www.kvkk.gov.tr

Kişisel Verileri Koruma Dergisi

Cilt: 2, Sayı: 2

Geliş: 30.05.2020
Kabul: 30.11.2020

E-Gizlilik Tüzüğü Çalışmaları Işığında Türk Hukukunda Elektronik Haberleşmenin Gizliliğinin Korunması

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
2018 yılında yürürlüğe giren Genel Veri Koruma Tüzüğü'nün elektronik haberleşme alanındaki ayağı olan E-Gizlilik Tüzüğü, Avrupa Birliği'nde 2017 yılından bu yana süren çalışmalara rağmen yürürlüğe konulamamıştır. Ancak taslak üzerinde yapılan tüm tartışmalar ve değişiklikler dikkate alındığında, bu Tüzüğün çerçevesi ana hatlarıyla tespit edilebilmektedir. Bu tespit neticesinde yapılacak karşılaştırmalı bir inceleme ise Türk hukuk mevzuatının, elektronik haberleşme sektöründe kişisel verilerin gizliliği bakımından, Avrupa Birliği (AB) hukuku uygulama ve mevzuatının gerisinde kaldığını göz önüne sermektedir. Nitekim yürürlükteki mevzuatımız, doğrudan elektronik haberleşmede e-gizliliğin korunması amacıyla hazırlanmamıştır. Veri akışının önemli ölçüde arttığı ve dijitalleşmenin çığ gibi büyüdüğü dünyada, Türkiye'nin AB başta olmak üzere tüm ülkeler ile sağlam ve sürdürülebilir ekonomik ve politik ilişkiler kurabilmesi için elektronik haberleşme alanındaki ulusal mevzuatın en kısa sürede çağın gereklerine uygun olarak güncellenmesi gerekmektedir.
Anahtar Sözcükler: KVKK, Kişisel Verilerin Korunması, Elektronik Haberleşme, Gizlilik, Çerez

A Review of Protection of Privacy of Electronic Communications under Turkish Law in the Light of the Draft E-Privacy Regulation

ABSTRACT
E-Privacy Regulation, which is part of the reform of the personal data protection legislation in the European Union (EU), has not been finalized since 2017 despite all efforts in the European Union. Nevertheless, the framework of the Regulation can be determined from all discussions and changes made to the draft. Based on this framework, a comparative review between the E-Privacy Regulation and Turkish legislation gives remarkable insights. The Turkish legislation does not directly focus on personal data protection in electronic communications. Issues vital for the regulation of e-privacy, such as cookies, are also not included in the scope of the Turkish legislation. Therefore, legislation lags behind EU legislation in terms of the privacy in the electronic communication sector. In a world where data flow is increasing significantly, and digitalization is growing like an icefall, Turkish legislation in the field of electronic communication must be updated in accordance with the requirements of the digital world for Turkey in order to establish robust and sustainable economic and political relations with all countries, especially the EU.
Keywords: Data Protection, Electronic Communication, GDPR, Privacy, Cookies

Atıf Gösterme Aksoy, H. C. ve Halıcıoğlu, M. (2020). E-Gizlilik Tüzüğü Çalışmaları Işığında Türk Hukukunda Elektronik Haberleşmenin Gizliliğinin Korunması. *Kişisel Verileri Koruma Dergisi. 2*(2), 1-18.

GİRİŞ

2018 yılında Genel Veri Koruma Tüzüğü'nün (GVKT) yürürlüğe girmesi ile kişisel verilerin korunması alanında reform yapan Avrupa Birliği (AB), bu reformun elektronik haberleşme alanındaki ayağı olan E-Gizlilik Tüzüğü'nü (Tüzük) 2017 yılından bu yana süren çalışmalara rağmen yürürlüğe koyamamıştır. Nitekim, telekomünikasyon alanında gizliliği koruyan, 2002 tarihli E-Gizlilik Direktifi'nin (Direktif) teknolojik gelişmeler karşısında kendisinden beklenen korumayı sağlayamadığı gerekçesiyle, bu Direktifin yerini almak üzere ilk olarak 2017 yılının Ocak ayında yayınlanan E-Gizlilik Tüzük taslağı, o tarihten bu yana yapılan çok sayıda değişikliğe rağmen nihai halini alamamıştır.

E-Gizlilik Tüzüğü'nün yürürlüğe girebilmesi için Avrupa Komisyonu, Avrupa Parlamentosu ve Avrupa Konseyi'nin üçlü mutabakatı gerekmektedir. Bununla birlikte, AB'nin yetkili karar organlarının E-Gizlilik Tüzüğü'nün metni üzerinde yakın bir tarihte anlaşmaya varmaları ve Tüzüğün yürürlüğe girmesi, bu çalışmanın kaleme alındığı Mayıs 2020 tarihi itibariyle çok olası gözükmemektedir. Bu çerçevede, Tüzüğün yürürlüğe girmeden önce kaç değişiklikten daha geçeceği belirsiz olduğundan, bu çalışma, Tüzükte yer alan somut düzenlemeleri değerlendirme amacı gütmemektedir. Bununla birlikte, E-Gizlilik Tüzüğü konusundaki çalışmaların yıllardır ısrarla sürdürülmesi, Tüzüğe olan ihtiyacın boyutunu ve AB'nin Tüzüğü yürürlüğe koymaktaki kararlılığını ortaya koymaktadır. Ayrıca, taslak üzerinde yapılan tüm tartışmalar ve değişiklikler dikkate alındığında, nihayetinde yürürlüğe girecek olan Tüzüğün çerçevesinin ana hatlarıyla tespit edilebilmesi mümkündür. Bu çalışmada, E-Gizlilik Tüzüğü'ne olan ihtiyaç, Tüzüğün amacı, kapsamı ve başlıca özellikleri irdelenecek ve özellikle Türk Hukukuna olası yansımaları tespit edilmeye çalışılacaktır. Keza, veri koruma hukuku perspektifinden, elektronik haberleşme alanındaki ulusal mevzuatın çağın gereklerine uygun olarak güncellenmesine yönelik önerilerde de bulunulacaktır.

