

AMERİKA BİRLEŞİK DEVLETLERİ'NDE MOBİL CİHAZLARLA KONUM VERİSİNİN TOPLANMASI VE İŞLENMESİNE İLİŞKİN FTC SORUŞTURMALARINI VE ÜLKEMİZDE KONUM VERİSİ İLE İLGİLİ GELİŞMELER^(*)

FTC INVESTIGATIONS REGARDING THE COLLECTION AND PROCESSING OF LOCATION DATA WITH MOBILE DEVICES IN THE UNITED STATES OF AMERICA AND DEVELOPMENTS REGARDING LOCATION DATA IN OUR COUNTRY

Dr. Öğr. Üyesi Mükerrerem Onur BAŞAR^(**)

Öz

Yeni gelişen teknolojik gelişmeler karşısında özellikle mobil cihazlarla toplanan konum verisi ve bu verinin işlenmesi önemli bir meseleyi oluşturmaktadır. Teknolojinin süratle geliştiği günümüzde kişilerin mobil cihazları ile angajmanları da her geçen gün artmaktadır.

Reklam teknolojileri, veriye dayalı ve hedefe yönelik reklamcılık yöntemleri ile geleneksel reklamcılığı değiştirmektedir. Amerika Birleşik Devletleri'nde reklam teknolojileri şirketleri, tüketici davranışını, tercihlerini ve satın alma kalıplarını tanımlamak amacıyla büyük miktarda konum verisi toplamak için gelişmiş konum tabanlı teknolojiler kullanmaktadırlar. Bu yeni konum tabanlı teknolojiler, son derece kişiselleştirilmiş ve etkili reklamları doğru hedef kitleye doğru zamanda sunmalarına olanak tanımaktadır. Konum verilerini toplama ve kullanma yeteneği, şirketlerin tüketicilere kişiselleştirilmiş ve alakalı içerik sunmasına olanak tanımaktadır. İşte bu noktada mobil cihazlarla kişilerin konum verisinin toplanıp işlenmesi suretiyle, reklam ve pazarlama faaliyetlerinin doğru hedef kitesine ulaştırılması temin edilmektedir.

Amerika Birleşik Devletleri'nde, ülkemiz düzenlemelerinden ve Avrupa Birliği düzenlemelerinden farklı olarak, kişisel verilerin korunmasına yönelik federal düzeyde düzenleyici merkezi bir idari otorite bulunmamakta olup, icrai yetkiler ile donatılmış ve yaptırım makamı olarak birçok farklı konuda görevi bulunan FTC (Federal Ticaret Komisyonu) konunun ele alınmasında ve düzenlenmesinde etkin bir rol oynamaktadır. FTC, yeni gelişen teknolojik gelişmeler karşısında özellikle mobil cihazlarla toplanan konum verisine ilişkin olarak birtakım soruşturmalarda bulunmuştur. Bu soruşturmalar ile ele alınan benzeri konu ve hassasiyetlerin ülkemiz düzenleminde de ele alınması gerçekçi bir beklentiyi oluşturmaktadır. Makalemizde konum verisi ile ilgili olarak ülkemizdeki gelişmelere ve Amerika Birleşik Devletleri'nde toplanması ve işlenmesine dair yakın geçmişteki FTC soruşturmalarına yer verilmiştir.

Anahtar Kelimeler

Kişisel Veri, Konum Verisi, Federal Ticaret Komisyonu, Konum Verisinin Toplanması ve İşlenmesi.

^(*) (Araştırma Makalesi, Geliş Tarihi: 23.10.2023 / Kabul Tarihi: 23.12.2023).

^(**) İstanbul Sabahattin Zaim Üniversitesi, Hukuk Fakültesi, Medeni Usul ve İcra İflas Hukuku Anabilim Dalı, İstanbul - Türkiye, (E-posta: mukerrem.basar@izu.edu.tr, ORCID ID: 0000-0002-5002-6132).

Atıf/Citation: Başar, Mükerrerem Onur (2024), "Amerika Birleşik Devletleri'nde Mobil Cihazlarla Konum Verisinin Toplanması ve İşlenmesine İlişkin FTC Soruşturmaları ve Ülkemizde Konum Verisi ile İlgili Gelişmeler", TFM, C: 10, S: 1, s. 63-77.

Abstract

In the face of new technological developments, location data collected especially with mobile devices and the processing of this data have become an important issue. Nowadays, as technology develops rapidly, people's engagement with their mobile devices increases day by day.

Advertising technologies are disrupting traditional advertising by offering new, data-driven and targeted advertising methods. In the United States of America advertisement technology companies use advanced location based technologies to gather vast amounts of location data so as to identify consumer behaviour, preferences and buying patterns. This new location based technologies allow them to deliver highly personalized and effective advertisements to the right target audience at the right time. The ability to collect and leverage location data has allowed companies to deliver personalized and relevant content to consumers. At this point, by collecting and processing people's location data via mobile devices, it is ensured that advertising and marketing activities are delivered to the correct target audience.

I. GİRİŞ

Kişisel verilerin korunması ve tüketicilerin korunması düzenlemeleri kimi zaman kesişmekte ve birbirleriyle etkileşmektedir. Bu bağlamda, kişisel verilerin korunmasına ilişkin düzenlemelere dair hukuk politikası tercihlerinde tüketicilerin korunması hassasiyeti göz önünde tutulmaktadır. Bu vesile ile belirtmekte yarar bulunmaktadır ki; özellikle, Amerika Birleşik Devletleri'nde kişisel verilerin korunması düzenlemeleri bakımından tüketicilerin korunması amacının oldukça ön planda tutulduğunu ifade etmek hatalı bir tespiti oluşturmamaktadır¹.

Kişisel verilerin işlenmesi önemli sosyal ve ekonomik yararlar ortaya koymakla birlikte kişilerin mahremiyetinin korunması bakımından da önemli hassasiyetleri gündeme getirmektedir². Bu bağlamda, kişisel verilerin korunması bakımından “mahremi-

In the United States of America, unlike our country's regulations and the European Union regulations, there is no central regulatory authority for the protection of personal data on federal level, and the FTC (Federal Trade Commission), which is equipped with executive powers and has duties as a sanctioning authority on many different issues, is effective in handling and regulating the issue. In response to new technological developments, the FTC has conducted a number of investigations, especially regarding location data collected via mobile devices. It is a realistic expectation that similar issues addressed in these investigations will be addressed at the level of our country as well. Our article covers developments regarding location data and recent FTC investigations into the collection and processing of location data in the United States and our country.

Keywords

Personal Data, Location Data, Federal Trade Commission, Collection and Processing of Location Data.

yet” terimi merkezi bir kavramı oluşturmakta; farklı hukuk kültürlerinde değişik içeriklerde söz konusu kavramın anlamlandırılması olasıdır. Farklı kültürel, sosyal ve iktisadi değerler ve inançlar mahremiyet kavramının sınırlarının çizilmesinde ve içeriğinin doldurmasında doğal olarak farklı yaklaşımların ortaya konulmasına sebebiyet vermektedir³. Bu bağlamda, Avrupa Birliği'nde mahremiyet kişisel verilerle yakinen ilgili bir kavram olarak ele alınırken; Amerika Birleşik Devletleri'nde veriler bir emtia olarak değerlendirilmekte ve verilerin iktisadi yönü gerekli kıldığı ölçekte mahremiyete ilişkin hassasiyetler önem taşımaktadır⁴. Bu yönü ile Amerika Birleşik Devletleri'nde kişisel veriler kişilik hakları ve insan hakları

¹ Julie Brill, 'The Intersection of Privacy and Consumer Protection', Evan Selinger, Jules Polonetsky ve Omer Tene (Editörler) *The Cambridge Handbook of Consumer Privacy* (Cambridge University Press) 355; Rebecca Lipman, 'Online Privacy and the Invisible Market for Our Data' (2016) 3, 788.

² Ira Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 2 *International Data Privacy*, 74; Joanna Kulesza, 'International Law Challenges to Location Privacy Protection' [2013] *International Data Privacy Law*, 165.

³ Teknolojinin göstermiş olduğu gelişim ile paralel olarak kişisel verilerin korunmasına yönelik hassasiyetler de gün geçtikçe önem kazanmıştır. Konu önem kazandıkça kişisel verilerin tanımlanması ve işlenmesi meselelerinin yeknesaklaştırılmasına ilişkin çalışmalar, örneğin, Kişisel Verilerin Mahremiyetinin Korunmasına ve Sınır Ötesi Akışına İlişkin OECD İlkeleri gibi düzenlemeler gündeme gelmiştir. Organization for Economic Co-operation and Development, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Publishing, Paris' <<https://doi.org/10.1787/9789264196391-en>> s.e.t 1 Nisan 2023; World Economic Forum, 'Rethinking Personal Data: A New Lens for Strengthening Trust' <https://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf>.

⁴ Kulesza (n 2) 158; Rubinstein (n 2) 82.

perspektifinden ziyade liberal ekonomik düzlemde tedavülü mümkün olan bir emtia olarak ele alınmakta ve özellikle tüketiciler cephesinde bu durumun oluşturacağı olumsuzluklar meselenin özünü oluşturmaktadır⁵. Bu bilgiler ışığı altında, Amerika Birleşik Devletleri'nde kişisel veri merkez kavramından ziyade konu veriler ve tüketicilerin menfaatleri çerçevesinde yoğun bir şekilde ele alınmaktadır.

II. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN OLARAK FARKLI BİR YAKLAŞIM

A. LIBERAL BİR YAKLAŞIM OLARAK ABD MODELİ

Amerika Birleşik Devletleri'nde kişisel verilerin korunması bakımından Avrupa Birliği ülkeleri ve ülkemizin tutumunun aksine merkezi tek bir düzenleme ile konunun ele alınması yerine, farklı konulara ilişkin spesifik düzenlemelerde kişisel verilerin korunmasına ilişkin kurallara yer verilmesinin tercih edilmiş olduğu gözlenmektedir⁶. Bir başka ifadeyle, Amerika Birleşik Devletleri'nde "kişisel veri" merkez kavramının yerine kazuistik düzenlemeler ile benzer hassasiyetleri hukuki bir rejime bağlama amacı güdülmekle birlikte, konu bizim hukuk sistemimizden farklı olarak federal düzeyde tek bir düzenleme ile yoğun bir içerikte ele alınmamaktadır⁷. Bu bağlamda, Amerika Birleşik Devletleri'nde ülkemiz düzenlemelerinden ve Avrupa Birliği düzenlemelerinden farklı olarak kişisel

verilerin korunmasına yönelik düzenleyici merkezi bir idari otorite bulunmamakta olup, icrai yetkiler ile donatılmış ve yaptırım makamı olarak birçok farklı konuda görevi bulunan FTC (*Federal Trade Commission/Federal Ticaret Komisyonu*) konunun ele alınmasında ve düzenlenmesinde etkin rol oynamaktadır.

Nitekim, Amerika Birleşik Devletleri'nde tüketicilerin korunması saiki ile FTC kimi zaman oldukça cesur adımlar atmakta ve Facebook ve Google gibi dünya devlerine birtakım soruşturmalar açmıştır⁸. Bu vesile ile paylaşmak isteriz ki, FTC, yeni gelişen teknolojik gelişmeler karşısında özellikle mobil cihazlarla toplanan konum verisine ilişkin olarak da birtakım soruşturmalarda bulunmuştur⁹.

Yukarıda ifade edildiği üzere FTC'nin bu konudaki amaç ve hassasiyetinin odak noktasında bilhassa tüketiciler yer almaktadır¹⁰. Bu bağlamda, Amerika Birleşik Devletleri'nde kişisel verilerin korunması konusu müstakil bir konu olmaktan ziyade; tüketicilerin menfaatinin korunması çerçevesinde ele alınan ve her geçen gün gelişen dinamik ve multidisipliner bir alanı oluşturmaktadır¹¹.

⁵ Kulesza (n 4) 163.

⁶ Örneğin, Adil Kredi Raporlama Yasası (Fair Credit Reporting Act), alacaklıların borçlular ile nasıl temasa geçebileceği ve borçlunun borçlu olduğu vakasının üçüncü kişilerle paylaşılamayacağı kuralı gibi bir takım kişisel verilerin korunması alanını ilgilendiren spesifik düzenlemelere yer vermektedir. 'Fair Credit Reporting Act' <<https://www.ftc.gov/legallibrary/browse/statutes/fair-credit-reporting-act>>; 'Telemarketing Sales Rule' <<https://www.federalregister.gov/regulations/3084-AA98/telemarketing-sales-rule>> s.e.t. 17 Mart 2023; 'Children's Online Privacy Protection Act' <<http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim>> s.e.t. 17 Mart 2023; 'Gramm Leach Bliley Act' <<https://www.congress.gov/bill/106thcongress/senate-bill/900/text>> s.e.t. 4 Nisan 2023; 'Health Insurance Portability and Accountability Act' <<https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996>> s.e.t. 5 Nisan 2023; Murugan Anandarajan, Rob D'Ovidio and Jenkins Alexander, 'Safeguarding Consumers against Identity-Related Fraud: Examining Data Breach Notification Legislation Through the Lens of Routine Activities Theory' (2013) 1 International Data Privacy Law 54.

⁷ Kulesza (n 4) 164.

⁸ Google'a karşı FTC tarafından yürütülen bir soruşturmada, elektronik posta hizmetleri dışında Google'un bir başka hizmetini oluşturan sosyal medya platformu Google Buzz platformunda, gmail elektronik posta servisi kullanıcıları bilgilerinin ilgili kullanıcıların rızası alınmaksızın kullanılmasının, kullanıcıların mahremiyetini ihlal ettiği iddiası ele alınmıştır. Bu bağlamda, gmail kullanıcıları Google Buzz'a açık rızaları olmaksızın dahil edilmiştir. Kullanıcılara ait verilerin toplanması ve işlenmesi ile ilgili olarak yayınladığı politikalarda Google'un esaslı değişiklikler yapmadan önce kullanıcıların açık rızalarını alma(ma)sı bu soruşturmanın önemli bir odak noktasını oluşturmuştur. 'FTC v. Google Inc. Docket No: C-4336' <<https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf>> s.e.t. 17 Mart 2023; 'FTC v. Facebook Inc. Docket No: 0913284' <<https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf>> s.e.t. 17 Mart 2023.

⁹ 'FTC v. Goldenshores Technologies, LLC, and Erik M. Geidl Docket No. C-4446' <<https://www.ftc.gov/system/files/documents/cases/140409goldenshorescmpt.pdf>> s.e.t. 17 Mart 2023; 'FTC v. InMobi Pte Ltd. Docket No. 3:16-Cv-3474' <<https://www.ftc.gov/system/files/documents/cases/160622inmobicmpt.pdf>> s.e.t. 17 Mart 2023; 'FTC v Kochava, Inc. Docket No. 2:22-Cv-377' <https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf> s.e.t. 17 Mart 2023.

¹⁰ Brill (n 1) 357.

¹¹ Wall Street Journal, 'Should the U.S. Adopt European-Style Data-Privacy Protections' (8 Mart 2013) <<https://www.wsj.com/articles/SB10001424127887324338604578328393797127094>> s.e.t. 31 Mart 2023.

B. BİR VERİ ÇEŞİDİ OLARAK KONUM VERİSİNİN TAŞIDIĞI ÖNEM

Teknolojinin süratle geliştiği günümüzde kişilerin mobil cihazları ile angajmanları da her geçen gün artmaktadır. Kişiler mobil cihazları ile iletişim kurmakta, alveriş yapmakta, oyun oynamakta ve sosyal medyada gezinmekte ve dolayısıyla mobil cihazları ile konum verisinin oldukça erişilebilir ve yoğun bir şekilde izler bıraktığı bir ekosistem oluşmaktadır. Bu bağlamda, konum verisi özellikle aplikasyon geliştiricileri, telefon operatörleri, işletim sistemi hak sahipleri veya telefon üreticileri tarafından toplanabilmektedir¹². Nitekim, konum verisi büyük veri teknolojisi bakımından da önem taşımakta büyük veriler içerisinde de toplanan ve işlenen önemli bir veri türünü oluşturmaktadır¹³.

Liberal ekonomik anlayışın ve tüketimin ege-men olduğu bir toplum olan Amerika Birleşik Devletleri'nde tüketicilerin alışkanlıklarının tayini ve tespiti oldukça önem taşımaktadır. Zira, reklam harcamalarında reklamın doğru hedefe ulaşması büyük önem taşımakta olup; reklam ve pazarlama faaliyetlerinin doğru hedef kitlesine ulaşmasında kişisel veriler ve bu verilerin analizi oldukça önemli bir yer tutmaktadır¹⁴. İşte bu noktada mobil cihazlarla kişilerin konum verisinin toplanıp işlenmesi suretiyle, reklam ve pazarlama faaliyetlerinin doğru hedef kitlesine ulaştırılması temin edilmektedir¹⁵. Örneğin, İstanbul'a gelen Asyalı turistleri hedeflemek isteyen bir restoran işletmecisi, restoranına yakın mesafede bulunan Asyalı turistleri, bu kişilere ait telefon di-

linin herhangi bir Asya dili olması koşulunu tercih ederek ve restoranına 3 km uzaklıkta bulunması gibi koşulların tercih edilmesi suretiyle dijital reklam ve pazarlama faaliyetinin hedef kitlesi haline getirebilmektedir. Bu bağlamda, konum verisinin yardımı ile kişilerin anlık bulunduğu lokasyonlar, dijital reklam çalışmaları bakımından hedeflenebildiği gibi, geriye dönük olarak belli bir zaman aralığında belli bir lokasyonda bulunan kişiler dahi dijital reklam çalışmaları bakımından hedefleme faaliyetine konu edilebilmektedir. Dijital reklam çalışmaları bilhassa internet siteleri, çevrimiçi video ve ses yayınları gibi dijital platformlar üzerinden gerçekleştirilen pazarlama faaliyetlerini tanımlamaktadır. Nitekim, bu tür reklamlar; metin, görüntü, ses ve video gibi çeşitli medya formatlarını içerebilmektedir. Bir başka ifadeyle, konum verisi ayrıca zaman boyutu ile eklenerek reklamın doğru hedef kitlesi ile buluşması temin edilmektedir. Öte taraftan, konum verisi yardımı ile konvansiyonel reklam mecralarının etkinliği de analiz edilebilmektedir. Örneğin, bir bankanın reklamının yer aldığı reklam panosu / billboard yakınından geçen kişilerden kaçının daha sonrasında belli bir zaman aralığında söz konusu reklam veren bankanın şubesinde bulunup bulunmadığı tarzında ölçümlenmeler de konum verisinin yardımı ile yapılabilmektedir.

