KVKK KİŞİSEL VERİLERİ KORUMA KURUMU
www.kvkk.gov.tr

Kişisel Verileri Koruma Dergisi

Cilt: 3 Sayı: 1

Geliş:25.05.2021
Kabul:21.06.2021

AB ve Türk Hukuklarında Çerezler: Kişisel Verilerin Korunması Açısından Karşılaştırmalı Bir Değerlendirme

Hüseyin Can, Aksoy
Bilkent Üniversitesi Hukuk Fakültesi Medeni Hukuk Ana Bilim Dalı,Ankara, Türkiye, hcaksoy@bilkent.edu.tr
ORCID: https:// orcid.org/0000-0002-9243-189X

Mesut, Halıcıoğlu
LL.M., KU Leuven,Leuven, Belgium, mesuthalicioglu@gmail.com
ORCID: https:// orcid.org/0000-0002-1503-0339

ÖZ
Çerezler, Avrupa Birliği'nde 2002/58/EC sayılı Direktif (E-Gizlilik Directifi) ile özel olarak düzenlenmektedir. Ancak, teknojik gelişme ve modern ihtiyaçlara cevap veremeyen bu düzenlemenin yakın bir gelecekte yerini E-Gizlilik Tüzüğüne bırakması beklenmektedir. E-Gizlilik Tüzüğü, Genel Veri Koruma Tüzüğü'nün elektronik haberleşme sektöründeki yansıması ve parçası olarak hazırlanmış olup, Tüzük kapsamında öne çıkan konulardan başlıca bir tanesi ise çerez uygulamalarıdır. AB hukukundan farklı olarak, Türk hukukunda tüm çerez uygulamaları bakımından doğrudan doğruya uygulanabilir bir düzenleme bulunmadığından, çerezlerin tabi olduğu kurallara ilişkin bir belirsizlik söz konusudur. Bu bağlamda, Türk hukuku çerez düzenlemeleri bakımından AB mevzuatının gerisinde kalmakta, güncel ihtiyaçlara yanıt verememekte ve sektörün beklentilerini karşılayamamaktadır. 6698 sayılı Kişisel Verilerin Korunması Kanunu da münhasıran çerezlerin tabi olacağı hukuki rejimi düzenlemek amacıyla kaleme alınmadığından, güncel soru ve ihtiyaçlara yanıt verememektedir. Dijital çağın gereklerini yakalayabilmek ve AB ile sürdürülebilir bir ekonomik ve politik ilişki kurabilmek için, Türk hukukunun AB mevzuatı ve teknolojik gelişmelerle uyumlu hale getirilmesi gerekmektedir.
Anahtar Sözcükler: Kişisel Verilerin Korunması, Elektronik Haberleşme, GDPR, Gizlilik, Çerez

Cookies in EU and Turkish Law: A Comparative Review with respect to Data Protection

ABSTRACT
In the European Union, cookies have been specifically regulated under 2002/58/EC (E-Privacy Directive). However, such Directive fails to reflect technological advancements and to answer modern needs. Therefore, it is expected to be replaced by the E-Privacy Regulation soon. E-Privacy Regulation is an extension of the General Data Protection Regulation in the field of electonic communications sector and one of the main subjects that stands out within the Regulation is cookies. Unlike EU law, in Turkish law, there is no direct regulation applicable to all cookies and this causes uncertainty with respect to the applicable rules. In this regard, Turkish law falls behind EU standards in terms of cookie regulations and currently Turkish law is unable to respond to current needs and to meet the expectations of the market. Personal Data Protection Law No. 6698 is also unable to answer current problems as it has not prepared to exclusively legislate cookies. To catch up with the needs of the digital era and establish sustainable relations with European Union, Turkish law must be revised in accordance with the EU law and the latest technological advancement.
Keywords: Data Protection, Electronic Communication, GDPR, Privacy, Cookies

Atıf Gösterme	Aksoy, H. C. ve Halıcıoğlu, M. (YYYY). AB ve Türk Hukuklarında Çerezler, *Kişisel Verileri Koruma Dergisi. 3*(1), ss-ss. DOI:

GİRİŞ

Avrupa Birliği'ndeki Dijital Tek Pazar Stratejisi kapsamında, 2018 senesinde "Genel Veri Koruma Tüzüğü" (GVKT) yürürlüğe girmiştir (Avrupa Komisyonu, 2015). İlgili düzenleme, kişisel verilerin korunması bakımından bir reform niteliği taşımaktadır. Bu reformun elektronik haberleşme sektörünü düzenleyen parçası "E-Gizlilik Tüzüğü'dür ("Tüzük")[1]. Tüzük, telekomünikasyon alanında gizliliği sağlama amacı taşıyan 2002 tarihli E-Gizlilik Direktifi'nin (Direktif) çarpan etkisiyle artan dijitalleşme karşısında bu gelişmelere ayak uyduramaması ve yeterli korumanın Direktif aracılığıyla tam olarak sağlanamaması sebebiyle, ilk olarak 2017 yılının Ocak ayında taslak olarak yayınlanmıştır. Tüzük henüz nihai halini almamış ve yürürlüğe girmemiş olmakla birlikte, Tüzük kapsamında öne çıkan konulardan başlıca bir tanesi çerez uygulamalarıdır.

Günümüzde, çerezlerin, veri sahiplerinin gizliliğini ihlal etme riski taşıdıkları tereddütsüz şekilde kabul edilmektedir. Zira, kullanıcılar bilgisayarlarında çok sayıda ve çeşitte kişisel verilerini depolamaktadırlar. Bununla birlikte, çerezleri, gizlilik konusunda potansiyel olarak tehlikeli kılan husus kullanıcının bilgisayarında depolanan bilgiler değildir. Bu konudaki tehlike, söz konusu bilgilere çerezler aracılığıyla erişebilme imkanı olan kurum ve kuruluşların, bu bilgileri nasıl ve ne amaçla kullanacaklarıdır (Edenberg ve Jones, 2019, s. 1805; Jones, 2020, ss. 89-90). Öyle ki, şirketler, çerez teknolojilerini kullanarak kullanıcıların kişisel bilgilerini elde edebilmekte ve bu bilgiler ile kullanıcıları tanımlayan dijital profiller oluşturabilmektedir. Bu profiller agresif pazarlama uygulamalarına konu oldukları gibi, bu profiller sayesinde şirketler kişisel reklamlar oluşturabilmektedir. Bu durum, özellikle kullanıcıların gizlilik hakları bakımından belli endişeler yaratmaktadır. Bu bağlamda, bazı çerezler gizlilik açısından "az tehlikeli" sınıfında yer almakta, bazı çerez uygulamaları ise kullanıcılar nezdinde ciddi gizlilik ihlali endişeleri yaratabilmektedir.

Avrupa Birliği'nde 2002 yılından bu yana çerezlere ilişkin hukuki düzenlemeler bulunmaktadır. O tarihten günümüze kadar geçen sürede çerezler, teknoloji hukukunu yakından ilgilendiren pek çok konunun merkezinde yer almıştır. Özellikle 2002/58/EC sayılı Direktif'te yapılan değişikliklerle birlikte çok daha büyük önem kazanmıştır(Garzaniti ve O' Regan, 2010, ss. 237-239). Nitekim, 2009 yılındaki değişiklikle sonrasında "Çerez Kanunu" olarak da anılan Direktif, kullanıcıların kişisel verileri ile özel hayatlarının gizliliğini çerez uygulamaları karşısında daha etkin şekilde korumayı amaçlamaktadır. Her ne kadar bu hedef tam anlamıyla sağlanamamış ise de Avrupa Birliği'nde çerezlere yönelik düzenlemeler çehre değiştirmeye devam etmektedir. Halihazırda müzakere edilmekte olan E-Gizlilik Tüzüğü, çerezlere yönelik olarak günümüz teknolojik gelişmelerine uygun ve çok daha kapsamlı düzenlemeler öngörmektedir.

AB hukukundan farklı olarak, Türk hukukunda çerezlerin tabi olduğu kurallar bakımından bir belirsizlik söz konusudur. Nitekim, çerez uygulamalarına, 6698 sayılı Kişisel Verilerin Korunması Kanunu, 5809 sayılı Elektronik Haberleşme Kanunu ve ilgili yönetmelik hükümlerinin ne ölçüde uygulanabileceği tartışmaya açıktır. Bununla birlikte, hukukumuzda, çerezler bakımından açık ve ayrıntılı hükümler bulunmaması, önemli hukuki sorunları ve soruları beraberinde getirmektedir.

Bu çalışmada, Türk hukukunda çerezlere yönelik açık ve genel kapsamlı bir düzenlemenin bulunmamasının beraberinde getirdiği hukuki soru ve sorunlar, Avrupa Birliği düzenlemeleriyle karşılaştırmalı şekilde değerlendirilecektir. Çalışma kapsamında, çerez uygulamaları, AB ve Türk mevzuatları kapsamında irdelenecek ve çerezler aracılığıyla kişisel veri işlenmesi bakımından dayanılabilecek veri işleme şartlarının neler olabileceği değerlendirilecektir. Ayrıca çalışmada, Türk hukukunda olası bir mevzuat değişikliği açısından önerilerde bulunulacaktır.

ÇEREZ KAVRAMI VE TÜRLERİ

Çerez, "*kullanıcının ziyaret ettiği web siteleri tarafından oluşturulan ve Üstün Metin Transfer Protokolü (Hyper Text Transfer Protocol – HTTP) kapsamında aktarımı gerçekleşen küçük dosyalardır*"(Castelluccia ve Narayanan, 2012)**.** Kullanıcı bir web sitesini ziyaret etmek istediğinde, söz konusu kullanıcının web tarayıcısı (örneğin, Google Chrome veya Microsoft Edge) sunucuya kullanıcının erişim talebini göndermekte, sunucu ise gelen talep sonrasında kullanıcının talep ettiği bilgileri ve kullanıcıya ait bilgileri web tarayıcısına iletmektedir[2]. HTTP iletişiminde çerezler sayesinde, sunucu, kullanıcının geçmişteki ziyaretleri sırasında gerçekleştirdiği eylemlerini ve bilgilerini hatırlayabilmekte, kullanıcının, aynı web tarayıcısı ile ziyaret ettiği diğer web sitelerindeki eylemlerini ve bilgilerini bunlarla birleştirerek, kullanıcının tüm bilgilerini güncel tutabilmektedir. Ayrıca, çerezler, kullanıcıların kişisel tercihlerinin kaydedilebilmesi amacıyla da kullanılmaktadır(Skouma ve Léonard, 2015; Vaughan, 2020). Bu bağlamda, çerezleri, gizlilik konusunda potansiyel olarak tehlikeli kılan husus, kullanıcının bilgisayarında depolanan bilgilere çerezler aracılığıyla erişebilme imkanı olan kurum ve kuruluşların, bu bilgileri nasıl ve ne amaçla kullanacaklarıdır.

Çerezler aracılığıyla elde edilen veriler, tercih edilen dil ayarları gibi kişisel veri niteliği taşımayan bilgiler olabileceği gibi, IP adresi, kullanıcı adı, benzersiz tanımlayıcı veya e-posta adresi gibi kişisel veriler de olabilir (Data Protection Commision(DPC), 2020, s. 3). Örneğin, IP adreslerinin toplanması ve çerezler yoluyla benzersiz tanımlayıcılar kullanılarak belirli bir bilgisayarın farklı (dinamik) IP adresleri kullanılması durumunda dahi takip edilebilmesi mümkün olabilmektedir. Böylelikle, veri sahiplerinin isimleri bilinmese dahi bu kişiler diğer kişilerden ayırt edilebilmektedir. Toplanan bilgiler ise bir kişinin özelliklerine ve davranışlarına ilişkin olup o kişiyi etki altında bırakmak amacıyla (örneğin, davranışsal reklamcılık için) kullanılabilmektedir (Article 29 Data Protection Working Party, 2010, s. 9). Bu nedenle, çerezler, kişisel verilerin korunması ile doğrudan doğruya ilişkilidir.

Çerezleri, kaynaklarına göre "birinci taraf çerezler - üçüncü taraf çerezler"; saklanma sürelerine göre "geçici süreli çerezler (oturum çerezleri) - kalıcı çerezler"; ve kullanım amaçlarına göre "zorunlu çerezler - işlevsellik çerezleri - performans çerezleri (analitik çerezler) - reklam/pazarlama çerezleri" şeklinde sınıflandırmak mümkündür (Doğan ve Bozkurt, 2020; Zorer, 2019).

Çerezler, kaynaklandıkları alana (domain) göre "birinci taraf çerezleri" ve "üçüncü taraf çerezleri" şeklinde iki sınıfa ayrılabilir. Birinci taraf çerezler, kullanıcının ziyaret ettiği web sitesi tarafından oluşturulmakta ve web sitesinin sahibi olan gerçek veya tüzel kişi kendi sitesini ziyaret eden kullanıcıyla doğrudan ilişki içerisinde bulunmaktadır(OneTrust, 2020, s. 6). Üçüncü taraf çerezlerde ise web sitesinin sahibi olan gerçek veya tüzel kişiler, üçüncü kişilerin oluşturdukları çerezlere kendi web sitelerinde kullanılmak üzere izin vermekte ve üçüncü kişiler bu çerezler aracılığıyla kullanıcıyı izleyebilmektedirler(Castelluccia ve Narayanan, 2012, s. 3; Skouma ve Léonard, 2015, s. 41). Birinci taraf çerezler, kontrolü mümkün ve hangi amaçla kullanılacağının belirlenmesi daha kolay çerezlerken; üçüncü taraf çerezler, bunlara başvuran üçüncü kişilerin kontrolünün çok zor olması ve ilişki yapısının çok daha karmaşık olması sebebiyle önemli gizlilik risklerini muhtevasında barındırmaktadır(Article 29 Data Protection Working Party, 2012; Skouma ve Léonard, 2015). Örneğin, Google, Yandex ve Facebook benzeri teşebbüsler, üçüncü taraf çerezler vasıtasıyla, bu siteleri hiç ziyaret etmeyen kişilerin verilerini dahi elde edebilmekte, bunları farklı sitelerden gelen çerez bilgileri ile eşleştirebilmekte, analiz edebilmekte ve kullanıcılar hakkında profil oluşturabilmektedirler(Zorer, 2019).

Çerezler bakımından yapılabilecek bir diğer ayrım ise, çerezlerin kullanım süresine ilişkin ayrımdır. "Geçici süreli çerezler" ("oturum çerezleri"), kullanıcı gizliliği açısından daha az risk barındıran, kullanıcıya ait bilgileri yalnızca web sitesi açıkken toplayan ve web sitesi kapandığında otomatik olarak silinen çerezlerdir. Lokasyon tercihleri bu çerezler bakımından toplanan bilgilere verilebilecek en tipik örneklerden biridir (Direktif m. 5/3). "Kalıcı çerezler" ise web tarayıcısı kapatılsa dahi silinmeyen, silinmesi için kullanıcının aktif eylemini gerektiren çerezler olup bu çerezler aracılığıyla kullanıcının tercihlerine, ilgi alanlarına, kimlik doğrulama gibi bilgilerine erişilmekte ve bu bilgiler ile kullanıcıya dair dijital bir profil oluşturulabilmektedir(Borgesius ve McDonald, 2015; Information Commissioner's Office (ICO), 2019)**.** Bu özelliğiyle, kalıcı çerezler kullanıcı gizliliği açısından önemli endişelere sebebiyet vermektedir. Zira, kalıcı çerezler aracılığıyla oluşturulan dijital kullanıcı profilleri, davranışsal hedefleme veya kişisel reklamlar gibi agresif ve ilgili kişinin gizlilik haklarına müdahale eden uygulamaların konusu olmaktadır.

