Araştırma Makale | Research Article

KHM, Cilt:6 Sayı:1, 2026, s. 311-334.
Geliş Tarihi | Received: 19.12.2025
Kabul Tarihi | Accepted: 06.04.2026
Yayın Tarihi | Published: 30.04.2026
doi: 10.59909/khm.06.01.010

İntihal | Plagiarism: Bu makale, en az iki hakem tarafından incelendi ve intihal içermediği teyit edildi.
| This article has been reviewed by at least two referees and scanned via a plagiarism software.

AVRUPA BİRLİĞİ PERSPEKTİFİNDEN KAMUSAL ALANDA ÖZEL GÖZETİM VE VERİ KORUMA HUKUKU: RYNEŠ KARARI VE HANE İSTİSNASININ DÖNÜŞÜMÜ

Private Surveillance in Public Spaces and Data Protection Law from The European Union Perspective: The Ryneš judgment and The Transformation of The Household Exemption

Ali Mert Gürkan*

Öz

Düşük maliyetli ve yaygın biçimde erişilebilir hâle gelen gözetim teknolojileri, kamusal alanın görünürlüğünü ve denetlenme biçimlerini köklü şekilde dönüştürmüştür. Ev tipi Closed-Circuit-Television (CCTV) sistemleri, akıllı kapı zilleri, araç içi kameralar, drone'lar ve akıllı kent altyapılarında kullanılan sensörler, bireylerin kamusal ve yarı kamusal alanlarda sürekli olarak kayıt altına alınmasına imkân tanımaktadır. Bu gelişme, gözetimi yalnızca devlet tarafından yürütülen dikey bir kontrol mekanizması olmaktan çıkararak, özel kişilerin ve ticari aktörlerin de aktif rol oynadığı çok katmanlı bir yapıya dönüştürmüştür. Bu bağlamda, kamusal alanda mahremiyetin hukuki olarak korunup korunamayacağı sorusu veri koruma hukukunun temel tartışma alanlarından biri hâline gelmiştir.

Avrupa Birliği veri koruma rejimi, kişisel verilerin işlenmesine ilişkin kapsamlı bir çerçeve sunmakla birlikte, tamamen kişisel veya ev içi faaliyetler kapsamında gerçekleştirilen veri işleme faaliyetlerini uygulama alanı dışında bırakmaktadır. Başlangıçta düşük riskli ve kapalı faaliyetler için öngörülen bu hane istisnası, modern ev içi gözetim teknolojilerinin kamusal alanı da kapsamasıyla birlikte belirsizleşmiştir. Avrupa Birliği Adalet Divanı'nın Ryneš kararı, kamusal alanı görüntüleyen özel gözetim faaliyetlerinin istisna kapsamında değerlendirilemeyeceğini ortaya koymuştur. Ancak mekân merkezli bu yaklaşım, güncel ve hareketli gözetim teknolojileri karşısında yetersiz kalmaktadır. Makale, bağlamsal ve teknoloji-duyarlı bir yorumun hem AB hukuku hem de Türk hukuku bakımından zorunlu olduğunu savunmaktadır.

Anahtar Kelimeler Gözetim, Kamusal Alan, Veri Koruma, Avrupa Birliği Adalet Divanı, Rynes

* Bologna Üniversitesi Hukuk Fakültesi ve Lüksemburg Üniversitesi Bilgisayar Mühendisliği Fakültesi Doktora Araştırmacısı

Bu çalışma, Milli Eğitim Bakanlığı YLSY bursu tarafından desteklenmiştir.

0009-0003-5292-2875 gurkanalimert@gmail.com

ABSTRACT

The proliferation of low-cost and easily accessible surveillance technologies has profoundly altered the visibility and governance of public space. Devices such as home Closed-Circuit-Television (CCTV) systems, smart doorbells, dashcams, drones, and smart city sensors now enable continuous recording of individuals in public and semi-public environments. This shift has transformed surveillance from a predominantly state-centered, vertical practice into a diffuse and horizontal ecosystem in which private individuals and commercial actors increasingly participate. As a result, the legal question of whether and how privacy can be protected in public space has become a central challenge for contemporary data protection law.

Within the European Union, personal data processing is governed by Directive 95/46/EC and, subsequently, the GDPR. Both instruments exclude from their scope processing carried out in the course of a purely personal or household activity. Originally intended to shield low-risk, inward-facing practices such as family photo albums or private correspondence, this household exemption has become increasingly problematic as domestic surveillance technologies now routinely capture data extending into public space. The Court of Justice of the European Union addressed this tension in its landmark Ryneš judgment, holding that the monitoring of public space by a private CCTV system falls outside the household exemption. While this narrow, spatial interpretation strengthens fundamental rights protection, it struggles to accommodate mobile, automated, and data-intensive surveillance technologies. This article argues for a contextual and technology-sensitive reinterpretation of the household exemption, drawing on subsequent case law and extending the analysis to comparable provisions in Turkish data protection law.

Keywords Surveillance, Public Space, Data Protection, Court of Justice of the European Union, Rynes

GİRİŞ

Düşük maliyetli ve kullanıcı dostu gözetim araçlarının yaygınlaşması, günümüz toplumlarında görsel kayıt teknolojilerini gündelik yaşamın sıradan bir parçası hâline getirmiştir. Kapı zili kameraları, ev tipi Closed-Circuit-Television (CCTV) sistemleri, otomobil içi kayıt cihazları, drone kameraları ve akıllı kent altyapısına gömülü sensörler, bireylerin hem kamusal hem yarı-kamusal alanlarda sürekli olarak izlenebilir olmasına yol açmaktadır. Bu teknolojik dönüşüm, yalnızca devlet kurumlarının değil, giderek daha fazla oranda özel bireylerin ve şirketlerin de kamusal alanda görünürlüğü yönetebilmesini mümkün kılan geniş bir gözetim ekosistemi oluşturmuştur. Bu nedenle, mahremiyetin mekânsal olarak özel alanla sınırlı olmadığı; kamusal alanda dahi kişisel verinin toplanması, işlenmesi ve aktarılmasına ilişkin hukuki sınırların giderek daha fazla önem kazandığı bir döneme girilmiştir.

Avrupa Birliği hukuk düzeni, özellikle 1995 tarihli Veri Koruma Direktifi (95/46/EC) ve onu takip eden Genel Veri Koruma Tüzüğü (GDPR), kişisel verilerin işlenmesine ilişkin kapsamlı bir çerçeve sunar. Ancak bu çerçeve, başlangıçta özel kişilerin kişisel amaçlarla gerçekleştirdiği veri işleme faaliyetlerini, "tamamen kişisel veya ev içi faaliyet" istisnası kapsamında düzenleme dışına bırakmıştır. Bu istisnanın amacı, bireylerin aile albümü düzenlemek, arkadaşlarıyla fotoğraf paylaşmak veya ev içinde sınırlı güvenlik önlemleri almak gibi sıradan faaliyetlerinin veri koruma hukukuna tabi olmamasını sağlamaktır. Ne var ki, ev tipi kameraların teknik kapasitesi ile kamusal alanı kaydetme eğilimi arttıkça, bu istisnanın sınırları giderek daha tartışmalı hâle gelmiştir.

2014 tarihli C-212/13 Ryneš kararı, bu tartışmanın merkezinde yer alan dönüm noktası niteliğinde bir içtihattır.[1] Avrupa Birliği Adalet Divanı (ABAD), bu kararında evin dış cephesine yerleştirilen ve sokak ile komşu ev girişini kısmen izleyen bir CCTV sisteminin, tamamen kişisel veya ev içi faaliyet kapsamında değerlendirilemeyeceğine hükmetmiştir. Divan, kameranın kamusal alana yöneltilmiş olması nedeniyle işleme faaliyetinin kişisel kullanım sınırını aştığını ve veri koruma hukuku kapsamına girdiğini tespit etmiştir. Böylece karar, kişisel verinin mekânsal olarak nerede toplandığına ilişkin bir "alan temelli ölçüt" geliştirerek, AB veri koruma hukukunda istisnaların dar yorumlanması gerektiğini hem vurgulamış hem kurumsallaştırmıştır.

Bu içtihat, teknolojinin toplumsal gözetim yapılarını dönüştürdüğü bir dönemde, kamusal alan mahremiyetine ilişkin hukuki korumanın kapsamını güçlendirmesi bakımından geniş yankı uyandırmıştır. Kararın aynı zamanda AB Temel Haklar Şartı kapsamındaki özel hayatın korunması ve kişisel verilerin korunması haklarının etkili biçimde uygulanmasının gereği olarak görüldüğü de belirtilmelidir. Divan'ın yaklaşımı, verinin toplandığı yerin kamuya açık olup olmamasının, bireyin temel haklarını ortadan kaldırmadığı gerçeğine dayanır. Böylece Ryneš, kamusal alanın "mahremiyetsiz" bir alan olarak görülmesine karşı güçlü bir normatif pozisyon ortaya koymuştur.

[1] Case C-212/13 (Ryneš v Úřad pro ochranu osobních údajů) (The Court of Justice of the European Union (CJEU) 11 Aralık 2014), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62013CJ0212.

Bununla birlikte, hükmün getirdiği mekânsal kriter, gelişen teknolojik gözetim araçları karşısında bazı önemli sınırlamalar barındırmaktadır. Drone kameraları, giyilebilir kameralar, araç içi sensörler, yüz tanıma özellikli akıllı kapı zilleri ve geniş ölçekli nesnelerin interneti (IoT) ağlarının çoğu, sabit bir mekâna bağlı olmaksızın veri toplamaktadır. Bu dinamik sistemlerde kamu–özel alan ayrımının belirsizleşmesi, Ryneš kararının sunduğu katı mekânsal çerçevenin uygulanabilirliğini zorlaştırmaktadır. Ayrıca, modern gözetim pratikleri yalnızca görüntü toplamaktan ibaret değildir; konum verisi, davranış örüntüleri, sosyal ağ ilişkileri, hatta biyometrik özellikler çoğu zaman tek bir cihaz üzerinden otomatik olarak işlenmektedir. Bu nedenle, Avrupa Birliği'nin veri koruma rejimi, kamusal alanın içinde ve çevresinde konumlanan bu yeni tür gözetime karşı daha bütüncül, amaç ve bağlam temelli bir yorum gerektirmektedir.