Yukarıda temas edildiği üzere, konum verisi sadece dijital reklam faaliyetlerinde değil, aynı zamanda bir takım görüş ve düşüncelerin ilgili kitlelere ulaştırılması bakımından da önem arz edebilmektedir. Örneğin, kürtaj karşıtları bu hususa ilişkin görüş ve düşüncelerini kürtaj merkezlerinin bulunduğu lokasyonları coğrafi olarak hedefleyerek, burada yer alan kişilerin mobil cihazları ile internete eriştiklerinde, söz konusu kürtaj karşıtı görüşü savunanlara ait paylaşımların hedef kitlesini oluşturabilmektedir. Nitekim, bu tarz bir faaliyetin de bireylerin mahremiyetine bir müdahale olarak değerlendirilmesi oldukça mümkündür.

Özü itibariyle bireylerin mobil cihazları ile bıraktığı konum verisine dair izler, bireylerin yeni medya ekosisteminde hedeflenmelerine olanak tanımaktadır¹⁶. Bu bağlamda, bireylerin mahremiyeti ile

¹² Martin Kirsten and Katie Shilton, 'Mobile Privacy Expectations: How Privacy is Respected with Mobile Devices', *The Cambridge Handbook of Consumer Privacy* (1st Baskı, Cambridge University Press 2018) 85; Caitlin D Cottrill, and Piyushimita Vonu Thakuriah, 'Privacy in Context: An Evaluation of Policy-Based Approaches to Location Privacy Protection' (2014) 2 179; Kulesza (n 4) 165; Colleen Tressler, 'Mobile Phone Maker Misled People on Privacy & Security' <<https://consumer.ftc.gov/consumer-alerts/2018/04/mobile-phone-maker-misled-people-privacy-security>> s.e.t. 27 Mart 2023; s.e.t. 12 Kasım 2023; <<https://www.apple.com/legal/privacy/pdfs/apple-privacy-policy-en-ww.pdf>> s.e.t. 27 Mart 2023.

¹³ Rubinstein (n 4) 76.

¹⁴ Brill (n 3) 357.

¹⁵ Öte taraftan konum verisi sadece dijital reklam hizmetleri için önem taşımamakta, örneğin, haritalama ve navigasyon hizmetlerinin sadeleştirilmesi ve kalitesinin artırılması gibi hizmetler bakımından da önem arz etmektedir. Rubinstein (n 4) 76.

¹⁶ Yeni medya terimi, geleneksel ve alışlagelmiş medyadan (kitap, televizyon, gazete ve radyo) farklı olarak, dijital medyayı, özel-

iktisadi faaliyetlerin gerçekleştirilmesi için harcanan reklam bütçelerinin doğru hedefe yönlendirilmesi arasındaki menfaat dengesinin adilane bir şekilde ele alınması oldukça önem taşımaktadır.

C. KONUM VERİSİNİN TOPLANMASININ VE İŞLENMESİNİN FTC PERSPEKTİFİNDEN HUKUKİ ANALİZİ

1. Genel Olarak

Bilgisayar ve benzeri cihazlardan farklı olarak mobil cihazlar ile toplanan konum verisi mobil cihazların sürekli ilgili kişinin zilyetliğinde bulunması ve yoğun bir kullanıma tabi olması gerekçesiyle çok daha yoğun bir içerikte ilgili kişinin lokasyonuna dair veriler içermektedir. Özellikle, mobil cihazlar çevrimiçi iken taranan internet siteleri, alışveriş alışkanlıkları gibi konularda bilgi toplanmakta; öte taraftan, çevrim dışı iken seyahat rotaları, sıklıkla bulunan lokasyonlar, bulunma süreleri gibi birtakım veriler de mobil cihazlar ile toplanabilmektedir¹⁷. Bir başka deyişle bu veriler marifetiyle tüketici davranış ve alışkanlıkları ölçümlenerek bir profillemeye çalışması yapılmaktadır.

Nitekim, mobil cihazlar sadece konum verisi değil, aynı zamanda hareket, iletişim verisi, uygulama içi aktiviteler gibi oldukça farklı verileri de toplamakta ve işlemektedir¹⁸. Bu bağlamda, hukuken analiz edilmesi gereken en önemli mesele, kişilerin farkındalığı, bilgisi ve rızası olmaksızın konum verisinin toplanmasının herhangi bir hukuki değerlendirilme

dirmeye muhtaç olup olmadığı meselesidir¹⁹. Zira, kişilerin mobil cihazlarının topladığı konum verisi ile pazarlama faaliyetlerinin süjesi olması kişinin mahremiyetinin korunması perspektifinden ele alınması gereken önemli ve hassas bir konuyu oluşturmaktadır. Öte taraftan konum verisinin toplanması ve işlenmesi ile kişiler fiziksel ve psikolojik bir gözleme tabi tutulmaktadır²⁰.

Yukarıda ifade edildiği üzere, Amerika Birleşik Devletleri'nde sağlık verisinin mobil cihazlarla toplanması ve küçüklere/çocuklara ilişkin kişisel verilerin toplanması dışında konunun düzenlenmesi ve takibi tamamen FTC'ye bırakılmıştır²¹. Bu bağlamda FTC, gayri adil ve yanıltıcı ticari uygulamaları engelleme ve cezalandırma yetki ve sorumluluğu kapsamında bu faaliyetleri icra etmektedir²². Nitekim, bu kapsamda FTC, mobil cihaz uygulama geliştiricileri için de bir kılavuz yayınlamıştır²³.

Bu noktada, üzerinde durulması gereken önemli konulardan bir tanesi de kişisel verilere ilişkin aşırı hassasiyetlerin ve katı kuralların inovasyonu ve teknolojik gelişimi ciddi bir surette baltalayacağı gerçektir. Bu yönü ile kişisel verilerin korunması, esasında bir risk yönetimi tercih ve rejimidir²⁴. Öte taraftan, arama motorları, işletim sistemleri, sosyal medya uygulamaları ve bilhassa mobil cihaz operatörleri ve mobil cihaz uygulamaları kişilerin çevrim içi aktivitelerine dair önemli ölçekte veri toplamaktadır. Kişilerin bu tür faaliyetler karşısındaki korunmaya değer bir mahremiyeti söz konusu olmaktadır.

likle etkileşimsel medyayı, internet ağlarını ve sosyal iletişim medyasını nitelemek için kullanılmakta olup ve bilgi-iletişim teknolojileri ile bunlarla bağlantılı sosyal bağlamları, iletişim becerilerini arttıran cihazları, bu cihazlar kullanılarak geliştirilen iletişim etkinlikleri ile pratiklerini ve bu cihazlarla pratikler etrafında şekillenen sosyal düzenleme veya örgütlenmeleri kapsamakta olduğu ifade edilmektedir. Mete Ogün Parlak, 'Yeni Medya ve Haberciliğin Dönüşümü' (2018) 14 Ufuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi 59, 68.

¹⁷ Nazmun Naher and Tanzima Hashem, 'Think Ahead: Enabling Continuous Sharing of Location Data in Real-Time with Privacy Guarantee' (2019) 1 1, 1; Leyla Keser- Berber, *Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması* (On İki Levha Yayıncılık 2014) 21-26; Adrian Fong, 'The Role of App Intermediaries in Protecting Data Privacy' 2 International Journal of Law and Information Technology 85, 85; Kirsten and Shilton (n 14) 87; Kulesza (n 4) 165.

¹⁸ Kirsten and Shilton (n 14) 86; Kulesza (n 4) 165; Fong (n 19) 88.

¹⁹ Andrew Blumberg and Peter Eckersley, 'On Locational Privacy, and How to Avoid Losing It Forever' <<https://www.eff.org/files/eff-locational-privacy.pdf>> s.e.t. 3 Nisan 2023; World Economic Forum and Bain Company, 'Personal Data: The Emergence of a New Asset Class' <https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf> s.e.t 3 Mart 2023.

²⁰ Raphaël Gellert, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 International Data Privacy Law 5; Fong (n 19) 93.

²¹ Kirsten and Shilton (n 14) 91; 'Health Insurance Portability and Accountability Act', (n 8); 'Children's Online Privacy Protection Act' (n 8).

²² Kirsten and Shilton (n 14) 91; Lipman (n 3) 789.

²³ Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change' <<https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policy-makers>> s.e.t 10 Mart 2023.

²⁴ Raphaël (n 22) 5.

Bu bağlamda, FTC'nin bu mahremiyeti korumakta kullandığı merkez kavram ise “*Haksız ve Aldatıcı Uygulamalar*” (*Unfair or Deceptive Practices*) kavramı olmaktadır. İşte bu kavramlar çerçevesinde FTC çeşitli soruşturmalar açarak konum verisinin toplanması ve işlenmesi meselelerine temas etmiştir.