Son olarak, çerezler işlevlerine/amaçlarına göre dörtlü bir ayrıma tabi tutulmaktadır("Cookies, the GDPR, and the ePrivacy Directive", 2020; OneTrust, 2020, ss. 6-7). "Zorunlu çerezler", bir web sayfasını gezmek ve/- web sitesinin içeriğinden faydalanmak için kullanılması mutlaka gerekli olan çerezlerdir. Bu çerezler genel olarak "birinci taraf çerezlerdir"("Cookies, the GDPR, and the ePrivacy Directive", 2020). "Tercihlere ilişkin çerezler" veya diğer ismiyle "işlevsellik çerezleri", web sitesine, kullanıcının geçmişte yapmış olduğu internet üzerindeki tercihlerini hatırlayabilme işlevi sunan çerezlerdir. Bu çerezler aracılığıyla, web sitesi işletmecisi, kullanıcının dil seçimi, hangi bölgede bulunduğu, hangi kullanıcı ismi ve şifreyi kullandığı gibi bilgileri depolayabilmektedir. Böylelikle, bu çerezler, ziyaret edilen web sitesinin içeriğinin, ziyaretçilerin tercihlerine göre bireyselleştirilmesine hizmet etmektedirler. Üçüncü grup çerezler, "istatistik çerezleri" veya diğer adıyla "performans çerezleri"dir (analitik çerezler). Bu çerezler sayesinde, kullanıcının web sitesini kullanma şekli (hangi sayfayı ziyaret ettiği, hangi linke tıkladığı gibi) tespit edilebilmekte ancak bu tespitler hiçbir surette kişinin kimliğini tespit etmek amacıyla kullanılmamaktadır. Bu çerezlerin temel işlevi, anonim bilgiler aracılığıyla web sitesinin işlevlerini arttırmak ve kullanıcı dostu bir web sitesi oluşturmaya yardımcı olmaktır. Son olarak, reklam/pazarlama çerezleri, kullanıcılar hakkında bilgi toplayarak, kendilerinin ilgisini çekecek türden içerik ve reklamlar sunmaktadırlar. Bu çerezler, genellikle "kalıcı süreli" ve "üçüncü taraf" çerezler sınıfında da yer almakta olup bu çerezler sayesinde kullanıcının çevrimiçi eylemleri ve dijital ayak izleri takip edilerek kişiye özel ve doğrudan kendisini hedef alan reklamlar oluşturulmaktadır[3].

AB MEVZUATINDA ÇEREZLER

2002/58/EC Sayılı Direktif Kapsamındaki Çerez Düzenlemeleri

2002 yılında yürürlüğe giren E-Gizlilik Direktifi, elektronik haberleşme alanında kişisel verilerin işlenmesi bağlamında, bireylerin mahremiyetini korumayı amaçlamaktadır (Direktif madde 1). 2009 yılında Direktif'in kimi hükümlerinde önemli değişiklikler yapılmış ve web üzerinden kullanıcıların terminal cihazlarına çerez yerleştirilebilmesi ve bu cihazlarda halihazırda yerleşik olan çerezlere erişilebilmesi, kural olarak kullanıcıların rızaları şartına bağlanmıştır. 2009 yılında yapılan değişikliklerden sonra 2002/58/EC sayılı Direktif, "Çerez Kanunu" adıyla anılmaya başlanmıştır. Bu düzenleme AB üye ülkelerinin iç hukuklarına da aktarılmış olup, aşağıda, ülkeler arasındaki belli başlı yaklaşım farklılıklarına da değinilecektir.

Çerezlerin ve benzer teknolojilerin kullanımı, geleneksel web siteleri ve web tarayıcıları ile sınırlı olmayıp, veri korumasına ilişkin kuralları, mobil uygulamalar dahil olmak üzere, abonenin veya kullanıcının terminal cihazında bilgi depolayan veya depolanan bilgilere erişen herhangi bir teknik için geçerli kabul edilmelidir(Information Commissioner's Office (ICO), t.y., s. 16). Bu bağlamda, ilgili

düzenlemelerin, çerezlere ilaveten, kullanıcı veya abonenin terminal cihazında bilgi depolayan veya bu depolanmış bilgiye ulaşan (pikseller, yerel nesneler, tarayıcı parmak izi teknolojiler vb.) benzer teknolojilere de uygulanacağı kabul edilmektedir(CNIL, 2020, s.3; Voisin ve arkadaşları, 2020). Keza, çerezlerin yerleştirilebileceği terminal cihazlar da, kişinin bilgisayarından ibaret değildir. Örneğin, akıllı telefonlar ve akıllı televizyonlar gibi internete bağlı diğer cihazlar terminal cihaz kapsamında yer aldığı gibi nesnelerin interneti bağlamındaki cihazlar da bu kapsamda değerlendirilir(CNIL, 2020, s.3; Information Commissioner's Office (ICO), 2019, s. 43).

Çerezler, Direktif'in Gerekçesinin (Recital) 24 ve 25. maddelerinde ve Direktif'in 5. maddesinin 3. fıkrasında düzenlenmektedir. Bu düzenlemeler incelendiğinde göze çarpan ilk husus, hukuka uygun/meşru (legitimate) işleme amacıdır. Gerekçe madde 24 ve 25'te terminal cihazlarda işlenecek verilerin ve bilgiye erişimin ancak hukuka uygun amaçların varlığı halinde mümkün olabileceği ifade edilmektedir. Direktifin "İletişimin Gizliliği" başlıklı 5. maddesinin 3. fıkrasında yer alan kurala göre ise: "***bir abonenin veya kullanıcının terminal cihazında bilginin depolanması veya halihazırda depolanmış olan bilgilere erişim elde edilmesi, yalnızca ilgili abonenin veya kullanıcının, işlemenin amaçları hakkında açık ve kapsamlı şekilde bilgilendirilmesi neticesinde rızasını vermiş olması koşuluyla"*** mümkündür**.** Yine aynı hükümde bu kuralın istisnalarına da yer verilmektedir.

Kural: Açık ve Kapsamlı Bilgilendirmeye Dayalı Rıza

Direktif, bir abonenin veya kullanıcının terminal cihazında bilginin depolanması veya halihazırda depolanmış olan bilgilere erişim elde edilmesini kural olarak, ilgili abonenin veya kullanıcının, işlemenin amaçları hakkında açık ve kapsamlı şekilde bilgilendirilmesi neticesinde rızasını vermiş olması koşuluna bağlamaktadır. ABAD'ın Planet 49 kararında (C-673/17) da ifade edildiği üzere, Direktif m. 5/3 hükmü, kişisel veri niteliği taşısın veya taşımasın, her türlü çerez bakımından uygulanacaktır(*Planet 49 Kararı*, 2019).

Kullanıcı veya abonelerden, çerezlere ilişkin olarak alınan rızaların geçerli olacağı ve çerezlerin, kullanıcı veya abonelerin terminal cihazlarında kullanılabileceği azami süreye ilişkin olarak farklı görüşler mevcut olup AB üye devletleri arasında bu konuya ilişkin bir görüş birliği bulunmamaktadır. Örneğin, İngiliz Veri Koruma Kurumu ICO, çerezlerin kullanım süresinin, bunların varlık amacıyla orantılı olması gerektiğini ifade etmektedir(Information Commissioner's Office (ICO), 2019, s. 41). İspanyol Veri Koruma Kurumu AEPD ise, alınan rızanın 24 ay sonra yenilenmesi gerektiğini ve bu süre içerisinde kullanıcılardan tekrar rıza istenmemesini önermektedir(AEPD, 2020, s. 29).

Aşağıda öncelikle bilgilendirme yükümlülüğünden, sonra da geçerli rıza bakımından aranacak özelliklerden bahsedilecektir.

Bilgilendirme Yükümlülüğü

Kullanılan çerezlerin türünden bağımsız olarak, veri sorumlularının ilgili kişileri bilgilendirme yükümlülüğü bulunmaktadır. Bilgilendirmenin ne zaman ve ne şekilde yapılması gerektiği meselesini 2013 yılında ele alan Article 29 Çalışma Grubu, kullanıcı veya abonenin, bir web sayfasına giriş yaptığı sırada ve karşısına çıkan ilk sayfada, çerezlerin kullanımına ilişkin açık, kapsamlı ve görünür bir bildirim yapılması gerektiğini ifade etmektedir. Bu aşamada, kullanıcılar, web sitesi tarafından farklı amaçlarla kullanılan tüm çerez türlerine ilişkin bilgiye erişebilmelidirler. Bu çerçevede, web sitesi tarafından kullanılan tüm çerez türlerinin listelendiği bir sayfanın bağlantı bilgisinin (link) paylaşılabileceği de ifade edilmektedir. Yine bu aşamada, çerezlerin kullanım amaçlarına, kullanılan üçüncü taraf çerezlere ve çerezler yoluyla üçüncü taraflara veri aktarımına ilişkin bilgilendirme yapılmalıdır. Çerezlerin hangi süreyle saklanacağı da kullanıcı veya abonelerle paylaşılması gereken hususlardandır. Son olarak, kullanıcı ve abonelere, sahip oldukları seçenekler (çerezlerin tamamını

veya bir kısmını kabul etmek veya hiçbirini kabul etmemek) ve gelecekte bu tercihi nasıl değiştirebilecekleri konusunda da bilgi verilmelidir(Article 29 Data Protection Working Party, 2013, s. 3).

Kullanıcılara ve abonelere, yapılacak bilgilendirme, AB veri koruma mevzuatına uygun nitelikte olmalı ve bu kişilere tanınan veri işlemeyi reddetme hakkı mümkün olduğunca "kullanıcı dostu" bir yöntemle sunulmalıdır(CNIL, 2020; Information Commissioner's Office (ICO), 2019, s. 43). Yine, Gerekçe madde 25'te, bilgilendirmenin ve reddetme hakkının kullanıcıya tek bir kez ve pek çok araçtaki çerez kullanımına yönelik olarak sunulmasının mümkün olduğu ve bu cihazlar ile sonradan yapılacak bağlantılar bakımından da geçerli olacağı ifade edilmektedir. Her ne kadar, Direktif içerisinde bu hususa yönelik açık bir düzenleme bulunmamakta ise de bu düzenlemenin, kullanıcı odaklı olduğu ve çerez kullanımlarında "rıza yorgunluğu"nun (consent fatigue) (Gonzalez ve arkadaşları, 2020, s. 284) önlenebilmesi amacıyla getirildiği düşünülmektedir(DUMORTIER ve DE PRETER, 2006, s. 452).

Burada üzerinde özel olarak durulması gereken meselelerden bir tanesi, özellikle üçüncü taraf çerezleri bakımından aydınlatma metinlerinin ne şekilde kaleme alınması gerektiğidir. Fransız Veri Koruma Kurumu CNIL, bilgilendirmeye dayalı rızadan söz edilebilmesi için, veri sahiplerinin, veri sorumlularının tamamını tespit edebilmeleri gerektiğini ifade etmektedir. Bu bağlamda, CNIL, söz konusu üçüncü tarafların kapsamlı ve düzenli olarak güncellenen bir listesinin, rızalarının alındığı sırada veri sahipleri ile paylaşılması gerektiğini ifade etmektedir. Bu türden bir aydınlatma, ilgili kişilerin tüm veri sorumlularını tanıyabilmesini sağlayacaktır(CNIL, 2020, s.4). Benzer şekilde, AEPD de, üçüncü tarafların adları veya tanınmış markaları ile bu tarafın kullandığı çerezler hakkında bilgi içeren bağlantı linklerinin kullanıcıların erişebileceği şekilde sunulması gerektiğini ifade etmiştir(AEPD, 2020, s. 16). ICO da söz konusu üçüncü tarafların kim olduklarının açıkça ve münferiden belirtilmesi ve söz konusu üçüncü tarafların elde ettikleri bilgiyi ne amaçla kullanacaklarını açıklamaları gerektiği görüşündedir(Information Commissioner's Office (ICO), 2019, s. 11).

ICO ve İrlanda Veri Koruma Kurumu DPC, kullanıcılar tarafından çerezlerin kabul edilmesi ve reddedilmesinin eşit kolaylıkta olması gerektiğini ifade etmektedir. Bu bağlamda, kullanıcı rızalarının yer aldığı ara yüzde, "tümünü kabul et" seçeneği bulunuyorsa, bunun yanında "tümünü reddet" seçeneğine de yer verilmesi önerilmektedir(Data Protection Commision(DPC), 2020, s. 9).

Rızanın Özellikleri

Çerez kullanımına ilişkin olarak alınması gereken rızanın özellikleri veri koruma hukukunun önemli meselelerindendir. 2013 yılında konuyu ele alan Article 29 Çalışma Grubu, rızanın: özgür iradeyle, belirli bir konuya ilişkin ve bilgilendirmeye dayalı olarak alınması gerektiğini; veri işleme faaliyetinin başlangıcından önce alınması gerektiğini; muğlak olmayan şekilde ve ilgili kişinin aktif davranışıyla verilmesi gerektiğini ifade etmiştir(Article 29 Data Protection Working Party, 2013, s. 3). Rızanın aktif bir davranışla verilmesi gerektiği, Avrupa Adalet Divanı'nın 1 Ekim 2019 tarihinde yayınlanan ve çerez kullanımında kullanıcı rızalarının Direktif açısından ele alındığı Planet49 kararında (C-673/17) da ifade edilmiştir. Söz konusu kararda ABAD, bu rızaların, önceden işaretlenmiş halde sunulan kutucuklar aracılığıyla elde edilemeyeceği açıkça dile getirmiştir. Bu bağlamda, bir kimsenin belirli bir web sayfasından ayrılmaması aktif davranış olarak değerlendirilemeyecektir(Article 29 Data Protection Working Party, 2013, s. 5; CNIL, 2020, s.21).

Article 29 Çalışma Grubuna göre, rızanın özgür iradeyle verildiğinden söz edilebilmesi için bir web sayfasına erişim, söz konusu internet sitesinin çalışması için zorunlu olanlar dışındaki çerezlerin bir kısmının veya tamamının kabul edilmesi şartına bağlanmamalıdır. Keza kullanıcılara, çerezleri kabul

etmenin yanı sıra çerezler arasında tercih yapma imkanı da verilmelidir. Seçeneklerin, farklı türdeki çerezler arasında ayrım yapılarak katmanlı olarak sunulması da önemlidir(Article 29 Data Protection Working Party, 2013, s. 5)[4]. Zira GVKT'nin gerekçesinin 43. maddesinde de, somut olayda uygun olmasına rağmen, kullanıcıların farklı kişisel veri işleme amaçlarına ayrı ayrı rıza vermelerine izin verilmiyorsa, rızanın özgür iradeyle verildiğinden söz edilemeyeceği vurgulanmaktadır.

ICO'ya göre, bir kullanıcının aynı web sayfasını her ziyaretinde kendisinden yeniden rıza alınması gerekmemektedir. Zira, çerezler vasıtasıyla bir kimsenin aynı sayfayı daha önce ziyaret ettiği ve rızasının kapsamı anımsanabilmektedir. Bu nedenle, kişinin geçmişte vermiş olduğu rızanın geçerli olduğu varsayılabilmelidir. Ancak, web sitesindeki çerezlerde meydana gelebilecek (örneğin, zorunlu olmayan türden yeni bir üçüncü taraf çerezin eklenmesi veya mevcut çerezlerin kullanım amacının değişmesi gibi) kimi değişiklikler, rızanın yeniden alınmasını gerektirebilir(Information Commissioner's Office (ICO), 2019, s. 39).

İstisnalar: Kriter A ve Kriter B

Direktif kapsamında çerez kullanımı bakımından genel kural, çerezlerin kullanıcıların rızaları alınarak kullanılması ise de Direktif m. 5/3 altında çerez kullanımına yönelik istisnalar da düzenlenmektedir. Buna göre, çerezlerin yalnızca haberleşmenin elektronik haberleşme ağı üzerinden iletiminin sağlanması amacıyla kullanılması veya çerez kullanımının, abone veya kullanıcı tarafından açıkça talep edilen bir bilgi toplumu hizmetinin sunulması bakımından mutlak surette zorunlu olması durumlarında, rıza alınmasına ilişkin kural uygulanmayacaktır.