Bu makalenin temel araştırma sorusu şu şekilde formüle edilebilir: *Ryneš kararı özel kişilerin gerçekleştirdiği gözetimi hukuken nasıl yeniden tanımlamakta ve bu yaklaşım yeni nesil gözetim teknolojileri karşısında ne derece yeterli kalmaktadır?* Buna ek olarak çalışma, kararın kamusal alanda mahremiyetin korunması, sorumluluk rejimi, özel aktörlerin veri işleme faaliyetlerinin niteliği ve kişisel verinin mekânsal sınırlar içinde korunması gibi konulara etkisini sistematik biçimde değerlendirmektedir.

Yöntem olarak çalışma, öncelikle Ryneš kararının dogmatik analizi üzerinden AB veri koruma hukukunda istisnaların yorumlanması, temel haklar yaklaşımı ve mekânsal kriterin ortaya çıkışı gibi meseleleri incelemektedir. Ardından çağdaş gözetim literatürü, smart city uygulamaları ve birey temelli gözetim araçlarına ilişkin disiplinlerarası kaynaklar kullanılarak kararın toplumsal bağlamı ortaya konulmaktadır. Çalışma, son olarak ABAD'ın TK C-708/18 kararında geliştirdiği daha esnek "meşru menfaat–orantılılık–gereklilik" testini analiz ederek, Ryneš sonrasında oluşan yeni hukuki yaklaşımı değerlendirmektedir.

Bu tartışma yalnızca Avrupa Birliği hukuku bakımından değil, Türk hukuku açısından da doğrudan önem taşımaktadır. Zira 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 28. maddesinde yer alan ve kişisel verilerin üçüncü kişilere aktarılmamak ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla, gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesini istisna kapsamına alan düzenleme, AB hukukundaki hane istisnası ile büyük ölçüde paralellik göstermektedir. Bu nedenle Ryneš ve devamındaki içtihatlar çerçevesinde yapılan analizler, KVKK m.28'in yorumlanması ve ev içi gözetim faaliyetlerinin Türk hukukundaki sınırlarının belirlenmesi bakımından da yol gösterici nitelik taşımaktadır.

Bu makale, kavramsal ve normatif bir çerçeve sunarak iki önemli katkıda bulunur. Birincisi, özel kişilerin kamusal alan gözetimine ilişkin hukuki sınırları, temel haklar ışığında yeniden tanımlar. İkincisi, mekânsal kriterin öngördüğü sınırlı yaklaşımın, hızla gelişen teknolojik gözetim yöntemleri karşısında revize edilmesi gerektiğini savunur ve bunu sağlayabilecek normatif ilkeler önerir.

I. GÖZETİM, KAMUSAL ALAN VE TEKNOLOJİK YOĞUNLAŞMA: KURAMSAL ARKA PLAN

Gözetim olgusu, modern toplumların örgütleniş biçimini belirleyen en temel yapısal unsurlardan biri hâline gelmiştir. Kamera teknolojilerinin ucuzlaması, veri depolama kapasitesinin artması, mobil cihazların neredeyse tüm yaşam alanlarına nüfuz etmesi ve kent altyapısının dijital ağlarla bütünleşmesi, gözetimi hem niceliksel hem niteliksel olarak dönüştürmektedir. Bu dönüşüm, sadece devlet kurumlarının uyguladığı klasik gözetim pratiklerini genişletmekle kalmayıp, özel sektörün ve bireylerin de kamusal alanda görünürlüğü yönetebilir aktörler hâline gelmesine imkân tanımaktadır. Gözetim, böylece tek bir merkezden gerçekleştirilen bir kontrol faaliyeti olmaktan çıkarak, çoklu aktörlerin katkı sunduğu, katmanlı, dağınık ve süreklileşmiş bir toplumsal düzenleme biçimine dönüşmektedir.

Bu bağlamda "gözetim toplumu" kavramı, Lyon'un ifade ettiği üzere, bireylerin günlük yaşam pratiklerinin kaçınılmaz biçimde veri üretimiyle iç içe geçtiği yeni bir yaşam formuna işaret eder.[2] Gözetim, artık yalnızca devletin suçla mücadele veya ulusal güvenlik gerekçeleriyle uyguladığı bir mekanizma değil; tüketici davranışlarını izleyen algoritmaların, alışveriş merkezlerini yöneten özel güvenlik şirketlerinin, sosyal medya platformlarının kullanıcıları kategorilere ayırma süreçlerinin ve hatta komşuların birbirini görüntülemesine imkân tanıyan ev tipi kameraların bütünsel bir bileşenidir. Ball, Haggerty ve Lyon'un belirttiği gibi modern gözetimin ayırt edici özelliği, kişisel verilerin toplanması, işlenmesi, sınıflandırılması ve ticari ya da yönetsel amaçlarla çeşitli kurumsal ağlar arasında dolaşıma sokulmasıdır.[3]

Özellikle veri işleme kapasitesindeki artış, gözetimin temel fonksiyonlarını genişletmiş ve onu "izleme" eyleminden çıkararak risk yönetimi, davranış tahmini ve profil oluşturma gibi yeni işlevlerle donatmıştır. Bu bağlamda gözetim, Giddens'ın tanımladığı modern devletin "idari rasyonalizasyon" süreçleriyle birleşmiş; halkın yönetimi, güvenliği ve ekonomik davranışlarının düzenlenmesi için zorunlu bir araç hâline gelmiştir.[4] Ancak modern gözetimin özgün yönü, yalnızca devletin bununla sınırlı olmaması; aynı zamanda büyük ölçüde ticarileşmiş olmasıdır. Turow'un çalışmalarının gösterdiği üzere, piyasa aktörleri artık tüketiciler hakkında birbirinden bağımsız veri noktalarını bir araya getirerek büyük ölçüde kişiselleştirilmiş gözetim rejimleri kurmakta, reklam, sigorta veya kredi gibi alanlarda bireylere farklı muamele edilmesine yol açmaktadır.[5] Bu süreç, Lyon'un "sosyal sınıflandırma" olarak adlandırdığı yapısal bir ayrım mekanizması üretmektedir.[6]

Bu çok katmanlı gözetim düzeninin bir diğer sonucu, Bentham'ın panoptikon modelinden farklı, "akışkan" ve çoğu zaman görünmez nitelikte bir izleme biçiminin ortaya çıkmasıdır.[7] Bauman ve Lyon'un "liquid surveillance" kavramsallaştırması, gözetimin artık

[2] David Lyon, *Surveillance society* (McGraw-Hill Education (UK), 2001).
[3] Kirstie Ball vd., *Routledge handbook of surveillance studies* (Routledge, 2012).
[4] Anthony Giddens, "The nation-state and violence", *Capital & Class* 10, sy 2 (1986): 216-20.
[5] Joseph Turow, "11 Cracking the Consumer Code: Advertisers, Anxiety, and Surveillance in the Digital Age", *The new politics of surveillance and visibility*, 2006, 279.
[6] David Lyon, *Surveillance after september 11*, c. 11 (Polity, 2003).
[7] Jeremy Bentham, *The panopticon writings* (Verso Books, 2020).

belirli bir mekâna veya merkezi otoriteye bağlı olmayan; ağlar üzerinden yayılan ve gündelik yaşam akışına nüfuz eden bir nitelik kazandığını vurgular.[8] Bu akışkanlık, özellikle kamusal alanda mahremiyetin korunmasını daha karmaşık hâle getirir. Çünkü bireyler kamusal alanda bulunurken, yalnızca devlet kameraları tarafından değil; alışveriş merkezlerinin, toplu taşıma araçlarının, özel binaların ya da sıradan bireylerin mobil telefonlarının kameraları tarafından da sürekli olarak görüntülenmektedir. Böylelikle kamusal alan, farklı aktörlerin birbirini izlediği ve görünürlüğün karşılıklı olarak dağıldığı bir "izleme matrisi"ne dönüşür.

A. Akıllı Kentsel Yapılar ve Bilgisel Mekânsallaşma

Gözetim toplumunun dönüşümünde, akıllı kent teknolojilerinin oynadığı rol kritik önemdedir. Firmino ve Duarte'nin kavramsallaştırdığı biçimiyle, akıllı kent (smart city) modelleri kenti yalnızca fiziksel bir yerleşim alanı olarak değil; sensörler, kameralar, yazılımlar ve veri akışlarıyla örülü bir "bilgisel mekân" olarak yeniden tanımlar.[9] Bu yaklaşımda bilgi ve iletişim teknolojileri (ICT), kent yönetiminin yan bileşeni olmaktan çıkıp, doğrudan kentin kurucu unsuru hâline gelir. Sokak lambalarına gömülü sensörlerden trafik yönetim sistemlerine, yüz tanıma tabanlı erişim noktalarından kent genelinde dağıtılmış Wi-Fi ağlarına kadar geniş bir teknoloji ekosistemi, kent içindeki hareketleri, davranış örüntülerini, araç trafiğini ve kalabalık dinamiklerini gerçek zamanlı olarak toplar ve işler.

Bu dijitalleşmiş çevre, kentsel mekânda üç tür egemenlik alanı yaratır: klasik sosyal–hukuki mekân; devlet ve özel sektörün kurduğu kodlanmış teknolojik mekân; ve bireylerin kendi cihazlarıyla oluşturduğu dağınık, görünmez mikro-mekânlar.[10] Bu mikro-mekânsallaşma, modern kentlerde mahremiyetin yalnızca devlet gözetimine karşı değil, birbirini denetleyen bireylere karşı da daha kırılgan hâle gelmesine yol açar. Örneğin sıradan bir apartman sakininin kapı önüne yerleştirdiği akıllı kapı zili, sokaktan geçen yüzlerce kişinin görüntüsünü işleyebilir; komşuların davranışlarını kayıt altına alabilir; hatta bu verileri bulut tabanlı platformlara aktarabilir. Böyle bir durumda veri işleme faaliyeti, bireyin kişisel güvenliği amacıyla başlamış olsa da kamusal alanın görünürlüğünü özel bir kişinin kontrolüne bırakır.

Bu noktada Ryneš kararının ortaya çıkardığı hukuki sorun açıkça görülür: eğer kişisel güvenlik amacıyla yapılan bir görüntü kaydı kamusal alana taşarsa, artık bu faaliyet "ev içi" olarak nitelendirilemez. Ancak modern akıllı kent pratiklerinde veri akışı zaten mekânsal sınırları aşacak biçimde tasarlandığından, Divan'ın mekân merkezli ölçütünün ne kadar sürdürülebilir olduğu tartışmalıdır. Kent genelinde konumlandırılmış kameralardan gelen görüntüler, özel güvenlik şirketlerinin sensörleriyle birleşmekte; yüz tanıma algoritmaları kamusal alan ile yarı-özel alanları ayırt etmeksizin işlemektedir. Böyle bir ortamda, kameraların tam olarak nerede bulunduğu veya hangi mekâna yöneldiği sorusu anlamını yitirmeye başlar.