2. Konum Verisinin Mahremiyetinin Korunması Bakımından Mekanik Bir Tedbir: Tasarımda Mahremiyet Prensibi

Amerika Birleşik Devletleri'nde yayımlanan Hızlı Değişim Gösteren Bir Çağda Tüketici Mahremiyetinin Korunması isimli raporda özellikle mobil cihazlar ile toplanan ve işlenen kişisel veriler bakımından mahremiyetin esas olduğu kanaati ön plana çıkmaktadır²⁵. Bu bağlamda, öne çıkan değerlerin söz konusu uygulamaların daha tasarımı aşamasında tüketicinin mahremiyetinin göz önünde tutulması, ilgili uygulamaların geliştirilmesinin her aşamasında bu hassasiyetin göz önünde tutulması, tüketiciyle alakalı kişisel verilerinin saklanması ve işlenmesi ile ilgili olarak doğru zamanda, yeterli düzeyde aydınlatılmış bir irade ile karar vermesine olanak tanıyan bir bilgilendirmenin yapılmış olması ve takip etme (*do not track*) mekanizmasına yer verilmesi tüketicinin mahremiyeti bakımından önemli esaslar olarak belirtilmiştir.

FTC, bilhassa tüketiciler nezdinde kişisel verilere ilişkin farkındalığın yaratılmasının ve ayrıca süratle değişen ve gelişen teknolojiler karşısında bu farkındalığın güncel tutulmasının güçlüklerine de temas etmiştir²⁶. Bu kaygı ile yeni bir konsept gündeme gelmiş, bu konsept de “*tasarımda mahremiyet*” (*privacy by design*) prensibi olarak ifade edilmiştir²⁷. Bu

bağlamda, uygulamaların tasarımında kişilere ait verilerin ihtiyaç olanlarının toplanması ve ihtiyaç olan süre kadar saklanması ve muhafaza edilmesi önem taşımakta olup, ayrıca aydınlatma metinlerinin de kısa ve anlaşılabilir olması, tasarımda mahremiyet prensibinin önemli boyutlarını oluşturmaktadır²⁸. Dolayısıyla, sürecin daha başından itibaren kişilere ait verilerin toplanması ve işlenmesinde uygulamaların daha tasarlanırken yeterli mahremiyete sahip olması, önem taşıyan pratik bir yaklaşımı oluşturmaktadır²⁹. Öte taraftan, FTC, verilerin mahremiyetinin korunmasında dünyanın farklı bölgelerinde farklı düzenlemelerin var olduğunun bilincinde hareket etmekte ve bu düzenlemeler arasında uyumun önemini de hafife almamakta ve söz konusu karar ve politikalarında bu hassasiyetin üzerinde durmaktadır.

III. AMERİKA BİRLEŞİK DEVLETLERİNDE KONUM VERİSİNİN TOPLANMASI VE İŞLENMESİ MESELESİNE TEMAS EDEN FTC SORUŞTIRMALARI

A. GENEL OLARAK

Mobil cihazlar, kişilerin her gittikleri yerde onlara eşlik eden taşınabilir cihazlardır. Öte taraftan, söz konusu bu taşınabilir cihazlar, sürekli olarak nerede bulunduğumuza dair konum verisi toplamaktadır. Daha da önemlisi kişilerin bilgisi olmaksızın bu veriler toplanmakta ve bu veriler dijital reklam faaliyetinde bulunan kurumların istifade edebileceği platformlarda pazarlanmaktadır. Bahse konu bu pazar yeterince şeffaf ve erişilebilir olmadığı için kimin bizim lokasyon verimiz hakkında bilgiye sahip olduğunu ve

on Technology 303; Jasmontaite Lina and others, 'Data Protection by Design and by Default' (2018) 2 European Data Protection Law Review 168; Lee A Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' Oslo Law Review' (2017) 2 Oslo Law Review 105, 105; Daniel Le Mé-tayer, 'Privacy by Design: A Matter of Choice', *Serge Gutwirth & Yves Pouillet & Paul De Hert (editörler) Data Protection in a Profiled World*, (1st Baskı, Springer Dordrecht) 323; European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0' <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_data-protection_by_design_and_by_default_v2.0_en.pdf> s.e.t. 19 Mart 2023.

²⁵ Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change' (n 25).

²⁶ Raphaël (n 22) 5.

²⁷ Adamantia Rachovitsa, 'Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue' (2016) 4 International Journal of Law and Information Technology, 374; Blumberg and Eckersley (n 21) 2; Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) madde 25 veri sorumlusunun, verilerin işlenmesi hususunda yeterli teknik ve organizasyonel tedbirleri alması sorumluluğunu düzenleme altına almıştır. Nitekim bu düzenlemenin tasarımı mahremiyet prensibinin bir yansıması olduğu da belirtilmiştir. Rachovitsa 387; Alessandro Mantelero, and others, 'The Common EU Approach to Personal Data and Cybersecurity Regulation' (2020) 4 International Journal of Law and Informati-

²⁸ Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change' (n 25) 23.

²⁹ Blumberg and Eckersley (n 21) 5; Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change' (n 25) 22.

bu bilgilerle ne yaptığını anlamak mahremiyetimizin korunması açısından oldukça önem taşımaktadır. İşte bu noktada FTC, yakın geçmişte konuya ilişkin olarak aşağıda ayrıntıları ile ele alınan birtakım değerlendirme ve aksiyonlarda bulunmuştur.

1. Goldenshore Soruşturması

Android işletim sisteminde “Brightest Flashlight App” uygulamasının geliştiricisi olan Goldenshore Technologies LLC'e ve kurucusuna karşı FTC, bir soruşturma açmıştır³⁰. Söz konusu bu soruşturmanın konusunu oluşturan uygulama Google Play'de 10 milyondan fazla kez mobil cihazlara indirilmiştir. Bahsi geçen bu uygulama flaş ışık dahil bir mobil cihazdaki tüm ışıkların aktif hale gelmesini kolaylıkla temin etmektedir. Bununla birlikte, bu uygulama kullanıldığında kişiye ait konum verisi reklam platformları dahil üçüncü kişilere aktarılmakta ve ayrıca kullanıcıların lokasyonu bu uygulama ile takip edilebilmektedir. Öte taraftan, FTC, söz konusu bu uygulamanın tanıtım belgelerinin, hiçbir surette konum verisinin bu uygulama ile toplandığı ve üçüncü kişilerle paylaşıldığına dair herhangi bir bilgi ve uyarı içermediğini ve bu durumun da kullanıcıların ilgili uygulamayı yükleme ve kullanma hususundaki iradelerinin oluşumunda bir sakatlık oluşturduğunu savunmuştur.

Bu soruşturmada FTC, Brightest Flashlight uygulamasına ilişkin lisans sözleşmesini potansiyel kullanıcılar okuduğu esnada dahi söz konusu uygulamanın potansiyel kullanıcıların konum verisini toplamakta olduğuna, bu durumun da kullanıcıların uygulamayı yükleme ve kullanma iradesinin oluşumunda sakatlıklar oluşturduğunu, bu tarz esaslı hususlarda kullanıcıların aydınlatılmamasının aldatıcı bir yaklaşım oluşturduğuna temas etmiştir³¹.

Özetle bu soruşturmada uygulama geliştiricisinin kullanıcıların, konum verisini (tanıtıcı bir ID atayarak) reklam pazarlama ağları ile paylaşmasını ve bu verileri topladığını beyan etmemesi ve bu konuda potansiyel kullanıcılar dahil kullanıcılarını aydınlatmayı ihmal etmesinin aldatıcı bir yaklaşım oluşturduğunu FTC savunmuştur.

³⁰ 'FTC v. Goldenshores Technologies, LLC, and Erik M. Geidl' Docket No. C-4446' (n 11).

³¹ a.g.e.

Söz konusu bu soruşturmada Goldenshore'un herhangi bir ceza ödemesine hükmedilmemekle birlikte, kullanıcıların konum verisinin toplanmasından, kullanılmasından ve paylaşılmasından önce ilgili kişilerin açık rızalarının alınması FTC'nin tarafı olduğu sulhun bir gereğini oluşturmuştur. Bu bağlamda, konum verisinin toplanmasından önce uygulamanın konum verisini topladığı ve üçüncü kişilere aktardığı hususuna ilişkin kullanıcıların açık rızasının lisans sözleşmesi, gizlilik politikası, kullanım koşulları gibi düzenlemelerden farklı bir ekran görüntüsü içerisinde alınması gerektiği FTC ile yapılan sulhun bir koşulu olarak yer almıştır. Buna ilaveten kullanıcıların konum verisinin toplandığına, konum verisinin nasıl kullanılacağına, neden konum verisinin toplandığına ve ayrıca konum verisinin paylaşılacağı üçüncü kişilerin kimlik detaylarına ilişkin olarak kullanıcıların bilgilendirilmesi gerektiği de taraflar arasındaki sulhun bir hükmünü teşkil etmiştir.