E-GİZLİLİK DİREKTİFİ'NDEN E-GİZLİLİK TÜZÜĞÜ'NE: ELEKTRONİK HABERLEŞMEDE KİŞİSEL VERİLERİN KORUNMASI

Elektronik Haberleşme Alanında Kişisel Verilerin Korunmasına İlişkin Özel Nitelikli Mevzuat İhtiyacı ve E-Gizlilik Direktifi

1990'lı yılların başından itibaren, teknolojik gelişmeler, dijitalleşme ve Internet (Web 2.0) gibi teknolojilerin Avrupa ülkelerinde yaygınlaşmasının etkisiyle, AB'de liberalleşme ve globalleşme politikalarına hız verilmiştir (Avrupa Komisyonu, 1988). Bu değişim ile birlikte, teknolojik tarafsızlık, rekabetin sağlanması ve korunması gibi ilkeler bu dönemde gerçekleştirilen düzenlemelere hakim ilkeler olarak ön plana çıkmıştır (Avrupa Komisyonu, 2001). Ayrıca, AB'de benimsenen bu yeni yaklaşım, pek çok sektörü de temelinden etkilemiştir. Bu bağlamda, liberalleşme ve globalleşme temelli politika değişikliklerinden en çok etkilenen sektörlerden biri olan telekomünikasyon sektöründe, inovasyonun sürekli hale getirilmesinin yanında Amerika ve Asya endüstrisi ile güçlü bir rekabetin tesis edilmesi amacıyla bir dizi düzenleme paketi yürürlüğe konmuş ve telekomünikasyon sektörü çehre değiştirmiştir (Avrupa Komisyonu, 2001).

AB'deki liberalleşme ve globalleşme odaklı bu yeni yaklaşım, yalnızca telekomünikasyon sektöründe faaliyet gösteren teşebbüsleri değil, telekomünikasyon şirketleri ile doğrudan veya dolaylı bir şekilde ilişki içinde bulunan tüm gerçek kişileri de etkilemiştir. Bu çerçevede, dijitalleşme ve inovasyon ile doğru orantılı olarak veri üretimi de artış göstermiş ve çoğu zaman veri toplama faaliyetinin farkında

dahi olmayan kişiler, yeni dönemde olabildiğince çok veriye sahip olma yarışına giren şirketler karşısında korunmasız hale gelmişlerdir. Bu yüzdendir ki, telekomünikasyon sektörüne yönelik olarak yapılan düzenlemelerin temelinde, pazarda tekelleşmenin ortadan kaldırılması ve serbest rekabetin tesis edilmesi ilkelerinin yanı sıra; AB'de geçmişten günümüze taşınmış olan özgürlük, demokrasi, insan hakları, hukukun üstünlüğü gibi ortak değerler de yerini almıştır. Bu tür düzenlemelerin belirgin örneklerinden bir tanesi ise 2002/58/EC sayılı "*E-Gizlilik Direktifi*"dir.

Direktif, "2002 Düzenleme Paketi"nin bir parçası olup 95/46/EC sayılı Veri Koruma Yönergesi'ni tamamlayıcı nitelikte olan ve Avrupa'da telekomünikasyon sektöründe veri koruma kurallarını düzenleyen 97/66/EC sayılı "Telekomünikasyon Veri Koruma Yönergesi"ni mülga etmek suretiyle, 12 Temmuz 2002 yılında Avrupa Toplulukları Resmi Gazetesi'nde yayımlanarak yürürlüğe girmiştir (Garzaniti, O' Regan, 2010). Bu bağlamda, Direktif'in yürürlüğe girmesiyle birlikte, 97/66/EC sayılı Telekomünikasyon Veri Koruma Direktifi'nde yer alan kavramların çoğu modernize edilmiş ve genişletilmiştir[1].

Direktif'in kapsam ve amaç maddesi incelendiğinde, üye devletlere, elektronik haberleşme sektöründe işlenen kişisel verilere ilişkin olarak kullanıcıların temel hak ve özgürlüklerinin, özellikle özel yaşamın gizliliği hakkının korunmasının sağlanması ile verilerin ve elektronik haberleşme ekipman ve servislerinin topluluk sınırları içinde serbest dolaşımının tesis edilmesi ödevlerinin yüklendiği görülmektedir (E-Gizlilik Direktifi m. 1).

Direktif dört ana başlık üzerinde yoğunlaşmaktadır. Bunlar; (i) veri işleme güvenliği (m. 4), (ii) iletişimin gizliliği (m. 5), (iii) veri saklama (m. 6, 9 ve 15) ve (iv) kullanıcının rızası olmaksızın gerçekleşen iletişim (spam) (m.13) olarak ifade edilebilir. Ayrıca, Direktif'in gerekçesinde tanımlanan ve m. 5/3 kapsamında ele alınan "çerez" (cookies) uygulamaları karşısında kişilerin gizlilik haklarının korunması hususu da AB e-gizlilik kuralları açısından önemli bir yere sahiptir. Nitekim çerez uygulamaları, 2002 yılından günümüze kadar geçen sürede dijital pazarlama, profilleme, davranışsal hedefleme gibi teknoloji hukukunun yakından ilgilendiği konuların merkezinde yer almıştır (Garzaniti, O' Regan, 2010).