Zorunlu çerezler olarak da ifade edilebilecek olan bu istisnalar, Article 29 Çalışma Grubu'nun konuya ilişkin rehberinde (Çerez Rıza Rehberi) oldukça ayrıntılı bir şekilde düzenlenmiştir(Article 29 Data Protection Working Party, 2012, s. 9). Çerez Rıza Rehberi'nde, "Kriter A" ve "Kriter B" çerezleri olarak anılan bu istisnalardan "Kriter A" çerezler, yalnızca haberleşmenin elektronik haberleşme ağı üzerinden iletiminin sağlanması amacıyla kullanılan çerezler olarak; "Kriter B" çerezler ise abone veya kullanıcı tarafından açıkça talep edilen bir bilgi toplumu hizmetinin sunulması bakımından bu erişimin sağlanması için kullanımı zorunlu olan çerezler olarak tanımlanmaktadır.

Kriter A İstisnası

"Kriter A" çerezleri, haberleşmenin elektronik haberleşme ağı üzerinden iletiminin sağlanması için kullanılması zorunlu olan çerezlerdir. Bu çerezler bakımından, kullanım amacı konusunda yoruma açık bir durum olmadığı ve bu istisnanın ancak bu çerezlerin kullanılmaması halinde iletişimin iletiminin mümkün olmayacağı durumlar için geçerli olacağı ifade edilmektedir. Haberleşmenin sağlanması bakımından mutlak surette zorunlu olma koşulu ise üç temel kullanım şeklini ifade etmektedir. Bunlar; (i) haberleşmenin rotasını belirleyen ve iletişimi doğru varış noktasına ulaştıran çerez uygulamaları, (ii) iletişim kanalındaki bilgilerin ve iletişimin karşılıklı akışını ve veri paketlerinin kullanıcılara taşınmasını sağlayan çerez uygulamaları ve (iii) iletim hataları ve veri kaybını tespite yarayan çerez uygulamaları olarak tanımlanmaktadır. Bu bağlamda, Çalışma Grubu 29 veya yeni ismiyle Avrupa Veri Koruma Otoritesi, Kriter A istisnası bakımından ancak bu üç durumdan birinin gerçekleşmesi halinde çerez kullanımının kullanıcı tercihine bırakılamayacağı ve kullanıcının bu çerezler bakımından reddetme hakkı olmayacağı kanaatindedir(Article 29 Data Protection Working Party, 2012, s. 7). Bu bağlamda, yalnızca haberleşmenin iletiminin hızlandırılması, düzenlenmesi veya bu iletime katkı sağlanması amacıyla kullanılan çerezler bu istisna kapsamında değerlendirilemeyecektir.

Kriter B İstisnası

"Kriter B" çerezleri, bir bilgi toplumu hizmetinin sağlanmasına ilişkindir. ABAD'ın 2 Aralık 2010 tarihli Ker-Optika kararında (C-108/09) ifade edilen "bilgi toplumu hizmeti" çevrimiçi olarak akdedilen veya iletilen sözleşme ve diğer hizmetleri kapsar(Avrupa Veri Koruma Kurulu, 2020, s. 27). Bu tanım, Avrupa Veri Koruma Kurulu tarafından da benimsenmiştir.

"Kriter B" çerezleri bakımından iki hususun varlığı zorunludur. Buna göre, abone veya kullanıcının bir bilgi toplumu hizmetini açıkça talep ettiğine yönelik aktif bir eylemi bulunmalı ve bilgi toplumu hizmetinin sağlanabilmesi için çerezin kullanımı mutlak surette zorunlu olmalıdır. Bir çerez kullanılmadıkça, kullanıcının talep ettiği bilgi toplumu hizmetinin sunulması mümkün olmamalı ve kullanıcının talebi, söz konusu hizmetin bir parçası olarak yerine getirilmelidir (Direktif Gerekçe Başlık 46). Ayrıca, rızaya tabi olmayan çerezler, yalnızca yerleştirilme amaçlarıyla doğrudan orantılı bir süre için varlığını muhafaza etmeli ve ortalama bir kullanıcı veya abonenin makul beklentileri dikkate alınarak, ihtiyaç ortada kalktıktan sonra kullanım sona ermelidir (Article 29 Data Protection Working Party, 2012, s. 5).

Örneğin, bir çevrimiçi alışveriş sitesinde bir kimsenin alışveriş sepetine eklediği ürünlerin, sayfalar arasında dolaşırken ve ödeme sayfasında hatırlanması çerezler sayesinde söz konusu olabilmektedir. Keza, internet bankacılığında güvenliğin sağlanması bakımından da oturum çerezlerinin kullanılması zorunludur. İş yükünü birden çok bilgisayar arasında dağıtarak web sayfalarının hızlı ve etkin şekilde yüklenmesini sağlayan yük dengeleme (load balancing) çerezleri de bu kapsamda değerlendirilmektedir(Information Commissioner's Office (ICO), 2018, s. 32). Keza, yasal yükümlülüklerin yerine getirilmesi bakımından, örneğin, veri koruma mevzuatının öngördüğü güvenlik koşullarının sağlanması bakımından da bir çerezin kullanılması mutlak surette zorunlu olabilir(Information Commissioner's Office (ICO), 2019, s. 14). Bununla birlikte ICO, isabetli olarak, bir çerezin kullanımının mutlak surette zorunlu olup olmadığı değerlendirmesinin kullanıcı açısından yapılması gerektiğini ifade etmektedir. Örneğin, reklam çerezleri, web sitesinin kazancını arttırdığı için veri sorumlusu bakımından mutlak surette zorunlu olsa dahi kullanıcılar bakımından aynı durum söz konusu değildir(Information Commissioner's Office (ICO), 2019, s. 14).

Article 29 Çalışma Grubu da, hangi çerezlerin, Kriter A veya B kapsamında mutlak surette zorunlu sayılabileceğine ilişkin olarak örnek niteliğinde bir liste yayınlamıştır(Article 29 Data Protection Working Party, 2012, s. 6)[5]. Buna göre: *i.* Sunulan hizmete ilişkin (alışveriş sepeti gibi) kullanıcı girdilerini takip etmek için yerleştirilen birinci taraf oturum çerezleri (Kriter B kapsamında); *ii.* (Örneğin internet bankacılığına girerken) kimlik doğrulama amacıyla yerleştirilen birinci taraf oturum çerezleri (Kriter B kapsamında); *iii.* Kullanıcı tarafından talep edilen bir hizmetin güvenliğini artırmak amacıyla yerleştirilen (örneğin, mükerrer defa başarısız olan giriş teşebbüslerini takip eden; veya dolandırıcılığın önlenmesine hizmet eden) birinci taraf çerezleri (Kriter B kapsamında); *iv.* İçerik sağlayıcıların video ve ses akışı için kullandıkları multimedya oynatıcı oturum çerezleri (Kriter B kapsamında); *v.* Şebekenin yönetilmesi ve yük dengelemesi amacıyla kullanılan oturum çerezleri (Kriter A kapsamında); *vi.* Kullanıcıların (dil benzeri) tercihlerini hatırlamak için kullanılan kısa süreli kullanıcı arabirimi uyarlama çerezleri (Kriter B kapsamında); ve *vii.* Veri sahiplerinin, sosyal paylaşım sitelerine abone olmaları ve sistemden çıkış (log-out) yapmamış olmaları kaydıyla sosyal eklenti içeriği paylaşım çerezleri (Kriter B kapsamında) veri sahiplerinin rızası aranmaksızın veri sahiplerinin terminal cihazlarına yerleştirilebilir.

Çerez teknolojisinin kullanıldığı ilk zamanlarda, birinci taraf çerezler ve üçüncü taraf çerezler bakımından Kriter A ve Kriter B ayrımının yapılması imkânı bulunmaktayken günümüzde bu tarz kesin bir ayrımın yapılması neredeyse mümkün değildir. Zira, ilk zamanlarda Kriter A çerezleri, daha çok birinci taraf çerezler ile ilişkilendirilebilirken, çok amaçlı çerezlerin yaygınlaşması ile bu ayrım ortadan kalkmıştır. Öyle ki, "Kriter A" veya "Kriter B" istisnasını karşılayan bir çerez, aynı zamanda profilleme ve pazarlama amacıyla kullanılma işlevini de sağlamaktadır. Mutlak surette zorunlu olduğu

gerekçesiyle veri sahibinin rızası olmaksızın yerleştirilen çerezlerin, yalnızca yerleştirilme amacı doğrultusunda kullanılması gereklidir. Çok amaçlı çerezlerin kullanımı halinde, istisna kapsamına girmeyen amaçlar bakımından -ilgili çerez Kriter A veya Kriter B kapsamındaki amaçları taşısa dahi- kullanıcıdan ikinci amaca yönelik rıza alınması gerekecektir (Article 29 Data Protection Working Party, 2012, s. 7)[6]. Gerçekten de bir çerezin çeşitli amaçlarla kullanılabilmesi mümkündür. O nedenle, veri koruma hukukuna ilişkin risk, çerezde yer alan bilgiden ziyade, işleme amaçlarıyla ilişkilidir. Örneğin bir çerez, hem kullanıcı tercihlerini hatırlamak hem de kullanıcı davranışlarını izlemek için kullanılabilir. Kullanıcı davranışlarının izlenmesi, hiçbir surette Kriter A veya B kapsamında değerlendirilemeyeceğinden, bu çerezin, veri sahibinin rızası olmaksızın yerleştirilebilmesi ve kullanıcı davranışlarının izlenmesi mümkün değildir(Article 29 Data Protection Working Party, 2012, s. 6).

Yukarıda da ifade edildiği üzere, günümüz teknolojisinde çerezlerin kullanım amaçlarına yönelik kesin ayrım ve belirlemeler yapılması kolay olmamaktadır. Ancak AB mevzuatı açısından Kriter A ve Kriter B istisnalarına girmeyeceği kabul edilen bazı çerezler bulunmaktadır. Article 29 Çalışma Grubuna göre, sosyal takip çerezleri (social plug-in tracking cookies); üçüncü taraf reklam çerezleri (third party advertising cookies); ve analitik çerezleri ancak veri sahibinin rızası ile işlenebilir(Article 29 Data Protection Working Party, 2012, s. 6; Information Commissioner's Office (ICO), 2019, s. 35).

i. *Sosyal takip çerezleri*, kullanıcının internet üzerindeki ayak izlerini takip edebilen ve üçüncü taraf çerezler aracılığıyla davranışsal reklamcılık, veri analitiği veya pazar araştırması gibi amaçlara da hizmet eden çerezlerdir. Avrupa Veri Koruma Kurulu nezdinde bu amaçla kullanılan çerezlerin "mutlak surette gerekli olma" kriterinin sağlayacağının kabul edilmesi mümkün değildir(Article 29 Data Protection Working Party, 2012, ss. 9-10).

ii. *Üçüncü taraf pazarlama çerezleri* ise pazar araştırması, dolandırıcılığın önlenmesi gibi Kriter B koşullarıyla bağdaştırılabilecek amaçlarla kullanılsa dahi istisna dışında tutulacak olup bunun sebebi, "Takip Etme" (Do Not Track) ve "Toplama" (Do Not Collect) kriterlerinin tüm Avrupa Birliği vatandaşları bakımından denk bir standartta uygulanması gerekliliği olarak ifade edilebilir(Borgesius ve McDonald, 2015; Kamara ve Kosta, 2016; Kosta, 2013). Bu durumun Direktif'teki dolaylı yansıması ise m. 6/3'tür. Buna göre, kullanıcı trafik verilerinin -ki ilgili verilerin toplanmasında çerezler araç olarak kullanılmaktadır- pazarlama faaliyeti amacıyla kullanılması halinde bu kullanım ancak kullanıcının rızası ile mümkün olabilecektir.

iii. *Analitik çerezler*, ziyaretçi sayıları, görüntülenen sayfalar, ziyaret saatleri ve süreleri gibi bir internet sitesini geliştirmeye yardımcı olan ve istatistiki bilgi elde etmek amacıyla kullanılan çerezlerdir. Her ne kadar bu tür çerezler bir internet sitesinin gelişmesine hizmet etse de, bunların söz konusu site üzerinden haberleşmenin sağlanabilmesi bakımından zorunlu olmadıkları ifade edilmektedir.

Article 29 Çalışma Grubu, analitik çerezlerin, ister birinci taraf ister üçüncü taraf olsun, mutlak anlamda zorunlu olmadıkları görüşündedir. Bununla birlikte, birinci ve üçüncü taraf analitik çerezler arasında ayrım yapan Çalışma Grubu, veri sahiplerinin bilgilendirilmesi ve gerekli güvenlik önlemlerinin alınması neticesinde ve yalnızca toplulaştırılmış ve anonim nitelikte istatistiksel veri elde etmek amacıyla kullanılan birinci taraf analitik çerezlerin, üçüncü taraf analitik çerezlere kıyasla veri sahipleri bakımından daha düşük risk taşıdığını ifade etmektedir (Article 29 Data Protection Working Party, 2012, s. 10; Ayrıca benzer bir liste için bkz. CNIL, 2020, s.9). Avrupa Veri Koruma Kurulu da, izleyici ölçümüne yönelik istisnanın, kullanıcı tarafından talep edilen hizmetin performansının analizi için gerekli olan, yalnızca hizmet operatörüne istatistik sağlamakla sınırlı analizler için ve yalnızca birinci taraf çerezler bakımından uygulanması gerektiğini savunmaktadır. Böylelikle, bu işleme faaliyeti, tek başına veya diğer verilerle birleştirilerek, profilleme amacıyla

kullanılamayacaktır(Avrupa Veri Koruma Kurulu, 2021, s. 3). Bu görüş, Tüzük taslağına da yansımış olup Tüzük taslağı incelediğinde birinci taraf analitik çerezlerin kullanımı bakımından belli istisnalar getirildiği görülmektedir.

Article 29 Çalışma Grubu ile benzer şekilde, ICO da her iki tür analitik çerez bakımından rıza alınmasının zorunlu olduğunu, bunların mutlak anlamda gerekli çerezlerden sayılamayacaklarını ifade etmektedir(Information Commissioner's Office (ICO), 2019, s. 34). Farklı görüşte olan CNIL ise, münhasıran kullanıcı ölçümü amacıyla kullanılan ve anonim veri sağlayan çerezlerin, bir site veya uygulamanın düzgün şekilde çalışması için genellikle zorunlu olduğunu kabul ederek, bunların kullanıcı rızası olmaksızın yerleştirilebileceğini belirtmektedir (CNIL, 2020, s.9).

E-Gizlilik Tüzüğünde Çerezler

Yürürlüğe girdiği 2002 yılından bu yana, Direktif'te önemli değişiklikler yapılmış ise de Avrupa Birliği toplumunun geçirdiği hızlı dijital dönüşüm, "Çerez Kanunu"nun çağın getirdiği yenilikleri takip edememesine sebebiyet vermiştir(Avrupa Parlamentosu, 2017). Elektronik haberleşme hizmeti sunan teşebbüslerin, "veri gözetimi (data surveillance)" uygulamalarını arttırması, yapay zeka alanındaki gelişmeler ve otomatik veri işleme sistemlerinin yaygınlaşması karşısında, yeni bir düzenleme yapılması kaçınılmaz olmuştur (Cofone, 2017; Custers, 2018, ss. 113-115; Hildebrandt, 2008, ss. 306-307).

Avrupa Parlamentosu ve Avrupa Veri Koruma Kurulu da 2009 değişikliğinin beklenen etkiyi ve değişimi sağlayamadığını, aksine bu değişikliklerin, beraberinde çerez duvarlarını ve kullanıcılar yönünden ise rıza yorgunluğunu getirdiğini, bu kapsamda çerez düzenlemelerinde köklü ve teknolojik gelişmelere uygun bir değişiklik yapılması gerektiği görüşünü farklı rehber ve kamuoyu açıklamalarında ifade etmişlerdir(Avrupa Parlamentosu, 2017).