2. Kochava Inc. Soruşturması

FTC, Kochava Inc aleyhine milyonlarca mobil cihazdan konum verisinin toplanması ve bu verinin pazarlanması ile ilgili olarak, bu faaliyetin durdurulması ve cezalandırılmasına karar verilmesini konu alan bir davayı bir soruşturma konusu yaparak ilgili mahkemede açmıştır³². FTC, bu soruşturma ile Kochava Inc. tarafından tüketicilerin konum verilerinin toplanması ve bilhassa sağlık ve tedavi kuruluşlarının bulunduğu lokasyonlar gibi bir takım hassasiyet taşıyan yerler hedeflenerek konum verilerinin toplanmasının ve paylaşılmasının durdurulmasına ilişkin olarak ilgili yargısal süreci başlatmıştır³³.

FTC'nin dava konusu yaptığı bu olayda tüketicilerden toplanan ve üçüncü kişilere satışı gerçekleştirilen verileri cihazın kimliği (*device ID*), cihazın bulunduğu konum ve bulunma zamanı oluşturmaktadır. Bu bağlamda, Kochava Inc. tarafından mobil cihazın bulunduğu konum, zaman ve cihazın kimliği (*device ID*) eşleştirilerek bir mobil pazarlama kimliği ilgili kul-

³² 'FTC v Kochava, Inc. Docket No. 2:22-Cv-377' (n 11).

³³ Federal Trade Commission, 'FTC Sues Kochava for Selling Data That Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations' <<https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-oth>> s.e.t. 21 Mart 2023.

lanıcıya tanımlanmaktadır (“MAID”)³⁴. Kochava Inc. topladığı bu konum verisini, mobil pazarlama kimliği ile kendi platformu üzerinden üçüncü kişilere pazarlamaktadır. Bu bağlamda, Kochava’nın ayda yaklaşık 94 milyar konum verisi işlediği ifade edilmektedir³⁵.

Bu davada FTC, konum verisiyle mobil pazarlama kimliğinin eşleştirilmesi suretiyle ilgili kişilerin kimlik bilgileri, yerleşim yeri bilgileri gibi birtakım verilere ulaşılabilmesinin mümkün olduğunu ifade etmiş; bu durumun da tüketicilerin ve bireylerin mahremiyetinin istismar edilebilmesine imkân tanıdığının altını çizmiştir. Nitekim bir araştırmaya göre anonimleştirilmiş konum verisinin analizi suretiyle ilgili kişinin kimliği %95 başarı ile tespit edilebilmektedir³⁶.

FTC bu soruşturmada, kişilerin sağlık kuruluşları, ibadet kurumları gibi birtakım hassasiyetleri bünyesinde barındıran lokasyonlarda bulunma zamanı ve sıklığına dair verilerin Kochava Inc. tarafından toplanıyor olmasını bilhassa değerlendirmeye değer bulmuştur³⁷. Özellikle konum verisi marifetiyle bir takım hassas yerlerde bulunulmasının ölçülmesi suretiyle bir profillemeye çalışması ortaya koymak mümkün olmaktadır³⁸. İlgili davada FTC, sağlık kuruluşları, ibadethaneler, sığınma evleri, psikolojik destek mekanlarının hassas lokasyonlar olduğunu, bu tarz yerlerde bulunmanın hassas verilerin tespit ve çıkarılmasına olanak tanıdığını belirtmiştir.

³⁴ Yapılan bir araştırmaya göre 101 tane oldukça yaygın kullanılan ve talep gören uygulamanın 56 tanesinin cihazın kimliğini (Device ID) ve 47 tanesinin konum verisini topladığını ve üçüncü kişilere aktardığı ifade edilmiştir.

Scott Thurm and Yukari Kane, ‘Your Apps Are Watching You’ *The Wall Street Journal* (2010).

³⁵ Lesley Fair, ‘FTC Says Data Broker Sold Consumers’ Precise Geolocation, Including Presence at Sensitive Healthcare Facilities’ <<https://www.ftc.gov/business-guidance/blog/2022/08/ftc-says-data-broker-sold-consumers-precise-geolocation-including-presence-sensitive-healthcare>> s.e.t 13 Mart 2023; Adam Schwartz, ‘FTC Sues Location Data Broker’ <<https://www.eff.org/deeplinks/2022/09/ftc-sues-location-data-broker>> s.e.t. 3 Nisan 2023.

³⁶ Sweeney, ‘K-Anonymity: A Model for Protecting Privacy’ 558; Kulesza (n 4) 166.

³⁷ **Federal Trade Commission**, FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations <<https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other>> s.e.t. 21 Mart 2023.

³⁸ Kulesza (n 4) 165.

FTC, söz konusu bu verilerin üçüncü kişilere pazarlanmasını tüketicilerinin mahremiyetine hukuka aykırı bir müdahale olarak değerlendirmiştir.

Kochava soruşturmasında konum verisinin üçüncü kişilere pazarlanması hususunda konum verisine bu platform üzerinden erişimi olan üçüncü kişiler bakımından herhangi bir kontrolünün bulunmaması da FTC’nin getirmiş olduğu önemli bir eleştiriyi oluşturmuştur. Öte taraftan, tüketicilerin konum verisinin kimler tarafından toplandığını ve ne maksatla kullanıldığını bilmediği için tüketicilerin mahremiyetlerine sessiz bir müdahale olduğunun da altı çizilmiştir. Bu bağlamda, bilhassa Kochava tarafından toplanan konum verilerinin tüketicilerin daha önce hiç duymadığı hiç temasa geçmediği kişi ve kurumlara pazarlanmasının bir yönü ile rahatsız edici bir gelişme olduğu belirtilmiştir. Zira konum verisini satın alan kurumlar, konum verisinin analizi suretiyle kişilerin bulunduğu lokasyonları, bu lokasyonlarda bulunma süre ve sıklığını analiz ederek, pazarlama faaliyetlerinin doğru kişiye ulaşmasını amaçlamakta; bu bağlamda, tüketiciler sessiz bir şekilde pazarlama faaliyetleri ile dijital ortamda kuşatılmaktadır.

FTC, Kochava yargılamasında, tüketicilerin konum verisinin ve bilhassa sağlık ve tedavi kuruluşlarının bulunduğu lokasyonlar gibi bir takım hassasiyet taşıyan yerler hedeflenerek konum verilerinin toplanmasının ve toplanan konum verilerinin 3. kişilere pazarlanması suretiyle tüketicilerin profillemeye çalışmasına konu edinilmesini ve veri öznelinin kimlik bilgilerinin konum verisi marifetiyle tespit edilmesine engel olan teknik tedbirlerin alınmamasını haksız ve aldatıcı uygulama teşkil ettiğini savuna gelmiş olup; hali hazırda ilgili yargılama devam etmektedir.

3. InMobi Soruşturması

InMobi davası reklamcılarının tüketicileri nasıl hedeflediklerini anlatan ve lokasyon bazlı dijital reklam ekosistemini en iyi şekilde takdim eden FTC soruşturmalarından bir tanesini oluşturmaktadır.

InMobi’nin platformu ile mobil cihazlarda yer alan uygulamalar üzerinden reklam verenlerin çeşitli formatlarda, örneğin, banner reklam, bir sayfadan diğer sayfaya geçerken ki reklamlar gibi reklamları yayınlaması söz konusu olabilmektedir. Bu platform

üzerinden reklam verenler, InMobi platformuna entegre olmuş uygulamaları kullanan tüketicileri dijital reklam faaliyetleri bakımından hedefleyebilmektedir. 2015 Şubat ayında InMobi yaklaşık bir milyar mobil cihaza ulaştığını ve bir günde yaklaşık ortalama altı milyar reklam talebine cevap verdiğini ifade etmiştir³⁹. Söz konusu bu rakamlar göz önünde tutulduğunda tüketicilerin dijital reklamların optimizasyon ve hedefleme faaliyetleri ile kuşatılmış olduğu şüpheden uzak olan bir husustur.

FTC'nin InMobi soruşturmasının daha iyi anlaşılabilmesi için InMobi platformunun dijital reklam verenlere ne tarz imkanlar sunduğunu anlamak önem taşımaktadır. InMobi platformu üzerinden reklam verenler konum bazlı olmak üzere üç farklı türde hedefleme yapabilmektedir. Bu bağlamda, "hedefleme" ifadesi ile kişilerin coğrafi konumuna göre dijital reklam çalışmalarının hedefi; bir başka anlamıyla, muhatabı olması kastedilmektedir.

InMobi platformunda "Şimdi" özelliği ile tüketicilerin o anda bulunduğu lokasyon hedeflenebilmektedir. InMobi platformu üzerinde reklam verenler tüketicilerin o anda bulunduğu lokasyonu -örneğin, bir oto galerisini - hedefleyebilmektedir. "Şartlı" seçeneğinin tercih edilmesi durumunda ise, örneğin belli bir zaman diliminde ziyaret veya belli bir zaman diliminde birden fazla ziyaret gibi koşullar seçilerek hedefleme yapılabilmesi söz konusu olabilmektedir. Örneğin, bir kahve dükkanının bulunduğu lokasyon sabah 07:00-10:00 arasında veya bu lokasyonda haftanın belli günleri yahut birden fazla kez bulunma koşulu gibi koşullarla hedefleme yapılabilir. "Psikografik" seçeneğinin tercih edilmesi durumunda ise iki aya kadar kişinin bulunduğu coğrafi lokasyonlar esas alınarak bir hedefleme yapılabilir. Örneğin, son iki ayda lüks semtlerde yaşayan ve lüks oto galerileri ziyaret eden kişiler hedeflenebilmektedir. Bu seçeneklerin de ortaya koyduğu üzere tüketicilerin bulunduğu lokasyon ve bulunma zaman dilimi esas alınmak suretiyle tüketici yaklaşım, ihtiyaç ve davranış modelleri hakkında fikir sahibi olmak oldukça gerçekçi ve rasyonel bir yaklaşımı oluşturmaktadır. Özetle InMobi'nin sunmuş olduğu hedefleme seçenekleri, şu anda belli bir lokasyonda bulunanlar veya belli

bir zaman diliminde belli bir lokasyonda bulunanlar olarak farklı seçenekler temin etmektedir.