Yürürlüğe girmesinden 7 yıl sonra, 2009 yılında, E-Gizlilik Direktifi'nin kimi maddelerinde 2009/136/EC sayılı Direktif ile değişiklik yapılmıştır. Bu değişikliğin başlıca sebepleri, dijitalleşme ile teknolojik gelişmelerin hız kazanmış olması ve özellikle elektronik ticaret, dijital pazarlama, sosyal medya gibi uygulamaların toplumda yaygın hale gelmesidir. Elektronik iletişim sektöründe gizliliğin ve kişisel verilerin korunmasını güçlendirmeyi amaçlayan bu değişiklik neticesinde, (i) elektronik haberleşme servisi sağlayıcıları (örneğin, telekom sağlayıcıları ve ISS'ler) bakımından kişisel veri ihlallerine ilişkin bildirimde bulunma zorunluluğu getirilmiş, (ii) spam uygulamalarına yönelik önlemler genişletilmiş ve (iii) çerezler bakımından kişisel verilerin korunmasını ve özel hayatın gizliliğini güçlendirecek nitelikte değişiklikler yapılmıştır. Bu bağlamda, çerezlere yönelik "opt-out" (kullanıcının yapacağı işlemle çerez uygulamalarını reddetmesi) rejimi terk edilerek "opt-in" (kullanıcıdan çerez uygulamaları bakımından aktif rıza alınması) uygulamasına başlanması, önemli bir değişiklik olarak ön plana çıkmaktadır. Ayrıca, çerezlere yönelik yükümlülükler, telekom sektöründeki şirketlere ek olarak tüm internet sitesi operatörlerini de kapsayacak şekilde genişletilmiştir.

En son 2009 yılında "güncellenen" E-Gizlilik Direktifi'nde son 11 yılda herhangi bir değişiklik yapılmamış olmakla birlikte, geçen süre içerisinde dijitalleşme ve teknolojik gelişmeler çarpan etkisiyle artış göstermeye devam etmiştir. Özellikle OTT (Over The Top – Şebekte Üstü Hizmet) servis uygulamalarının yaygınlaşması, anlık mesajlaşma ve videolu görüşme uygulamalarının artması, profilleme ve veri gözetim faaliyetlerinin önemli şirket faaliyetleri haline gelmesi gibi gelişmeler karşısında, E-Gizlilik Direktifi kendisinden beklenen hukuki çözümleri sunamaz hale gelmiştir (Buttarelli, 2017). Bunun yanı sıra, AB'de ve tüm dünyada meydana gelen önemli gelişmeler de

Direktif'in çağa ayak uyduramamasına yol açmıştır. Örneğin, "Dijital Tek Pazar" politikası AB yasa yapıcılarının en önemli gündem maddelerinden birisi haline gelmiş; verinin "yeni petrol" hatta "yeni para birimi" olarak değerlendirildiği bir dünya düzeninin oluşması ile kişisel verilerin korunması meselesine 2000'li yılların başına göre çok daha fazla önem atfedilmeye başlanmıştır (Marcus, Petropoulos, Yeung, 2019). Bu gelişmeler karşısında atılan en önemli hukuki adımlardan biri olan, kişisel verilerin korunması konusunda öncül düzenleme olarak kabul edilebilecek olan "Genel Veri Koruma Tüzüğü" (GVKT) de yine bu dönemde yürürlüğe girmiştir. Yine, e-gizlilik kurallarını doğrudan ilgilendiren Elektronik Haberleşme Yasası (2018/1972 sayılı Direktif)[2] hazırlanmış olup bu düzenleme elektronik haberleşme kavramının tanımını genişletmesi sebebiyle e-gizlilik kuralları bakımından çok önemli görülmektedir. Keza, tüm bu gelişmeler E-Gizlilik Direktifi'nin güncellenmesini de zorunlu hale getirmiş ve böylelikle E-Gizlilik Tüzüğü taslağının hazırlanmasına giden yol açılmıştır.

E-Gizlilik Direktifi ve Genel Veri Koruma Tüzüğü ile İlişkisi

Kanımızca, Avrupa'da kişisel verilerin korunması hukukunun geçirdiği değişimin aşamaları irdelenmeksizin E-Gizlilik Tüzüğü'ne duyulan ihtiyacı anlayabilmek mümkün değildir. Nitekim, 1995 yılında AB Veri Koruma Direktifi yürürlüğe girdikten sonra teknoloji hızla gelişmiş ve mevcut mevzuat kişisel verileri korumak bakımından yetersiz kalmıştır. Kişisel verilerin ve özel yaşamın sektörel bazda özel olarak korunması ihtiyacı önce E-Gizlilik Direktifi'nin yürürlüğe sokulmasını, ardından GVKT'nin kabul edilmesini gerektirmiştir.

GVKT ve E-Gizlilik Direktifi arasındaki ilişkinin özellikleri ve bu düzenlemelerin "ilgili kişiler" bakımından sağladıkları temel hak ve özgürlükler, hem dijital yaşamda kendi verileri üzerinde kontrolleri önemli ölçüde azalan "ilgili kişiler" için üçüncü kişilere karşı önemli bir koruma kalkanı sağlamış hem de E-Gizlilik Tüzüğü taslağına açılan kapıyı aralamıştır. Nitekim, devam eden teknolojik gelişmeler nedeniyle E-Gizlilik Direktifi'nin de kendisinden beklenen işlevi sağlayamaz hale gelmesi, E-Gizlilik Tüzüğü'ne duyulan ihtiyacı meydana getirmiştir. Bu ihtiyacın ortaya konulabilmesi için öncelikle E-Gizlilik Direktifi ve GVKT arasındaki ilişki ele alınmalıdır.

Hem E-Gizlilik Direktifi hem de GVKT, AB vatandaşlarının dijital gizliliğinin sağlanmasına yönelik düzenlemelerdir. Ancak söz konusu iki düzenleme işlevleri bakımından birebir örtüşmemektedir. Direktif'in iki temel işlevi bulunmaktadır. Bunlardan ilki, daha fazla açıklık ve öngörülebilirlik getirerek, GVKT'de benimsenen ilkelerin iletişim alanında da uygulanabilirliğini sağlamaktır. İkinci olarak Direktif, temel haklar arasında sayılan haberleşme özgürlüğüne anlam kazandıran AB yasal düzenlemesidir (Naranjo, 2017).

