılık ilkesi çerçevesinde değerlendirilmelidir (AB Genel Veri Koruma Tüzüğü, 2016).

Kamu otoritelerinin görevlerini anlatan 5. maddesine göre; birlik üyesi olan devletler, görevlerini yerine getirmek veya başka bir üye devlet adına görevleri yürütmek için kişisel verileri paylaşmaya ve iş birliği

yapmaya davet edilmektedir. Verilerin korunmasına ilişkin hazırlanan 84. maddeye göre; kişisel veri işleme faaliyetlerinin bireylerin hak ve özgürlükleri açısından yüksek risk oluşturması durumunda, veri sorumlusu tarafından bir veri koruma etki değerlendirmesi (DPIA) yapması mecburidir. Bu değerlendirme kapsamında, riskin niteliği, kaynağı ve ciddiyeti analiz edilir. Değerlendirme neticesinde, uygun önlemler belirlenerek veri işleme süreçlerinin tüzüğe uygunluğu sağlanmalıdır. Risklerin uygun tedbirlerle azaltılamadığı durumlarda, veri işleme faaliyeti öncesinde denetleyici otoritenin görüşüne başvurulmalıdır (AB Genel Veri Koruma Tüzüğü, 2016).

Tüzükte yer alan 51. madde gereğince kişisel verilerle ilgili yapılacak işlemlerin denetlenmesi için her üye ülkenin bağımsız denetleyici kurum kurması gerektiği bildirilmiştir. Her AB üyesi ülke, tüzüğün uygulanmasını denetlemek, bireylerin temel hak ve özgürlüklerini korumak ve kişisel verilerin serbest dolaşımını sağlamak amacıyla bir veya daha fazla bağımsız denetleyici otorite oluşturmalı, tüzüğün AB genelinde tutarlı bir şekilde uygulanmasını sağlamak için birbirleriyle ve Avrupa Komisyonu ile iş birliği yapmalıdır. Bir üye ülkede birden fazla denetleyici otorite varsa, ülke bu otoriteleri temsilen bir otoriteyi belirlemeli ve diğer otoritelerin tüzüğün tutarlılık mekanizmasına uygun çalışmasını sağlamak için gerekli düzenlemeleri yapmalıdır (AB Genel Veri Koruma Tüzüğü, 2016).

Tüzüğün çizmiş olduğu çerçeveye ek olarak AB Adalet Divanı'nın (ABAD) vermiş olduğu kararlar doktrin bazında önemli hususlara ışık tutmaktadır. Bu kararlardan olan 6 Ekim 2015 tarihli ve C-362/14 (Schrems I) ve 16 Temmuz 2020 tarihli C-311/18 (Schrems II) kararlarında, AB'den ABD'ye kişisel veri aktarımı konusu, kişisel verilerin korunmasına ek olarak istihbarat faaliyetleri açısından da ele alınmıştır (Soysal, 2020).

25 Haziran 2013'te Avusturyalı Max Schrems, Facebook'un İrlanda'daki ofisinin kullanıcı verilerini ABD'ye aktarmasının kişisel verilerin korunması ilkesine aykırı olduğunu belirterek İrlanda Veri Koruma Komisyonu'na (DPC) başvuruda bulunmuştur. Schrems, özellikle Edward Snowden tarafından ortaya konan ABD istihbarat faaliyetleri karşısında bireylerin yeterli hukuki güvencelerden yoksun olduğunu vurgulamıştır. Komisyon ise, AB ile ABD arasındaki "Güvenli Liman Anlaşması"nı esas alarak başvuruyu reddetmiştir (Soysal, 2020).

Konu ABAD'a taşınmıştır. ABAD Schrems I kararında, Avrupa Komisyonu'nun 2000/520 sayılı "Güvenli Liman" kararını geçersiz ilan etmiştir. Mahkeme, ABD'de yürürlükte olan yasal düzenlemelerin ve uygulamaların, özellikle ulusal güvenlik ve kamu menfaati gerekçeleriyle kişisel verilere geniş erişim imkânı tanıdığını ve bunun orantılılık ilkesine aykırı olduğunu belirtmiştir. Ayrıca, AB vatandaşlarının ABD'deki veri işleme faaliyetlerine karşı etkili bir yargı yoluna sahip olmamaları, temel haklarının ihlali olarak değerlendirilmiştir. Divan, bu bağlamda, Komisyon kararları bulunsa dahi ulusal veri koruma makamlarının veri aktarımının uygunluğunu denetleme yetkisinin sınırlandırılamayacağını vurgulamıştır. Bu karar, kişisel verilerin üçüncü ülkelere aktarımında yalnızca kurumsal mekanizmalara değil, bireysel temel hakların etkin şekilde korunmasına da öncelik verilmesi gerektiğini ortaya koymuştur (CURIA - Documents, 2015).

Facebook İrlanda ofisi Schrems I kararının ardından ABD'ye veri aktarımının Standart Sözleşme Maddeleri (SCCs) çerçevesinde gerçekleştirildiğini belirtmiştir. Bunun üzerine Max Schrems, 2015 yılında ABAD'a yeniden başvurarak, kişisel verilerinin FBI ve NSA gibi ABD kamu otoriteleri tarafından erişilebilir hale gelmesinin, AB Temel Haklar Şartı'nın 7, 8 ve 47. maddelerine aykırı olduğunu iddia etmiştir (Soysal, 2020).

Başvuruyu inceleyen ABAD Schrems II kararında, ABD istihbarat makamlarının kişisel verilere orantısız ve geniş erişim yetkisine sahip olduğunu, bu nedenle AB vatandaşlarının temel haklarının yeterince korunmadığını ve etkili bir yargı yoluna erişimlerinin bulunmadığını tespit ederek Privacy Shield adlı veri aktarım mekanizmasını geçersiz ilan etmiştir. Buna karşılık, Standart Sözleşme Maddeleri (SCCs) prensip olarak geçerli sayılmış, ancak bu araçların kullanımında, aktarım yapılan ülkenin veri koruma düzeyinin GDPR ile "özdeş veya eşdeğer" olması gerektiği vurgulanmıştır. Mahkeme ayrıca, veri sorumlularının gerekli önlemleri alamadığında aktarımı durdurmaları gerektiğini ve bu süreçte ulusal veri koruma otoritelerinin aktif denetim ve müdahale yükümlülüğü bulunduğunu belirtmiştir (*CURIA - Documents,* 2020).

Netice itibariyle ABAD kararları incelendiğinde bireylerin temel haklarının korunması, korunmadığı durumlarda etkili yargılama yolunun erişilebilir olması, aktarım yapılacak ülkenin veri koruma düzeyinin en az GDPR seviyesinde olması şartıyla veri paylaşımına izin verildiği görülmektedir. Bir sonraki kısımda AİHM kararları incelenecektir.