Gerek IOS ve gerekse Android işletim sistemlerinde kişilerin konum verisine erişimi izne bağlanmaktadır⁴⁰. Mobil cihaz kullanıcıları bu izni vermediği müddetçe bu işletim sistemleri tabanlı uygulamaların kişilerin konum verisini InMobi platformu ile paylaşması mümkün ol(a)mamaktadır. Bununla birlikte, tüketicilerin mobil cihaz uygulamalarında konum verisine erişimi kısıtlamasına rağmen, mobil cihazların çevrelerindeki WIFI ağları ile temasları ile tüketicilerin konum verisini InMobi toplayabilmektedir⁴¹.

2015 sonuna doğru InMobi uygulamasında değişiklikler yaptığından artık, WIFI ağları vasıtasıyla mobil cihaz kullanıcılarına ait konum verisini toplaması mümkün ol(a)mamaktadır⁴². Bu bağlamda, FTC özellikle, InMobi'nin tüketicilerin lokasyonlarının mahremiyetinin korunması hakkında aydınlatılmış bir karar veremediklerini ve InMobi platformuna entegre olmuş yüzlerce uygulama vasıtasıyla tüketicilerin konumuna dair bilgi toplan(ma)ması hakkında bir kontrollerinin olmamasının hukuki olmadığını savunagelmıştır⁴³. Bu soruşturmada konularının mahremiyeti hakkında gereken hassasiyeti gösterdiğine inandıkları uygulamaları yüklediklerini düşünen tüketicilerin mahremiyetlerinin InMobi uygulaması marifetiyle istismar edilmesi, FTC'nin temel argümanlarından bir tanesini oluşturmuştur.

a. InMobi Kararında Önemle Üzerinde Durulan Bir Hassasiyet: Çocukların Çevrimiçi Mahremiyeti

InMobi uygulaması marifetiyle çocuklara dair konum verisi toplanmış ve bu süreçte bu konuda

³⁹ 'FTC v. InMobi Pte Ltd. Docket No. 3:16-Cv-3474' (n 11).

⁴⁰ Apple (n 14); 'Your Android Privacy on Your Terms' <<https://www.android.com/safety/privacy/>> s.e.t 12 December 2023.

⁴¹ 'FTC v. InMobi Pte Ltd. Docket No. 3:16-Cv-3474' (n 11).

⁴² Federal Trade Commission, 'Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission' <<https://www.ftc.gov/news-events/news/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked-hundreds-millions-consumers>> s.e.t. 12 Aralık 2023; 'FTC v. InMobi Pte Ltd. Docket No. 3:16-Cv-3474' (n 11).

⁴³ 'FTC v. InMobi Pte Ltd. Docket No. 3:16-Cv-3474' (n 11).

özel bir düzenleme olan Çocukların Çevrimiçi Mahremiyetinin Korunmasına Dair Kurallar (*Children's Online Privacy Protection Rule*) ihlal edilmiştir⁴⁴. Bu bağlamda, InMobi, çocukların konum verisini toplayarak onların ilgi ve davranışlarına uygun reklamların hedef kitlesi haline gelmesini temin etmiştir.

InMobi kararındaki göze çarpan başlıca hukuka aykırılık, InMobi'nin o dönemdeki politikasında, 13 yaşından küçük çocuklara ilişkin olarak bilgileri dahilinde olmaksızın herhangi bir verinin InMobi tarafından toplanmadığı ve böyle bir verinin toplanmasının öğrenilmesinden itibaren derhal silindiği kuralına yer verilmesine rağmen; InMobi platformuna entegre olan uygulamalar vasıtasıyla milyonlarca çocuğun verisini yukarıda atfı geçen COPPR kurallarına aykırı olarak toplamış ve bu uygulamalar vasıtasıyla üçüncü kişilerle paylaşmıştır. Bu bağlamda FTC, çocuklara ilişkin verilerin toplanması bakımından InMobi'nin aydınlatma metninin açıkça ve yeterince bilgi sunmadığını ve verilerin toplanmasından önce çocuğun velilerinin aydınlatılmadığını ve rızalarının alınmasının söz konusu olmadığını, dolayısıyla, bu yaklaşımın da COPPR kuralını ihlal ettiğini savunmuştur.

InMobi 2015 yılına kadar rıza olmaksızın konum verisi toplamadığını beyan etmesine rağmen, esasında WIFI networkleri vasıtasıyla konum verisini toplamakta; bu minvalde haksız ve aldatıcı uygulamalarda bulunmaktadır. InMobi ve FTC söz konusu bu davayı sulh ile çözüme kavuşturmuş olup, InMobi yaklaşık 4 Milyon Amerikan Doları sulh tutarını ödemeyi kabul etmiş, ayrıca InMobi'nin çocuklara ilişkin verilerin toplanmasında velilerin rızasının alınmasına ilişkin uygun bir mekanizma oluşturması, velilerin toplanan verilerin türünü takip edip silebilmesine olanak tanıyan bir mekanizma oluşturması, FTC ile taraf olunan sulhun bir gereği olarak hüküm altına alınmıştır. Ayrıca sulhun gereği olarak konum verisinin toplanmasından önce kullanıcıların açık rızasının alınması gerektiği ve kişisel verilerin korunması için detaylı bir uyum ve raporlama mekanizmasının tesisi ve daha önce toplanan ve sulh sözleşmesinde öngörülen standartları taşımayan tüm konum verilerinin silinmesi de FTC ile yapılan sulhun bir gereği olarak öngörülmüştür.

⁴⁴ Çocukların Çevrimiçi Mahremiyetinin Korunmasına İlişkin Yasa (Children's Online Privacy Protection Act) çevrimiçi ortamda çocuklara ait verilerin ve bizatihi çocukların korunmasını düzenlemektedir. 'Children's Online Privacy Protection Act' (n 8).

IV. AVRUPA BİRLİĞİ'NDE VE ÜLKEMİZDE KONUM VERİSİNİN KORUNMASINA İLİŞKİN GELİŞMELER

A. AVRUPA BİRLİĞİ'NDE KONUM VERİSİNİN MAHREMİYETİNİN KORUNMASI HAKKINDA GELİŞMELER

13/2011 sayılı akıllı cihazlarda coğrafi konum hizmetleri ve 2/2013 sayılı akıllı cihazlarda uygulamalara ilişkin Avrupa Veri Koruma Kurulu'nun görüşleri 95/46/EC sayılı Veri Korumasına İlişkin Direktif döneminde yayınlanmış olsa da bugün hala geçerliliğini muhafaza etmektedir. Bu bağlamda, 13/2011 sayılı görüşte, akıllı cihazların ilgilisi ile yoğun bir şekilde ilişkili ve ilintili olduğu ve bu cihazların ortaya koyduğu konum verilerinin de kişisel veriler olarak nitelendirilmesi gerektiği belirtilmiştir. Nitekim, bu istikamette olmak üzere Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), açık bir şekilde konum verisini kişisel veri kategorisi içerisinde değerlendirmektedir. Bu baskın eğilime paralel olarak, Avrupa İnsan Hakları Mahkemesi de GPS cihazı ile kişilerin bulunduğu konuma ilişkin bilgilerin toplanmasını kişisel verilerin toplanması olarak nitelendirmiş⁴⁵.

Nitekim coğrafi konum hizmeti sağlayıcıları, kullanıcılarının alışkanlıkları ve tutumları hakkında oldukça detaylı bir profil oluşturma kabiliyetine sahip olmaktadır. Öte yandan, yukarıda da ifade edildiği üzere konum verisi marifetiyle hassas kişisel verilere ulaşmak da mümkündür. Örneğin, konum verileri hastanelere veya ibadet yerlerine yapılan ziyaretleri açıkça ortaya koyabilmektedir. Nitekim, konum verisi, E-Mahremiyet Direktifi (E-Privacy Directive) madde 2(c)'de "*halka açık elektronik iletişim hizmeti kullanıcısının coğrafi konumunu gösteren elektronik iletişim ağlarında işlenen herhangi bir veri*" olarak tanımlanmış olup, E-Mahremiyet Direktifi'nin Giriş Kısmınının 14'üncü maddesi de konum verisini kullanıcının enlem, boylam ve rakım bilgisini ortaya koyan, kullanıcının belli bir zaman diliminde nerede olduğunu ortaya koyan veri olarak tanımlamaktadır⁴⁶.

⁴⁵ *Uzun v Germany* AİHM 35623/05; *Florindo de Almeida Vasconcelos Gramaxo v Portugal* AİHM 26968/16.