E-Gizlilik Direktifi, AB elektronik haberleşme sektörüne yönelik olarak çok çeşitli konularda (faturalandırma işlemleri [m. 7] gibi) düzenlemeler içermekte ise de temelde kişilerin dijital gizliliğini korumaya yönelik insan hakları temelli bir içerik sunmaktadır. Direktif'in tamamında bu yaklaşımın yansımalarını görmek mümkündür. "Haberleşmenin gizliliği" başlıklı, Direktif m. 5 ve 2009 değişikliği kapsamında içeriği genişletilen çerez uygulamalarına yönelik düzenlemeler, bu konuda verilebilecek en iyi örneklerdir. Bu yaklaşım, farklı Avrupa Birliği Adalet Divanı (ABAD) kararlarında da görülebilir (örn. Planet 49 Kararı, 2019; İrlanda Dijital Haklar Kararı, 2014; Tele2 Kararı, 2016)[3].

GVKT ise Avrupa'da kişisel verilerin korunmasına dair düzenlemelerin çağın gereklerine uyarlanması ihtiyacının bir sonucu olan Veri Koruma Reformu'nun bir ürünüdür. Söz konusu reform, dijital çağda kişilerin temel hak ve özgürlüklerinin daha etkin şekilde korunması ve Avrupa Dijital Pazarı'ndaki işletmelerin faaliyet göstermelerini kolaylaştırmak bakımından atılan önemli bir adımdır (Avrupa Komisyonu, 2017). Ayrıca, kişisel verilerin korunmasına yönelik düzenlemeler konusunda AB üye

ülkelerinde bir yeknesaklık bulunmaması ve bu durumun ülkeler arasında uygulama farklılıklarına sebebiyet vermesi de GVKT'nin hazırlanmasındaki en büyük etkenlerden biri olmuştur (Lambert, 2017). Öyle ki, özellikle "Schrems Kararı" ve "İrlanda Dijital Haklar Kararı" gibi kararlar, 95/46/EC sayılı Direktif ve bu direktifi tamamlayıcı nitelikteki düzenlemelerin, AB toplumu için artık yeterli olmadığını ve Avrupa'da, bireylerin kişisel verilerine ilişkin hakları açısından endişe duyulmaya başlandığını ortaya koymuştur (Dülger, 2019). Bu gelişmeler neticesinde, Avrupa Parlamentosu tarafından 24 Mayıs 2016 tarihinde iki yıllık bir geçiş süresi de öngörülerek GVKT onaylanmış ve yürürlüğe konulmuştur.

Direktiften farklı olarak, bir tüzük olan GVKT, AB üye ülkeleri bakımından doğrudan uygulanır niteliktedir. Böylelikle, Avrupa Birliği üye ülkelerinin, kişisel verilerin korunması hususunda hukuki açıdan tamamen uyumlu hale gelmesi amaçlanmıştır. Gerçekten de GVKT'nin yürürlüğe girmesi ile birlikte veri koruma politikası üye ülkeler arasında yeknesak bir şekilde uygulanmaya başlanmış ve kişisel verilerin serbest dolaşımı konusundaki problemler büyük ölçüde ortadan kaldırılmıştır (Voigt, Von Dem Bussche, 2017). GVKT aracılığıyla, dijitalleşmeye uygun değişiklikler ve düzenlemeler getirilmiş ve Avrupa'da veri koruma alanında adeta yeni bir çağ başlamıştır.

E-Gizlilik Direktifi ile GVKT arasındaki benzerlikler nedeniyle, ilk bakışta her iki düzenlemenin birbiriyle kesiştiğini söylemek mümkün olabilir (Avrupa Veri Koruma Kurulu, 2019). Ancak, bu durumu bir çatışma olarak değerlendirmek doğru olmayacaktır. Zira, Avrupa Veri Koruma Kurulu'nun (EDPB) söz konusu iki düzenleme arasındaki ilişki konusunda hazırlamış olduğu raporda, Direktif ve GVKT arasındaki ilişkinin bir "bütünleşme" olarak değerlendirilmesi gerektiği ve her iki düzenlemenin birbirini tamamlayıcı nitelikte düzenlemeler olduğu ifade edilmiştir (Avrupa Veri Koruma Kurulu, 2019).

Kişisel verilerin korunması amacına yönelik bu iki düzenleme, birbirini tamamlayıcı nitelikte ve aralarında *lex specialis-lex generalis* (özel kanun – genel kanun) ilişkisi bulunan düzenlemelerdir (Avrupa Veri Koruma Kurulu, 2019). GVKT'nin odağında genel olarak kişisel verilerin korunması yer alırken, Direktif buna kıyasla daha dar kapsamlı ve özel bir meseleyi düzenlemektedir. Nitekim Direktif'in yöneldiği koruma, dijital gizlilik ve iletişim özgürlüğünün sağlanmasını amaçlayan ve elektronik haberleşme sektörü odaklı bir korumadır. Yine, kişisel verilerin korunmasını amaçlayan GVKT kapsamındaki düzenlemeler ise yalnızca elektronik haberleşme sektörü veya servislerine yönelik değil; tüm şirketlere, organizasyonlara, kurumlara, kısaca veri sorumlusu olarak tanımlanabilecek tüm gerçek ve tüzel kişilere yöneliktir. EDPB raporunda bu durum, "*GVKT genel hususlara değinirken, E-Gizlilik Direktifi ise konuyu sektör özelinde ayrıntılandırmakta ve özelleştirmektedir*." şeklinde ifade edilmektedir.