2.3 Avrupa İnsan Hakları Mahkemesi Kararları

AİHM tarafından incelenerek karara bağlanan 35252/08 başvuru numaralı Centrum för Rättvisa v. İsveç, 70078/12 başvuru numaralı Ekimdzhiev ve Diğerleri v. Bulgaristan ve 37138/14 başvuru numaralı Szabo ve Vissy & Macaristan kararı olmak üzere toplam üç adet dava incelenmiştir. Bu davalarda ilgili devletler tarafından istihbarat faaliyeti kapsamında vatandaşlarına yönelik yürütülen veri toplama sürecine ilişkin kanun tarafından verilen yetkinin orantısız kullanımı, toplanan verilerin başka ülkelerle paylaşımı ve bu faaliyetlerin denetiminde yaşanan eksiklikler incelenmiştir. AİHM tarafından başvurucular lehine hak ihlali kararı verilmiştir. Bu kararlar, millî güvenlik gerekçesiyle yürütülen istihbari faaliyetler sebebiyle olsa dahi, AİHM'in kişisel verilerin korunmasıyla ilgili dikkat ettiği hususlar hakkında bilgi vermek amacıyla seçilmiştir.

a. Centrum för Rättvisa v. İsveç kararı (Başvuru No. 35252/08, 25 Mayıs 2021)

Başvuru sahibi Centrum för Rättvisa isimli insan hakları alanında faaliyet yürüten bir sivil toplum kuruluşu olup, İsveç'in sinyal istihbaratı yoluyla kitlesel haberleşmeyi toplu biçimde izlemesinin Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde güvence altına alınan özel hayata saygı hakkını ihlal ettiğini ileri sürmüştür (Centrum För Rättvisa v. Sweden, 2021).

Mahkeme, toplu gözetimin ulusal güvenliğe yönelik tehditlerle mücadelede meşru bir araç olduğunu, ancak böylesi geniş kapsamlı yetkilerin, sıkı yasal güvenceler ve denetim mekanizmalarıyla

desteklenmesi gerektiğini vurgulamıştır. Mahkeme, sinyal istihbaratı çerçevesinde yürütülen veri toplama sürecini incelemiştir. İnceleme neticesinde kişisel veri niteliğinde olmayan bilgilerin imha sürecinin net bir şekilde yasal zemine oturtulmaması, eldeki verilerin yabancı istihbarat teşkilatlarıyla paylaşılması durumunda gizlilik hakkının yeterince korunmaması, veri toplama faaliyetini denetleyecek bağımsız mekanizmaların eksik olması sebebiyle İsveç'in yürüttüğü sinyal istihbaratı faaliyetinin özel hayatın gizliliğine ilişkin haklara yeterli koruma sağlamadığını belirlemiş ve bu nedenle AİHS'nin 8. maddesinin ihlâl edildiğine hükmetmiştir (Centrum För Rättvisa v. Sweden, 2021).

Mahkeme verdiği kararla dijital çağda devletlerin sahip olduğu gözetim ve veri toplama enstrümanlarının çeşitlenmesiyle birlikte milyonlarca verinin kısa sürede toplanabildiği bir ortamda, bireylerin mahremiyet haklarının korunmasının kamu otoritesi açısından temel bir yükümlülük olduğunu açıkça belirtmiştir.

b. Ekimdzhiev ve Diğerleri v. Bulgaristan kararı (Başvuru No 70078/12, 11 Ocak 2022)

Başvuru sahibi Mihail Tiholov Ekimdzhiev ve Aleksandar Emilov Kashamov ile beraber Avrupa Entegrasyon ve İnsan Hakları Derneği ile Bilgiye Erişim Derneği adlı iki STK'dir. Başvurucular, Bulgaristan'daki istihbarat toplama faaliyeti kapsamında iletişim verilerinin saklanması ve yetkililerce erişilmesine yönelik uygulamalarını, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesine aykırı olduğunu ileri sürmüşlerdir (Ekimdzhiev and Others v. Bulgaria, 2022).

Mahkeme yaptığı inceleme neticesinde Bulgaristan'daki istihbarat toplama faaliyeti kapsamında gerçekleştirilen gözetim (surveillance) uygulamalarının hukuka uygunluk, meşru amaç ve demokratik toplumda gereklilik şartlarını sağlamadığına karar vermiştir. Kararda, gözetim uygulamalarının çoğunlukla şablon kararlarla yürütüldüğü, hâkimlerin gerekli bireysel incelemeleri yapmadan izin verdiği ve etkili bir bağımsız denetim mekanizmasının bulunmadığı vurgulanmıştır. Mahkeme, ayrıca iletişim verilerinin saklanmasına ilişkin uygulamaları da değerlendirmiştir. Elektronik haberleşme hizmeti sağlayıcılarının topladığı verilerin ne kadar süreyle, hangi koşullarda ve kimler tarafından erişilebileceği konusunda yasal çerçevenin açık ve anlaşılabilir olmaması sebebiyle bireylerin özel hayatına yönelik ciddi bir müdahale oluşturduğu belirtilmiştir. Sonuç olarak Mahkeme hem gizli gözetim sistemi hem de iletişim verilerinin saklanması ve erişimi yönünden AİHS'nin 8. maddesinin ihlal edildiğine hükmetmiştir (Ekimdzhiev and Others v. Bulgaria, 2022).

AİHM verdiği kararla devletlerin istihbarat toplama kapsamında yürüttüğü gözetim faaliyetlerinin yasal çerçevesinin net ve anlaşılır olması gerektiği, bu faaliyetleri denetleyecek mekanizmaların da etkili şekilde görev yapmasının yüksek önemde olduğunu vurgulamıştır.

c. Szabo ve Vissy & Macaristan kararı (Başvuru numarası 37138/14, 12 Ocak 2016)

Macaristan'da sivil toplum kuruluşu olarak faaliyet gösteren Eötvös Károly Kamu Politikası Enstitüsü'nün çalışanları AİHS'nin 8. maddesi kapsamında, özellikle yargısal denetimin eksikliği nedeniyle, ulusal güvenlik amacıyla gerçekleştirilen gizli gözetim faaliyetlerini düzenleyen '7/E (3)

gözetimi' yasası kapsamında yapılacak iletişimin izlenmesi, ses ve görüntü kaydı alınması, yer tespiti yapılması ve kişisel alanlara gizlice girilmesi faaliyetleri sebebiyle bireylerin haksız ve orantısız müdahalelere maruz kalma riskinden dolayı AİHM'e başvurmuşlardır (Szabó and Vissy v. Hungary, 2016, s. 1).

Mahkeme, '7/E (3) gözetimi' adlı yasal düzenlemenin, gözetim yetkilerinin suistimalini önleyecek yeterli hukuki güvence sağlamadığını, Adalet Bakanı tarafından yetkilendirilen bu gözetimin siyasi bir nitelik taşıdığını ve yargısal bağımsızlığının bulunmadığını belirtmiştir (Szabó and Vissy v. Hungary, 2016, s. 39).