⁴⁶ 'Mahremiyet ve Elektronik İletişim Direktifi' <<https://eur-lex.europa.eu/legalcontent/EN/ALL/?uri=CELEX%3A32002L0058>> s.e.t. 24 August 2023.

Amerika Birleşik Devletleri'nden farklı olarak Avrupa Birliği mevzuatı, konum verisini genel çerçevede düzenleme altına almakta, bu verinin işlenmesi, toplanması ve paylaşılmasını diğer kişisel verilerin korunmasında olduğu gibi düzenlemeye tabi tutmakta; bu bağlamda, konum verisinin toplanmasında ve işlenmesinde ilgili kişinin açık rızasının alınması merkez düzenlemeyi oluşturmaktadır.

B. ÜLKEMİZDE KONUM VERİSİNİN MAHREMİYETİNİN KORUNMASI BAKIMINDAN GELİŞMELER

Kişisel Verilerin Korunması Kanunu (KVKK) çerçevesinde konum verisi bir kişisel veri olarak değerlendirilebilir. Zira konum verisi marifetiyle kimliği belirlenebilir bir gerçek kişiye ulaşılması mümkün olabilmektedir. Özellikle konum verisi sayesinde ilgili kişinin kim olduğunun doğrudan anlaşılması, fakat başka verilerle birleştirilince ilgili kişinin tam kimliğinin saptanabildiği durumlarda, ilgili kişinin dolaylı olarak belirlenebilir olmasından söz edilebilecektir⁴⁷.

İnternet arama motorlarında yer alan adres bilgisi ile konum verisinin tamamlanarak ilgili kişinin kim olduğunun tespiti mümkün olabilir. Tüm bu bilgiler ışığı altında soyut konum verisinin bir takım civar verilerle eşleştirilerek tamamlanması pratik olarak mümkün olabilmektedir. Öte taraftan ifade etmek gerekir ki, ilgili kişinin dolaylı olarak belirlenebilir olması ile mutlaka o kişinin ismen belirlenmesi tarzında dar bir çerçeveden konunun ele alınması da icap etmemektedir. Nitekim, özel bir düzenleme olan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelikte konum verisi "*Kamuya açık elektronik haberleşme hizmeti kullanıcılarına ait bir cihazın coğrafi konumunu belirleyen ve elektronik haberleşme şebekesinde veya elektronik haberleşme*

hizmeti aracılığıyla işlenen belirli veri" olarak tanımlanmaktadır. Ülkemizde konum verisinin mobil cihazlarda yer alan uygulamalar ile toplanabilmesi ve toplanan bu kişisel verilerin işlenebilmesi için hukuksal bir temelin bulunması zorunludur. Bu bağlamda, mobil cihazlarda yer alan uygulamalar düzleminde konum verisinin toplanabilmesi ve işlenebilmesi için ilgili kişinin açık rızasının elde edilmesi önem taşımaktadır. Nitekim, Covid-19 dönemlerin Kişisel Verileri Koruma Kurulu yayınlamış olduğu bir duyuruda konum verisini kişisel veri olarak nitelendirmiş olup; konum verisinin Covid-19'un sebebiyet verdiği salgın hastalığın kamu güvenliğini ve kamu düzenini tehdit etmesi sebebiyle hastalığın yayılımını engellemek amacıyla KVKK madde 18/1(ç) hükmü kapsamına giren kamu kurum ve kuruluşları tarafından işlenmesinin önünde bir engel bulunmadığını ifade etmiştir⁴⁸.

Konum verisinin toplanmasında, işlenmesinde ve saklanmasında saydamlık ve şeffaflık oldukça önem taşımaktadır. Özellikle reklam verenlerin dijital reklam faaliyetlerinin doğru hedefe ulaşması ile kişilerin mahremiyetinin korunması arasında adilane bir dengenin kurulması, bu denge kurulurken de ilgili kişilerin konum verisinin toplanmasında, işlenmesinde ve üçüncü kişilere aktarılmasında aydınlatılmış bir irade ile açık rızalarının alınması mevzuata uygun bir yaklaşımı oluşturacaktır⁴⁹. Uygulamalar vasıtasıyla konum verisinin toplanması ve dijital reklam faaliyetleri için işlenmesi bakımından, ilgili

⁴⁷ Volkan Dülger, *Kişisel Verilerin Korunması Hukuku*, (3rd Baskı, İstanbul Hukuk Akademisi 2020) 159; Dr Elif Beyza Akkanat Öztürk, *Karşı Edim Olarak Kişisel Veriler* (On İki Levha Yayıncılık 2022) 53; Şehriban İpek Aşkoğlu, *Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri* (On İki Levha Yayıncılık 2018) 109; Çiğdem Ayözger-Öngün, *Kişisel Verilerin Korunması Hukuku* (2.baskı, Beta) 9; Serdar Çelikel, *Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri* (Seçkin 2022) 69; Nilgün Başalp, *Kişisel Verilerin Korunması ve Saklanması* (Yetkin 2004) 33; Elif Küzeci, *Kişisel Verilerin Korunması* (2. Baskı, Turhan Kitabevi 2018) 320.

⁴⁸ Kişisel Verileri Koruma Kurulu, 'Kamuoyu Duyurusu Covid-19 İle Mücadelede Konum Verisinin İşlenmesi ve Kişilerin Hareketliklerinin İzlenmesi Hakkında Bilinmesi Gerekenler' <<https://www.kvkk.gov.tr/Icerik/6726/Covid-19-ile-Mucadelede-Konum-Verisinin-Islenmesi-ve-Kisilerin-Hareketliklerinin-Izlenmesi-Hakkinda-Bilinmesi-Gerekenler-2->> s.e.t 15 Eylül 2023.

⁴⁹ Nitekim, benzer hassasiyetler bir tüketim ürününü piyasaya süren kişilerin ürün ömrünü kasten kısaltmak üzere kullandıkları her türlü teknik olarak planlı eskitme uygulaması bakımından da dile getirilebilir. Bu bağlamda, tüketicilerin iradesinin sağlıklı bir şekilde oluşabilmesi için tüketicilerin yeterli ve olması gerektiği içerikte bilgilendirilmesi oldukça önem taşımaktadır. Bu konuda salt tüketicilerin aydınlatılması ile yetinilmemeli, aynı zamanda tüketicilerin bilinçlendirilmesi ile ilgili çalışmalara önem verilerek firmaların tüketicileri olumsuz yönde etkileyen ulusal ve uluslararası düzeydeki tüm kötü niyetli iş uygulamalarının engellenmesi temin edilmesi gerektiği ifade edilmiştir. İbrahim Kulular and Merve Ayşegül, 'Psikolojik Planlı Eskitme ve Covid 19 Pandemisinde Durum' (2021) 2 Türkiye Adalet Akademisi Dergisi 391, 397.

kişilerin açık rızasının alınması gerektiği kuralına veri sorumlusunun meşru menfaatinin bulunduğu gerekçesiyle (KVKK m.5/2.f) bir istisna tanınması da adilane bir yaklaşımı oluşturmayacaktır. Nitekim bu yaklaşımın bir sonucu olarak da Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunmasına İlişkin Yönetmelik madde 8/1(c) ve madde 9 konum verisinin işlenmesi öncesinde işleme amaç ve süresi hakkında bilgilendirme yükümlülüğü getirdiği gibi ilgisinden açık rıza temin edilmesi yükümlülüğünü de öngörmüştür.

V. SONUÇ

Teknolojinin hızlı gelişimi kimi zaman hukukun bir takım konuları ele almasında bir takım komplikasyonları da gündeme getirmiştir. Mobil cihazlarla konum verisinin işlenmesinde, ülkeler düzleminde kişisel verilerin korunması mevzuatı önemli bir rol oynadığı kadar, işletim sistemlerinin (IOS, Android vb.) de bu konudaki tavır ve yaklaşımı oldukça büyük öneme sahiptir. Bu bağlamda, işletim sistemlerinin uygulamaların yüklenmesinde sunmuş olduğu politikalarda, tasarımda mahremiyet prensibine önem atfederek sorunun kaynakta çözülmesine olanak tanınması, konum verisinin toplanması ve işlenmesinde ilgili kişilerin açık rızasının alınmasını araması önem taşımaktadır. Diğer yandan, konum verisinin yardımı ile kişilerin anlık bulunduğu lokasyonların, dijital reklam çalışmaları bakımından hedeflenebilmesi amacıyla konum verisinin toplanmasında ve işlenmesinde meşru menfaat bulunduğu savı ile açık rıza gereğinden taviz verilmesi kişilerin mahremiyetine makul olmayan bir müdahaleyi oluşturacaktır.