Direktif ve GVKT birbirlerini tamamlayıcı nitelikte olsalar da yürürlüğe girdikleri dönem ve hazırlık gerekçeleri dikkate alındığında Direktif, GVKT'nin düzenlemiş olduğu pek çok konuda hüküm ihtiva etmemekte ve dijital çağın yeni sorun ve ihtiyaçlarına cevap verememektedir. Bu sebepledir ki, özellikle Dijital Tek Pazar politikalarının hız kazandığı 2015 yılından sonra, Direktif'in çağın gereklerine yanıt verebilecek şekilde güncellenmesi zorunluluğu ortaya çıkmıştır. Böylelikle, 2017 yılının ocak ayında E-Gizlilik Tüzüğü taslağı yayınlanmıştır.

Söz konusu Tüzük taslağı ile GVKT arasındaki ilişki de tıpkı E-Gizlilik Direktifi ve GVKT arasındaki ilişkiye benzemektedir. Daha açık bir ifadeyle, E-Gizlilik Tüzük taslağı elektronik haberleşme sektöründe gizliliğin sağlanmasına yönelik düzenlemeler içermekte olup, bu bağlamda GVKT ile arasında özel kanun-genel kanun ilişkisi bulunmaktadır.

E-Gizlilik Tüzüğü Taslağının Hazırlanması İhtiyacını Doğuran Sebepler

25 Ocak 2012 tarihinde Avrupa Komisyonu, dijital gizlilik hakkının güçlendirilmesi ve Avrupa dijital ekonomisine ivme kazandırılması amacıyla 95/46/EC sayılı Direktifi özelinde reform gerçekleştirilmesini teklif etmiştir[4]. 2012 yılında yapılan bu teklif ile başlayan süreçte, AB'deki veri koruma düzenlemeleri önemli ölçüde değişikliğe uğradığı gibi, bu reform "Dijital Tek Pazar" politikalarının mihenk taşlarından birisi olmuştur. En nihayetinde, 2016 yılının Nisan ayında, GVKT yürürlüğe girmiş ve E-Gizlilik Direktifi'nin gözden geçirilerek "Dijital Tek Pazar" politikalarına uyumlu bir elektronik haberleşmenin gizliliği düzenlemesinin gerekli olduğu Avrupa yasama organları tarafından dile getirilmeye başlanmıştır.

6 Mayıs 2015 tarihli "Dijital Tek Pazar" stratejisi, AB'nin son on yılda belirlediği en önemli politik stratejilerinden biri olup temelde üç amaç üzerine kuruludur. Bunlar: tüketicilerin ve işletmelerin Avrupa sınırları içinde çevrimiçi mal ve hizmetlere daha hızlı ve verimli erişiminin sağlanması, dijital ağlar ve hizmetler için doğru koşulların oluşturulması ve Avrupa dijital ekonomisinin büyüme potansiyelinin en üst seviyeye çekilmesidir (Avrupa Komisyonu, 2015). Verilerin serbest dolaşımı ve kişisel verilerin korunması da bu amaçların en önemli parçalarındandır. Keza, E-Gizlilik düzenlemeleri de bu strateji ile doğrudan ilintilidir. Nitekim, Avrupa Komisyonu tarafından yayınlanan "Avrupa için Dijital Tek Pazar" strateji raporunda, E-Gizlilik Direktifi dahil olmak üzere veri korumaya ilişkin düzenlemelerin çağın gereklerine uygun olmadığı ifade edilmiş ve üstü kapalı bir şekilde E-Gizlilik Direktifi'nin de yeniden gözden geçirilmesi gerektiği belirtilmiştir (Avrupa Komisyonu, 2015).

E-Gizlilik Direktifi, elektronik haberleşme servisi sağlayan geleneksel telekomünikasyon şirketlerini dikkate alarak hazırlanmıştır. Ancak, Direktif'in son kez güncellendiği 2009 yılından Dijital Tek Pazar stratejisinin yayınlandığı 2015 yılına kadar geçen sürede, dünya, teknolojik gelişmeler bakımından büyük bir değişikliğe uğramıştır. Bununla ilintili olarak, söz konusu dönemde elektronik iletişim servisleri de önemli ölçüde değişmiştir. Örneğin, tüketiciler ve işletmeler iletişim kurma yöntemi olarak anlık mesajlaşma (WhatsApp, Telegram), IP üzerinden görüşme (SkypeOut, Google Hangouts) ve web tabanlı e-posta (Gmail) uygulamaları gibi internet tabanlı servisleri yaygın olarak tercih etmeye başlamışlardır. Mevcut e-gizlilik kuralları bu uygulamaları kapsamadığından, bu durum kullanıcıların gizlilik ve veri koruma hakları bakımından büyük bir tehlike yaratmıştır. Bu çerçevede, Dijital Tek Pazar stratejisinin önemli bir hedefi olan, Dijital Tek Pazar'da serbest veri dolaşımın sağlanması ve veri güvenliğinin güçlendirilmesi amacı doğrultusunda, E-Gizlilik Tüzüğü taslağı oluşturulmuştur. Yine bu dönemde, e-gizlilik düzenlemeleri ile doğrudan ilintili olan GVKT ve Elektronik Haberleşme Yasası (2018/1972 sayılı Direktif) gibi düzenlemeler de yürürlüğe girmiş olup, e-gizlilik düzenlemelerinin söz konusu yeni mevzuatla uyumlu hale getirilmesi kaçınılmaz bir hal almıştır.