Bu doğrultuda, 10 Ocak 2017'de Genel Veri Koruma Tüzüğü'nün elektronik haberleşme alanındaki tamamlayıcısı nitelikteki E-Gizlilik Tüzüğü'nün ilk taslağı yayınlanmıştır. 10 Şubat 2021 tarihi itibariyle üzerinde mutabık kalınan ve yakın gelecekte son haliyle yürürlüğe girmesi beklenen Tüzük ile birlikte özellikle çerez kullanım istisnalarının daha net bir çerçeveye oturtulması ve Direktif uygulamalarındaki yoruma açık ve belirsiz konuların önemli ölçüde azalması beklenmektedir. Zira, Tüzük taslağı, çerez uygulamalarına ilişkin olarak, Direktif'ten farklı bir çerçeve ve daha uzun bir istisnalar listesi öngörmektedir.

Öte yandan, Tüzük altındaki çerez düzenlemeleri incelendiğinde rızanın genel kural olarak kalmaya devam ettiği görülmektedir (Boban, 2019). Yine, Kriter A ve Kriter B istisnası da Tüzük kapsamında yerini almıştır; ancak Avrupa Veri Koruma Kurulu'nun önerileri de dikkate alınmak suretiyle, bu kuralın istisnaları daha ayrıntılı ve çağın ihtiyaçlarına uygun şekilde düzenlenmiştir. Ayrıca, Tüzük, hali hazırda çok tartışılan "çerez duvarları", "rıza yorgunluğu" ve "veri sorumlusu" konularında da düzenlemeler ihtiva etmektedir.

Rıza Kuralı ve İstisnaları

Genel Veri Koruma Tüzüğü'nün yürürlüğe girmesi ve GVKT'nin özellikle rızaya ilişkin yeni ölçütler belirlemesi, çerezlere ilişkin tartışmalara yeni bir boyut kazandırmıştır. Öyle ki, ziyaretçilerinin terminal cihazlarına çerez yüklemek isteyen işletmeler, bu faaliyetlerini GVKT'ye uygun şekilde gerçekleştirmek zorunda kalmışlardır. Bu bağlamda, zorunlu olmayan çerez ve benzeri takip teknolojilerinin kullanılabilmesi bakımından kullanıcıların rızasını almak zorunda olan web siteleri, ziyaretçilerine, çerez politikalarını kabul edip etmediklerini sormaya başlamışlardır(Cairoli ve Olivi,

2020). Bu süreçte, kullanıcılarına "kullanıcı dostu" bilgilendirme yapmak zorunda olan işletmeler, rıza alma yöntemleri bakımından da değişikliğe gitmişlerdir.

Tüzük, Direktif'te bulunan kullanıcı rızasına ilişkin temel kuralı benimsemektedir. Keza, Kriter B istisnası da muhafaza edilmiştir. Bununla birlikte, teknolojik gelişmeler ve mevcut tartışmalar da dikkate alınarak, Kriter A'nın kapsamında önemli bir takım değişiklikler yapılmış, ayrıca Direktif'te bulunmayan bir dizi yeni istisna getirilmiştir (Tüzük taslağı m. 8).

i. Kriter A istisnasına ilişkin değişiklikler: Direktif'te elektronik haberleşme kapsamındaki iletişimin sağlanması amacı ön plana çıkarken, Tüzük'te bu istisna "elektronik haberleşme hizmetinin" sağlanması amacıyla kullanılan çerezler olarak ifade edilmiştir. Bu değişikliğin önemli olmasının sebebi, e-gizlilik kurallarını doğrudan ilgilendiren Elektronik Haberleşme Yasası'nın (2018/1972 sayılı Direktif)("EECC")[7] hazırlanmış olması ve elektronik haberleşme servislerinin çeşitliliğinin bu yasa ile arttırılmasıdır.

Hangi hizmetlerin "elektronik haberleşme hizmeti" kapsamında sayılacağı hususu ABAD'ı da meşgul etmiştir. Zira bu mesele, bir şirketin telekom mevzuatına ve onun öngördüğü yükümlülük ve sorumluluklara tabi olup olmayacağı açısından son derece önemlidir. Konuyla ilgili iki farklı karar vermiş olan ABAD'ın kararlarından birisi Gmail (C-193/18) diğeri ise Skype (C-142/18) ile ilgilidir. Google'ın web-temelli e-posta servisi olan ve bir tür OTT hizmeti olan Gmail'in elektronik haberleşme şebekeleri üzerinden kısmen veya tamamen sinyal iletimi hizmeti sunmadığını; fakat sinyallerin e-posta kullanıcılarının internet servis sağlayıcıları tarafından iletildiğini belirten ABAD, bu sebeple Gmail'in elektronik haberleşme hizmeti gerçekleştirmediğini kabul etmiştir. Skype bakımından ise aksi yönde karar veren ABAD, telekom operatörleriyle Skype arasında akdedilen ve internet üzerinden (VoIP) sabit hatlar ile cep telefonlarının aranmasına imkân sağlayan sözleşmeler nedeniyle Skype'ın sunmuş olduğu hizmetin elektronik haberleşme hizmeti teşkil ettiğini kabul etmiştir. Bununla birlikte, bu kararlar günümüzde önemini yitirmiştir. Zira 21 Aralık 2020 tarihinde Elektronik Haberleşme Yasası'nın yürürlüğe girmesiyle birlikte e-posta servisleri tarafından gerçekleştirilen faaliyetlerin de elektronik haberleşme hizmeti kapsamına gireceği açıkça kabul edilmiştir.

EECC'nin hedeflerinden başlıca bir tanesi tüm piyasa oyuncularına eşit şartlar sağlamaktır(Losnedahl, 2018). Bu çerçevede, EECC'nin getirdiği en önemli yeniliklerden birisi de, öncesinde "elektronik haberleşme hizmeti" sayılmayan birçok OTT sağlayıcının faaliyetlerinin de bu kapsamda ele alınmasıdır. EECC, elektronik haberleşme hizmetinin bir alt kategorisi olarak kabul ettiği "kişilerarası haberleşme hizmetlerini" numaraya dayalı ve numaradan bağımsız olmak üzere ikiye ayırmakta ve iki grup bakımından farklı düzeyde regülasyon öngörmektedir. İlk kategori klasik telefon hizmetlerini kapsarken, ikinci grupta OTT'ler yer almaktadır. Bu bağlamda, internet üzerinden yapılan VoIP, mesajlaşma uygulamaları ve e-posta hizmetleri de kişilerarası haberleşme hizmetleri kapsamına girmektedir. Bununla birlikte, web sayfaları ile sosyal ağlar bu tanım kapsamına girmemektedir.

E-Gizlilik Direktif'nin 2. maddesinde yer alan atıf nedeniyle, EECC'deki geniş kapsamlı elektronik haberleşme servisi kavramı, E-Gizlilik Direktifi bakımından da geçerli hale gelmiştir. Benzer şekilde, E-Gizlilik Tüzük taslağında da EECC'de yer alan elektronik haberleşme hizmetleri tanımına atıf yaptığı görülmektedir (Tüzük Giriş madde 11). Böylelikle, EECC'nin yürürlüğe girmesiyle birlikte geleneksel telekomünikasyon servis sağlayıcılarının sunduğu servislerin yanı sıra, anlık mesajlaşma (WhatsApp, Telegram), IP üzerinden görüşme (SkypeOut, Google Hangouts) ve web tabanlı e-posta (Gmail) uygulamaları gibi internet tabanlı servisler de elektronik haberleşme hizmetinin kapsamına alınmıştır. Tüzüğün yürürlüğe girmesinin ardından, geleneksel telekomünikasyon işletmelerinin yanı sıra, internet tabanlı servis sağlayıcılarının da mevzuat kapsamına gireceği ve çerezlere ilişkin düzenlemelere daha fazla sayıda işletmenin tabi olacağı söylenebilir.

Haberleşmenin gizliliği, Avrupa Birliği Temel Haklar Şartı'nın 7. maddesi kapsamında korunan temel bir haktır. Bu hak, alıcıya hangi yolla gönderildiklerine bakılmaksızın her elektronik haberleşmeye uygulanmalı ve tüm kullanıcıların terminal cihazlarının bütünlüğünü korunmalıdır(Avrupa Veri Koruma Kurulu, s. 1). Ancak Direktif, işlevsel olarak eşdeğer bir hizmet sunmalarına rağmen, internet üzerinden faaliyet gösteren sağlayıcılar tarafından sunulan elektronik haberleşme hizmetlerini kapsamamaktadır. Bu nedenle, Avrupa Veri Koruma Kurulu, Tüzüğün kapsamının işlevsel olarak eşdeğer hizmetler sunan OTT'leri de kapsar genişlikte olmasını isabetli bulduğunu ifade etmektedir(Avrupa Veri Koruma Kurulu, s. 2).

ii. Birinci taraf analitik çerezler: Tüzük taslağına göre, yalnızca kullanıcı davranışlarının istatistiki amaçla ölçümlenmesi için çerez kullanımında, kullanıcının rızasının alınması gerekli olmayacaktır. Ayrıca, bu istatistiki ölçümlemenin üçüncü kişiler tarafından işletme adına veya işletme ile müşterek sorumlu sıfatıyla gerçekleştirilmesi durumunda da söz konusu üçüncü kişiler, GVKT'nin müşterek veri sorumlusu ve veri işleyenin sorumluluklarının düzenlendiği m. 26 ve 28 kapsamındaki gereklilikleri sağlamak koşuluyla bu istisnadan yararlanabilecektirler.

iii. Bilgi toplumu hizmetlerinin veya terminal cihazların güvenliğinin sağlanması, dolandırıcılığın önlenmesi ve teknik hataların tespit edilmesi ve önlenmesi: Bilgi toplumu hizmetlerinin veya terminal cihazların güvenliğinin sağlanması, dolandırıcılığın önlenmesi ve teknik hataların tespit edilmesi amacıyla kullanılan çerezler, bu amacın var olma süresiyle sınırlı olmak üzere, kullanıcı rızası alınmaksızın kullanılabilecektir.

iv. Yazılım güncellemesi: Tüzük ile birlikte, yazılım güncellemesi bakımından kullanılacak çerezler de belirli koşulların sağlanması amacıyla istisna kapsamına sokulmaktadır. Buna göre, yazılım güncellemesinin güvenlik nedeniyle gerekli olması ve bu güncellemenin kullanıcının seçmiş olduğu gizlilik ayarlarında değişikliğe neden olmaması; her bir güncelleme yüklenmeden önce, kullanıcının güncellemeye ilişkin aydınlatılması ve kullanıcıya bu güncellemelerin otomatik kurulumunu erteleme veya kapatma imkânı verilmesi halinde, söz konusu terminal araçların kullanımı istisna kapsamında değerlendirilecektir.

v. Acil durumlarda konum tespiti: Elektronik Haberleşme Yasası'ndaki yeni düzenlemelere uygun olarak, 112 acil numarasının arandığı acil durumlarda, kişinin bulunduğu yerin tespiti için kullanılacak konum tespit çerezleri de istisna kapsamına alınmıştır.

vi. Başka bir amaçla veri işleme: Tüzük kapsamında, bir çerezin, yerleştirilme amacından farklı amaçlarla kullanılması durumu da düzenlenmektedir. Bu bağlamda, verilerin, elde edilme amacından farklı bir amaçla işlenmesi bakımından kullanıcının rızası veya AB ya da üye ülkelerin iç hukukunda bir yasal dayanak bulunmayan hallerde, başka bir amaçla veri işleme hususu bakımından iki aşamalı bir inceleme yapılacaktır. Tüzük m. 8/1-g maddesine göre, öncelikle başka veri işleme amacının, söz konusu verilerin elde edilmesi sırasındaki işleme amacıyla uyumlu olup olmadığının belirlenmesi gerekmektedir. Bu değerlendirmede; veri işleme faaliyeti bakımından kullanıcı ve çerezi kullanan işletme arasındaki ilişki, veri işleme faaliyetinin niteliği, farklı amaçla veri işlemenin olası sonuçları ve gerekli güvenlik tedbirlerinin alınıp alınmadığı da dikkate alınacaktır. Söz konusu işleme faaliyetinin, ilk veri işleme amacı ile uyumlu olduğu kanaatine varılırsa, bu tür bir veri işleme amacı ancak; (i) bu amaçla elde edilen bilgilerin, amacın gerçekleşmesiyle birlikte silinmesi veya anonim hale getirilmesi, (ii) elde edilen bilgilerin bulanık (pseudonymised) olması ve (iii) bu amacın kullanıcı profili oluşturmaya yönelik olmaması koşullarının birlikte varlığı halinde kullanıcının rızasını gerektirmeyecektir.

Çerez Duvarları

Çerezlerle ilgili olarak Direktif uygulaması bakımından sıkça tartışılan hususlardan bir diğeri ise, "çerez duvarları"nın yasaklanması gerekip gerekmediği konusudur. Çerez duvarı, kullanıcıyı çerez uygulamalarına rıza vermeye zorlayan ve verilecek rızayı tek seferle ve tüm çerezlerle sınırlayan, rıza verilmemesi durumunda internet sitesine girişi engelleyen hibrid bir çerez yasaklama aracıdır. Bu bağlamda, çerez duvarı kullanan web siteleri, cihazlarına çerez yerleştirilmesine izin vermeyen kullanıcıların girişlerine izin vermezler.

GVKT'ye göre, kişisel verilerin işlenmesine ilişkin rızanın "özgür bir şekilde" verilmiş olması gerektiğinden, bir web sayfasının, kullanıcıya sunulan hizmet karşılığında ücret ödeme veya çerez kullanımına izin verme seçeneklerini sunmasının GVKT'nin aradığı bu şartın sağlanması bakımından yeterli olup olmadığı tartışma konusu olmuştur(Information Commissioner's Office (ICO), 2019; "Tracking Under the E-Privacy Regulation", 2021; Voss, 2017).

AB hukukunda modern eğilimin, çerez duvarlarının kullanımına belirli şartlar altında izin verilmesi olduğu söylenebilir. Örneğin, geçmişte, çerez duvarların kullanımına mutlak ve genel surette karşı olan CNIL, Fransız Yargıtay'ının bu konudaki yaklaşımını da dikkate alarak görüş değiştirmiş ve çerez duvarlarının veri sahiplerinin rıza verip vermeme konusundaki özgürlüğüne etkisinin ve çerez duvarlarının hukuka uygunluğunun, somut olay bazında değerlendirilmesi gerektiğini ifade etmiştir. Bu bağlamda, kullanıcılar, çerez duvarı kullanılan hallerde (özellikle, rıza vermemeleri durumunda söz konusu site veya uygulamanın içeriğine erişemeyecekleri durumlarda) tercihlerinin sonuçları hakkında açıkça bilgilendirilmelidirler(CNIL, 2020, s.4).

Bu tartışmalar sürerken, Avrupa Veri Koruma Kurulu, 4 Mayıs 2020 tarihinde yayınladığı tavsiye kararları ile çerezlerin kullanımına ilişkin rızanın, bir web sayfasına giriş için şart koşulamayacağını ifade etmiştir (Avrupa Veri Koruma Kurulu, 2020). Ancak Kurul, 2021 yılında yayınladığı açıklamada, bu katı yaklaşımını bir miktar yumuşatmış ve aynı hizmet sağlayıcılar tarafından, ilgili hizmeti elde edebilmeleri için *kullanıcılara adil alternatifler sunulmadıkça* çerez duvarlarının kullanımının, rızanın özgür iradeyle verilmesi koşulunu sakatlayacağını ifade etmiştir(Avrupa Veri Koruma Kurulu, 2021, s. 3; benzer görüş için bkz. AEPD, 2020, s. 30).

Tüzük düzenlemesi ise çerez duvarlarının kullanımına belli koşullar altında izin vermektedir. Bu bağlamda, Tüzük gerekçesinin 20aaaa maddesinde; kullanıcılara, kullanılan çerezlerin ve benzer tekniklerin amaçları hakkında açık, kesin ve kullanıcı dostu bilgiler verilmesi ve web sitesine erişim bakımından, çerezlerin kabul edilmesi koşuluna muadil ve denk bir alternatif sunulması koşuluyla, çerez duvarlarının kullanılabileceği ifade edilmektedir. Buna karşılık, kullanıcı ile hizmet sağlayıcıların denk olmadıkları durumlarda (örneğin, kamu kurumlarınca sunulan hizmetleri konu alan web sitelerine erişim bakımından) çerez duvarlarının, kullanıcıları özgür seçim haklarından mahrum bırakabileceği ifade edilmektedir.