KAYNAKÇA

- Akkanat Öztürk DrEB, *Karşı Edim Olarak Kişisel Veriler* (On İki Levha Yayıncılık 2022).
- Anandarajan M, D'Ovidio R and Alexander J, 'Safeguarding Consumers against Identity-Related Fraud: Examining Data Breach Notification Legislation Through the Lens of Routine Activities Theory' (2013) 1 International Data Privacy Law.
- Apple I, 'About Privacy and Location Services in iOS, iPadOS, and watchOS' <<https://support.apple.com/en-us/102515>> s.e.t. 12 Aralık 2023.
- Aşıkoğlu Şİ, *Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri* (On İki Levha Yayıncılık 2018).
- Ayözger-Öngün Ç, *Kişisel Verilerin Korunması Hukuku* (2nd Baskı, Beta).
- Başalp N, *Kişisel Verilerin Korunması ve Saklanması* (Yetkin 2004).
- Blumberg A and Eckersley P, 'On Locational Privacy, and How to Avoid Losing It Forever' <<https://www.eff.org/files/eff-locational-privacy.pdf>> s.e.t. 3 Nisan 2023.
- Brill J, 'The Intersection of Privacy and Consumer Protection', *The Cambridge Handbook of Consumer Privacy* (Cambridge University Press).
- Bygrave LA, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' Oslo Law Review' (2017) 2 Oslo Law Review 105.
- Çelikel S, *Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri* (Seçkin 2022).
- 'Children's Online Privacy Protection Act' <<http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim>> s.e.t. 17 Mart 2023.
- Cottrill, CD and Thakuriah, PV, 'Privacy in Context: An Evaluation of Policy-Based Approaches to Location Privacy Protection' (2014) 2.
- Dülger V, *Kişisel Verilerin Korunması Hukuku*, (3rd Baskı, İstanbul Hukuk Akademisi 2020).
- European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0' <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf> s.e.t. 19 Mart 2023.
- 'Fair Credit Reporting Act' <<https://www.ftc.gov/legallibrary/browse/statutes/fair-credit-reporting-act>>.
- Fair L, 'FTC Says Data Broker Sold Consumers' Precise Geolocation, Including Presence at Sensitive Healthcare Facilities' <<https://www.ftc.gov/business-guidance/blog/2022/08/ftc-says-data-broker-sold-consumers-precise-geolocation-including-presence-sensitive-healthcare>> s.e.t. 13 Mart 2023.
- Federal Trade Commission, 'FTC Sues Kochava for Selling Data That Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations' <<https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-oth>> s.e.t. 21 Mart 2023.
- , 'Marketing Your Mobile App'.
- , 'Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission' <<https://www.ftc.gov/news-events/news/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked-hundreds-millions-consumers>> s.e.t. 12 Aralık 2023.
- , 'Protecting Consumer Privacy in an Era of Rapid Change' <<https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policy-makers>> s.e.t. 10 Mart 2023.
- Fong A, 'The Role of App Intermediaries in Protecting Data Privacy' 2 International Journal of Law and Information Technology 85.
- 'FTC v. Facebook Inc. Docket No: 0913284' <<https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf>> s.e.t. 17 Mart 2023.
- 'FTC v. Goldenshores Technologies, LLC, and Erik M. Geidl Docket No. C-4446' <<https://www.ftc.gov/system/files/documents/cases/140409goldenshorescmpt.pdf>> s.e.t. 17 Mart 2023.
- 'FTC v. Google Inc. Docket No: C-4336' <<https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf>> s.e.t. 17 Mart 2023.
- 'FTC v. InMobi Pte Ltd. Docket No. 3:16-Cv-3474' <<https://www.ftc.gov/system/files/documents/cases/160622inmobicmpt.pdf>> s.e.t. 17 Mart 2023.
- 'FTC v Kochava, Inc. Docket No. 2:22-Cv-377' <https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf>.
- 'Gramm Leach Bliley Act' <<https://www.congress.gov/bill/106thcongress/senate-bill/900/text>> s.e.t. 4 Nisan 2023.
- 'Health Insurance Portability and Accountability Act', <<https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996>> s.e.t. 5 Nisan 2023.

- Jasmontaite Lina and others, 'Data Protection by Design and by Default' (2018) 2 *European Data Protection Law Review*.
- Keser- Berber L, *Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması* (On İki Levha Yayıncılık 2014).
- Kirsten M and Shilton K, 'Mobile Privacy Expectations: How Privacy is Respected with Mobile Devices', *The Cambridge Handbook of Consumer Privacy* (1st Baskı, Cambridge University Press 2018).
- Kişisel Verileri Koruma Kurulu, 'Kamuoyu Duyurusu Covid-19 İle Mücadelede Konum Verisinin İşlenmesi ve Kişilerin Hareketliklerinin İzlenmesi Hakkında Bilinmesi Gerekenler' <<https://www.kvkk.gov.tr/Icerik/6726/Covid-19-ile-Mucadelede-Konum-Verisinin-Işlenmesi-ve-Kisilerin-Hareketliklerinin-Izlenmesi-Hakkında-Bilinmesi-Gerekenler-2->> s.e.t. 15 September 2023.
- Kulesza J, 'International Law Challenges to Location Privacy Protection' [2013] *International Data Privacy Law* 158.
- Kulular İ and Aşşegül M, 'Psikolojik Planlı Eskitme ve Covid 19 Pandemisinde Durum' (2021) 2 *Türkiye Adalet Akademisi Dergisi* 391.
- Küzeci E, *Kişisel Verilerin Korunması* (2nd Baskı, Turhan Kitabevi 2018).
- Lipman R, 'Online Privacy and the Invisible Market for Our Data' (2016) 3 777.
- 'Mahremiyet ve Elektronik İletişim Direktifi' <--> <<https://eur-lex.europa.eu/legalcontent/EN/ALL/?uri=CELEX%3A32002L0058>> s.e.t. 24 August 2023.
- Mantelero, A and others, 'The Common EU Approach to Personal Data and Cybersecurity Regulation' (2020) 4 *International Journal of Law and Information Technology*.
- Mesut, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku* (3rd Baskı, On İki Levha Yayıncılık 2020).
- Métayer DL, 'Privacy by Design: A Matter of Choice', *Data Protection in a Profiled World* (1st Baskı, Springer Dordrecht).
- Naher N and Hashem T, 'Think Ahead: Enabling Continuous Sharing of Location Data in Real-Time with Privacy Guarantee' (2019) 1 1.
- Organization for Economic Co-operation and Development, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Publishing, Paris' <<https://doi.org/10.1787/9789264196391-en>> s.e.t. 1 Nisan 2023.
- Parlak, MO, 'Yeni Medya ve Haberciliğin Dönüşümü' (2018) 14 *Ufuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* 59.
- Rachovitsa A, 'Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue' (2016) 4 *International Journal of Law and Information Technology*.
- Raphaël G, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 *International Data Privacy Law*.
- Rubinstein I, 'Big Data: The End of Privacy or a New Beginning?' (2013) 2 *International Data Privacy* 74.
- Schwartz A, 'FTC Sues Location Data Broker' <<https://www.eff.org/deeplinks/2022/09/ftc-sues-location-data-broker>> s.e.t. 3 Nisan 2023.
- Sweeney, 'K-Anonymity: A Model for Protecting Privacy' 'Telemarketing Sales Rule' <<https://www.federalregister.gov/regulations/3084-AA98/telemarketing-sales-rule>> s.e.t. 17 Mart 2023.
- Thurm S and Kane Y, 'Your Apps Are Watching You' *The Wall Street Journal* (2010).
- Tressler C, 'Mobile Phone Maker Mised People on Privacy & Security' <<https://consumer.ftc.gov/consumer-alerts/2018/04/mobile-phone-maker-mised-people-privacy-security>> s.e.t. 27 Mart 2023.
- Wall Street Journal, 'Should the U.S. Adopt European-Style Data-Privacy Protections' (8 Mart 2013) <<https://www.wsj.com/articles/SB10001424127887324338604578328393797127094>> s.e.t. 31 Mart 2023.
- World Economic Forum, 'Rethinking Personal Data: A New Lens for Strengthening Trust' <https://www3.weforum.org/docs/WEF_RethinkingPersonalDataANewLens_Report_2014.pdf>.
- World Economic Forum and Bain Company, 'Personal Data: The Emergence of a New Asset Class' <https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf> s.e.t. 3 Mart 2023.
- 'Your Android Privacy on Your Terms' <<https://www.android.com/safety/privacy/>> s.e.t. 12 Aralık 2023.
- <<https://www.apple.com/legal/privacy/pdfs/apple-privacy-policy-en-ww.pdf>> s.e.t. 27 Mart 2023.
- Florindo de Almeida Vasconcelos *Gramaxo v Portugal* AİHM 26968/16.
- Uzun v Germany* AİHM 35623/05.

Etik Beyanı: Bu çalışmanın hazırlanma sürecinde etik kurallara uyulduğunu yazar beyan etmektedir. Aksi bir durumun tespiti halinde Ticaret ve Fikri Mülkiyet Hukuku Dergisi (TFM) hiçbir sorumluluğu kabul etmemektedir. Sorumluluk, çalışmanın yazarına aittir.

Katkı Oranı Beyanı: Söz konusu çalışmanın hazırlanması ve yazımı aşamasında yazarın katkı oranı %100'dür.

Varsa Destek ve Teşekkür Beyanı: Yoktur.

Çatışma Beyanı: Yoktur.

Ethics Statement: *The author declares that ethical rules are followed in all preparation processes of this study. In case of detection of a contrary situation, TFM does not have any responsibility and all responsibility belongs to the author of the study.*

Contributions Statement: *Author has contributed %100 into preparing and writing this study.*

Statement for Support and Appreciation If Any: *None.*

Statement for Conflict of Interest: *None.*