[8] Zygmunt Bauman ve David Lyon, *Liquid surveillance: A conversation* (John Wiley & Sons, 2013).
[9] Rodrigo Firmino ve Fabio Duarte, "Private video monitoring of public spaces: The construction of new invisible territories", *Urban Studies* 53, sy 4 (2016): 741-54.
[10] Firmino ve Duarte, "Private video monitoring of public spaces: The construction of new invisible territories".

B. GÖZETİMİN ÖZELLEŞMESİ VE HİBRİD GÜVENLİK REJİMLERİ

Kamusal alan gözetiminin dönüşümünde bir diğer önemli eğilim, güvenlik işlevlerinin giderek özel aktörlere devredilmesidir. Wakefield'ın "mass private property" kavramı, büyük alışveriş merkezleri, plaza kompleksleri ve özel yönetilen kamusal alanların, geniş kapsamlı özel güvenlik rejimleri tarafından kontrol edildiğini açıkça göstermektedir.[11] Bu alanlarda özel güvenlik birimleri kamuya açık mekânın fiilî yöneticileri hâline gelmekte; davranış düzenlemeleri, erişim kontrolü ve görüntü kaydı gibi faaliyetlerde devletle benzer yetkiler kullanmaktadır. Dahası, çoğu durumda polis ile özel güvenlik şirketleri arasında veri paylaşımı gerçekleşmekte; özel kameralar devlet soruşturmalarında delil olarak kullanılmaktadır.[12] Böylece kamusal alanın yönetimi, devlet–özel sektör işbirliğine dayalı "melez" bir güvenlik modeline evrilmektedir.

Bireylerin gözetim faaliyetlerine aktif biçimde katılması ise bu melez yapıyı daha da genişletmektedir. Akıllı telefon kameraları, kısa süre içinde "vatandaş gözetimi"ni sıradanlaştırmış; kentsel olayların kaydı, paylaşımı ve raporlanması gündelik hayatın olağan pratiklerinden biri hâline gelmiştir. Koskela'nın "wikiveillance" olarak kavramsallaştırdığı bu süreç, vatandaşları fiilen polisin gözü ve kulağına dönüştürmekte; gözetimin toplumsal dağılımını artırmaktadır.[13] Böylece kamusal alan, yalnız devletin değil, özel güvenlik personelinin, ticari aktörlerin ve sıradan bireylerin birbirini gözetlediği yoğun bir veri üretim alanına dönüşmektedir.

Tüm bu dönüşümlere rağmen kamusal alan mahremiyeti ortadan kalkmış değildir. Mahremiyet hakkı mekânsal olmaktan ziyade bireysel bir haktır ve kişi, kamusal alanda dahi kimliğinin, hareketlerinin ve davranışlarının sürekli olarak izlenmemesini talep edebilir. Cavoukian'ın belirttiği gibi, kamusal alanda bulunmak ile sürekli takip edilmek arasındaki fark, modern mahremiyet hukukunun en kritik ayrımlarından biridir.[14] Bu nedenle, teknolojinin yarattığı sınırsız görünürlük kapasitesi, bireyin "gözetlenmeme" yönündeki makul beklentisini ortadan kaldırmak için yeterli değildir.

Ryneš kararı bu normatif pozisyonu güçlendirme yönünde bir adım olsa da, mekâna dayalı yaklaşımının teknolojik dönüşüm karşısında sınırlı kalabileceği açıktır. Bu nedenle sonraki bölümlerde, kararın hukuki mantığı ile modern gözetim yapılarını bir arada değerlendiren daha kapsamlı bir analiz sunulacaktır.

II. RYNEŠ KARARI: ARKA PLAN, HUKUKİ SORULAR VE MAHKEME ANALİZİ

Avrupa Birliği Adalet Divanı'nın (ABAD) 2014 tarihli *C-212/13 Ryneš kararı*, özel kişilerin güvenlik amaçlı video gözetimi ile AB veri koruma hukuku arasındaki ilişkinin

[11] Alison Wakefield, "The public surveillance functions of private security", *Surveillance & Society* 2, sy 4 (2004).
[12] Wakefield, "The public surveillance functions of private security".
[13] Hille Koskela, "Hijackers and humble servants: Individuals as camwitnesses in contemporary controlwork", *Theoretical Criminology* 15, sy 3 (2011): 269-82.
[14] Ann Cavoukian, *Surveillance, then and now: Securing privacy in public spaces* (Information and Privacy Commissioner of Ontario, Canada, 2013).

sınırlarını belirleyen dönüm noktası niteliğinde bir içtihattır.[15] Bu karar yalnızca ev tipi CCTV kullanımının hukuki niteliğini aydınlatmakla kalmamış, aynı zamanda kamusal alan gözetiminin temel haklarla ilişkisini yeniden tanımlamıştır. Dolayısıyla, veri koruma hukukunun kapsamı bakımından "ev içi faaliyet" istisnasının sınırlarını şekillendirmesi yönüyle hem pratik hem normatif sonuçlar doğurmuştur.

Davanının arka planında, Çekya'da ailesiyle birlikte yaşayan ve mülkü uzun bir süre boyunca tekrarlanan vandalizm saldırılarına maruz kalan Jaroslav Ryneš bulunmaktadır. Yaşanan bu saldırılar, hem maddi zarara yol açmış hem de Ryneš ve ailesi açısından ciddi bir güvenlik kaygısı yaratmıştır. Bu tehditleri önlemek ve olası failleri tespit edebilmek amacıyla Ryneš, konutunun giriş bölümüne sabit bir kapalı devre kamera sistemi yerleştirmiştir. Kurulan CCTV sistemi ses kaydı içermemekte, ancak görüntüleri sürekli ve otomatik biçimde kaydetmektedir. Kayıtlar, sınırlı bir süre boyunca döngüsel şekilde sabit bir depolama alanında muhafaza edilmektedir.

Kameranın görüş alanı yalnızca Ryneš'in mülküyle sınırlı kalmamış, aynı zamanda konutun önündeki sokağın bir bölümünü ve karşı komşunun giriş kapısını da kapsamıştır. Bu teknik konumlandırma, sistemin kamusal alanda bulunan kişilerin görüntülerini de kayıt altına almasına yol açmıştır. 2007 yılında gerçekleşen bir vandalizm olayında kamera kayıtları, saldırıyı gerçekleştiren kişilerin yüzlerinin açık ve seçilebilir biçimde tespit edilmesini sağlamıştır. Ryneš, bu kayıtları yetkili kolluk kuvvetleriyle paylaşarak soruşturmaya katkıda bulunmuştur.

Ancak söz konusu faillerden biri, görüntülerin hukuka aykırı şekilde elde edildiğini ileri sürerek şikâyette bulunmuştur. Bu şikâyet üzerine Çek Veri Koruma Otoritesi, Ryneš'in görüntü işleme faaliyetini incelemiş ve veri koruma mevzuatına aykırı davranıldığı sonucuna ulaşmıştır. Otoriteye göre Ryneš, kamusal alanda bulunan kişilerin kişisel verilerini açık rıza almaksızın işlemiş, ilgili kişileri görüntü kaydı yapıldığı konusunda bilgilendirmemiş ve ayrıca söz konusu veri işleme faaliyetini yetkili veri koruma makamına bildirmemiştir. Bu gerekçelerle Ryneš hakkında idari yaptırım uygulanmasına karar verilmiştir.

Ryneš, bu karara karşı yargı yoluna başvurmuş ve veri işleme faaliyetinin tamamen kişisel güvenlik amacı taşıdığını ileri sürerek hane istisnası kapsamında değerlendirilmesi gerektiğini savunmuştur. Uyuşmazlığı inceleyen ulusal mahkeme, meselenin Avrupa Birliği veri koruma hukukunun yorumuna ilişkin olduğunu tespit ederek, 95/46 sayılı Veri Koruma Direktifi'nde yer alan "tamamen kişisel veya ev içi faaliyet" istisnasının kapsamına ilişkin bir ön karar sorusunu Avrupa Birliği Adalet Divanı'na yöneltmiştir. Böylece kamusal alanı da görüntüleyen bir ev güvenlik kamerasının hane istisnası kapsamında değerlendirilip değerlendirilemeyeceği sorusu Divan'ın önüne taşınmıştır.

Davanın temel odak noktası, 95/46 sayılı Direktif'in 3(2) maddesinde yer alan istisnanın yorumudur. Bu istisna, kişisel verilerin "tamamen kişisel veya ev içi bir faaliyet" kapsamında işlenmesi hâlinde, Direktif hükümlerinin uygulanmayacağını düzenler. Direktif'in

[15] *Case C-212/13 (Ryneš v Úřad pro ochranu osobních údajů).*

orijinal hazırlık sürecinde bu istisna, aile albümleri, kişisel adres defterleri veya ev içinde sınırlı ölçekte yürütülen tamamen özel iletişim gibi gündelik faaliyetleri korumayı amaçlamaktadır.[16]

Ancak temel sorun şudur: modern video gözetimi, ev güvenliği amacıyla başlasa bile, kamusal alanın görüntülenmesi durumunda başka kişilerin verilerini de işler. Bu kişilerin evle ilişkisi yoktur ve kayıt faaliyeti onların bilgisi dahilinde değildir. Dolayısıyla istisnanın kapsamı, teknik kapasitenin genişlemesiyle birlikte belirsizleşmiştir.

ABAD'nın bu konuda vereceği karar, yalnızca özel kameraların değil; drone'ların, araç içi kameraların, komşu kapı kameralarının ve hatta giyilebilir kayıt cihazlarının hukuki niteliğini etkileyebilecek geniş kapsamlı sonuçlar doğuracaktır.

A. Mahkemenin Kişisel Veri ve İşleme Tanımı

Mahkeme, Ryneš kararında öncelikle kamera tarafından kaydedilen görüntülerin kişisel veri niteliği taşıyıp taşımadığını değerlendirmiştir. Divan'a göre bir kişinin yüzünün, fiziksel görünümünün, yürüyüş biçiminin veya başka ayırt edici özelliklerinin görüntü üzerinden tanımlanabilir olması, bu görüntülerin kişisel veri olarak kabul edilmesi için yeterlidir.[17] Bu değerlendirmede belirleyici olan unsur, görüntünün kime ait olduğu veya hangi amaçla kaydedildiği değil, teknik olarak belirli ya da belirlenebilir bir kişiyi tanımlama kapasitesidir. Bu nedenle ev tipi kameralarla elde edilen görüntüler, içerdikleri potansiyel tanımlanabilirlik nedeniyle veri koruma hukukunun maddi kapsamı içine girmektedir.