Rıza Yorgunluğu

Direktif uygulamaları bakımından bir diğer hukuki tartışma da, kullanıcıların maruz kaldıkları çok sayıda rıza talebi nedeniyle oluşan "rıza yorgunluğu" ve buna bağlı olarak ortaya çıkan hukuki sorunlardır (Boban, 2019; Georgiev, 2020). Rıza yorgunluğuna bağlı olarak, kullanıcılar iki farklı bilinçsiz tercihte bulunabilmektedir. Bu tercihlerin ilki, sonucunu düşünmeksizin çerez uygulamalarını reddetmektir. Zira, daha güvenli bir yol olacağı düşüncesiyle bu tercihi yapan kullanıcılar, bir web sitesine giriş yaptıklarında veya bir uygulamayı kullanmak istediklerinde ilk yaptıkları tercihlerinden dolayı farklı çerez engelleyiciler ile karşılaşmaktadırlar. Öte yandan, kullanıcılar rıza yorgunluğu sonucunda, bilinçsiz olarak tüm çerez uygulamalarını kabul de edebilmekte olup; bunun sonucunda

agresif veri işleme, profilleme gibi kullanıcının zaman zaman gizlilik haklarını ihlal eden veri işleme faaliyetlerine maruz kalmaktadır. Bu bağlamda, kullanıcılara, tarayıcı ayarlarında değişiklik hakkı verilmesi ve bir veya daha fazla servis sağlayıcının sunduğu çerezler bakımından, bu çerez uygulamalarını güvenli uygulama listesine alabilme olanağı tanınması konusu tartışılmıştır (Georgiev, 2020).

Avrupa Veri Koruma Kurulu da e-Gizlilik Tüzüğü'nün, kontrolü yeniden kullanıcılara vererek mevcut durumu iyileştirmesi ve "rıza yorgunluğunu" dikkate alan düzenlemeler getirmesi gerektiği görüşünü ifade etmiştir. Bu bağlamda, Kurul, tarayıcı ve işletim sistemlerine, kullanıcı dostu ve etkili bir rıza mekanizması uygulamaya koyma yükümlülüğü getirilmesini önermektedir(Avrupa Veri Koruma Kurulu, 2021, s. 3). CNIL ise, günümüz teknolojisinde tarayıcılar üzerinden yapılacak ayarlamaların veri koruma hukuku anlamında geçerli bir rıza teşkil etmeyeceği görüşündedir. Zira tarayıcılar üzerinden yeterli düzeyde bilgilendirme yapılması veya çerezlerin türlerine göre sınıflandırma yapılabilmesi mümkün değildir(CNIL, 2020, s.8). Article 29 Çalışma Grubu ise, yalnızca, varsayılan olarak tüm çerezleri reddeden tarayıcılarda, belirli web sitelerince yüklenecek çerezlerin, kullanıcı tarafından aktif bir davranışla kabul edilmesi halinde geçerli bir rızadan söz edilebileceği görüşündedir(Article 29 Data Protection Working Party, 2010, s. 4).

Tüzük ile birlikte bu tartışmalar önemli ölçüde azalacaktır. Zira, Tüzük, yazılımcılara, çerez rızaları konusunda daha basit ve kullanıcı dostu uygulamalar geliştirmeleri konusunda tavsiyede bulunduğu gibi, teknik açıdan uygulanabilir olması halinde, kullanıcılara da belirli sağlayıcıların, kullanıcı tarafından tür ve amaçlarına göre belirlenecek çerezlerini güvenli listeye alma veya bu listeden çıkarma hakkı tanımaktadır (E-Gizlilik Tüzüğü Gerekçe Madde 20a).

Veri Sorumlusu

Üçüncü taraf çerezlerin yerleştirildiği web sitelerinde, veri koruma mevzuatına uygun şekilde hareket edilmemesinden kimin sorumlu olacağı meselesi gündeme gelmektedir. Direktif'te bu tartışmaya yönelik bir düzenleme bulunmamaktadır. Bununla birlikte, üçüncü taraf çerezler bakımından web sitesi işletmecisi ve üçüncü taraf çerez sahibinin, "terminal araç kullanan kişi" olarak kullanıcının doğru şekilde aydınlatılması ve rıza alınması sorumlulukları olacağı açıktır. Ancak pratikte, üçüncü taraf çerezlerin işletmecisi kişinin takibinin ve kontrolünün zor olması, kullanıcının bu çerezler üzerinde doğrudan kontrolünün bulunmaması önemli riskler doğurmaktadır(Information Commissioner's Office (ICO), 2019; Naranjo, 2017; Voss, 2017).

Üçüncü taraf çerezler bakımından, kullanıcının gizliliğine ilişkin riskler mevcut olduğu gibi, kullanıcının şikayetlerini üçüncü kişiye mi web sitesi işletmecisine mi yönlendireceği de tartışmalıdır. Bu konu uygulamada farklı üye devlet veri koruma otoriteleri tarafından da değerlendirilmiş olup genel kanı, üçüncü taraf çerezlere ilişkin olarak tarafların sorumluluğu ve taraflarca alınacak önlemler bakımından, web sitesi işletmecisi ve üçüncü taraf arasındaki sözleşmesel düzenleme yapılması gerektiği yönündedir(CNIL, 2019; Globocnik, 2019; Information Commissioner's Office (ICO), 2019). Örneğin, ICO, bir web sitesinde üçüncü taraf çerezlerin yer alması halinde, veri sahiplerinin açık bir şekilde bilgilendirilmesi ve gerekli rızanın alınmasından hem ilgili web sayfasının hem de üçüncü tarafın sorumlu olduğunu ifade etmektedir. Uygulamada, kullanıcıyla ara yüz üzerinde daha az ilişki içinde olan üçüncü tarafın bunu başarması daha zor olduğundan, üçüncü taraflar ile web yayıncıları arasında yapılacak sözleşmesel bir düzenlemeyle, web yayıncısına, aydınlatmaların yapılması ve rızaların alınmasına ilişkin bir yükümlülük yüklenmesi önerilmektedir(Information Commissioner's Office (ICO), 2019, s. 33). Bu yöntem sayesinde, rızanın geçerli ve Direktif'e uygun şekilde alınabilmesi de mümkün olabilecektir. Ek olarak, GVKT m. 25 ışığında, web sitesi işletmecilerinin, web sitelerini "privacy by design" ilkesine uygun olarak ve gizlilik risklerini önceden

dikkate almak suretiyle tasarlamaları da önerilen çözüm yöntemlerinden biridir(Information Commissioner's Office (ICO), 2019).

GVKT m. 26, iki veya daha fazla veri sorumlusunun, işleme amaçlarını ve yöntemlerini birlikte belirledikleri takdirde "müşterek veri sorumlusu" olacaklarını kabul etmiştir. Buna göre, ilgili kişi, GVKT'den doğan haklarını, müşterek veri sorumlularından her birine karşı ileri sürebilir. ABAD da, Temmuz 2019'da verdiği Fashion ID kararında (C-40/17), web sitesinde, bir sosyal medya eklentisine yer veren ve bu vesileyle söz konusu sosyal medya sağlayıcısına, kendi sitesini ziyaret eden kişilerin kişisel verilerini ileten bir site operatörünü veri sorumlusu olarak kabul etmiştir. Karara göre, söz konusu veri sorumlusunun sorumluluğu, ilgili web sitesinin işlenme amaç ve araçlarını belirlediği işlemler ile sınırlıdır.

Ulusal veri koruma otoriteleri de benzer görüşler paylaşmaktadırlar. Örneğin, ICO, başka birinin yazılım bileşenini, örneğin üçüncü taraf kodunu kullanan veri sorumlularının da bir kullanıcının cihazında bilgileri depolayabilecek veya depolanan bilgilere erişebilecek herhangi bir yazılım bileşeninin davranışını anlamakla yükümlü olduğunu ifade etmektedir(Information Commissioner's Office (ICO), 2019, s. 16). Keza, bir web sitesini ziyaret eden kişilerin terminal cihazlarına, bu web sitelerinin izni doğrultusunda sosyal medya platformları tarafından çerezler yüklenmekteyse, söz konusu web sitesi ve platformun, müşterek veri sorumlusu olacakları ifade edilmektedir. Zira, söz konusu web sitesi, platformun oluşturduğu çerezleri doğrudan kontrol edemezse de, o platformda varlık gösterip göstermemeye kendisi karar vermektedir. Keza, bu ziyaretçilerin kişisel verilerinin işlenmesinin amacını (bu veriler kullanılarak oluşturulacak istatistiki bilgileri) ve araçlarını belirlemekten ötürü sosyal medya platformuyla müştereken sorumlu olacaktır(Information Commissioner's Office (ICO), 2019, s. 42). Benzer bir görüş CNIL tarafından da ifade edilmektedir. CNIL'e göre, kendi sitesinden veya mobil uygulamasından üçüncü taraf çerezler yerleştirilmesine izin veren kuruluş, kullanıcı izni almak için bir mekanizmanın etkin bir şekilde varlığını sağlamalıdır. Zira söz konusu web sitesi, ziyaretçileri ile doğrudan iletişim içinde olup gerekli bilgilendirmeleri en kolay şekilde yapabilecek durumdadır. Söz konusu web sitesi ve üçüncü taraf, veri işlemenin amaç ve araçlarını birlikte belirledikleri durumda müşterek veri sorumlusu olarak nitelendirileceklerdir(CNIL, 2020, s.7).

Tüm bu çözüm önerilerinin varlığına rağmen, üçüncü taraf çerezlerde hangi tarafın sorumlu olacağı ve rızanın nasıl alınması gerektiği konusu, çerezler bakımından en tartışmalı ve çözümü en zor konulardan biri olmaya devam etmektedir. Tüzük kapsamında bu hususa yönelik açık bir düzenleme bulunmadığından, bu tartışmanın Tüzük yürürlüğe girse dahi son bulmayacağı düşünülmektedir. Öte yandan, günümüzde üçüncü taraf çerezlerin kullanımı farklı web sağlayıcıları tarafından engellenmeye veya kısıtlanmaya başlanmıştır. Zira, Google 2022 itibariyle üçüncü taraf çerez uygulamalarını aşamalı olarak durduracağını açıklamıştır. Safari ve Firefox da benzer bir uygulama yürütmektedir. Bu kısıtlamalar ışığında, üçüncü taraf çerezlerin yakın gelecekte kullanımının sona ereceği ve üçüncü taraf çerezlere ilişkin sorumluluk tartışmalarının bu nedenle son bulacağı düşünülmektedir (Bump, 2021; Schechner, 2021).

TÜRK HUKUKUNDA ÇEREZLER

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun Çerezlere İlişkin Kapsamı

Çerezler, gerçek kişilerin ziyaret ettikleri internet sitesi operatörlerince bu kişilerin bilgisayarlarına yerleştirilen metin dosyalarıdır. Bunlar, rakam ve harf kombinasyonları içermekte olup tek başlarına kişisel veri niteliği taşımazlar. Ne var ki, çerezlerin başka bilgilerle birleşmek suretiyle dahi bir

kimseyi belirlenebilir kılmaları mümkündür(Çekin, 2018, s. 188; Oy, 2021). Örneğin, kullanıcıların IP adreslerini toplayan ve işleyen çerezler ile bir internet sayfası üzerindeki bir kayıt ya da satış formuna girilen isim ve e-posta adresi gibi bilgileri toplayan çerezler kişisel veri kabul edilmelidir(Oy, 2021).

6698 sayılı Kanun, kimliği belirli veya belirlenebilir gerçek kişilere ilişkin her türlü bilginin işlenmesini konu almaktadır. O halde, çerezler de tek başına veya başka bilgilerle birlikte kullanıldıklarında, kimliği belirlenebilir bir kişiyle ilişkilendirilebildikleri ölçüde 6698 sayılı Kanun kapsamına girecektir. Bu bağlamda, çerezlerin tek başına veya birtakım başka bilgilerle birleştirilmeleri suretiyle bir gerçek kişi ile ilişkilendirilmeleri mümkün olduğundan, çerezler suretiyle 6698 sayılı Kanun kapsamında kişisel veri işleme faaliyetinin gerçekleşmesi söz konusu olabilir.

Kişisel Verileri Koruma Kurulu da çerez uygulamalarının KVKK kapsamına girdiği görüşündedir. Nitekim Kurul, Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkında verdiği 2020/173 sayılı kararda, web sitesine girişle birlikte, çerezler vasıtasıyla kişisel verilerin işlenmeye başlamasına karşın aydınlatmanın yapılmaması ve rızanın alınmaması nedeniyle 6098 sayılı Kanun kapsamında yaptırım uygulamıştır[8].

Elektronik Haberleşme Kanunu ve Çerez Uygulamaları İlişkisi

Türk hukukunda, özel olarak çerezlere ilişkin yegane hüküm 5809 sayılı Elektronik Haberleşme Kanunu'nda (EHK) yer almaktadır. İlgili Kanunun 51. maddesinin 3. fıkrasına göre: *"Elektronik haberleşme şebekeleri, haberleşmenin sağlanması dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili abonelerin/kullanıcıların verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve açık rızalarının alınması kaydıyla kullanılabilir."*

Yukarıdaki fıkra bahsi geçen, "abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak" ifadesi, bu kişilerin bilgisayar, cep telefonu, tablet ve benzeri cihazlarına çerez ve benzeri uygulamalar yerleştirilmesini ifade etmektedir. O halde, elektronik haberleşme sektöründe, işletmeciler tarafından çerezler aracılığıyla kişisel veri işlenmesi EHK kapsamına girmektedir. Bu çerçevede, tıpkı AB mevzuatında olduğu gibi, bir kimsenin terminal cihazına çerez yerleştirilmesi için, kural olarak bu kişinin açık ve kapsamlı bilgilendirmeye dayalı açık rızası alınmalıdır. İstisnaen, haberleşmenin sağlanması bakımından gerekli olan çerezlerin bu tür rıza alınmaksızın dahi yerleştirilmesi mümkündür.

EHK m. 51 hükmünde yer alan istisnanın kaynağının, 2002/58/EC sayılı Direktifin 5. maddesinin 3. fıkrasına dayandığı söylenebilir. Nitekim, söz konusu hükümde, çerezlerin aydınlatılmış rıza aranmaksızın yerleştirilmesine izin verilen iki halden söz edilmektedir. EHK m. 51/3 hükmünde belirtilen istisna ise, bu istisnalardan Kriter A'yı karşılamaktadır. Bunun dışında, Kriter B veya Tüzük ile yürürlüğe konulması düşünülen istisnalardan hiçbirisi, EHK'da yer almamaktadır.

EHK Kapsamına Giren Çerezler Bakımından KVKK'daki Veri İşleme Şartlarına Dayanılabilir Mi?

Yukarıda ifade edildiği üzere, Türk hukukunda çerezler hem KVKK'nın hem de EHK'nın kapsamına girmektedir. O halde, çerezler aracılığıyla gerçek kişilere ait verilerinin işlendiği hallerde bu iki kanundan hangisinin uygulanacağının ortaya konulması gereklidir. Bu husus özellikle çerezlerin kullanımına yönelik "veri işleme şartları" bakımından önem taşımaktadır. Zira EHK'da belirtilen veri işleme şartları, KVKK'da sayılanlardan daha dar kapsamlıdır.