E-Gizlilik Tüzüğü taslağının hazırlanmasındaki bir diğer önemli sebep de E-Gizlilik Direktifi'nin, AB Hukuku sistematiğinde, direktif niteliği taşımasından kaynaklanan sorunlardır. E-Gizlilik Direktifi'nin üye devletler bakımından doğrudan uygulanabilir niteliği[5] bulunmaması sebebiyle, Direktif içindeki düzenlemelerin üye ülkelerin iç hukuklarına geçişi sağlanırken sıkıntılar yaşanmıştır (Avrupa Komisyonu, 2019, a). Sonuç itibariyle, AB içinde yeknesak bir e-gizlilik politikası oluşturulması tam anlamıyla ve istenen seviyede söz konusu olamamıştır.

E-Gizlilik Tüzüğü'ne duyulan ihtiyacın altında yatan sebeplerden bir diğeri ise genel veri koruma kurallarını belirleyen GVKT'nin, elektronik haberleşme sektörüne yönelik özel düzenlemeleri içerisinde barındırmamasıdır. Bu durum, elektronik haberleşme servisleri sunan şirketlerin veri koruma uyumluluk faaliyetleri bakımından sorunlar ve kafa karışıklıkları doğurmuştur. Ancak, GVKT karşısında *lex specialis* olan E-Gizlilik Tüzüğü'nde düzenlenmeyen pek çok konunun GVKT'de

düzenlenmiş olduğu hususu da gözden kaçırılmamalıdır. Bu bağlamda, E-Gizlilik Direktifi'nde bulunmayan hususlar bakımından, elektronik haberleşme servisi sağlayıcıları GVKT'ye de tabi olmaktadır. Örneğin, GVKT (m. 25) ile düzenlenen başlangıçtan ve tasarımdan itibaren veri koruması ("privacy by default" ve "privacy by design") gibi ilke ve kurallar, tıpkı şu anda olduğu gibi E-Gizlilik Tüzüğü'nün yürürlüğe girmesinin ardından da elektronik haberleşme servisleri bakımından geçerli olacaktır. Öte yandan, GVKT'nin, "2002/58/EC sayılı Direktif ile İlişki" başlıklı 173 sayılı gerekçesi incelendiğinde, GVKT'nin kişisel verilerin işlenmesi bakımından temel hak ve özgürlüklerin korunmasına ilişkin tüm meselelere uygulanmakta olduğu; ancak E-Gizlilik Direktifi kapsamında düzenlenen sektör spesifik düzenlemeleri kapsamadığı, GVKT ile E-Gizlilik Direktifi arasındaki ilişkiyi açık hale getirebilmek için Direktif'in buna göre güncellenmesi ve GVKT kuralları ile uyumlu hale getirilmesi gerektiği ifade edilmektedir.

Yukarıda sayılanlara ilaveten, elektronik iletişim servisleri sunan şirketlerin haberleşme faaliyetine yönelik olarak işledikleri verilerin düzenlenmesi bakımından, GVKT isabetli çözümler sunamamaktadır. Özellikle, "veri gözetimi (data surveillance)" faaliyeti yürüten şirketlerin sayısı, yapay zekâ teknolojisinin gelişmesi ve otomatik veri işleme sistemlerinin yaygınlaşması ile artış göstermiş olup, GVKT bu iş modellerini layıkıyla düzenlemek bakımından yetersiz kalmakta ve bu sebeple de eleştirilmektedir (Hildebrandt, 2008; Custers, 2018). Hatta, elektronik haberleşme servisi sağlayan şirketlerin GVKT'deki veri koruma kurallarına tabi olmasının haksızlık teşkil ettiği ve ekonomik açıdan sürdürülemez bir durum olduğu dahi ifade edilmektedir (Buttarelli, 2018). Bu çerçevede, bu tip faaliyetler gerçekleştiren işletmelerin yapısını ve ihtiyaçlarını da göz önünde bulunduran güncel ve sektörel bir düzenlemeye ihtiyaç vardır.

Tüm bu gelişmeler ve nedenler ışığında, 2017 yılının ocak ayında E-Gizlilik Tüzüğü'nün ilk taslağı yayınlanmış ve elektronik haberleşmeye yönelik işlenen verilerin gizliliğinin sağlanması ve korunması bakımından AB'de önemli bir adım atılmıştır.

E-GİZLİLİK TÜZÜĞÜNÜN AMACI, KAPSAMI VE BAŞLICA ÖZELLİKLERİ

Aşağıda, E-Gizlilik Tüzüğü'nün amacı, kapsamı ve başlıca özellikleri açıklanacaktır. E-Gizlilik Tüzüğü'ne duyulan ihtiyaç, elektronik haberleşmede kişisel verileri koruyan mevcut AB düzenlemelerinin dijital çağın gereklerine yeterli ölçüde cevap verememelerinden kaynaklanmaktadır. O nedenle Tüzüğün amacı, kapsamı ve başlıca özelliklerinin irdelenmesi; E-Gizlilik Tüzüğü'nün yürürlüğe girmesi halinde doğuracağı başlıca sonuçları tespit edebilmek ve Türk Hukukuna ilişkin öngörü ve önerilerde bulunabilmek bakımından gereklidir.

Amacı

E-Gizlilik Tüzüğü, elektronik haberleşme alanında gizliliği korumayı amaçlamaktadır (Buttarelli, 2017). Bu bağlamda, haberleşmenin gizliliği kişisel verilerin korunması ile sınırlı olmayan, bundan daha geniş kapsamlı bir meseledir (Buttarelli, 2017). Örneğin, bir kimsenin bilgisayarına veya diğer terminal cihazına çerez yerleştirilmesi, ilk aşamada kişisel veriler ile ilişkili olmasa dahi o kişinin özel yaşamıyla ilgilidir. Zira, yerleştirilen çerezler vasıtasıyla kullanıcı davranışlarının takip edilebilmesi, kişinin profilinin çıkarılması ve bu profilin çeşitli amaçlarla kullanılması mümkün olabilecektir (Ascroft, 2020). Bu nedenle, E-Gizlilik Tüzüğü, kişisel verilerin korunmasını değil, teknoloji vasıtasıyla, bireylerin gizlilik hakkının ihlal edilmemesinin sağlanmasını amaçlamaktadır.