Mahkeme ayrıca bu görüntülerin sürekli biçimde kaydedilmesi ve depolanmasının, 95/46 sayılı Direktif'in 2(b) maddesinde tanımlanan otomatik veri işleme faaliyetini oluşturduğunu tespit etmiştir. Görüntülerin insan müdahalesi olmaksızın kaydedilmesi, saklanması ve gerektiğinde erişilebilir hâle gelmesi, işleme faaliyetinin otomatik nitelik taşıdığını göstermektedir. Bu çerçevede ev güvenliği amacıyla kullanılan bir CCTV sistemi dahi hukuken veri işleme faaliyeti olarak değerlendirilmiştir.

Bu tespit, modern gözetim teknolojileri açısından önemli bir ilkeyi ortaya koymaktadır. Bir görüntü kaydının kişisel veri sayılabilmesi için kayıt sahibinin niyeti, amacı veya iyi niyeti değil; kaydın teknik olarak bir kişiyi tanımlayabilir nitelikte olup olmadığı esas alınmaktadır. Böylece Mahkeme, öznel amaçlardan bağımsız, nesnel ve teknoloji temelli bir veri tanımı benimsemiştir.

B. Ev İçi Faaliyet İstisnasının Dar Yorumlanması

Mahkemenin Ryneš kararındaki en kritik yönlerinden biri, ev içi faaliyet istisnasını son derece dar bir biçimde yorumlamasıdır. Divan, 95/46 sayılı Veri Koruma Direktifi'nde yer alan "tamamen kişisel veya ev içi faaliyet" ifadesindeki "tamamen" vurgusunun, istisnanın yalnızca istisnai ve sıkı biçimde sınırlandırılmış durumlar için geçerli olabileceğini açıkça ortaya koyduğunu belirtmiştir. Bu yaklaşım, ev içi faaliyet istisnasının genişletilmesinin veri koruma hukukunun temel amaçlarıyla bağdaşmayacağı yönünde normatif bir tutum içermektedir.

[16] Hielke Hijmans, "On Private Persons Monitoring the Public Space", *Eur. Data Prot. L. Rev.* 1 (2015): 149.
[17] *Case C-212/13 (Ryneš v Úřad pro ochranu osobních údajů)*.

Mahkeme'ye göre, istisnaların geniş yorumlanması kişisel verilerin korunmasına ilişkin temel hakkın içeriğini zayıflatma ve uygulamada etkisiz hâle getirme riski taşımaktadır.

Bu çerçevede Mahkeme, ev içi faaliyet kavramını yorumlarken kamusal alan ile özel alan arasındaki ayrımı belirleyici bir ölçüt olarak ele almıştır. Divan'a göre bir izleme faaliyetinin görüş alanı, ev sınırlarını aşarak kamusal alana yönelmişse, bu faaliyet artık "tamamen kişisel" veya "ev içi" olarak nitelendirilemez. Kamusal alanda bulunan bireylerin, izleme faaliyetini gerçekleştiren kişiyle herhangi bir kişisel ilişkilerinin bulunmaması, bu kişilerin verilerinin ev içi faaliyet istisnası kapsamında değerlendirilmesini hukuken imkânsız kılmaktadır. Bu nedenle Mahkeme, kamusal alanı kapsayan her türlü görüntü kaydının veri koruma hukukunun uygulama alanına girdiğini kabul etmiştir.

Bu yaklaşım, kararın mekânsal bir ölçüte dayandığını açıkça göstermektedir. Mahkeme, veri işleme faaliyetinin amacıyla ilgilenmekten özellikle kaçınmış; ev güvenliği gibi meşru ve haklı gerekçelerin dahi tek başına istisna uygulanması için yeterli olmadığını ortaya koymuştur. Dolayısıyla karar, amaç temelli bir değerlendirme yerine, verinin toplandığı alanın niteliğini esas alan katı bir mekânsal analiz benimsemiştir. Bu durum, ev içi faaliyet istisnasının yalnızca kapalı ve tamamen özel alanlarla sınırlı tutulması gerektiği yönündeki yorumu pekiştirmektedir.

Mahkeme'nin değerlendirme mantığı, bu mekânsal yaklaşımı üç aşamalı bir analiz çerçevesi üzerinden inşa etmektedir. Öncelikle kamera kayıtlarının kişisel veri niteliği taşıdığı kabul edilmiştir. Bir görüntünün kişisel veri sayılabilmesi için yalnızca olay faillerini değil, yoldan geçen herhangi bir kişiyi tanımlayabilir olması yeterlidir. Ardından, bu görüntülerin sürekli olarak kaydedilmesi ve depolanması otomatik veri işleme faaliyeti olarak değerlendirilmiştir. Son aşamada ise kamusal alanın kayıt kapsamına girmesi, ev içi faaliyet istisnasının tamamen ortadan kalkmasına yol açmıştır. Böylece Mahkeme, kamusal alanda bulunan bireylerin varlığını, istisnanın uygulanamayacağının kesin göstergesi olarak kabul etmiştir.

Kararın bu yönü, özellikle akıllı ev sistemleri ve kapı zili kameraları (örneğin Ring, Google Nest) bağlamında büyük önem taşır. Bu sistemler çoğu zaman hem özel mülkün önünü hem de kaldırımın bir bölümünü görüntüler. Ryneš sonrası AB üyesi ülkelerde bu sistemlerin önemli kısmı veri koruma otoriteleri tarafından düzenlemeye tabi tutulmuştur.

Mahkeme, kararını yalnızca Direktif metnine değil, aynı zamanda *AB Temel Haklar Şartı'nın 7. (özel hayatın korunması) ve 8. (kişisel verilerin korunması) maddelerine* dayandırmıştır.[18] Böylece şu ilkeyi ortaya koyar: *Özel kişilerin yaptığı gözetim dahi, başkalarının temel haklarını ihlal edemez.*

Bu yaklaşım, veri koruma hukukunu, yalnızca devlet müdahalelerine karşı koruyan bir mekanizma olmaktan çıkarıp, özel kişiler arasındaki ilişkileri de düzenleyen yatay bir hak alanı

[18] Bart van de Sloot, "Home is where the heart is: the household exemption in the 21st century", *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 14 (2023): 34.

hâline getirmiştir. Özellikle komşuluk ilişkileri, apartman içi kameralar, konut site yönetimlerinin kamera uygulamaları gibi durumlarda bu yatay koruma büyük önem taşır.

C. MEKÂNSAL ÖLÇÜTÜN DOĞURDUĞU SORUNLAR

Her ne kadar Ryneš kararı ev içi faaliyet istisnasının sınırlarını belirleme bakımından açık ve öngörülebilir bir çerçeve sunmuş olsa da, benimsenen mekânsal ölçüt modern gözetim teknolojileri karşısında ciddi uygulama sorunları doğurmaktadır. Güncel gözetim araçlarının büyük bir bölümü sabit ve sınırlı bir mekânsal kapsama sahip değildir. Örneğin drone kameraları, kısa süreler içerisinde özel mülk sınırlarından çıkarak kamusal alanları görüntüleyebilmekte; bu geçiş çoğu zaman kullanıcının bilinçli bir yönlendirmesi olmaksızın gerçekleşmektedir. Benzer şekilde giyilebilir kameralar, kullanıcı hareketlerine bağlı olarak sürekli değişen bir görüş alanı yaratmakta ve verinin nerede toplandığını hukuken belirlemeyi güçleştirmektedir.

Akıllı kapı zili kameraları ve ev tipi güvenlik sistemleri de geniş açılı lensleri nedeniyle teknik olarak kamusal alanı görüntülemekten kaçınamamaktadır. Bu tür cihazlar, ev güvenliği amacıyla kurulmuş olsalar dahi kaldırım, sokak veya komşu mülklerin girişlerini kayıt altına alabilmektedir. Araç içi kameralar ise doğaları gereği kamusal alanda sürekli veri işleyen sistemlerdir ve yol üzerindeki tüm kişilerin görüntülerini otomatik olarak kaydetmektedir. Bu teknolojilerin ortak özelliği, kamusal alanı kaçınılmaz biçimde kapsayan bir veri işleme pratiği üretmeleridir.

Bu durum, Ryneš kararının pratik sonucunu daha da ağırlaştırmaktadır. Karar, sıradan bireyleri dahi fiilen veri sorumlusu konumuna getirerek kapsamlı hukuki yükümlülüklerle karşı karşıya bırakmaktadır. Bu nedenle kararın sonraki içtihatlarda nasıl yorumlandığı ve geliştirildiği, ev içi faaliyet istisnasının geleceği açısından belirleyici öneme sahiptir. Bir sonraki bölüm, bu içtihadı daha geniş ve bağlamsal bir normatif çerçeve içerisinde ele alacaktır.

III. VERİ KORUMA HUKUKUNDA HANE İSTİSNASININ YORUMU VE UYGULAMA SORUNLARI

Hane istisnası, Avrupa Birliği veri koruma hukukunun tartışmalı kavramlarından biri olmaya devam etmektedir. Özellikle Ryneš kararının ardından, bu istisnanın kapsamı, dayandığı normatif mantık ve modern gözetim teknolojileri karşısındaki işlevi yeniden değerlendirilmek zorunda kalmıştır. Kararın ortaya koyduğu çerçeve, ev içi faaliyetlerin yalnızca tamamen özel nitelikteki işlemleri kapsadığını, kamusal alanın en küçük bir bölümünü dahi kayıt altına alan faaliyetlerin veri koruma hukukunun uygulanabilirliğinden muaf tutulamayacağını açık biçimde ortaya koymuştur.[19] Bu yaklaşım, bireylerin ev güvenliği amacıyla kullandığı sıradan kamera sistemlerinin dahi hukuken veri sorumluluğu doğurabileceği anlamına geldiğinden, hem teorik hem pratik açıdan geniş sonuçlar yaratmaktadır. Hane istisnasının içeriği, yalnızca bu kararın dar yorumuyla değil, aynı zamanda

[19] Zuzanna Warso, "There's more to it than data protection–Fundamental rights, privacy and the personal/household exemption in the digital age", *Computer Law & Security Review* 29, sy 5 (2013): 491-500.

çağdaş teknolojiler, bireysel gözetim pratikleri ve özel yaşamın dönüşen anlamı bağlamında da yeniden tartışılmalıdır.