Kararda, ilgili yasada öngörülen adli denetim eksikliğinin temel hakların korunmasında büyük bir eksikliğe sebep olduğu belirtilmiştir. Adalet Bakanı'nın kararlarına gerekçe sunma zorunluluğunun bulunmadığı ve bu durumun keyfiliğe yol açabileceği vurgulanmıştır. AİHM tarafından, gizli gözetim faaliyetlerinin, demokratik bir toplumda gerekli olabilmesi için daha sıkı ve belirli şartlara bağlanması, buna ilaveten adli denetimin şeffaf olması gerektiği belirtilmiştir. Bu sebeple Macaristan'ın AİHS'nin 8. maddesini ihlal ettiğine karar verilmiştir (Szabó and Vissy v. Hungary, 2016, s. 43-44).

AİHM tarafından verilen üç karar birlikte ele alındığında, istihbarat faaliyeti kapsamında yürütülen veri toplama ve kitlesel gözetim uygulamalarında bireyin devlete karşı savunmasız kalması, yürütülen faaliyetlerin denetim ve şeffaflıktan uzak olması sebebiyle mahkeme tarafından hak ihlali kararı verildiği görülmektedir. AİHM verdiği bu kararlarda çözüm olarak istihbarat faaliyetlerinin net bir yasal çerçevede sıkı bir şekilde denetlenmesi gerektiğini belirtmiştir. Bir sonraki bölümde AİHM'in önerdiği denetim mekanizmalarının Almanya ve Fransa'da nasıl uygulandığı incelenmiştir.

2.4 Avrupa Birliği Üye Ülkelerindeki İstihbarat Denetim Mekanizmaları (Almanya ve Fransa Örnekleri)

Denetim ifadesinden genellikle bireysel özgürlük ile kolektif güvenlik arasında bir denge kurmayı amaçlayan uzmanlaşmış, kurumsal ve kısmen ayrıcalıklı bir düzenleme anlaşılmaktadır. Kniep'e göre istihbaratın demokratik denetimi yalnızca resmî kurumlarla sınırlı olmamalı, sivil toplum kuruluşları, medya ve hukuk yoluyla yapılan denetimlerin de sürece dahil edilmesi gerekmektedir (Kniep vd., 2024).

Ancak Ott'a göre denetim mekanizmalarının oluşturulmasında siyaset rol aldığı için, politik iklimde yaşanacak herhangi bir kutuplaşma denetim sürecini olumsuz etkileyebilir ve istihbarat faaliyetlerinin etkinliği zarar görebilir. Bu yüzden denetim mekanizmalarını oluştururken katılımın genişliğinden ziyade denetimin etkinliği hedeflenmeli ve komisyonlarda istihbaratla ilgili tecrübeli insanlar görevlendirilmelidir (Ott, 2019).

İstihbarat faaliyetleri siyasi veya diplomatik olarak ele alınsa bile, uygulamada hukuki denetimden tamamıyla muaf olması mümkün olmayabilir. Diğer kamu faaliyetleri gibi istihbarat faaliyetlerinin çerçevesi yasal düzenlemelerle belirlenir. Bu sebeple yetki kapsamı ve denetimle ilgili sorunlar yalnız siyasi değil, hukuki niteliktedir (Born vd., 2011, s. 7).

İstihbarat teşkilatları tarafından gerçekleştirilen faaliyetleri denetleyerek, devlet tarafından verilen yetkinin kötüye kullanımını ve olası suistimalleri önlemek amacıyla çeşitli ülkelerde meclis veya senato çatısı altında denetim yetkisine sahip komisyonlar kurulmuştur.

Denetim komisyonlarında görev alan kişilerin halkın seçtiği temsilcilerden oluşan meclis veya senato üyeleri arasından seçilmesinin sebebi, sürecin demokrasiye uygun olarak yürütülmesidir. Denetim komisyonlarında; mecliste temsil edilen partilerden seçilen temsilcilerin bulunması sağlanarak, denetim sürecinin belirli bir siyasi partinin çıkarından ziyade kamu yararı gözetilerek yapılması amaçlanmıştır (Birsan, 2012, s. 56).

Bu kısımda Avrupa Birliği'nin karar alma mekanizmalarındaki ağırlıkları, askerî, ekonomik ve siyasi önemleri sebebiyle Almanya ve Fransa'daki istihbarat denetim mekanizmaları ele alınmıştır. Almanya ve Fransa AB politikalarının şekillenmesinde karar verici nitelikte olup aldıkları kararlar küresel çapta yankı bulmaktadır. Bu çerçevede, bu iki ülkenin istihbarat denetimine ilişkin yaklaşımları ve kurdukları mekanizmalar incelenmiştir.

2.4.1 Almanya'daki İstihbarat Denetim Mekanizmaları

Almanya'da kullanılan denetim mekanizması çok katmanlı düzeyde hazırlanmış olup idari denetim, parlamenter denetim, yargı denetimi ve veri koruma denetimi olmak üzere dört temel hususa dayanmaktadır (Supervision and Oversight, 2025).

Bu dört husus kapsamında Almanya'da faaliyet gösteren istihbarat kurumlarını denetlemekle yetkili yapılar aşağıda listelenmiştir (BfDI - Supervision over federal intelligence services, t.y.).

- Parlamento Denetim Kurulu-PKGr
- G10 Komisyonu
- Federal Veri Koruma ve Bilgi Özgürlüğü Komiserliği-BfDI
- Bağımsız Denetim Konseyi

PKGr Almanya'daki üç federal istihbarat servisi olan Dış İstihbarat Teşkilatı (BND), Anayasayı Koruma Dairesi (BfV) ve Askerî İstihbarat Servisi (MAD) üzerindeki parlamento denetimini gerçekleştirmek üzere 2009 yılında Almanya Federal Cumhuriyeti Anayasasının 45d maddesine istinaden kurulmuştur. PKGr'nin G10 Komisyonu, Bağımsız Denetim Konseyi ve Federal Veri Koruma ve Bilgi Edinme Komiseri gibi diğer denetim organlarıyla iş birliği, 2021 tarihli yasa değişikliğiyle güçlendirilmiş, bu sayede PKGr'nin istihbarat denetimindeki merkezi rolü pekiştirilmiştir. Komisyon denetim faaliyetleriyle ilgili yıllık raporlar hazırlayıp parlamentoya sunar. Komisyon üyeleri Federal Meclis (Bundestag) üyeleri arasından seçilmektedir (Deutscher Bundestag - Einführung, t.y.).

G10 Komisyonu, federal istihbarat servisleri (BND, BfV, BAMAD) tarafından haberleşme, posta ve telekomünikasyon gizliliği alanında (Anayasa'nın-Almanca Grundgesetz- 10. maddesi uyarınca) uygulanan tüm kısıtlayıcı önlemlerin gerekliliği ve kabul edilebilirliği konusunda karar verir. İstihbarat teşkilatı telefon dinlemesi yapmak isterse, teşkilat ilk olarak Federal İçişleri Bakanlığına yazılı ve

gerekçeli bir talep sunmak zorundadır. Bakanlık bu talebi onaylarsa, süreç G10 Komisyonu'na iletilir. Komisyonun onayı olmadan gözetleme faaliyeti gerçekleştirilemez (Deutscher Bundestag - Arbeit Und Aufgaben, t.y.).