Kişisel verilerin korunması ve elektronik haberleşme alanında gizliliğin korunması, birbiriyle ilişkili olmakla birlikte iki farklı mesele olduğundan, GVKT ve E-Gizlilik Tüzüğü, Avrupa Birliği Temel Haklar Bildirgesi'nin farklı maddelerine dayanır. Gerçekten de GVKT, Avrupa Birliği Temel Haklar Bildirgesi'nin kişisel verileri koruyan 8(1) maddesi ile ilişkilidir[6]. Buna karşılık, E-Gizlilik Tüzüğü,

aynı Bildirgenin 7. maddesinde düzenlenen özel ve aile yaşamına saygı hükmü ile bağlantılıdır[7]. Nitekim, bu maddeye göre "*Herkes, özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesini isteme hakkına sahiptir.*" Bir kimsenin iletişiminin gizliliği de bu hakkın esaslı bir uzantısı olduğundan, kişinin özel yaşam alanın korunması, elektronik haberleşme dahil olmak üzere iletişimin her türünde sağlanmalıdır.

Kapsamı

E-Gizlilik Tüzüğü'nün kapsamı, bu düzenlemenin kimler arasındaki ve hangi tür meselelere uygulanacağı sorusuna ilişkindir. Ancak, bu sorunun yanıtlanabilmesi için Tüzüğün kapsamı ikili bir ayrıma tabi tutularak değerlendirilmelidir. Bu bağlamda, Tüzüğün hangi konuları kapsadığı meselesi aşağıda "maddi kapsam" başlığı altında ele alınacak; bu düzenlemenin hangi coğrafyada faaliyet gösteren kişiler bakımından hüküm ve sonuç doğuracağı ise "bölgesel kapsam" başlığı altında değerlendirilecektir.

Maddi Kapsamı

Bilindiği üzere, GVKT yalnızca gerçek kişilere ilişkin kişisel verilerin korunmasını konu edinmektedir. Buna karşılık, E-Gizlilik Tüzüğü, yukarıda da ifade edildiği üzere elektronik haberleşmenin gizliliğini korumayı amaçlamaktadır. Söz konusu amaç farklılığın belki de en önemli sonucu, E-Gizlilik Tüzüğü'nün kişisel veri niteliği taşımayan veriler ile tüzel kişilere ilişkin verileri de kapsamına almasıdır (Voss, 2017; Gonzalez, De Hert ve Papakonstantinou, 2020). Bu bağlamda, gerçek kişilere ilaveten, ticari işletmeler arasındaki haberleşmeler de E-Gizlilik Tüzüğü'nün kapsamına girmektedir. Bu açıdan bakıldığında, E-Gizlilik Tüzüğü, hâlihazırda yürürlükte olan E-Gizlilik Direktifi ile benzerlik göstermektedir. Bununla birlikte, Direktif klasik anlamda telekom operatörlerinin faaliyetlerini konu edindiğinden zamanın ihtiyaçlarını karşılayamamaktadır.

Direktif'in klasik anlamda telekom operatörlerinin faaliyetlerini düzenleyen dar kapsamına karşılık, E-Gizlilik Tüzüğü, online iletişim sağlayıcılarını da geleneksel iletişim sağlayıcıları ile eş değer kabul etmektedir. Bu husus, Avrupa Komisyonu'nun kıyaslanabilir nitelikteki dijital hizmetlerin aynı veya benzer kurallara tabi olmaları gerektiği görüşü ile de uyumludur (Avrupa Komisyonu, 2016). Bu çerçevede, Gmail, Skype, Facebook Messenger ve WhatsApp gibi uygulamaların da kullanıcılarının veri güvenliğini geleneksel iletişim sağlayıcıları ile eşit düzeyde temin etmeleri gerekmektedir. Keza, doğrudan pazarlama, çerezler, makineler arası iletişim ve nesnelerin interneti de E-Gizlilik Tüzüğü'nün kapsamına giren başlıca konulardandır.

Bölgesel Kapsamı

Tıpkı GVKT gibi E-Gizlilik Tüzüğü de bölgesel kapsamı itibariyle AB sınırları dışında gerçekleştirilen kimi veri işleme faaliyetlerini de kapsamaktadır. Bu bağlamda, AB'de bulunan kullanıcılara sunulan elektronik haberleşme hizmetleri kapsamında işlenen her türlü veri, işleme faaliyeti AB dışında gerçekleşse dahi E-Gizlilik Tüzüğü'ne tabi olacaktır. O nedenle, AB pazarında faaliyet göstererek AB'de bulunan kişilerin elektronik iletişim verilerini işleyen veya AB'de bulunan kişilere doğrudan pazarlama amaçlı materyal gönderen tüm işletmeler, merkezleri AB dışında bulunsa dahi E-Gizlilik Tüzüğü'nün kapsamına gireceklerdir.

Başlıca Özellikleri

AB'nin yetkili karar organları, E-Gizlilik Tüzüğü taslağı üzerinde henüz uzlaşamadıkları gibi, Tüzüğün yakın bir gelecekte yürürlüğe girme ihtimali de çok yüksek görünmemektedir. Buna karşılık,

Direktif'in çağın ihtiyaçlarını karşılayamadığı ve er ya da geç yerini yeni bir düzenlemeye bırakacağına kesin gözüyle bakılabilir. Bu çerçevede, Tüzüğün taslakları üzerinden yapılan tartışmalar ve bu tartışmaların kümelendiği meseleler, AB'de kabul edilecek nihai düzenlemenin hangi eksende yer alacağını büyük ölçüde göz önüne sermektedir. Bu bağlamda, öncelikli olarak ele alınan başlıca meseleler: çerezler; üst verilerin (metadata) korunması; ve doğrudan dijital pazarlama faaliyetleridir.