Ryneš, hane istisnasını yalnızca tamamen mahremiyet alanına ilişkin faaliyetlerle sınırlı tutarak temel hakların korunmasını önceleyen bir yaklaşımı benimsemiştir. Bu yaklaşım, Temel Haklar Şartı'nın 7. ve 8. maddelerinin herkesin mahremiyet ve kişisel veri koruma hakkını güvence altına alan hükümleriyle uyumludur.[20] Ancak yakın tarihli değerlendirmeler, hane istisnasının tarihsel olarak yalnızca belirli, sınırlı ve teknolojik olarak ilkel faaliyetler için tasarlanmış olduğunu ortaya koymaktadır. Van der Sloot'a göre, istisnanın hukuki gerekçesi modern dijital yaşamın dinamik ve geçirgen doğasına karşı yetersizdir; çünkü modern hane artık yalnızca "kapalı ve içe dönük" bir alan olmaktan çıkmış, çevrimiçi yaşamın ve dijital temasların yoğunlaştığı bir merkez hâline gelmiştir.[21]

Bu bağlamda hane istisnasının klasik yorumu, modern hanelerin farklı aktörlerle kurduğu veri alışverişi ilişkilerini görmezden gelir. Örneğin akıllı kapı zili kameraları, sensör tabanlı ev otomasyon sistemleri, mobil uygulamalar üzerinden yönetilen güvenlik cihazları ve bulut tabanlı video saklama teknolojileri, ev içi faaliyetlerin dışarıdan bağımsız olmadığını gösteren yapılardır. Bu teknolojilerin tamamı, veriyi çoğu zaman yurt dışındaki şirketlere aktarır. Bu nedenle hane istisnasını yalnızca mekâna ve kullanıcı niyetine bağlı olarak belirlemeye çalışmak, güncel verinin dolaşım biçimlerini hesaba katmayan sınırlı bir değerlendirme sonucunu doğurur.[22]

Ryneš kararında benimsenen mekânsal yaklaşım, kameranın kamusal alanı görüntülediği her durumda hane istisnasının uygulanamayacağını söyler. Ancak mekânsal ölçüt günümüz teknolojileri açısından hem yapısal hem kavramsal bir yetersizlik taşır. Ev içi kameraların büyük çoğunluğu, teknik özellikleri gereği, evin girişini izlerken aynı zamanda komşu kapıyı veya karşı kaldırımın bir kısmını görüntüler. Mekânın bu tür bir geçirgenliği, hane istisnasını mekânsal konumlanmaya bağlamayı sorunlu hâle getirir.[23]

Sabit kameralar açısından dahi geçerli olmayan bu kural, drone kameraları, araç içi kameralar veya giyilebilir kameralar gibi hareketli teknolojiler karşısında tamamen işlevsizleşmektedir. Bu teknolojilerde görüntünün nerede alındığını belirlemek çoğu zaman mümkün değildir. Hareketli cihazların sürekli değişen bir mekânsal bağlamda veri üretmesi, sabit bir istisna tanımını anlamsızlaştırır. Bu nedenle Ryneš'in mekâna dayalı katı testi, teknolojinin evrimsel hızına ayak uyduramayan bir içtihat olarak değerlendirilmektedir. Nissenbaum'un bağlamsal bütünlük yaklaşımı, veri pratiklerinin mekânsal değil, bağlamsal ve normatif beklentiler çerçevesinde değerlendirilmesi gerektiğini savunur. Bu yaklaşım, Ryneš kararının mekân merkezli modeline yapılan teorik eleştirilerden biridir.[24]

[20] Orla Lynskey, *The foundations of EU data protection law* (Oxford University Press, 2015).
[21] van de Sloot, "Home is where the heart is: the household exemption in the 21st century".
[22] Hielke Hijmans, "The European Union as guardian of internet privacy", *The Story of Art* 16 (2016).
[23] van de Sloot, "Home is where the heart is: the household exemption in the 21st century".
[24] Helen Nissenbaum, "Privacy in context: Technology, policy, and the integrity of social life", içinde *Privacy in context* (Stanford University Press, 2009).

Hane istisnasının dar yorumu, sıradan bireylerin hukuki yükümlülüklerle karşı karşıya kalmasına yol açar. Ev girişine kamera koyan herhangi bir kişinin veri sorumlusu olarak bilgilendirme yükümlülüğü, saklama süresi belirleme zorunluluğu, veri güvenliği tedbirleri geliştirme yükümlülüğü ve olası hak kullanım taleplerine yanıt verme gibi sorumlulukları yerine getirmesi beklenir. Ancak bu yükümlülükler, vatandaşların teknik bilgi düzeyleriyle uyumlu değildir ve geniş bir uyumsuzluk pratiği ortaya çıkarmaktadır. Bu uyumsuzluk, ulusal veri koruma otoritelerinin yükünü de artıracağından; kamusal otoriteler, komşuluk ilişkilerinden doğan şikâyetlerle aşırı meşgul hâle gelme durumu söz konusu olacaktır.

Bu açıdan bakıldığında, hane istisnasının hem "çok dar" hem de "çok geniş" bir risk doğurduğu görülür. İstisna çok dar yorumlandığında sıradan ev kullanıcılarının üzerinde ağır bir hukuki yük oluşurken, çok geniş yorumlandığında özel aktörlerin kamusal görünürlüğü kontrol etmesine olanak tanır. Her iki durum da temel haklar açısından sorunludur. Bu nedenle, hane istisnasının kapsamının yeniden tanımlanması gerektiği, özellikle ev içi teknolojilerin ticari şirketlerle olan veri akışlarının istisna kapsamından çıkarılması gerektiği ileri sürülmektedir.[25]

IV. YENİ TEKNOLOJİLER, AKILLI KENTLER VE ÖZEL GÖZETİM ÇÖZÜMLERİ KARŞISINDA HANE İSTİSNASININ UYGULANABİLİRLİĞİ

Hane istisnası, başlangıçta düşük teknolojili, yerel ve mekânsal olarak sınırlı veri işleme faaliyetlerini düzenleme dışı bırakmayı amaçlayan son derece dar bir hukuki kavram olarak ortaya çıkmıştır. Ancak teknolojinin hızlı evrimi ve dijital ağların toplumsal yaşam üzerindeki etkisinin genişlemesi, istisnanın uygulanabilirliğini temelden sarsmıştır. Bu nedenle, modern gözetim teknolojilerinin, akıllı kent altyapılarının ve ticari özel gözetim çözümlerinin hane istisnası üzerindeki etkisini tartışmaya açılmalıdır.

Ev içi faaliyetleri düzenlemenin hukuken kolay olduğu dönemlerde veri işleme büyük ölçüde pasif ve sınırlı nitelikteydi. Günümüzde ise haneler, sensör tabanlı teknolojilerin, bulut hizmetlerinin, kameraların, IoT cihazlarının ve algoritmik analiz tekniklerinin sürekli veri üretmesiyle birlikte mikro veri merkezlerine dönüşmüştür. Bu dönüşüm, ev içi ile ev dışı arasındaki sınırın hem teknik hem işlevsel olarak çözüldüğünü göstermektedir. Van der Sloot'un belirttiği gibi modern hane artık içe dönük kapalı bir alan değil, dijital dünyaya sürekli bağlı ve dış aktörlerle veri alışverişi içinde olan bir platformdur.[26] Bu nedenle, hane istisnasının mekânsal unsurlara dayanan klasik çerçevesi, teknolojinin yeni yapısal özellikleriyle bağdaşmamaktadır.

Akıllı kapı zili kameraları bunun belirgin örneklerinden biridir. Bu cihazlar, yalnızca ev girişini değil, karşı kaldırımın bir bölümünü ve komşu mülklerin girişlerini de görüntülemektedir. Geniş açılı lensler sebebiyle bu kameraların görüş alanını sadece özel mülkle sınırlamak teknik olarak neredeyse imkânsızdır. Bu durum Ryneš kararının mekânsal

[25] van de Sloot, "Home is where the heart is: the household exemption in the 21st century".
[26] van de Sloot, "Home is where the heart is: the household exemption in the 21st century".

mantığını zayıflatmaktadır; çünkü kameranın küçük bir miktar kamusal alanı görüntülemesi dahi işleme faaliyetinin hane istisnası kapsamı dışında kalmasına yol açar.

A. Akıllı Kent Ekosistemlerinde Hane Kavramının İşlevsizleşmesi

Akıllı kentler, kent yaşamını optimize etmek amacıyla sensörler, kameralar, kablosuz ağlar, veri analitiği sistemleri ve gerçek zamanlı izleme araçlarıyla donatılmış altyapılardır. Böyle bir ortamda gözetim yalnızca dikey bir devlet pratiği ya da yatay bir bireysel faaliyet olmaktan çıkıp, çok aktörlü ve ağ tabanlı bir niteliğe bürünmektedir. Bu bağlamda hane istisnası, mekâna dayalı bir analiz modeli sunması nedeniyle akıllı kentlerde veri işleme faaliyetlerinin karmaşık yapısını açıklamak için yetersiz kalır. Hijmans'ın belirttiği gibi veri akışlarının sınırlarının mekânsal değil topolojik olduğu ortamlarda kişisel verilerin korunması için klasik mekânsal ayrımlar işlevsizleşir.[27]

Akıllı kentlerde bireyler yalnızca kamusal alan kameralarıyla değil, diğer bireylerin kameraları, araç içi kayıt sistemleri, drone'lar, yüz tanıma algoritmaları ve hatta giyilebilir cihazlarla kayıt altına alınmaktadır. Bu nedenle özel gözetim ile kamusal gözetim arasındaki sınır silikleşmiştir. Hane istisnası ise bu karmaşık ilişkiler arasında yalnızca ev merkezli bir değerlendirme sunmakta, oysa veri akışları artık ev merkezli değildir. Modern veri ekosistemi, haneleri sistematik gözetim ilişkilerine bağlamakta ve istisnayı hukuki açıdan tarihsel bir anomali hâline getirmektedir.[28]

Ryneš kararının mekânsal yaklaşımı sabit bir kameranın sınırları için tasarlanmıştır. Ancak drone teknolojisi, araç içi kameralar ve giyilebilir cihazlar gibi hareketli sistemler bu yaklaşımı tamamen geçersiz kılmaktadır. Drone kameraları birkaç saniye içinde özel alandan kamusal alana geçebilir; araç içi kameralar şehir boyunca sürekli veri işleyebilir; giyilebilir kameralar ise kişinin yürüdüğü her mekânda görüntü kaydeder. Bu teknolojilerde veri akışı, mekânın sabit bir noktasına bağlı değildir. Dolayısıyla hane istisnası açısından "ev içi" ya da "ev dışı" ayrımını yapmanın hukuken anlamı kalmamaktadır. Nissenbaum'un "bağlamsal bütünlük" yaklaşımı, haklı bir şekilde böyle bir ortamda mekânı birincil kriter olarak almanın mahremiyetin gerçek risklerini ortaya koyamayacağını vurgular.[29]