Mektup, Posta ve Telekomünikasyon Gizliliğinin Sınırlandırılmasına İlişkin Kanun'un 15'inci maddesine göre, G10 Komisyonu üyeleri Federal Hükümet ile istişare sonrası PKGr tarafından atanır. Komisyon ayda en az bir kez toplanır ve kendi çalışma usullerini belirler. Bu usuller, PKGr'nin onayıyla yürürlüğe girer ve Federal Hükümet ile önceden istişare edilir. Komisyon hem resen hem de bireysel şikâyetler üzerine, istihbarat servisleri tarafından uygulanan gizlilik kısıtlamalarının hukuka uygunluk ve gereklilik açısından denetimini yapar (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, 2001).

Federal Veri Koruma ve Bilgi Özgürlüğü Komiserliği-BfDI, AB Genel Veri Koruma Tüzüğü (GDPR), Federal Veri Koruma Yasası (BDSG) ve Bilgi Edinme Hakkı Yasası kapsamında faaliyet gösterir. Almanya'daki federal kamu kurumları, vergi daireleri, telekomünikasyon ve posta hizmeti sunan kuruluşlar ile bazı sosyal güvenlik kuruluşlarının kişisel verileri işlemesini denetlemekle yükümlüdür. Herhangi bir ihlal durumunun tespiti halinde, BfDI ilgili kurumu uyarabilir, ihtar verebilir ya da yaptırım uygulayabilir. BfDI aynı zamanda Alman Federal Meclisi'ne (Bundestag) veri koruma konularında danışmanlık yapar. Gözetim ve danışmanlık görevlerinin yanı sıra, kamuoyunu kişisel verilerin işlenmesine ilişkin riskler, yasal düzenlemeler, güvenceler ve bireysel haklar konusunda bilgilendirme ve farkındalık yaratma çalışmaları da yürütür (BfDI - Tasks and powers, t.y.).

Federal Veri Koruma Yasasının 11. maddesine göre BfDI komiseri beş yıllık bir süre için görevlendirilir ve en fazla bir kez yeniden seçilebilir. Federal hükümetin gösterdiği aday meclis tarafından onaylandıktan sonra Cumhurbaşkanı tarafından atanır (Federal Data Protection Act (BDSG), 2017).

Almanya'nın iç istihbarat teşkilatı olan Federal Anayasa Koruma Dairesi'nin (BfV) idari ve teknik denetimi, Almanya İçişleri ve Toplum Bakanlığı (BMI) tarafından yürütülmektedir. Vatandaşlara ait verilerin korunmasından Federal Veri Koruma ve Bilgi Özgürlüğü Komiseri (BfDI) sorumludur; gerektiğinde BfV'nin dosyalarını inceleyerek denetim yetkisini kullanabilir. Alman Sayıştayı (Bundesrechnungshof - BRH), federal düzeyde istihbarat kurumlarının mali denetimini sağlar ve denetim sonuçlarını PKGr ve İçişleri Bakanlığı gibi ilgili kurumlarla paylaşır (Supervision and Oversight, 2025).

Haberleşmenin dinlenmesine dair kararlar PKGr tarafından onaylanmak zorundadır. 2015 yılında Avrupa Konseyi tarafından yayımlanan Venedik Komisyonu raporuna göre bu sayede, istihbarat toplama kapsamında gerçekleştirilen gözetim faaliyetlerinin ilk aşamasında PKGr'ye belirli bir kontrol yetkisi tanınmaktadır (Venice Commision Report, 2025).

Yargı denetimi ise bireylerin özel hayatına müdahaleyi içeren istihbarat işlemlerinin, G10 Komisyonu tarafından denetlenmesi yoluyla sağlanır. Ayrıca Federal Veri Koruma Komiseri (BfDI), kişisel verilerin

işlenmesi süreçlerini düzenli olarak izleyerek, anayasal hakların ihlal edilip edilmediğini kontrol eder. Bu kapsamlı denetim sistemi, istihbarat faaliyetlerinin demokratik ilkelere ve temel haklara uygun biçimde yürütülmesini sağlamayı amaçlamaktadır (Supervision and Oversight, 2025).

Dinleme faaliyetlerinde kullanılacak olan teknik filtreleme ölçütleri, BND'nin önerisi üzerine yine İçişleri Bakanlığı tarafından belirlenmekte, ancak bu işlem G10 Komisyonu'nun onayına sunulmaktadır. G10 Komisyonu, dört asil ve dört yedek üyeden oluşur; bu üyeler yasama dönemi başında PKGr tarafından seçilir. Komisyon başkanının yargıçlık yapabilecek niteliğe sahip olması gerekir. Bu özellikleriyle G10 Komisyonu, siyasi meşruiyetini PKGr'den alan yarı-yargısal bir denetim organı niteliğindedir (Supervision and Oversight, 2025).

Stratejik gözetim faaliyetlerinde, G10 Komisyonu seçici ölçütlerin hukuka uygunluğunu, özellikle orantılılık ilkesine göre denetler. Özel hayatın gizliliğini ilgilendiren verilerin toplanıp toplanmadığı konusunda Komisyon'a bilgi verilmek zorundadır; bazı durumlarda bu verilerin silinip silinmemesi yönünde kararı da G10 verir. Komisyon, veri tabanlarında periyodik denetimler yaparak gereksiz verilerin silinip silinmediğini kontrol eder. Ayrıca, elde edilen istihbaratın dost ülkelerin servislerine aktarılması durumlarında da bilgilendirilmesi gerekir (Supervision and Oversight, 2025).

Daha genel bir denetim açısından ise, hükümetin PKGr'ye her altı ayda bir G10 Yasası'nın uygulanmasına dair istatistiksel bilgi vermesi zorunludur. Bu bilgiler, stratejik gözetim yoluyla elde edilen kişisel verilerin yabancı devlet kurumlarına veya uluslararası kuruluşlara aktarımını da içermektedir. PKGr, bu süreçlerde re'sen soruşturma başlatma yetkisine ve gerekli kaynaklara sahiptir. PKGr politika düzeyindeki konularla ilgilenirken, G10 Komisyonu daha çok teknik ve idari denetim görevlerini yerine getirmektedir (Venice Commision Report, s. 30).

Almanya'daki denetim mekanizmasını oluşturan unsurlar geniş bir çerçevede incelendiğinde, temel hedefin istihbarat faaliyetlerinin demokratik şekilde denetlenmesi, bireysel hak ve özgürlüklerin korunmasının sağlanması olduğu görülmektedir. Almanya'daki denetim mekanizmaları bu bölümde incelenmiştir. Bir sonraki kısımda Fransa'daki istihbarat denetim mekanizmaları incelenecektir.