AB Hukukunda, çerezler aracılığıyla kişisel verilerin işlenmesi bakımından, GVKT'deki, veri işleme şartlarına dayanılmasının mümkün olup olmadığına ilişkin bir tartışma gündeme gelmemektedir. Zira, AB hukukunda, bir kimsenin terminal cihazına hangi surette çerez yerleştirilebileceği meselesi, GVKT karşısında özel hüküm niteliğinde olan e-Gizlilik Direktifi bağlamındadeğerlendirilmektedir. Söz konusu Direktif ise, açık rıza dışında bir kimsenin terminal cihazına çerezlerin yerleştirilebileceği iki istisnai hal öngörmüştür (Kriter A ve B). Oysa Türk hukukunda, doğrudan doğruya e-Gizlilik Direktifi'ne karşılık gelen bir düzenleme bulunmamaktadır. Buna karşılık, çerezlere ilişkin olarak e-Gizlilik Direktifi'nde öngörülen düzenlemenin bir benzeri, hukukumuzda Elektronik Haberleşme Kanunu'nun 51. maddesine derç edilmiştir. Bu nedenle, EHK m. 51 hükmünün kapsamı ve EHK kapsamına giren hallerde, KVKK'da sayılan veri işleme şartlarına dayanılarak çerez kullanımına başvurulmasının mümkün olup olmadığı tartışmaya açıktır.

EHK m. 51/3 hükmünün kapsamının tespiti bakımından yanıtlanması gereken ilk soru, hükümde geçen "işletmeci" ifadesinden ne anlaşılması gerektiğidir. Zira, EHK'da düzenlenen hüküm işletmeciler tarafından yerleştirilecek çerezleri konu almaktadır. Özellikle, web sayfası operatörleri (örneğin, Google) gibi diğer veri sorumlularının da hükmün kapsamına girip girmeyeceği tespit edilmelidir.

Kanımızca, hükümde geçen "işletmeciler" ifadesinin sadece elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve altyapısını işleten şirketleri kapsar şekilde dar anlaşılması gerekmektedir. Zira EHK, özel olarak elektronik haberleşme sektörünü düzenlemekte ve işletmeciler yönünden ağır yükümlülük ve sorumluluklar öngörmektedir. Bu nedenle, kanunda geçen işletmeci kavramı da "yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirketi" ifade etmektedir (EHK m. 3/1/z). Her ne kadar, teknolojik gelişmeler ile uyumlu olarak, AB mevzuatında da geleneksel telekomünikasyon işletmelerinin yanı sıra, internet tabanlı servis sağlayıcılarının çerez kullanımı bakımından geleneksel telekomünikasyon işletmeleri ile aynı hükümlere tabi tutulmaları hedeflenmekteyse de, EHK'da yer alan mevcut "işletmeci" tanımı, EHK m. 51/3 hükmünün OTT'lere veya diğer bilgi toplumu servis sağlayıcılarına uygulanmasına imkan vermemektedir.

İşletmeci kavramını tanımladıktan ve böylelikle EHK m. 51/3 hükmünün kişi yönünden kapsamını belirledikten sonra değerlendirilmesi gereken ikinci mesele, KVKK ile EHK arasındaki ilişkidir. Öğretide de isabetle savunulan ve bizim de katıldığımız görüşe göre, KVKK kişisel verilerin işlenmesi bakımından genel hüküm niteliğindedir. Bu nedenle, KVKK ister çerezler aracılığıyla ister başka yollarla gerçekleştirilen tüm veri işleme faaliyetlerini kapsamaktadır. Buna karşılık, EHK m. 51/3, doğrudan doğruya elektronik haberleşmeyi, çerezleri ve bunların işletmeciler tarafından kullanılmasını düzenleyen bir özel hüküm niteliğindedir[9]. Bilindiği üzere, aynı konuyu düzenleyen iki kanun bulunduğunda, bunlardan birisi özel diğeri genel hüküm niteliğinde ise özel hüküm uygulanacaktır (Article 29 Data Protection Working Party, 2010, s. 10). O halde, ister kişisel verilerin işlenmesi ister başka amaçlarla yerleştirilsin, hukukumuzda bir kimsenin terminal cihazına "işletmeciler tarafından" çerez yerleştirilmesine ilişkin özel düzenleme EHK m. 51/3 hükmüdür. Bu hükümde anılan istisnanın, EHK kapsamına giren hallere KVKK'nın uygulanması suretiyle genişletilmesi ise mümkün değildir.

Gerçekten de, EHK m. 51/3 hükmünde yer verilen tek bir istisna söz konusu olup, bu da söz konusu çerezin kullanılmasının, haberleşmenin sağlanması bakımından zorunlu olmasıdır. Buna göre, işletmeciler tarafından, bir kimsenin terminal cihazına, hükümde geçen surette çerez yerleştirilmesi için ya kişinin açık rızası bulunmalı ya da söz konusu çerez, haberleşmenin sağlanması bakımından zorunlu olmalıdır. Kanımızca, özel hükümde yer alan istisnaların genel hüküm niteliğindeki KVKK ile genişletilmesi mümkün olmadığından, yürürlükteki hukukumuza göre, KVKK'da sayılan veri işleme şartlarına dayanılarak, işletmecilerin, kullanıcı veya abonelerin terminal cihazlarına çerez

yerleştirmeleri mümkün değildir. Şüphesiz, yapılacak yasal bir değişiklik ile söz konusu istisnaların kapsamının çağın ihtiyaçlarına göre genişletilmesi isabetli olacaktır.

KVKK KAPSAMINDA ÇEREZLER YOLUYLA KİŞİSEL VERİ İŞLENMESİ BAKIMINDAN GEÇERLİ OLABİLECEK VERİ İŞLEME ŞARTLARI NELERDİR?

6698 sayılı KVKK, kişisel verilerin işlenme şartlarını düzenlediği 5. maddesinde, kişisel verilerin veri sahibinin açık rızasıyla işlenebileceği kuralını koyduktan sonra, bu kurala istisna teşkil eden bir dizi veri işleme şartı saymıştır. Bu şartlara dayanılarak bir kimsenin terminal cihazına kişisel veri işleyen çerezler yerleştirilmesinin veya mevcut çerezlere erişilmesinin mümkün olup olmadığı sorusu akla gelebilir.

Hemen belirtmek gerekir ki, özel nitelikli kişisel veriler bakımından Kanunun 6. maddesi devreye girecektir. Kanımızca, bu tür verilerin veri sahibinin açık rızası olmaksızın çerezler yoluyla işlenmesi son derece sınırlı hallerde mümkün olabilir. Zira, söz konusu maddenin üçüncü fıkrasına göre; sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, "*kanunlarda öngörülen hâllerde* ilgili kişinin açık rızası aranmaksızın işlenebilir". Sağlık ve cinsel hayata ilişkin kişisel veriler ise yalnızca "kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, *sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından*" veri sahibinin açık rızası aranmaksızın işlenebilir. O halde, özellikle çerez kullanımı bakımından, her iki istisnanın da son derece sınırlı hallerde karşımıza çıkabileceği görülmektedir.

Özel nitelikli veri olmayan kişisel veriler bakımından ise, özellikle, "bir sözleşmenin kurulması ve ifası amacıyla" ve/veya veri sahibinin "meşru menfaatine" dayalı olarak çerezlerin yerleştirilmesinin mümkün olup olmadığı sorusu sorulabilir[10].

Bir sözleşmenin kurulması veya ifası amacı

Kişisel verilerin işlenmesi bakımından dayanılabilecek sebeplerden bir tanesi, veri işleme faaliyetinin, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili ve gerekli olmasıdır (6698 sayılı Kanun. m 5/2/c). Örneğin, internet üzerinden yapılan bir satışta, satın alınan ürünlerin teslim edilebilmesi için alıcının adres bilgilerinin işlenmesi halinde veri sahibinin rızası aranmaz. Keza, ödemenin sağlanması amacıyla veri sahibinin kredi kartı bilgilerinin işlenmesi de bu çerçevede gerçekleştirilebilir(Avrupa Veri Koruma Kurulu, 2019, s. 10; Avrupa Veri Koruma Kurulu, 2020, s. 16). Yine bir işverenin, çalışanının maaş ve banka hesabı bilgilerini işlemesi de bir sözleşmeden doğan borcun ifasıyla doğrudan ilgilidir(Article 29 Data Protection Working Party, 2014, s. 16). Ancak hüküm yalnızca kurulmuş bir sözleşmenin ifası halini kapsamaz. Nitekim, bir sözleşmenin kurulması öncesinde gerçekleştirilen kimi veri işleme faaliyetleri de bu hükmün kapsamına girmektedir. Örneğin, bir sigorta şirketinden fiyat bilgisi isteyen bir kimsenin aracının marka ve model bilgilerinin işlenmesi söz konusu teklifin verilebilmesi bakımından gereklidir(Article 29 Data Protection Working Party, 2014, s. 18).

Her ne kadar KVKK'nın ilgili hükmünde yer almasa da, gerek 95/46/EC sayılı Direktif'te (m. 7/b) gerek GVKT'de (m. 6/1/b), bir sözleşmenin kurulması amacıyla kişisel verilerin işlenebilmesi için *veri sahibinin bu sözleşmenin kurulması yönünde bir talepte bulunması* gerektiği açıkça ifade edilmektedir. Bu bağlamda, istenmeyen pazarlama faaliyetleri ve veri sorumlusunun münhasıran kendi inisiyatifi ile veya üçüncü kişilerin talebi ile gerçekleştirilen diğer işlemeler söz konusu madde kapsamında yapılamaz(Avrupa Veri Koruma Kurulu, 2019, s. 13). Her ne kadar çevrimiçi davranışsal reklamcılık ve bununla ilişkili olarak veri sahiplerinin takip edilmesi ve profillerinin çıkarılması çevrimiçi

hizmetlerin finansmanında sıklıkla kullanılmaktaysa da, potansiyel bir sözleşmenin kurulması sebebi bu faaliyetler bakımından dayanak teşkil etmez. Zira, davranışsal reklamcılık, kullanıcı ile servis sağlayıcısı arasındaki sözleşmenin objektif amacından bağımsızdır(Avrupa Veri Koruma Kurulu, 2019, s. 14). Kanımızca, bir sözleşmenin kurulması amacıyla kişisel verilerin işlenebilmesi için veri sahibinin bu sözleşmenin kurulması yönünde bir talepte bulunması esasının, hükmün amaçsal yorumu vasıtasıyla KVKK bakımından da aranması uygun olacaktır. Aksi halde, veri sahiplerinin rızası olmaksızın verilerinin işlenmesi ve bu yolla kendilerine sınırsız sayıda sözleşme kurma önerisinde bulunulabilmesinin önü açılacaktır.

Kanımızca, veri sahibinin bir sözleşmenin kurulması yönünde bir talepte bulunması halinde, terminal cihazına çerez yerleştirilebilir. Örneğin, bir kimsenin bir e-ticaret sitesinde sepetine eklediği ürünlerin, çerezler vasıtasıyla işlenmesi, münhasıran bir sözleşmenin kurulması bakımından gerekli olduğu mülahazasıyla mümkün olabilir. Keza bu işleme faaliyeti, veri sahibinin taraf olduğu bir sözleşmeden doğan borcun ifası ile doğrudan doğruya ilgili ve gerekli olması halinde de gerçekleştirilebilir. Örneğin, bir internet sayfası tarafından kullanıcılara kişiselleştirilmiş içerik sunulması hizmeti kimi hallerde bir sözleşmenin ifası sebebine dayanılarak gerçekleştirilebilir. Bu bağlamda, söz konusu hizmetin doğası; ortalama veri sahibinin beklentileri ve söz konusu hizmetin kişiselleştirme faaliyeti gerçekleştirilmeksizin yerine getirilmesinin objektif olarak mümkün olup olmadığı belirleyici olur. Bu bağlamda, farklı haber kaynaklarını derleyerek kullanıcılarına tek bir arayüz üzerinden önceden bildirdikleri ilgi alanlarına göre haberler sunan bir çevrimiçi haber sitesi, kullanıcı verilerinin işlenmesi bakımından sözleşmenin ifası sebebine dayanabilir(Avrupa Veri Koruma Kurulu, 2019, s. 15). Bu durumda, kullanıcı tercihlerinin çerezler yoluyla işlenmesi mümkün olabilir. Bu bağlamda, söz konusu veri işleme sebebi, Direktif'te yer alan Kriter B istisnasını kısmen de olsa karşılamış olacaktır.

Meşru menfaat gerekçesi

KVKK (m. 5/2/f), "ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenebileceğini düzenlemektedir. Meşru menfaat istisnasının 95/46/EC sayılı Direktif (m. 7/f) ile onun yerini alan GVKT'de (m. 6/1/f) de kabul edildiği görülmektedir. Örneğin, dolandırıcılığın önlenmesi veya şebeke ve bilgi güvenliğinin sağlanması amacıyla kişisel verilerin işlenmesi ile grup şirketleri içinde iç idari işleyişin sağlanması amacıyla veri aktarımı yapılması GVKT'nin (Gerekçe m. 47 vd) meşru menfaatin varlığını kabul ettiği haller arasındadır. Keza doğrudan pazarlama amacıyla kişisel verilerin işlenmesi de meşru menfaat kapsamında *değerlendirilebilir*. Ne var ki doğrudan pazarlama amacıyla kişisel verilerin işlendiği hallerde veri sahiplerinin daima bu işlemeye itiraz hakkı bulunmaktadır (GVKT Gerekçe m. 70).

Meşru menfaatin varlığı, buna dayanılarak kişisel verilerin işlenmesi bakımından yalnızca ilk adımdır. Zira ikinci aşamada, veri işlemenin zorunlu olup olmadığı değerlendirilmelidir. Veri işlemenin zorunlu olduğunun tespit edilmesi halinde ise, bu işleme nedeniyle ilgili kişinin temel hak ve özgürlüklerinin zarar görüp görmeyeceği tespit edilmelidir. Bu noktada, KVKK'da yer alan düzenlemenin lafzına bakıldığında, meşru menfaat istisnasına dayanılarak ilgili kişilerin verilerinin işlenmesinin AB düzenlemelerinden daha kolay olacağını ifade etmek gerekir. Zira AB mevzuatında yalnızca ilgili kişilerin temel hak ve özgürlüklerine değil, "*menfaat veya* temel hak ve özgürlüklerine" atıfta bulunulmaktadır. Bu bağlamda, bir kimsenin temel hak ve özgürlükleri arasında sayılmayan bir menfaatine zarar veriliyor olması da, veri sorumlularının, meşru menfaat istisnasına dayanamamalarına yol açabilir. Buna karşılık, AB uygulaması, veri sorumlusunun meşru menfaatleri ile ilgili kişinin menfaat veya temel hak ve özgürlüklerinin dengelenmesi gerektiğinden söz eder. O halde, ilgili kişinin zarar gören menfaatinin, veri sorumlusunun meşru menfaati karşısında göz ardı edilebilir büyüklükte olması halinde, meşru menfaat sebebine dayanılarak veri işlenmesi mümkün olacaktır. Oysa, KVKK'ya göre, meşru menfaat gerekçesiyle veri işlenebilmesi "ilgili kişinin temel

hak ve özgürlüklerine zarar vermemek kaydıyla" mümkündür. O halde, ilgili kişinin temel hak ve özgürlüklerine zarar verilen hallerde meşru menfaat istisnasına dayanılmasının önü her durumda kapalıdır.

E-Gizlilik Direktifi'nde, çerezler bakımından meşru menfaat istisnasına dayanılabileceğine ilişkin bir hüküm bulunmamaktadır. Bu istisna, E-Gizlilik Tüzüğü taslağının eski versiyonlarında bulunmakla birlikte, fazla açık uçlu olduğu yönünde gelen sert eleştiriler dikkate alınarak son taslağa dahil edilmemiştir. Nitekim, Avrupa Veri Koruma Kurulu da, Tüzük'te, meşru menfaat gibi açık uçlu veri işleme şartlarına yer verilmemesi gerektiği görüşündedir(Avrupa Veri Koruma Kurulu, s. 1). Kimileri bu değişikliği övgüyle karşılarken, telekom şirketleri, Tüzük'te meşru menfaat istisnasına yer verilmemesinin, inovasyonu engelleyeceği ve AB'nin veri ekonomisine dayalı hedeflerini baltalayacağını dile getirmektedir(Stolton, 2020).