B. Özel Gözetim Çözümlerinin Ticarileşmesi ve Hane İstisnasının Geçersizleşmesi

Özel gözetim araçlarının ticarileşmesi, hane istisnasının bugün neden işlevsizleştiğini gösteren en kritik unsurlardan biridir. Akıllı kapı kameraları, bulut tabanlı depolama, yüz tanıma modülleri ve uzaktan erişim hizmetleri sunan şirketler, ev içi verilerin büyük bir kısmına erişim sağlamaktadır. Bu durum işleme faaliyetinin artık yalnızca ev sahibi tarafından gerçekleştirilmediğini, dolayısıyla hane istisnasının temel gerekçesini yitirdiğini gösterir. Bu kapsamda ticari hizmet sağlayıcıların veri zincirine dahil olduğu her durumda hane istisnasının

[27] Hijmans, "The European Union as guardian of internet privacy".
[28] van de Sloot, "Home is where the heart is: the household exemption in the 21st century".
[29] Nissenbaum, "Privacy in context: Technology, policy, and the integrity of social life".

ortadan kalkması gerektiğini savunulabilir; çünkü veri artık evde kalmamakta, platform ekonomisi aracılığıyla dolaşıma girmektedir.[30]

Bu perspektif, ev içi cihazların dış aktörlerle kurduğu veri ilişkilerini görmezden gelen Ryneš yaklaşımının neden dar bir çerçeve sunduğunu da açıklamaktadır. Ev içerisindeki cihazların bulut hizmetlerine bağlı olduğu günümüz koşullarında veri işleme faaliyetinin hanelerle sınırlı olduğunu varsaymak gerçekçi değildir.

Ryneš kararı veri koruma hukukunun gelişimi açısından önemli olsa da modern teknolojilerin sunduğu karmaşık veri akışlarına çözüm üretmek için yetersizdir. Avrupa Birliği Adalet Divanı'nın TK kararında[31] benimsediği daha esnek yaklaşım, hane istisnasının amaç, araç, işleme yoğunluğu ve orantılılık ilkeleri üzerinden değerlendirilmesi gerektiğini göstermiştir. Bu bakımdan hane istisnasının modern biçimi, yalnızca mekânsal sınırları değil, aynı zamanda işleme faaliyetinin toplumsal bağlamını da dikkate alan karma bir test gerektirmektedir.

V. TK KARARI VE RYNEŠ SONRASI YORUMUN EVRİMİ

Ryneš kararının ortaya koyduğu mekânsal odaklı ve katı yaklaşım, Avrupa Birliği Adalet Divanı'nın veri koruma hukukunun temel ilkelerini yeniden şekillendirdiği önemli bir aşamayı temsil etmektedir. Ancak bu yaklaşımın teknolojik gelişmeler, modern gözetim ekosistemleri ve ev içi veri akışlarının ticarileşmesi karşısında sınırlı bir işlevselliğe sahip olduğu zaman içinde daha belirgin hâle gelmiştir. Bu bağlamda TK kararı[32], Ryneš sonrası ortaya çıkan en önemli içtihadi dönüşüm olarak görülmektedir. TK kararı sadece hane istisnasının sınırlarını yeniden tanımlamakla kalmamış, Avrupa Birliği veri koruma hukukunda daha bağlamsal, amaç odaklı ve orantılılık merkezli bir yorumun kapısını aralamıştır. Bölümün devamı, TK kararının Ryneš ile karşılaştırmalı analizini yaparak istisnanın evrilen niteliğini ve geleceğe yönelik normatif yönelimleri tartışmaktadır.

Ryneš kararında kamera görüş alanının kamusal alana taşması, işleme faaliyetinin ev içi faaliyet sayılmasını engelleyen tek belirleyici unsurdu.[33] Bu nedenle karar büyük ölçüde kamusal alan–özel alan ayrımına dayanıyordu. Ancak verinin üretildiği yer ile verinin işlendiği, saklandığı, paylaşıldığı veya analiz edildiği yer arasındaki bağ günümüzde neredeyse tamamen kopmuştur. Van der Sloot, hane istisnasının mekânsal temelli yorumunun artık dijital çağın ihtiyaçlarına uygun olmadığını, çünkü modern veri ekosisteminin ev ile dış dünya arasındaki sınırı işlevsiz hâle getirdiğini vurgular.[34]

TK davasında Divan'ın önüne gelen sorun, bir apartmanda yer alan ortak alanların görüntülenmesine ilişkin toplu bir kamera sisteminin veri koruma hukukuna uygunluğuydu. TK kararı, Ryneš'in aksine yalnızca kameranın kamusal alanı görüp görmediğine bakmamış;

[30] van de Sloot, "Home is where the heart is: the household exemption in the 21st century".
[31] Case C-708/18 (TK v Asociația de Proprietari) (The Court of Justice of the European Union (CJEU) 11 Aralık 2019), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62018CJ0708.
[32] *Case C-708/18 (TK v Asociația de Proprietari)*.
[33] van de Sloot, "Home is where the heart is: the household exemption in the 21st century".
[34] van de Sloot, "Home is where the heart is: the household exemption in the 21st century".

işleme faaliyetinin amacını, gerekliliğini ve orantılılığını dikkate almıştır. Bu yaklaşım, kameranın apartmanda zorunlu güvenlik ihtiyacına dayalı olarak konumlandırılabileceğini, bunun meşru bir menfaat oluşturabileceğini ve işleme faaliyetinin bu amaçla sınırlı olduğu sürece hukuken kabul edilebilir olabileceğini ortaya koymuştur.[35] Bu yorum, veri koruma hukukunun statik mekân sınırlarına bağlı olmaktan çıkarak işleme faaliyetinin bütünsel analizine yöneldiğini göstermektedir.

TK kararında Divan, işleme faaliyeti ile ilgili kişilerin mahremiyeti arasında bir denge kurulması gerektiğini kabul ederek meşru menfaat testinin önemini vurgulamıştır. Bu testin üç aşamalı olması, veri sorumlularının işleme faaliyetini gerekçelendirmek için yalnızca amaç beyanında bulunmakla yetinmemesini gerektirir. Amaç meşru olmalı, işleme bu amaç için gerekli olmalı ve işleme faaliyetinin ilgili kişilerin mahremiyetine verdiği zarar ile veri sorumlusunun menfaati arasında makul bir denge bulunmalıdır. Bu yaklaşım, Ryneš'in mekânsal belirleyiciliğine kıyasla çok daha esnek bir değerlendirme modeli sunar. Bu gelişme, özellikle hane istisnası açısından önemlidir. Çünkü evlerde kullanılan akıllı kameralar veya IoT tabanlı güvenlik sistemleri çoğu zaman haklı bir güvenlik ihtiyacına dayanır. Ancak Ryneš'in katı yaklaşımı, küçük bir miktar kamusal alanın görüntülenmesi nedeniyle bu faaliyetleri tamamen veri koruma hukukuna tabi kılmaktadır. TK kararı ise bu alanı genişletmekte; her işleme faaliyetini otomatik olarak hukuka aykırı saymak yerine orantılılık ilkesine göre incelemeye yöneltmektedir.[36]

TK kararını hane istisnası tartışmaları bağlamında önemli bir dönemeç olarak değerlendirilmektedir. TK, Ryneš'in hane istisnasını gereğinden fazla daraltan ve sıradan bireyleri ağır yükümlülüklerle karşı karşıya bırakan anlayışını hafifletmiştir. TK'nın getirdiği bağlamsal yaklaşım, istisnanın yeniden dengelenmesini mümkün kılar; çünkü bu yaklaşım yalnızca kameranın neyi görüntülediğiyle değil, hangi bağlamda, hangi amaçla ve hangi yoğunlukta veri işlediğiyle ilgilidir.[37] Böylece hane istisnası yalnızca mekânsal kriterlere değil, işleme faaliyetinin toplumsal niteliğine de duyarlı hâle gelir. Bu çerçevede TK kararı, özellikle apartman ve site gibi yarı kamusal alanlarda kullanılan güvenlik kameralarının hukuki statüsünü daha öngörülebilir ve daha gerçekçi biçimde belirlemeye olanak tanır. Ryneš'in yaklaşımı bu alanlarda yaşayan bireyleri teknik olarak veri sorumlusu konumuna getirirken, TK bu yükü daha kolektif bir anlayışla değerlendirir. Bu nedenle TK kararını hane istisnasının çağdaş yorumu için bir "dönüşüm modeli" olarak görülebilir.

TK kararı, hane istisnasının gelecekte nasıl yorumlanması gerektiğine ilişkin normatif bir çerçeve sunmaktadır. Bu çerçeve, mekân merkezli bir değerlendirmenin yetersiz kaldığı durumlarda amaç, bağlam ve orantılılık analizini öne çıkarır. Bu yaklaşım Nissenbaum'un bağlamsal bütünlük teorisi ile de uyum içindedir. Çünkü Nissenbaum'a göre mahremiyet ihlali, verinin nerede toplandığına değil, hangi bağlamda nasıl aktığına göre belirlenmelidir.[38] TK'nın da benimsediği sonuç budur. Ev içi veya ev dışı ayrımı, teknolojinin doğrudan

[35] Hijmans, "On Private Persons Monitoring the Public Space".
[36] Lynskey, *The foundations of EU data protection law*.
[37] van de Sloot, "Home is where the heart is: the household exemption in the 21st century".
[38] Nissenbaum, "Privacy in context: Technology, policy, and the integrity of social life".

gözlemlenebilir sınırlarını yansıtmaz; bu nedenle hukuki analiz veri akışının bağlamına odaklanmalıdır.

Bu normatif köprü, özellikle akıllı kent ortamları, bulut hizmetleri ve platform tabanlı gözetim çözümleri karşısında önem kazanmaktadır. Modern veri işleme süreçlerinde verinin ev içi olması, onun ticari aktörlerle paylaşılmadığı anlamına gelmez. Dolayısıyla TK'nın sunduğu daha esnek çerçeve, hane istisnasının modern dijital yaşamın gereksinimlerine göre yeniden inşa edilmesi gerektiğini göstermektedir.

VI. KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDA DEGERLENDİRME

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (KVKK) 28. maddesinin birinci fıkrasının (a) bendi, kişisel verilerin "üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla, gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi" hâlinde Kanun hükümlerinin uygulanmayacağını düzenlemektedir. Bu düzenleme, Avrupa Birliği hukukundaki "tamamen kişisel veya ev içi faaliyet" istisnası ile hem yapısal hem de amaçsal olarak büyük ölçüde paralellik göstermektedir.