2.4.2 Fransa'daki İstihbarat Denetim Mekanizmaları

AB Temel Haklar Ajansı'nın (EU-FRA) 2023 yılında yayımlamış olduğu rapora göre Fransa'daki istihbarat denetim mekanizması Ulusal İstihbarat Tekniklerini Denetleme Komisyonu (CNCTR) ve Parlamento İstihbarat Delegasyonu (DPR) olmak üzere iki komisyon ön plana çıkmaktadır (Surveillance by Intelligence Services, 2023).

CNCTR; 24 Temmuz 2015 yılında yürürlüğe giren "Fransa İstihbarat Yasası" kapsamında Fransız İstihbarat teşkilatlarının faaliyetlerinin denetlenmesi amacıyla kurulmuştur. Komisyonun amacı; Fransa'da gerçekleştirilen istihbarat faaliyetlerinin kanunlara uygunluğunu bağımsız ve tarafsız şekilde denetlemektir. Komisyon, toplam dokuz üyeden oluşur ve bu üyeler Parlamento, Yargıtay, Devlet Konseyi ile Fransız Telekomünikasyon Düzenleme Kurumundan gelmektedir. Üyeler; parlamenterler,

yüksek yargı mensupları ve elektronik haberleşme alanında uzman kişilerden müteşekkildir. Komisyon başkanı Devlet Konseyi ve Yargıtay tarafından gönderilen üyeler arasından Cumhurbaşkanı tarafından seçilmektedir. Görev süresi altı yıl olup tekrar atanamazlar (Status | CNCTR, t.y.).

CNCTR tarafından her yıl gerçekleştirilen denetim faaliyetlerinde tespit edilen hususlar rapor halinde kamuoyuyla paylaşılmaktadır. 2023 yılında yayımlanan raporda gözetim altındaki kişi sayısı, teknik izleme taleplerinin sayısı, uluslararası haberleşme takip taleplerinin sayısı, istihbarat faaliyetleri kapsamında yaşanan sorunlar, yapay zekânın istihbarat faaliyetlerinde kullanımı, organize suç ve siber saldırılar incelenmiştir. Raporda tespit edilen hususların yanında hukuki, yapısal ve kapasite artırımına yönelik iyileştirme önerilerine de yer verilmektedir (CNCTR, 2023).

Parlamento İstihbarat Delegasyonu (DPR), 9 Ekim 2007 tarihli ve 2007-1443 sayılı yasa ile istihbarat faaliyetlerinin demokratik yollarla denetimini sağlamak amacıyla kurulmuştur. DPR, hem Meclis hem de Senato'ya karşı sorumlu olup iç güvenlik ve savunma işlerinden sorumlu daimî komisyon başkanları da dâhil olmak üzere dört milletvekili ve dört senatörden müteşekkildir (DPR, t.y.).

DPR, devam eden operasyonlar, faaliyetler ve yabancı istihbarat teşkilatlarıyla yürütülen ilişkiler hariç olmak üzere denetim faaliyeti için istihbarat teşkilatlarından her türlü bilgi ve belgeyi talep etme hakkına sahiptir. Bu kapsamda istihbarat servislerine ilişkin denetim raporlarının listesi düzenli olarak her altı ayda bir DPR'ye iletilmektedir. Buna ek olarak Delegasyon, her yıl Ulusal İstihbarat ve Terörle Mücadele Koordinatörü'nden Ulusal İstihbarat Rehberi'ni (PNOR) sunmasını talep edebilir (National intelligence authorities and surveillance in the EU, 2022, s. 9).

Almanya ve Fransa'daki istihbarat denetim mekanizmaları sayesinde, istihbarat teşkilatlarının faaliyetleri, çeşitli bağımsız denetim organları ve parlamento komisyonları aracılığıyla denetlenmektedir. Denetim mekanizmalarının temel hedefi istihbarat faaliyetlerine zarar vermeden hukuk içerisinde denetim görevini icra etmektir. Kişisel verilerin korunması ilkesiyle güvenlik gerekliliği arasında denge kurma çabası sebebiyle bu iki ülkenin izlediği yol incelemeye değerdir. Bir sonraki bölümde istihbarat faaliyeti aşamalarını oluşturan analiz ve üretim kısımları incelenmiştir.

3. İSTİHBARAT FAALİYETİ – ANALİZ VE ÜRETİM

Bu kısımda istihbarat çarkının analiz ve üretim aşamasında kişisel verilerin korunması hakkına yapılan müdahaleler incelenecektir. İstihbarat faaliyeti planlama, toplama, işleme, analiz ve üretim, yayma olmak üzere beş basamakta özetlenebilir. Bu basamakların oluşturduğu döngüye istihbarat çarkı denilmektedir. Çarkın başlangıç noktası planlama aşaması olup karar verici konumda bulunan hükümet yetkilileri tarafından istihbarat yapılacak konu veya hedef belirlenir. Konu belirlendikten sonra toplama aşamasına geçilerek hedefle ilgili bilgi toplanır. İşleme aşamasında toplanan veriler rapor haline getirilir. Analiz ve üretim evresinde işleme aşamasında hazırlanan raporda yer alan bilgiler yakından incelenip hedefle ilgili mevcut durumda neler olduğu, gerçekleşme sebepleri ve ilerde yaşanabilecek gelişmeler analiz edilir. Çarkın son aşaması olan yayma aşamasında karar verici noktada bulunan politika yapıcılara

hedefle ilgili hazırlanan rapor sunulur (ABD Merkezî İstihbarat Teşkilatı (CIA), İstihbarat Çarkı Tanımı, t.y.).

Terör tehdidinin amacını ve kapsamını belirlemek, olası tehditleri anlamak ve tespit etmek amacıyla kolluk kuvvetleri ve istihbarat birimlerinden gelen bilgileri analiz etmek ve işlemek gereklidir (Homeland Security Act, 2002, Madde 201(d)(1)).

Bilişim alanında yaşanan gelişmeler neticesinde veri analizi teknikleri kullanarak veriler arası örüntü bulmak mümkün olmakta, böylelikle iletişimin denetlenmesi yöntemiyle hedef ve hedefin bağlı olduğu kişiler hakkında istihbarat analizi yapılabilmektedir (Walker, 2011, s. 71).

Farklı kategorilerde yer alan hassas nitelikte ve büyük boyuttaki kişisel veriler kayıt altına alınmakta, paylaşılmakta, izlenmekte ve analiz edilmektedir. Veri madenciliği teknikleri kullanılarak terörizmle mücadelede yardımcı olabilecek büyük hacimli veri setlerinden anlamlı sonuçlar çıkarılmaktadır (Donohue, 2006, s. 1139-1140).