Yukarıda da ifade edildiği üzere, AB hukukunda çerez uygulamaları münhasıran Direktif'e tabi olup, çerezlerin kullanılması bakımından GVKT'de yer alan veri işleme şartlarına (istisnalara) dayanılması mümkün değildir. Ancak Türk hukukunda, EHK kapsamına girmeyen işleme faaliyetleri bakımından, KVKK'daki veri işleme şartlarına ve bu bağlamda, meşru menfaat istisnasına dayanılması mümkündür.

Kanımızca, Türk hukukunda, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması halinde, bir kullanıcı veya abonenin terminal cihazlarına çerez yerleştirilmesi veya bu cihazlarda bulunan çerezlere erişilmesinin mümkün olduğu kabul edilmelidir. Bununla birlikte, "meşru" menfaat kavramının kapsamına nelerin gireceği ve ilgili kişinin temel hak ve özgürlüklerinin çerçevesinin çizilmesi önem taşımaktadır. Örneğin, Article 29 Çalışma Grubu, Direktif'te yer alan düzenlemeye ilişkin olarak yayınladığı görüşünde, söz konusu menfaatin, genel anlamda toplumun menfaati olabileceği gibi bir şirketin potansiyel müşterileri hakkında olabildiğince fazla miktarda bilgiye sahip olmasını da kapsadığını ifade etmektedir. Ancak bu menfaatin "meşru" olabilmesi için hukuka uygun, yeterince belirli, gerçek ve mevcut bir menfaat olması gerekmektedir(Article 29 Data Protection Working Party, 2014, s. 24 vd).

Kanımızca, KVKK'daki meşru menfaat istisnası, Direktif'in Kriter A kapsamına soktuğu halleri kapsayacak niteliktedir. Bu bağlamda, bir web sitesinin çalışması bakımından zorunlu olan çerezlerin, hukukumuzda meşru menfaat istisnası kapsamında kullanılması mümkündür. Zira, bu durum, veri sahiplerinin temel hak ve özgürlükleri bakımından herhangi bir tehlike teşkil etmeyecektir. Keza, anonim veri işleyen ve profilleme amacıyla kullanılmayan analitik çerezlerin de veri sorumlularının meşru menfaatlerine dayanılarak kullanılması mümkün olmalıdır. Bunun kabulü, AB'deki mevcut yaklaşım ile de uyumlu olacaktır. Bu bağlamda, KVKK'daki veri işleme şartlarına dayanılarak çerezlerin kullanılmasına imkan tanıyan hukukumuz, GVKT'de sayılan veri işleme şartlarına başvurulmasına imkan tanımayan AB mevzuatından daha esnektir. Bununla birlikte, profilleme ve davranışsal reklamcılık amacıyla kullanılan çerezlerin, veri sahiplerinin meşru menfaatlerine dayanılarak, kullanılmasına izin verilmemelidir. Nitekim, veri sorumlularının, çerezlerin kullanımıyla sağlanacak ekonomik menfaatleri, kişilerin mahremiyetlerinin ihlalini meşru kılmayacaktır.

ÇEREZLER YOLUYLA VERİ İŞLEME FAALİYETİNDE AYDINLATMA YÜKÜMLÜLÜĞÜ VE RIZA

Çerez kullanımına ilişkin aydınlatmanın ne şekilde yapılması gerektiği de ele alınması gereken bir diğer meseledir. Zira, kullanılan çerezlerin türünden bağımsız olarak, kişisel verilerin işlendiği

hallerde, veri sorumlularının ilgili kişileri aydınlatma yükümlülüğü bulunmaktadır (6698 s. Kanun, m. 10). Aydınlatma yükümlülüğünün yerine getirilmesine ilişkin esaslar, 10 Mart 2018 tarihli ve 30356 sayılı Resmi Gazete'de yayınlanan tebliğ (Tebliğ) ile detaylıca ele alınmıştır. Keza, Nisan 2019'da Kişisel Verileri Koruma Kurumu tarafından yayınlanan, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi de meseleye ilişkin açıklayıcı bilgiler içermektedir.

Aydınlatma yükümlülüğü, ister ilgili kişinin açık rızasına, ister kanundaki diğer işleme şartlarına bağlı olarak yapılsın, kişisel verilerin işlendiği her durumda yerine getirilmelidir (m. 5/1/a). Bildirim; anlaşılır, açık ve sade bir dil kullanılarak yapılmalıdır (m. 5/1/ğ). Bununla birlikte, açık rıza şartına dayalı olarak kişisel verilerin işlenmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemleri ayrı ayrı yerine getirilmelidir (m. 5/1/f).

Tebliğde, rızanın, kişisel verilerin elde edilmesi sırasında ve ilgili kişilerin bilgilendirilmesi suretiyle alınması gerektiği belirtildikten sonra, yapılacak bilgilendirmede bulunması gereken asgari konular da sayılmıştır. Buna göre: veri sorumlusunun ve varsa temsilcisinin kimliği; kişisel verilerin hangi amaçla işleneceği; kişisel verilerin kimlere ve hangi amaçla aktarılabileceği; kişisel veri toplamanın yöntemi ve hukuki sebebi (veri işleme şartları); ilgili kişinin 6698 sayılı Kanunun 11 inci maddesinde sayılan diğer hakları hakkında bilgi verilmelidir (m. 4). Bunlar arasında, konumuz bakımından en önemli iki hak, kişisel verilerin silinmesini veya yok edilmesini isteme hakkı ile işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakkıdır. Zira, özellikle davranışsal pazarlama çerezlerinin, ilgili kişilerin aleyhine sonuç doğurması mümkündür.

Çerezler bağlamında aydınlatmanın nasıl yapılması gerektiği meselesini 2013 yılında ele alan Article 29 Çalışma Grubu, kullanıcının bir web sayfasına giriş yaptığı sırada ve karşısına çıkan ilk sayfada, çerezlerin kullanımına ilişkin açık, kapsamlı ve görünür bir bildirim yapılması gerektiğini ifade etmektedir. Bu aşamada, kullanıcılar, web sitesi tarafından kullanılan farklı amaçlarla kullanılan tüm çerez türlerine ilişkin bilgiye erişebilmelidirler. Bu çerçevede, web sitesi tarafından kullanılan tüm çerez türlerinin sunulduğu bir sayfanın bağlantı bilgisinin (link) paylaşılabileceği ifade edilmektedir. Keza, çerezlerin kullanım amaçları ile kullanılan üçüncü taraf çerezlere ve çerezler yoluyla üçüncü taraflara veri aktarımına ilişkin bilgilendirme yapılmalıdır. Çerezlerin hangi süreyle saklanacağı da paylaşılması gereken bilgilerdendir. Son olarak, kullanıcılara sahip oldukları seçenekler (çerezlerin tamamını veya bir kısmını kabul etmek veya hiçbirini kabul etmemek) ve gelecekte bu tercihi nasıl değiştirebilecekleri konusunda da bilgi verilmelidir(Article 29 Data Protection Working Party, 2013, s. 3). Kanımızca, bu esaslar Türk hukuku bakımından da kabul edilebilir.

Aydınlatmanın gerekli şekilde yapılması, kullanıcı veya veri sahibinden alınacak rızanın geçerliliği bakımından önemli bir unsur olmakla birlikte, tek ölçüt değildir. Zira, rıza internet sitesini giriş sırasında ve özgür iradeyle verilmelidir(Article 29 Data Protection Working Party, 2013, s. 2 vd.). ABAD'ın da benimsediği üzere, rıza aktif davranışla verilmelidir. Bu bağlamda, zorunlu çerezler dışındaki verilerin işlenmesine rıza verildiğine dair kutucuklar önceden işaretlenmemiş olmalıdır. Ayrıca, rızanın kademeli olarak, yalnızca belirli çerezler bakımından ayrı ayrı verilebilmesine imkân tanınmalıdır.

Kanımızca, Türk Hukukunda, web sitesinin çalışması bakımından zorunlu olan çerezlerin kullanıcının önüne seçili olarak gelmesinin mümkün olduğu; fakat analiz, performans, istatistik, reklam ve pazarlama çerezlerinin işaretlenmemiş (seçilmemiş) olarak kullanıcılara sunulması gerekeceği kabul edilmelidir (Dülger, 2021, s. 10; Information Commissioner's Office (ICO), 2019, s. 11). Çerez duvarlarının kullanımı ise, yalnızca, kullanıcılara, çerezleri kabul etmeksizin de söz konusu hizmeti elde edebilecekleri ve çerezlerin kabul edilmesine denk bir seçeneğin sunulması halinde mümkün

olabilmelidir. Kanımızca, bu türden bir seçeneğin bulunması durumunda, kullanıcıların verdikleri rızanın özgür iradeyle verildiğini kabul etmek isabetli olacaktır.

Ziyaret edilen internet sitesi tarafından oluşturulmayıp, diğer internet siteleri, iş ortakları veya servis sağlayıcıları tarafından oluşturulan üçüncü taraf çerezlerin kullanılması durumunda, bilgilendirme ve rıza alma yükümlülüğünün kime ait olacağı da cevaplanması gereken bir başka sorudur. Daha önce de ele aldığımız üzere, AB hukukunda genel eğilim, hem çerezin bulunduğu internet sayfası yayıncısının hem de üçüncü tarafın sorumlu tutulmalarıdır. Hatta bu iki taraf arasında akdedilecek sözleşmeye bir hüküm eklenmesi ve üçüncü taraf çerezler hakkında aydınlatma yapılması ve rızaların alınmasına ilişkin esaslar düzenlenmesi önerilmektedir(Information Commissioner's Office (ICO), 2019, s. 33).

GVKT m. 26, iki veya daha fazla veri sorumlusunun, işleme amaçlarını ve yöntemlerini birlikte belirledikleri takdirde "müşterek veri sorumlusu" olacaklarını kabul etmiştir. Buna göre, ilgili kişi, GVKT'den doğan haklarını, müşterek veri sorumlularından her birine karşı ileri sürebilir. KVKK'da bu konuda açık bir hüküm bulunmamakla birlikte, Türk Hukukunda da birden fazla veri sorumlusunun, kişisel verilerin işleme amaçlarını ve vasıtalarını birlikte belirlemeleri halinde, bu kişilerden her birisinin veri sorumlusu olarak ilgili kişiye karşı müteselsilen sorumlu olacakları savunulmaktadır(Develioğlu, 2017, s. 102). Bu bağlamda, üçüncü taraf çerezlerin kullanıldığı hallerde, veri sahiplerinin menfaatlerinin korunması gereği, ilgili web sitesi ile üçüncü tarafın her ikisinin de veri sorumlusu kabul edilmeleri isabetli olacaktır.

Türk Hukukunun AB Mevzuatı ve Güncel İhtiyaçlarla Uyumlaştırılması Bakımından Öneriler

Yukarıda da ifade edildiği üzere, AB hukukunda çerezlere ilişkin özel bir düzenleme bulunmakla birlikte, Türk hukukunda çerezlere ilişkin yegane özel hüküm EHK içerisinde yer almaktadır. Direktif bünyesinde yer alan; veri işleme güvenliği, iletişimin gizliliği, veri saklama ve trafik ve konum verilerinin işlenme usulleri gibi konular EHK ve ilgili mevzuatta belli bir çerçevede düzenlenmekte ise de, doğrudan çerezlere yönelik ve güncel AB düzenlemeleri standardında bir düzenleme Türk hukukunda mevcut değildir.

EHK m. 51/3 hükmü, kişi yönünden kapsamı itibariyle yalnızca işletmecilere uygulanabilir niteliktedir. Ayrıca, söz konusu hüküm, açık rıza dışında, yalnızca elektronik haberleşmenin sağlanması amacıyla çerezlerin kullanılmasına izin verdiğinden AB mevzuatının gerisinde kalmakta, güncel ihtiyaçlara yanıt verememekte ve sektörün beklentilerini karşılayamamaktadır. EHK kapsamına girmeyen çerez kullanımları bakımından KVKK hükümlerinin uygulanması mümkün ise de, KVKK da münhasır çerezlerin tabi olacağı hukuki rejimi düzenlemek amacıyla kaleme alınmamıştır. Bu nedenle, mevzuatımızda AB düzenlemeleri ve güncel gelişmeler dikkate alınarak değişiklik yapılması isabetli olacaktır.

Kişisel Verileri Koruma Kurulu'nun, çerezlere ilişkin vermiş olduğu Amazon Türkiye kararı meselenin Kurul'un radarına girdiğini gözler önüne sermektedir. Nitekim, ilgili kararda, Kurul, kullanıcılara bilgi verilmeksizin ve izinleri alınmaksızın web sitesine girişle birlikte çerezler vasıtasıyla kişisel verilerin işlenmeye başlanmasını hem işleme faaliyetindeki açık rıza şartına hem aydınlatma yükümlülüğüne aykırı bulmuştur. Kurul'un vermiş olduğu bu karar, meselenin önemini bir kez daha gözler önüne sermiştir.

Çerezlere yönelik düzenleme ihtiyacı, AB'ye uyum süreçleri için de kritik öneme sahiptir(Avrupa Komisyonu, 2019). Bu bağlamda, Türk hukukunda, doğrudan e-gizliliği konu alan bir yasal düzenlemeye ihtiyaç olduğu da açıktır. Söz konusu ihtiyaç, Bilgi Teknolojileri ve İletişim Kurumu 2019-2023 Stratejik Planı'nda da dolaylı olarak ifade edilmektedir. Stratejik Plan'da, yakın gelecekte tüketicilerin dijital anlamda gizlilik haklarının ve diğer tüketici haklarının korunması ve

güçlendirilmesi için mevzuatın sürekli olarak yenilenmesi ve yeni ihtiyaçlara göre şekillendirilmesinin önem arz ettiği açıkça ifade edilmiş olup, çerezlerin tüketicilerin dijital ayak izlerinin takip edilmesi için yoğun olarak kullanıldığı düşünüldüğünde çerezlere yönelik düzenlemelerin de Stratejik Plan'ın bir parçası olması gerektiği açıktır (Bilgi Teknolojileri ve İletişim Kurumu, 2018).

Yapılacak bu düzenlemeler bakımından, 6698 sayılı Kişisel Verileri Koruma Kanunu yapım sürecindeki hataya düşülmemesi ve hazırlık aşamasında, başta Tüzük olmak üzere güncel AB düzenlemelerinin dikkate alınması gerektiği düşünülmektedir. Öyle ki, Kişisel Verileri Koruma Kanunu'nun 95/46/EC sayılı Direktif'i model almış olması, Türk mevzuatının, GVKT'yi kabul eden AB'nin gerisinde kalmasına sebep olmuştur. Bu eksiklik, Kurul kararlarıyla kapatılmaya çalışılmakta ise de bu durumun uygulamada belirsizlik yarattığı aşikardır. Bu bağlamda, olası bir mevzuat değişikliği sürecinde dikkat edilmesi gerektiğini düşündüğümüz başlıca hususlar şunlardır:

i. Yürürlükteki mevzuatta bulunan "elektronik haberleşme" ve "işletmeci" kavramları, teknolojik gelişmeler dikkate alınarak güncellenmelidir. Bu bağlamda, AB'de kısa süre önce yürürlüğe giren Elektronik Haberleşme Yasası'ndaki (EECC) tanıma uygun olarak, anlık mesajlaşma, IP üzerinden görüşme ve web tabanlı e-posta uygulamalarındaki haberleşme ("Şebekeler Üstü Hizmet") ve bunları sağlayan bilgi toplumu servis sağlayıcılarını da kapsayacak şekilde yeni bir tanımın oluşturulması yoluna gidilmelidir. Böyle bir değişiklik, çerez uygulamalarından kaynaklanan sorumluluğa ilişkin belirsizlikleri de ortadan kaldıracağı gibi, "veri gözetimi" (data surveillance) faaliyetleri ve otomatik veri işleme yöntemlerinden kaynaklanan gizlilik riskleri de önemli ölçüde azalacaktır.

ii. AB mevzuatındaki aydınlatma ve rıza alma standartları dikkate alınmalıdır. Aydınlatma metinlerinde aranacak asgari koşullar ile geçerli rızanın özellikleri ile verilme usulü yasal düzenlemeye kavuşturulmalıdır. Ayrıca, web sitesi işletmecilerinin web sitelerini AB standartlarına uygun şekilde dizayn etmeleri sağlanmalıdır.

iii. Tüzük kapsamındaki istisnaların tamamı dikkate alınmalı ve dijital gelişmeleri bütünüyle kapsayacak bir düzenleme yapılmalıdır. Bu bağlamda, yalnızca Kriter A ve Kriter B benzeri istisnaların getirilmesinin, dijitalleşmenin tüm hızıyla arttığı dünyamız için yetersiz kalacağı düşünülmektedir.