Bu noktada Ryneš v Úřad pro ochranu osobních údajů kararında ortaya konulan yaklaşımın Türk hukuku bakımından da geçerli olduğu açıktır. Söz konusu kararda Divan, ev güvenliği amacıyla kurulan bir kamera sisteminin kamusal alanı görüntülemesi hâlinde, işleme faaliyetinin artık tamamen kişisel veya ev içi olarak değerlendirilemeyeceğini tespit etmiştir. Bu yorum, KVKK m.28 açısından da doğrudan uygulanabilir niteliktedir. Zira kamusal alanda bulunan üçüncü kişilere ait verilerin kaydedilmesi, KVKK'nın açıkça aradığı "üçüncü kişilere verilmemek" ve "yalnızca kendisiyle veya aynı konutta yaşayan kişilerle sınırlı faaliyet" şartlarıyla bağdaşmamaktadır. Başka bir ifadeyle, veri işleme faaliyetinin kapsamı hane sınırlarını aştığı anda, KVKK bakımından da istisnanın uygulanması mümkün değildir.

Benzer şekilde TK v Asociaţia de Proprietari bloc M5A-ScaraA kararında geliştirilen meşru menfaat, gereklilik ve orantılılık temelli yaklaşımın da Türk hukukunda karşılık bulduğu görülmektedir. KVKK'da açık rıza dışında veri işleme şartları arasında yer alan "veri sorumlusunun meşru menfaati" kavramı, AB hukukundaki düzenleme ile büyük ölçüde örtüşmektedir. Bu nedenle, hane istisnası kapsamı dışında kalan veri işleme faaliyetlerinin hukuka uygunluğu değerlendirilirken, yalnızca istisnanın uygulanıp uygulanmadığına bakmak yeterli olmayacak; aynı zamanda işleme faaliyetinin amacı, kapsamı ve ölçülülüğü de dikkate alınacaktır. Bu durum, makalede savunulan bağlamsal ve teknoloji-duyarlı yorum ihtiyacının Türk hukuku bakımından da geçerli olduğunu göstermektedir.

Bununla birlikte KVKK m.28 ile GDPR'ın Recital 18 hükmü arasında bazı önemli nüans farklılıkları da bulunmaktadır. GDPR Recital 18, istisnanın yalnızca "tamamen kişisel veya ev içi faaliyet" kapsamında ve profesyonel ya da ticari bir bağlantı olmaksızın gerçekleşen veri işleme faaliyetleri için geçerli olduğunu açıkça belirtmektedir. Ayrıca aynı gerekçe paragrafı, bu tür faaliyetler için teknik altyapıyı sağlayan veri sorumluları veya veri işleyenlerin

düzenleme kapsamı dışında kalmayacağını vurgulamaktadır. Buna karşılık KVKK m.28, istisnayı daha dar ve koşullu bir şekilde formüle etmekte; özellikle "üçüncü kişilere verilmemek" şartını açıkça düzenleyerek veri akışının sınırlandırılmasını istisnanın temel unsurlarından biri hâline getirmektedir. Bu yönüyle KVKK, istisnanın uygulanabilirliğini yalnızca faaliyetin niteliğine değil, aynı zamanda verinin dolaşımına da bağlamaktadır.

Özellikle modern gözetim teknolojileri bağlamında KVKK m.28'in klasik yorumunun ciddi sınırlılıklar içerdiği açıktır. Akıllı kapı zili kameraları, araç içi kayıt sistemleri, drone'lar ve IoT tabanlı gözetim araçları, veri işleme faaliyetini hem mekânsal hem de işlevsel olarak hane sınırlarının dışına taşımaktadır. Bu tür teknolojilerde verinin yalnızca ev içinde kalmadığı, çoğu zaman bulut hizmetleri aracılığıyla üçüncü taraf platformlara aktarıldığı dikkate alındığında, KVKK m.28'de öngörülen istisnanın uygulanma alanı son derece daralmaktadır. Bu durum, makalede ortaya konulan "mekânsal kriterin yetersizliği" eleştirisinin Türk hukuku bakımından da geçerli olduğunu açıkça ortaya koymaktadır.

Sonuç olarak, KVKK m.28 ile GDPR Recital 18 arasında mevcut olan yapısal paralellik, Avrupa Birliği hukukunda geliştirilen içtihatların Türk hukuku bakımından da yol gösterici olmasını sağlamaktadır. Ryneš kararının istisnayı dar yorumlayan yaklaşımı ve TK kararının getirdiği bağlamsal değerlendirme modeli birlikte ele alındığında, hane istisnasının Türk hukukunda da yalnızca kapalı, içe dönük ve üçüncü kişiler üzerinde etkisi bulunmayan veri işleme faaliyetleriyle sınırlı tutulması gerektiği sonucuna ulaşılmaktadır. Bu çerçevede, makalede geliştirilen normatif argümanların KVKK bakımından da geçerliliğini koruduğu ve özellikle yeni nesil gözetim teknolojileri karşısında istisnanın yeniden yorumlanmasının zorunlu olduğu değerlendirilmektedir.

SONUÇ VE ÖNERİLER

Hane istisnası, Avrupa veri koruma hukukunun en köklü kavramlarından biri olmasına rağmen, dijital çağın çok katmanlı ve ağ temelli gözetim ekosistemi karşısında giderek daha problemli ve uygulanması güç bir hukuki kategori hâline gelmiştir. Bu çalışma kapsamında ayrıntılı biçimde incelenen Ryneš kararı, hane istisnasının geleneksel olarak benimsediği mekânsal ve kişisel faaliyet merkezli yorumun, günümüz veri işleme pratiklerini açıklamakta ve düzenlemekte artık yetersiz kaldığını açıkça ortaya koymaktadır. Başlangıçta hane istisnası, düşük teknolojili, sınırlı kapsamlı ve esasen aile içi iletişim veya tamamen özel nitelikteki faaliyetleri veri koruma hukukunun dışında bırakmayı amaçlayan dar bir muafiyet olarak tasarlanmıştır. Oysa günümüzde haneler, sensörler, akıllı kameralar, bulut tabanlı uygulamalar ve platform ekonomisiyle bütünleşmiş dijital hizmetler aracılığıyla sürekli veri üreten ve bu verileri dış aktörlerle paylaşan yapılar hâline gelmiştir. Bu dönüşüm, hane ile kamusal alan, özel alan ile ticari alan arasındaki sınırları büyük ölçüde geçirgen kılmakta ve istisnanın klasik varsayımlarını geçersiz hâle getirmektedir. Bu nedenle hane istisnasının mevcut hukuk düzeni içinde modern, otomatik ve ticarileşmiş veri işleme pratiklerini karşılamakta ciddi zorluklar yaşadığı söylenebilir. Nitekim benzer bir yaklaşım Türk hukukunda da görülmekte; 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 28. maddesinde, kişisel verilerin üçüncü kişilere aktarılmamak ve veri güvenliği yükümlülüklerine uyulmak kaydıyla, gerçek kişiler tarafından

tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi istisna kapsamına alınmaktadır. Bu paralellik dikkate alındığında, bu makalede yapılan analizlerin ve ulaşılan sonuçların yalnızca Avrupa Birliği hukuku bakımından değil, Türk hukuku ve KVKK'nın yorumlanması açısından da doğrudan geçerlilik taşıdığı açıktır.

Ryneš kararı hane istisnasını olabildiğince dar yorumlayarak temel hakları koruma yönünde güçlü bir adım atmış olsa da, kararın mekânsal yaklaşımı günümüz teknolojileri açısından hem teorik hem pratik sınırlılıklar taşımaktadır. Kameranın kamusal alanı en küçük bir şekilde görüntülemesi dahi işleme faaliyetinin ev içi faaliyet kategorisinden çıkmasına yol açmaktadır.[39] Ancak veri akışlarının artık mekâna dayanmadığı ve kamusal ile özel alan ayrımının giderek anlamsızlaştığı bir dönemde, böylesine katı bir yaklaşımın sürdürülebilir olmadığı açıktır. Modern haneler artık kapalı ve mahrem alanlar olmaktan ziyade platform ekonomisi ve ticari gözetim hizmetlerinin merkezinde yer alan düğümler hâline gelmiştir.[40] Bu nedenle hane istisnasının içeriği, mekânsal sınırlara dayanan eski paradigmanın ötesinde yeniden düşünülmelidir.

Bu noktada TK kararı, Ryneš'in katı yorumundan daha esnek ve bağlamsal bir modele geçişi temsil etmektedir. TK kararının getirdiği üçlü test, yani meşru amaç, gereklilik ve orantılılık ilkelerinin birlikte değerlendirilmesi yaklaşımı, veri koruma hukukunun yalnızca bir konum değerlendirmesine değil, işleme faaliyetinin bütünsel niteliğine odaklanması gerektiğini göstermektedir.[41] Bu bağlamda TK, hane istisnasının modern biçiminin nasıl olması gerektiğine yönelik önemli bir ipucu sunmaktadır. Hane istisnası, yalnızca kullanıcı niyetine veya cihazın mekânsal konumuna göre değil, işleme sürecinin teknik mimarisine, veri akışının yönüne ve işleme faaliyetinin toplumsal bağlamına göre değerlendirilmelidir.

Güncel teknolojik gelişmeler, özellikle akıllı kapı zili kameraları, drone sistemleri, araç içi kameralar ve giyilebilir cihazlar, hane istisnasının klasik sınırlarını tamamen belirsizleştirmektedir. Bu teknolojilerin neredeyse tamamı, veriyi otomatik olarak işleyen ticari platformlara bağlıdır. Bu nedenle verinin ev içinde kalmadığı, aksine sistematik bir şekilde üçüncü taraflara aktarıldığı gerçeği dikkate alınmalıdır. Nissenbaum'un bağlamsal bütünlük teorisi, mahremiyetin mekânla değil, veri akışının toplumsal normlara uygunluğu ile belirlendiğini savunur.[42] Bu teori, hane istisnasının modern koşullara uyarlanması için en açıklayıcı çerçevelerden birini sunar. Çünkü hane içi veri işleme, artık doğal olarak özel veya masum kabul edilemez; aksine işleme sürecinin bağlamı ve veri akışının niteliği bu değerlendirmede belirleyici olmalıdır.