Anlık veri analizi ve hızlı istihbarat paylaşımı sayesinde, terör tehdidine karşı alınacak önlemler hızla uygulanmakta ve müdahale koşullarının iyileştirilmesi sağlanmaktadır. Bu sayede, terörle mücadele stratejileri önleyici nitelikte bir anlayışla yürütülerek daha etkin bir güvenlik atmosferi yaratmak mümkündür (Doğan & Taban, 2024, s. 339)

Veri analizi tekniklerinin yanında makine öğrenmesi vasıtasıyla kişisel veriler kullanılarak güvenlik açısından tehdit taraması yapılmaya başlanmıştır. Kitlesel gözetimin kapsamı makine öğrenmesinde kullanılan algoritmaların gelişmesiyle beraber genişlemiş; güvenlik-mahremiyet dengesi değişmiş, makine öğrenmesinde kullanılan tekniklerin etkinliği ile kişisel verilere müdahaleciliği arasındaki ilişkinin yeniden gözden geçirilmesi kaçınılmaz hale gelmiştir (Verhelst vd., 2020, s. 2976).

Kitlesel gözetim (mass surveillance-bulk collection) teknikleri kullanıldığında, yüksek derecede belirsizlik içeren sonuçlara sebep olabilir ve masum vatandaşların ve teröristlerin tehdit seviyesinin sınıflandırılmasında hatalara sebep olabilir. Makine öğrenimi yöntemi veya algoritması düzgün kurgulanmazsa, tehdit seviyesinin kolayca öngörülebilir olmasına veya ciddiye alınmamasına neden olabilir. Bu tarz olumsuz durumların önüne geçebilmek amacıyla insan faktörünün denetim sürecinde devreye girmesi gerekmektedir. Büyük insan topluluklarının izlenmesi, kullanılan algoritmalar ne kadar da yüksek doğruluk payına sahip olsalar bile çok sayıda hatalı sonuçlara sebep olabilir. 10 milyon kişinin oluşturduğu bir topluluğu analiz etmek için %99,9 doğruluk oranına sahip bir algoritmanın kullanıldığı varsayıldığında, 10.000 kişinin yanlış değerlendirilebileceği öngörülebilir. Popülasyonun artması veya algoritmanın sahip olduğu doğruluk payının düşmesi sebebiyle mağdur olabilecek insan sayısı daha da artacaktır (Verhelst vd., 2020, s. 2979).

İstihbarat servislerinin kişisel veri niteliğindeki bilgileri toplama yöntemleri hedefe yönelik (targeted) ve kitlesel (untargeted) olarak ikiye ayrılmaktadır. Hedefe yönelik yaklaşımda makul şüphe üzerine hedeflenen kişi veya örgütlere yönelik haberleşme veya iletişim takibi yapılmaktadır. Kitlesel

yaklaşımda ise şüphe şartı aranmadan ve hedef gözetmeden teknik olarak toplanabilecek bütün veriler kitlesel gözetim araçları vasıtasıyla elde edilmektedir (Schaller, 2018).

Gelişen teknolojik imkânlar sayesinde elektronik iletişim sinyalleri çeşitli yöntemlerle toplanabilmektedir. Uydu iletişim sinyallerinin takibi veya dünya üzerindeki belirli ülkeleri veya bölgeleri birbirine bağlayan fiber optik kabloların dinlenmesi bu yöntemler arasında sayılmaktadır. Büyük veri niteliğindeki datalara ulaşabilmek amacıyla internet servis sağlayıcılarının ağlarını birbirine bağlamak için kullandığı internet değişim noktaları sık sık hedef alınmaktadır. İstihbarat servisleri elde edilen büyük hacimli verileri filtreleyip ilgili ve ilgisiz verileri birbirinden ayırt etmek amacıyla karmaşık algoritmalar kullanmaktadır. Bu sistemler, genellikle "seçiciler" olarak adlandırılan ve teknik tanımlayıcılar (e-posta adresleri, telefon numaraları, IP adresleri vb.) veya belirli arama terimleri içeren veri filtreleme bileşenleriyle çalışmaktadır (Schaller, 2018, s. 945). Elde edilen iletişim verileri, içerik verisi ve meta veri olmak üzere ikiye ayrılmaktadır:

- İçerik verisi: Metin mesajları, konuşmalar ya da e-postaların içeriği, fotoğraflar, videolar vb.
- Meta veri: İletişim sürecine ilişkin kullanılan altyapı ve cihazların teknik tanımlayıcıları, iletişimin süresi, zamanı ve katılımcıların konumu gibi teknik detayları içerir (Schaller, 2018, s. 945).

Kişisel verilerin korunması ve güvenlik ilişkisi zemininde, kullanılan teknikler, hatalı sonuçlar doğurduğunda özel hayatın gizliliği ilkesinden feragat ederken, Millî güvenlikte elde edilen kazanımlar da zarara uğramaktadır. Makine öğreniminde kullanılan tekniklere ait olan zorluklar sebebiyle belirsizlik seviyesini en doğru ölçebilecek yöntemler kullanılmalıdır (Verhelst vd., 2020, s. 2980).

İstihbarat faaliyetinde yürütülen analiz ve üretim aşamasında kullanılan büyük veri ve makine öğrenmesi metotlarının kişisel verilerin korunması esnasında yaşatabileceği teknik zorluklar ve bu teknik sıkıntılar sonucu gerçekleşebilecek hatalı profillemelerin sebepleri olarak sınıf dengesizliği (class imbalance), boyutluluk laneti (the curse of dimensionality) ve sahte korelasyonlar (spurious correlations) hakkında konunun daha iyi anlaşılması amacıyla aşağıda kısa bir bilgilendirme yapılmıştır (Verhelst vd., 2020, s. 2975).

- Sınıf dengesizliği (class imbalance): Veri kümesinde bulunan sınıfların (örneğin, terörist vs. masum vatandaş) diğer sınıflara göre çok daha fazla veya çok daha az temsil edilmesi sonucu oluşan dengesizliktir (Amar Paul Singh, 2022, s. 38).
- Boyutluluk laneti (the curse of dimensionality): Veri kümesine eklenen değişkenlik veya özellik sebebiyle veri setinin karmaşıklaşması ve makine öğrenme sürecinin zora girmesine sebep olan etkendir (Amar Paul Singh, 2022, s. 39).

- Sahte korelasyonlar (spurious correlations): Veri kümesindeki bazı etiket veya özellikler arasında anlamsız bağlantı (korelasyon) bulması sebebiyle algoritmanın yanlış tahmin yapmasına sebep olabilen etkendir (Ye vd., 2024, s. 1).

Yukarıda bahsedilen sebepler nedeniyle vatandaşlar istihbarat faaliyeti aşamasında yürütülen analiz ve üretim sürecinde kişisel verilerinin doğru analiz edilmemesi sebebiyle algoritma mağduru olarak hatalı profilleme sebebiyle ayrımcılığa uğrama tehlikesiyle karşı karşıya kalabilir (Yu, 2019, s. 354-355).