SONUÇ

Çerezler nitelik itibariyle kişisel veri olmamakla birlikte, çerezler aracılığıyla elde edilen veriler, kişisel veri niteliği taşıyabilir. Avrupa Birliği'nde uzun yıllardan beri özel olarak düzenlenen bu konu, Türk hukukunda Elektronik Haberleşme Kanunu'nun 51. maddesinin 3. fıkrasında düzenlenmiştir. Ancak söz konusu hüküm yalnızca "işletmecilere" uygulanabilir niteliktedir. Bu nedenle, EHK kapsamına girmeyen hallerde, çerez uygulamalarına 6698 sayılı Kanun'un uygulanması mümkün olabilir.

6698 sayılı Kanun uyarınca, bir kimsenin terminal cihazına çerez yerleştirilebilmesi veya hali hazırda mevcut olan bir çerezin kullanılabilmesi için kural olarak ilgili kişinin açık rızası gerekmektedir. Ancak istisnaen, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili ve gerekli olması halinde ya da ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sahibinin meşru menfaatine dayanılarak da çerezlerin kullanılması kabul edilebilir. Örneğin, bir kimsenin bir e-ticaret sitesinde sepetine eklediği ürünlerin, çerezler vasıtasıyla işlenmesi, münhasıran bir sözleşmenin kurulması bakımından gerekli olduğu mülahazasıyla mümkün olabilir. Keza bu işleme faaliyeti, veri sahibinin taraf olduğu bir sözleşmeden doğan borcun ifası ile doğrudan doğruya ilgili ve gerekli

olması halinde de gerçekleştirilebilir. Ayrıca, zorunlu çerezler ile anonim veri işleyen ve profilleme amacıyla kullanılmayan analitik çerezlerin de veri sorumlularının meşru menfaatlerine dayanılarak kullanılması mümkün olmalıdır.

EHK m. 51/3 hükmü, kişi yönünden kapsamı itibariyle yalnızca işletmelere uygulanabilir nitelikte olmasının yanında barındırdığı veri işleme şartları yönünden de AB mevzuatının gerisinde kalmakta, güncel ihtiyaçlara yanıt verememekte ve sektörün beklentilerini karşılayamamaktadır. KVKK ise münhasır çerezlerin tabi olacağı hukuki rejimi düzenlemek amacıyla kaleme alınmadığından güncel soru ve ihtiyaçlara yanıt verememektedir. Bu nedenle, Türk hukukunda, tüm çerezlere ve benzer uygulamalara uygulanabilecek nitelikte bir düzenleme yapılarak, kanunlarımızın AB mevzuatı ve teknolojik gelişmelerle uyumlu hale getirilmesi gerekmektedir.

KAYNAKLAR

AEPD. (2020). *Guía sobre el uso de las cookies*. https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf adresinden erişildi.

Article 29 Data Protection Working Party. (2010). *Opinion 2/2010 on online behavioural advertising* (No: 00909/10/EN WP 171). Brussels: Article 29 Data Protection Working Party. https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2010/wp171_en.pdf, adresinden erişildi.

Article 29 Data Protection Working Party. (2012). *Opinion 04/2012 on Cookie Consent Exemption* (No: 00879/12/EN WP 194). Brussels.

Article 29 Data Protection Working Party. (2013). *Working Document 02/2013 providing guidance on obtaining consent for cookies* (No: 1676/13/EN WP 208).

Article 29 Data Protection Working Party. (2014). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (No: 844/14/EN WP 217). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf adresinden erişildi.

Avrupa Komisyonu. (2015). *A Digital Single Market Strategy for Europe* (No: COM(2015) 192). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192 adresinden erişildi.

Avrupa Komisyonu. (2019). *Turkey 2019 Report* (Progression Report No: SWD(2019) 220). https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-turkey-report.pdf adresinden erişildi.

Avrupa Parlamentosu. (2017). *Reform of the e-Privacy Directive* (No: PE 608.661). Briefing: EU Legislation in Progress. Brussels.

Avrupa Veri Koruma Kurulu. (2019). *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* (Guideline). https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf adresinden erişildi.

Avrupa Veri Koruma Kurulu. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679*.

Avrupa Veri Koruma Kurulu. (2021). *Statement 03/2021 on the ePrivacy Regulation*. https://edpb.europa.eu/system/files/202103/edpb_statement_032021_eprivacy_regulation_en_0.pdf adresinden erişildi.

Avrupa Veri Koruma Kurulu. (t.y.). *Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_en.pdf adresinden erişildi.

Bilgi Teknolojileri ve İletişim Kurumu. (2018). *2019-2023 Stratejik Planı*. https://www.btk.gov.tr/uploads/pages/yayinlar-stratejik-planlar/btk-2019-2023-stratejik-plani.pdf adresinden erişildi.

Boban, M. (2019). E-PRIVACY REGULATION – NEW EUROPEAN FRAMEWORK FOR REGULATION ON PRIVACY AND ELECTRONIC COMMUNICATIONS DESIGNED TO PROTECT USER PRIVACY IN THE DIGITAL AGE (ss. 176-187). 47th International Scientific Conference on Economic and Social Development, sunulmuş bildiri, Prague.

Borgesius, Z. ve McDonald, A. M. (2015). Do Not Track for Europe. *Information and Internet Policy paper* içinde . TPRC43: The 43rd Research Conference on Communications, sunulmuş bildiri, Amsterdam: TPRC.

Bump, P. (2021). The Death of the Third-Party Cookie: What Marketers Need to Know About Google's Looming Privacy Pivots. *HubSpot*. https://blog.hubspot.com/marketing/third-party-cookie-phase-out adresinden erişildi.

Cairoli, F. ve Olivi, G. (2020). Cookies and online advertising: An ongoing changing scenario. *JD Supra*. https://www.jdsupra.com/legalnews/cookies-and-online-advertising-an-43737/ adresinden erişildi.

Castelluccia, C. ve Narayanan, A. (2012). *Privacy considerations of online behavioural tracking*. The European Network and Information Security Agency (ENISA).

CNIL. (2019). *Cookies and Other Tracking Tools* (No: 2019-093). France.

CNIL. (2020). *Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019*. https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf adresinden erişildi.

Cofone, I. N. (2017). The way the cookie crumbles: Online tracking meets behavioural economics. *International Journal of Law and Information Technology*, *25*, 38-62.

Cookies, the GDPR, and the ePrivacy Directive. (2020). https://gdpr.eu/cookies/ adresinden erişildi.

Custers, B. (2018). Profiling as Inferred Data: Amplifier Effects and Positive Feedback Loops. *Being Profiled: Cogitas Ergo Sum* içinde. Amsterdam: Amsterdam University Press BV.

Çekin, M. S. (2018). *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku* (1. bs.). İstanbul: On İki Levha.

Data Protection Commision(DPC). (2020). *Cookies and Other Tracking Technologies* (Guidance Note). https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf adresinden erişildi.

Develioğlu, M. (2017). *6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku* (1. bs.). İstanbul: On İki Levha.

Doğan, B. ve Bozkurt, T. (2020). Kişisel Verilerin Korunması Çerçevesinde Çerezler; Türleri, Kullanımları ve Uygulama Örnekleriyle. *Lexpera Blog*.

DUMORTIER, J. ve DE PRETER, C. (2006). The European regulatory framework for security and privacy protection in electronic communications. *ANN. TELECOMMUN*, *61*(3-4), 443-457.

Dülger, M. V. (2021). Yurt Dışına Veri Aktarımında Milyonluk Ceza: Kişisel Verileri Koruma Kurulunun Amazon Kararı. *SSRN*. https://ssrn.com/abstract=3792388 adresinden erişildi.

Edenberg, E. ve Jones, M. L. (2019). Analyzing the legal roots and moral core of digital consent. *New Media & Society*, *21*(8), 1804-1823.

Garzaniti, L. ve O' Regan, M. (2010). *Telecommunications, Broadcasting and the Internet: EU Competition Law & Regulation* (3rd bs.). Londra: Sweet & Maxwell.

Georgiev, N. (2020). Whitelisting stalkers: The answer to fix EU's abhorrent cookie policy? *KU Leuven CITIP*. https://www.law.kuleuven.be/citip/blog/whitelisting-stalkers-the-answer-to-fix-eus-abhorrent-cookie-policy/ adresinden erişildi.

Globocnik, J. (2019). On Joint Controllership for Social Plugins and Other Third-Party Content – a Case Note on the CJEU Decision in Fashion ID. *IIC*, *50*, 1034-1044.

Healey, R. (2021). EPrivacy Regulation – What is It? *Formiti*. https://formiti.com/eprivacy-regulation-what-is-it/#:~:text=What%20Does%20the%20EPrivacy%20Regulation,cables%20and%20satellites%20are%20covered adresinden erişildi.

Hildebrandt, M. (2008). Profiling and the Identity of the European Citizen. *Profiling the European Citizen: Cross-Disciplinary Perspectives* içinde (ss. 303-343). Springer Science + Business Media B.V.

Information Commissioner's Office (ICO). (2018). *Privacy and Electronic Communications Regulations* (Guide).

Information Commissioner's Office (ICO). (2019). How do we comply with the cookie rules? https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply14 adresinden erişildi.

Information Commissioner's Office (ICO). (2019). *Use of cookies and similar technologies* (Guidance Note). UK. https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf adresinden erişildi.

Jones, M. L. (2020). Cookies: A legacy of controversy. *Internet Histories*, *4*(1), 87-104.

Kamara, I. ve Kosta, E. (2016). Do Not Track initiatives: Regaining the lost user control. *International Data Privacy Law*, *6*(4), 276-290.

Kosta, E. (2013). Peeking into the cookie jar: The European approach towards the regulation of cookies. *International Journal of Law and Information Technology*, *21*(4), 308-406.

Lee, P. (2011). The impact of cookie 'consent' on targeted adverts. *Journal of Database Marketing & Customer Strategy Management*, *18*, 205-209.

Losnedahl, T. (2018). When should service be regarded as 'electronic communicatiion' services? https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=9FC49697-3D3D-4D8C-B102-35FF8772CA7C adresinden erişildi.

Naranjo, D. (2017). e-Privacy Regulation: Good Intentions but a Lot of Work to Do. *European Data Protection Law Review*, *3*(2), 152-154.

OneTrust. (2020). *THE ULTIMATE COOKIE HANDBOOK FOR PRIVACY PROFESSIONALS*.

Oy, B. (2021). Use of Website Cookies under EU Privacy Law: Practical Tips for Better Compliance. *Lexology*. https://www.lexology.com/library/detail.aspx?g=64772d95-c4c7-4ad0-8a5c-ab66ff564e1e adresinden erişildi.

Planet 49. No. C-673/17 (Avrupa Birliği Adalet Divanı Oca. 11, 2019). http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2427389 adresinden erişildi.

Schechner, S. (2021). Google Pursues Plan to Remove Third-Party Cookies; Alphabet unit is seeking privacy friendly alternatives despite complaints from rivals that use cookies. *Wall Street Journal*. New York.

Skouma, G. ve Léonard, L. (2015). On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection. *Reforming European Data Protection Law* içinde , Law, Governance and Technology (C. 1-20, C. Privacy and Data Protection, ss. 35-63). Brüksel: Springer.

Stolton, S. (2020). German Presidency charts new COVID19 'metadata' rules in leaked ePrivacy text. *Euractiv*. https://www.euractiv.com/section/digital/news/german-presidency-charts-new-covid19-metadata-rules-in-leaked-eprivacy-text/ adresinden erişildi.

Tracking Under the E-Privacy Regulation. (2021). CMS. https://cms.law/en/deu/insight/e-privacy/tracking-under-the-e-privacy-regulation adresinden erişildi.

Vaughan, J. (2020). *Why Data Is Collected and How It Is Used* (Library Technology Report) (ss. 17-27). USA: alatechsource.

Voisin, G., Boardman, R., Assion, S., Nevola, C. C. ve Sampedro, L. (2020). ICO, CNIL, German and Spanish DPA Revised Cookies Guidelines: Convergence and Divergence. *IAPP*. https://iapp.org/resources/article/ico-and-cnil-revised-cookie-guidelines-convergence-and-divergence/ adresinden erişildi.

Voss, W. G. (2017). First the GDPR, Now the Proposed E-Privacy Regulation. *Journal of Internet Law*, 1-11.

Zorer, U. (2019). Çerezler Hakkında Hukuki Değerlendirme. *Medium.com*. https://medium.com/@umutzorer/%C3%A7erezler-hakk%C4%B1nda-hukuki-de%C4%9Ferlendirme-44c58d3eba32 adresinden erişildi.

EK NOTLAR

1. Tüzük taslağının son versiyonu için bkz. https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

2. Sunucu ile tarayıcı arasındaki bu iletişim, Üstün Metin Transfer Protokolü (HTTP) aracılığıyla sağlanmaktadır. Bu protokolü diğer protokollerden farklı kılan husus ise çerezlerin kullanılmasıdır(Skouma ve Léonard, 2015, s. 40). Zira, "*File Transport Protocol*" (FTP) gibi protokollerde sunucu, her web sitesi ziyaretini kullanıcının ilk ziyareti gibi değerlendirmekte ve kullanıcının web sitesini ziyaretinin sonunda sunucudaki bilgiler tamamen silinmektedir.

3. Bazılarına göre, işlevine göre çerez ayrımında "flash çerezler" de başka bir grubu oluşturmaktadır. Bu çerezler de "pazarlama çerezleri" gibi kullanıcıyı takip işlevi görmekte olup diğerlerinden farkı ise bu çerezlerin takibinin ve silinmesi çok daha zor olmasından ileri gelmektedir(OneTrust, 2020, s. 7).

4. Rızanın katmanlı olarak alınması hakkında detaylı bilgi için bkz. (Avrupa Veri Koruma Kurulu, 2020, s. 5)

5. ICO tarafından yayınlanan benzer liste için bkz. ICO, Guidance on the use of cookies and similar technologies, https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf, s.35 vd.

6. Aynı esas farklı veri koruma otoriteri tarafından da benimsenmektedir. Örneğin, bkz. ICO, Guidance on the use of cookies and similar technologies, https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf, s.15.

7. Söz konusu direktif ile "elektronik haberleşme servisi" tanımı değiştirilmiş ve anlık mesajlaşma, IP üzerinden görüşme ve makineden makineye iletişim servislerinin tamamı da bu kavramın altına alınmıştır. Üye ülkelerin, ilgili direktif düzenlemelerini iç hukuk düzenlerine aktarmaları için son tarih 21 Aralık 2020 olarak belirlenmiştir. (Ayrıntılı bilgi için bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN,E.T: 11.04.2021)

8. Kişisel Verileri Koruma Kurulu'nun, "Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili Kişisel Verileri Koruma Kurulu'nun 27/02/2020 Tarihli ve 2020/173 Sayılı Karar Özeti". Bu karar hk. ayrıntılı bilgi için bkz. "https://www.kvkk.gov.tr/Icerik/6739/2020-173" (E.T: 08.05.2021)

9. Benzer bir esas, Avrupa Birliği Genel Veri Koruma Tüzüğü ile e-Gizlilik Direktifi ve e-Gizlilik Tüzüğü bakımından da kabul edilmektedir(Article 29 Data Protection Working Party, 2010, s. 10; Healey, 2021).

10. Web sitesi tarafından verilen hizmetin niteliğine göre, zorunlu çerezlerin, KVKK kapsamında sözleşmenin ifası veya veri sorumlusunun meşru menfaati gerekçesiyle işlenebileceği görüşünde bkz. (Zorer, 2019)