Bu analizler ışığında hane istisnasına ilişkin politika önerileri geliştirmek zorunlu hâle gelmektedir. İlk olarak, hane istisnası modernize edilmeli ve teknoloji-nötr bir içerikle yeniden tanımlanmalıdır. İstisnanın yalnızca mekâna dayalı kriterlerle belirlenmesi yerine, veri işleme faaliyetinin kim tarafından, hangi amaçla, hangi araçlarla ve hangi yönlere doğru veri akışı üreterek gerçekleştirildiği dikkate alınmalıdır. Van der Sloot'un önerdiği üzere, ticari

[39] *Case C-212/13 (Ryneš v Úřad pro ochranu osobních údajů)*.
[40] van de Sloot, "Home is where the heart is: the household exemption in the 21st century".
[41] Hijmans, "On Private Persons Monitoring the Public Space".
[42] Nissenbaum, "Privacy in context: Technology, policy, and the integrity of social life".

platformların veri işleme faaliyetlerine dahil olduğu hiçbir süreç otomatik olarak hane istisnası kapsamında kabul edilmemelidir.[43] Bu, özellikle bulut tabanlı akıllı ev cihazlarının mevcut işleyişi düşünüldüğünde temel bir gerekliliktir.

İkinci olarak, veri koruma otoriteleri bireysel kullanıcılar için uygulanabilir rehberler geliştirmeli ve sıradan ev kullanıcılarının hukuki yükümlülüklerini anlaşılır hâle getirmelidir. Ryneš kararının geniş yorumlanması, teknik olarak sıradan bir ev kamerası sahibi olan bireyi bile karmaşık veri sorumlusu yükümlülükleriyle karşı karşıya bırakmaktadır. Bu nedenle otoritelerin amaç, orantılılık, saklama süresi ve teknik güvenlik önlemleri konusunda net rehberlik sağlaması gerekmektedir. Böyle bir yaklaşım, hem uyum sorunlarını azaltacak hem de mahremiyet hakkının korunmasını güçlendirecektir.

Üçüncü olarak, hane istisnasını düzenleyen açık ve kapsamlı bir normatif rehber hazırlanması önemlidir. Bu rehber Ryneš ve TK içtihatlarını uyumlaştırmalı, istisnanın kapsamını net ve teknoloji-duyarlı bir çerçeveyle belirlemelidir. Bu rehberin yalnızca hukukçular için değil, aynı zamanda teknoloji üreticileri ve sıradan ev kullanıcıları için de anlaşılır olması sağlanmalıdır.

Sonuç olarak, hane istisnası veri koruma hukukunun temel yapı taşlarından biri olmakla birlikte, mevcut haliyle dijital çağın karmaşık veri ekosistemini karşılayabilecek bir yapı sunmamaktadır. Ryneš kararının ortaya koyduğu dar yorum, temel hakların korunması açısından önemli olsa da modern teknolojiler karşısında yetersizdir. TK kararının bağlamsal yaklaşımı açısından bu makalede yapılan eleştirel analizi, istisnanın yeniden ele alınması gerektiğini göstermektedir. Bu nedenle hane istisnasının geleceği, mekânsal sınırlara dayalı bir modelden çok, veri akışlarının yapısına, toplumsal bağlama ve ticari ilişkilerin niteliğine duyarlı bir model doğrultusunda şekillenmelidir.

[43] van de Sloot, "Home is where the heart is: the household exemption in the 21st century".

KAYNAKÇA

Ball, Kirstie, Kevin Haggerty, ve David Lyon. *Routledge handbook of surveillance studies*. Routledge, 2012.

Bauman, Zygmunt, ve David Lyon. *Liquid surveillance: A conversation*. John Wiley & Sons, 2013.

Bentham, Jeremy. *The panopticon writings*. Verso Books, 2020.

Case C-212/13 (Ryneš v Úřad pro ochranu osobních údajů) (The Court of Justice of the European Union (CJEU) 11 Aralık 2014). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62013CJ0212.

Case C-708/18 (TK v Asociația de Proprietari) (The Court of Justice of the European Union (CJEU) 11 Aralık 2019). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62018CJ0708.

Cavoukian, Ann. *Surveillance, then and now: Securing privacy in public spaces*. Information and Privacy Commissioner of Ontario, Canada, 2013.

Firmino, Rodrigo, ve Fabio Duarte. "Private video monitoring of public spaces: The construction of new invisible territories". *Urban Studies* 53, sy 4 (2016): 741-54.

Giddens, Anthony. "The nation-state and violence". *Capital & Class* 10, sy 2 (1986): 216-20.

Hijmans, Hielke. "On Private Persons Monitoring the Public Space". *Eur. Data Prot. L. Rev.* 1 (2015): 149.

Hijmans, Hielke. "The European Union as guardian of internet privacy". *The Story of Art* 16 (2016).

Koskela, Hille. "Hijackers and humble servants: Individuals as camwitnesses in contemporary controlwork". *Theoretical Criminology* 15, sy 3 (2011): 269-82.

Lynskey, Orla. *The foundations of EU data protection law*. Oxford University Press, 2015.

Lyon, David. *Surveillance after september 11*. C. 11. Polity, 2003.

Lyon, David. *Surveillance society*. McGraw-Hill Education (UK), 2001.

Nissenbaum, Helen. "Privacy in context: Technology, policy, and the integrity of social life". İçinde *Privacy in context*. Stanford University Press, 2009.

Sloot, Bart van de. "Home is where the heart is: the household exemption in the 21st century". *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 14 (2023): 34.

Turow, Joseph. "11 Cracking the Consumer Code: Advertisers, Anxiety, and Surveillance in the Digital Age". *The new politics of surveillance and visibility*, 2006, 279.

Wakefield, Alison. "The public surveillance functions of private security". *Surveillance & Society* 2, sy 4 (2004).

Warso, Zuzanna. "There's more to it than data protection–Fundamental rights, privacy and the personal/household exemption in the digital age". *Computer Law & Security Review* 29, sy 5 (2013): 491-500.

EXTENDED SUMMARY

PRIVATE SURVEILLANCE IN PUBLIC SPACES AND DATA PROTECTION LAW FROM THE EUROPEAN UNION PERSPECTIVE: THE RYNEŠ JUDGMENT AND THE TRANSFORMATION OF THE HOUSEHOLD EXEMPTION

Ali Mert Gürkan
Bologna University, gurkanalimert@gmail.com
https://orcid.org/0009-0003-5292-2875

Introduction and Research Purpose

The rapid diffusion of low-cost, user-friendly surveillance technologies has fundamentally altered the governance and visibility of public space. Devices such as home CCTV systems, smart doorbell cameras, dashcams, drones, and sensor-based smart city infrastructures enable continuous monitoring of individuals in public and semi-public environments. Surveillance, once primarily exercised by the state through vertically organized mechanisms, has increasingly become decentralized and privatized, with private individuals and commercial actors assuming active roles. This transformation raises a central legal question for contemporary data protection law: to what extent can privacy and personal data protection be ensured in public spaces when surveillance is conducted by private persons rather than public authorities?

This article addresses this question through an in-depth analysis of the household exemption in European Union data protection law. Specifically, it examines how the Court of Justice of the European Union's (CJEU) judgment in Ryneš redefined the legal boundaries of private surveillance in public space and assesses whether this spatially oriented approach remains adequate in light of emerging surveillance technologies. The study further explores the relevance of this jurisprudence for Turkish data protection law, which contains a closely parallel household exemption.

Literature Review (Conceptual and Theoretical Framework)

Existing scholarship on surveillance and data protection highlights a shift from centralized, state-driven surveillance models toward dispersed and networked surveillance practices involving private actors. Surveillance theory emphasizes the growing opacity and pervasiveness of monitoring technologies, particularly within smart city environments and domestic security systems. At the same time, data protection literature has long treated the household exemption as a narrowly tailored derogation intended to exclude low-risk, purely personal activities from regulatory oversight.

However, the literature increasingly recognizes a tension between the original rationale of the household exemption and the technological reality of contemporary

domestic surveillance. Modern devices routinely capture data beyond the private sphere, extend into public space, and rely on cloud-based infrastructures operated by commercial platforms. While the Ryneš judgment has been widely acknowledged as a milestone in affirming the applicability of data protection law to private surveillance, critical accounts point to the limitations of its predominantly spatial logic. This article contributes to the literature by systematically linking surveillance theory, smart city studies, and data protection doctrine to demonstrate why a purely location-based interpretation of the household exemption is no longer sufficient.

Methodology and Findings

The study adopts a qualitative and doctrinal legal research methodology. First, it conducts a close textual and systematic analysis of the Ryneš judgment, focusing on the Court's interpretation of personal data, automated processing, and the scope of the household exemption. This doctrinal analysis is complemented by a contextual assessment informed by surveillance theory and interdisciplinary scholarship on smart cities and privatized security.

The findings demonstrate that Ryneš establishes a strict spatial criterion: once a private surveillance activity extends into public space, it falls outside the household exemption and becomes subject to data protection law. This interpretation strengthens fundamental rights protection by affirming that individuals do not lose their right to personal data protection merely by entering public space. However, the analysis also reveals that this spatial approach struggles to accommodate contemporary surveillance technologies that are mobile, automated, and detached from fixed physical locations.

The article further examines the CJEU's subsequent judgment in TK (C-708/18), which introduces a more flexible assessment based on legitimate interest, necessity, and proportionality. Unlike Ryneš, TK shifts the focus from where data is collected to why and how it is processed. This evolution suggests a gradual move toward a contextual evaluation of private surveillance activities rather than a rigid spatial test.

Conclusions, Limitations, and Recommendations

The article concludes that while the Ryneš judgment represents a significant advancement in protecting personal data in public spaces, its spatially centered reasoning is increasingly inadequate in the face of technologically intensified surveillance practices. Modern domestic surveillance systems blur the boundaries between private and public space, individual and commercial processing, and personal security and systematic monitoring. As a result, the household exemption can no longer be meaningfully interpreted solely through reference to physical location.

A key limitation of the study lies in its doctrinal focus, as it does not include empirical analysis of enforcement practices or user behavior. Nevertheless, this methodological choice allows for a precise normative evaluation of legal principles and judicial reasoning.

The article recommends a contextual and technology-sensitive reinterpretation of the household exemption, informed by the proportionality-based approach developed in TK. Such a framework would assess private surveillance activities by considering their purpose, intensity, technological architecture, and impact on the rights of others, rather than relying exclusively on spatial distinctions. This approach is equally relevant for Turkish law, where Article 28 of the Personal Data Protection Law mirrors the EU household exemption. Interpreting this provision in light of Ryneš and TK can help define the legal limits of domestic surveillance and clarify the data protection responsibilities of private individuals operating in public space.