4. ÖNERİLER

Devletler vatandaşlarını her türlü tehlikeden korumakla yükümlüdür. Ancak koruma görevini ifa ederken özel hayatın gizliliği ilkesini de ihlal etmemeleri gerekir. Bu sebeple güvenlik ve özgürlük arasında hassas bir denge sağlamak zorundadır. Millî güvenliği ve toplum huzurunu korumak için istihbarat faaliyeti gerçekleştirmek ve bu kapsamda veri toplamak elzemdir.

Bu kısımda, istihbarat faaliyeti (analiz ve üretim) kapsamında toplanan kişisel verilerin korunması ve olası mağduriyetlerin önüne geçilmesi amacıyla izlenebilecek yollarla ilgili öneriler sıralanmıştır.

- Yetkili Kurum/Kurumların Belirlenmesi: Kişisel verileri toplamak, analiz etmek, raporlamak ve arşivlemekle yükümlü kurum veya kurumlar belirlenmeli, hangi verileri toplayabilecekleri kanun yoluyla net bir şekilde ortaya konmalıdır. Bu sayede yetki karmaşası tehlikesi bertaraf edilmiş olur.

- Veri Arşivlemede Süre Sınırı Koyulması: Toplanan ve analiz edilen verilerin ne kadar süreyle saklanacağı, tehdit unsuru olarak görünmeyen kişilere ait verilerin ne zaman imha edileceği gibi hususlar belirlenerek gereksiz iş yükünün ve olası mağduriyetlerin önüne geçilebilir. Büyük hacimli verilerin arşivlenmesi önemli bir maliyet kalemi olarak düşünüldüğünde, yapılan analiz sonucu hakkında talebe esas herhangi bir bilgi bulunmayan kişilerin verileri belirli bir süre sonra (örneğin 3 yıl) imha edilebilir.

- İmha Prosedürü: Yapılan çalışmalar neticesinde hakkında Millî güvenliğe zarar verebilecek herhangi bir bilgi bulunmayan kişilere ait verilerin imhasına karar verecek ve gerçekleştirecek görevlilerin unvan ve makamları (Başkan, Başkan Yrd., Genel Müdür, Genel Müdür Yrd., Daire Başkanı vb.) yasal olarak net bir şekilde belirtilmelidir.

- İstihbarat Faaliyetinin Denetlenmesi: İstihbarat ve güvenlik kurumları tarafından gerçekleştirilen faaliyetlerin meclis veya senato çatısı altında oluşturulan bir komisyon vasıtasıyla belirli aralıklarla denetlenmesi; kişisel verilerin güvenliğini güvence altına alır, vatandaşların hak ve özgürlüklerinin korunmasına yönelik olası suistimal veya hataların önüne geçilmesini sağlar.

- Teknolojinin Etkin Kullanılması: Günümüzde gittikçe önemi artan yapay zekâ, veri analizi ve doğal dil işleme gibi teknolojik unsurlar kullanılarak kitlesel gözetim daha hızlı ve etkin

yapılabilir. Olası suistimal ve hataların önüne geçmek amacıyla belirli algoritmalar oluşturarak istihbarat raporunun sunulacağı makamlara daha hızlı ve etkin dönüş yapılabilir ancak bu çalışmalar esnasında oluşabilecek yanlış profilleme ve hatalı sınıflandırma gibi olumsuz durumlar sebebiyle mağduriyet yaşanmaması için algoritmayı denetleyecek ve üst makamlara raporlama yapılmadan önce ek bir denetim unsuru olacak şekilde insan kaynağı kullanılmalıdır.

5. SONUÇ

Bilişim alanında yaşanan gelişmeler sebebiyle insanlara ait kimlik, sağlık, iletişim ve eğitim gibi kişisel verilerin analizi, işlemesi, saklaması ve paylaşması her geçen gün daha da kolay hale gelmektedir. Makine öğrenmesi, doğal dil işleme, yapay zekâ ve büyük veri gibi teknolojik alanda gerçekleşen ilerlemeler sayesinde artık bu verileri kullanarak herhangi bir bireyin, topluluğun veya örgütün davranış şekillerini, rutinlerini ve ideolojisini tahmin etmek mümkün hale gelmektedir.

İstihbarat faaliyetleri neticesinde elde edilen analiz raporları incelenirken, analiz sürecinde kullanılan algoritmaların sadece önyargılı veya hatalı olabileceği değil, aynı zamanda bu hataların karar alma süreçlerine yapabileceği potansiyel etkilerin de göz önünde bulundurulmasında fayda vardır. Büyük veri setlerindeki bilgiler algoritma vasıtasıyla analiz edilirken çeşitli unsurlardan etkilenebilir, hatalı analizlere, eksik değerlendirmelere veya hatalı profilleme sebebiyle belirli topluluklara karşı ayrımcılığa sebep olabilir. Bu sebeple, kullanılan algoritmaların doğruluğu, tarafsızlığı ve güvenilirliği düzenli olarak gözden geçirilmeli ve insan faktörünün yer aldığı denetim mekanizmaları oluşturulmalıdır.

AB Veri Koruma Tüzüğü ve Avrupa İnsan Hakları Sözleşmesi gibi temel yasal düzenlemelerin amil hükümleri gereğince; devletler, vatandaşlarına ait kişisel verileri korumak, paylaşılmasını engellemek, paylaşanlar hakkında gerekli cezai ve idari süreçleri başlatmakla yükümlüdürler. Bu sayede vatandaşlara ait bilgiler, ulusal ve uluslararası yasal düzenlemeler vesilesiyle devlet güvencesi altına alınmıştır.

Ancak bahsi geçen sözleşmelerde kişisel verilerin işlenmesi hususunda Millî güvenlik politikaları çerçevesinde toplumun huzuru ve güvenliğini sağlamak amacıyla devletlere istisnai hak verilmiştir. Resmî istihbarat servisleri devlet politikası gereği her türlü veriyi toplama, işleme, analiz etme ve gerekli makamlarla paylaşma yetkisine sahiptir.

Devletler, kamu düzenini ve toplum huzurunu sağlamak amacıyla yürütülen istihbarat faaliyetlerinde kişisel verileri kullanabilir. Ancak kişisel verileri toplama, işleme, analiz etme, paylaşma ve arşivleme gibi işlemler yapılırken hangi kurumun veya kurumların yetkili olduğu, verilerin ne kadar süreyle arşivleneceği, bu süreci hangi makamın denetleyeceği gibi önemli hususlar net bir şekilde mevzuat yoluyla belirlenmelidir. Bu sayede vatandaşın devletine olan güven duygusu zedelenmemiş olur.

KAYNAKLAR

AB Genel Veri Koruma Tüzüğü, 2016/679 2016/679 (2016).

Amar Paul Singh, Dr. Y. M. (2022). Challenges and opportunities in Big data: A review. *International Journal of Research In Electronics And Computer Engineering*. https://www.researchgate.net/publication/366618139_Challenges_and_opportunities_in_Big_data_A_review

Avrupa Birliği Başkanlığı. (2023, Aralık 5). *AB Genel Veri Koruma Tüzüğü (GDPR) Türkçeye çevrildi*. https://www.ab.gov.tr/ab-genel-veri-koruma-tuzugu-gdpr-turkceye-cevrildi_53650.html

Avrupa İnsan Hakları Sözleşmesi, Avrupa İnsan Hakları Sözleşmesi (1950).

BfDI - Supervision over federal intelligence services. (t.y.). Erişim Adresi: https://www.bfdi.bund.de/EN/Fachthemen/Inhalte/Nachrichtendienste/Kontrollandschaft-Nachrichtendienste-des-Bundes.html

BfDI - Tasks and powers. (t.y.). Erişim Adresi: https://www.bfdi.bund.de/EN/BfDI/UeberUns/DieBehoerde/diebehoerde_node.html

Bilgi Güvenliği ve İstihbarat Yasası, Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto (2007).

Birsan, C.-M. (2012). *Intelligence Effectiveness in the European Union (E.U.) in the New Security Environment* [Naval Postgraduate School]. https://apps.dtic.mil/sti/citations/ADA573500

Born, H., Leigh, I., & Wills, A. (Ed.). (2011). *International Intelligence Cooperation and Accountability*. Routledge. https://doi.org/10.4324/9780203831731

Centrum För Rättvisa v. Sweden, No. 35252/08 (ECtHR [GC] 25 Mayıs 2021).

CIA. (t.y.). *İstihbarat Çarkı Tanımı*. ABD Merkezi İstihbarat Teşkilatı (CIA). Erişim Adresi: https://www.cia.gov/spy-kids/static/59d238b4b5f69e0497325e49f0769acf/Briefing-intelligence-cycle.pdf

CNCTR. (2023). *8th Activity Report*. Commission Nationale de Contrôle des Techniques de Renseignement. https://cms.cnctr.fr/uploads/CNCTR_Rapport_2023_ANGLAIS_vdef_numerique_e4de696836.pdf

Cole, D. (2013). Preserving Privacy in a Digital Age: Lessons of Comparative Constitutionalism. *Georgetown Law Faculty Publications and Other Works*. https://scholarship.law.georgetown.edu/facpub/1310

CURIA - Documents (AB Adalet Divanı 06 Temmuz 2015).

CURIA - Documents (AB Adalet Divanı 16 Temmuz 2020).

Deutscher Bundestag—Arbeit und Aufgaben. (t.y.). Deutscher Bundestag. Erişim Adresi: https://www.bundestag.de/ausschuesse/ausschuesse20/weitere_gremien/g10_kommission/aufgabe-868162

Deutscher Bundestag—Einführung. (t.y.). Deutscher Bundestag. Erişim Adresi: https://www.bundestag.de/ausschuesse/ausschuesse/parlamentarisches-kontrollgremium/einfuehrung-1061928

Doğan, İ., & Taban, M. H. (2024). Terörle Mücadelede Verinin Kullanımı. *Güvenlik Bilimleri Dergisi, 13*(2), Article 2. https://doi.org/10.28956/gbd.1531048

Donohue, L. (2006). Anglo-American Privacy and Surveillance. *Georgetown Law Faculty Publications and Other Works*. https://scholarship.law.georgetown.edu/facpub/790

DPR, A. (t.y.). *Délégation parlementaire au renseignement*. Assemblée Nationale. Erişim Adresi: https://www.assemblee-nationale.fr/dyn/17/organes/delegations-comites-offices/delegation-renseignement

Ekimdzhiev and Others v. Bulgaria, No. 70078/12 (ECtHR 11 Ocak 2022).

Federal Almanya Cumhuriyeti Anayasası (1949).

Federal Data Protection Act (BDSG) (2017).

Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, (Article 10 Law—G 10) (2001).

Guide on Article 8 of the European Convention on Human Rights. (2024). European Court of Human Rights. https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng

Homeland Security Act, Pub. L. No. 107-296 Homeland Security Act (2002).

Kişisel Verilerin Korunması Kanunu, 6698 (2016).

Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi. (2019). KVKK Yayınları No: 1. Erişim adresi: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF

Kniep, R., Ewert, L., Reyes, B. L., Tréguer, F., Cluskey, E. M., & Aradau, C. (2024). Towards democratic intelligence oversight: Limits, practices, struggles. *Review of International Studies*, *50*(1), 209-229. https://doi.org/10.1017/S0260210523000013

National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies. (2022). EU Agency for Fundamental Rights. Erişim adresi: https://fra.europa.eu/sites/default/files/fra_uploads/se-surveillance-report-update-2022-en.pdf

Ott, M. C. (2019, Nisan 17). *Intelligence Oversight in Congress: Perilous Times - Foreign Policy Research Institute*. Erişim adresi: https://www.fpri.org/article/2019/04/intelligence-oversight-in-congress-perilous-times/?utm_source=chatgpt.com

Schaller, C. (2018). Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden. *German Law Journal*, *19*(4), 941-980. https://doi.org/10.1017/S2071832200022926

Soysal, D. T. (2020). *Uluslararası Hukuk Bülteni*. Erişim adresi: https://diabgm.adalet.gov.tr/Resimler/Dokuman/16102024155743b%C3%BClten21say%C4%B1.pdf

*S*tatus | CNCTR. (t.y.). Status | CNCTR. G Erişim Adresi: https://www.cnctr.fr/en/statut#the-cnctrs-oversight-activities-are-coordinated-by-a-committee-of-nine-members

Supervision and oversight. (2025). BundesamtfuerVerfassungsschutz. Erişim adresi: http://www.verfassungsschutz.de/EN/about-us/mission-and-working-methods/supervision-and-oversight/supervision-and-oversight_node.html

Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU - 2023 update | European Union Agency for Fundamental Rights. (2023, Mayıs 22). Erişim adresi: https://fra.europa.eu/en/publication/2023/surveillance-update

Szabó and Vissy v. Hungary, No. 37138/14 (Avrupa İnsan Hakları Mahkemesi (AİHM) 12 Ocak 2016).

Venice Commision Report. (2025). V*enice Commision Council of Europe*. Erişim adresi: https://www.coe.int/en/web/venice-commission/-/CDL-AD(2015)011-e

Verhelst, H. M., Stannat, A. W., & Mecacci, G. (2020). Machine Learning Against Terrorism: How Big Data Collection and Analysis Influences the Privacy-Security Dilemma. *Science and Engineering Ethics*, *26*(6), 2975-2984. https://doi.org/10.1007/s11948-020-00254-w

Walker, C. (2011). *Terrorism and the Law*. Oxford University Press.

Ye, W., Zheng, G., Cao, X., Ma, Y., & Zhang, A. (2024). *Spurious Correlations in Machine Learning: A Survey* (No. arXiv:2402.12715). arXiv. https://doi.org/10.48550/arXiv.2402.12715

Yu, P. K. (2019). *The Algorithmic Divide and Equality in the Age of Artificial Intelligence* (SSRN Scholarly Paper No. 3455772). Social Science Research Network. Erişim adresi: https://papers.ssrn.com/abstract=3455772