Çerezler

İnternet kullanıcılarının, cep telefonu, bilgisayar ve tablet gibi terminal cihazlarına çerez yüklenerek bu kişilerle ilgili verilerin toplanması yeni bir uygulama değildir. Nitekim, bu uygulama dikkate alınarak 2009 yılında Direktif'te değişiklik yapılmış olup bu değişikliğin ardından Direktif, "Çerez Kanunu" olarak anılmaya başlanmıştır. Zira, söz konusu değişiklikler neticesinde, web sitelerince kullanıcıların cep telefonu, tablet, bilgisayar ve benzeri elektronik cihazlarına çerez yüklenebilmesi için kullanıcılardan onay alınması gerektiği kabul edilmiştir.

Aslında, 25 Mayıs 2018 tarihinde GVKT'nin yürürlüğe girmesi çerez kullanımlarını belli ölçüde sınırlandırmıştır. Yapılan çalışmalar, haber sitelerinde yer alan reklam ve pazarlama amaçlı üçüncü taraf çerezlerin, Nisan ve Temmuz 2018 ayları arasında %14 oranında azaldığını ortaya koymaktadır (Libert, Graves ve Nielsen, 2018). Bununla birlikte, ziyaretçilerinin terminal cihazlarına çerez yüklemek isteyen işletmeler ise bu faaliyetlerini GVKT'ye uygun şekilde gerçekleştirmek zorunda kalmışlardır. Bu bağlamda, ihtiva ettiği yükümlülüklerin ihlali halinde ağır yaptırımlar öngören GVKT'nin de yürürlüğe girmesi ile birlikte, çerez ve benzeri takip teknolojilerinin kullanılabilmesi bakımından kullanıcıların rızasını almak zorunda olan web siteleri, ziyaretçilerine, çerez politikalarını kabul edip etmediklerini sormaya başlamışlardır.

Çerez kullanımına ilişkin olarak, internet kullanıcılarının sıklıkla karşılaştıkları onay taleplerinin kullanıcılarda "rıza yorgunluğu" (consent fatigue) yarattığı ifade edilmektedir (Gonzalez ve arkadaşları, 2020). Nitekim ziyaretçiler, karşılarına çıkan onay kutucuklarını, çoğunlukla okumadan ve anlamadan tıklayarak, cihazlarına çerez yüklenmesine onay vermektedirler[8]. E-Gizlilik Tüzüğü, bu sorunun çözüme kavuşturulabilmesi amacıyla birtakım düzenlemeler getirmektedir. Örneğin, kullanıcıların, çerez ayarlarını internet tarayıcılarını henüz daha yüklerken ileride ziyaret edecekleri tüm web siteleri bakımından geçerli olacak şekilde yapabilmeleri öngörülmektedir. Ayrıca, bu ayarların kullanıcılar tarafından istenildiğinde tekrar değiştirilmesi mümkün olacaktır. Böylelikle, kullanıcılar internette gezinti yaparken- hemen hemen her sayfada karşılarına çıkan ve çoğu kez içeriğini okumadıkları- çerez kullanımına ilişkin rıza metinlerine maruz kalmayacaklardır.

Çerezlerle ilgili olarak E-Gizlilik Tüzüğü'nün önceki taslaklarında sıkça tartışılan bir diğer husus ise, "çerez duvarları"nın yasaklanması gerekip gerekmediğine ilişkindir. Çerez duvarları, cihazlarına çerez yerleştirilmesine izin vermeyen kullanıcıların girişlerine izin vermeyen web sayfalarını ifade etmektedir. 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 tartışılmaktadır. Tüm bu tartışmalar devam ederken, Avrupa Veri Koruma Kurulu 4 Mayıs 2020 tarihinde yayınladığı tavsiye kararlarında, çerezlerin kullanımına ilişkin rızanın, bir web sayfasına giriş için şart koşulamayacağını ifade etmiştir (Avrupa Veri Koruma Kurulu, 2020).

Üst veriler (Metadata)

"Veri hakkında veri" şeklinde ifade edilen üst veriler (metadata), bir bilgi kaynağını tanımlayan, açıklayan, onun yerini ortaya koyan veya onu elde etmeyi, kullanmayı ya da yönetmeyi kolaylaştıran

yapısal bilgilerdir (National Information Standards Organization, 2004). Örneğin, bir e-postanın gönderilmesi halinde, postanın konusu ve metni "içerik" olarak kabul edilirken, gönderici ve alıcının kim olduğu bilgileri üst veridir (Gonzalez ve arkadaşları, 2020).

E-Gizlilik Tüzüğü, üst verilerin de tıpkı iletişimin içeriğini oluşturan veri ile eş değer düzeyde korunması gerektiği esasını benimsemektedir. Böylelikle, iletişimin içeriğinden bağımsız olarak, konum, iletişim zamanı ve iletişim kurulan kişiler hakkındaki verilerin de -kural olarak- yalnızca rıza ile işlenebileceği esası kabul edilmektedir. Zira, konum verileri nerede yaşadığımızı, çalıştığımızı, alışveriş yaptığımızı ve benzeri bilgileri ortaya koymakta, kimlerle, hangi sıklıkta mesajlaştığımız veya konuştuğumuza ilişkin veriler ise sosyal konumumuzu ifşa etmektedir (Buttarelli, 2018). Örneğin, bir kimsenin haftanın belli günleri düzenli olarak bir ibadethaneye gitmesi halinde, konum verileri kullanılarak o kişinin dini inancı tespit edilebilir (Gonzalez ve arkadaşları, 2020). Konum ve trafik verileri, Avrupa Adalet Divanı'nın 2014 tarihli "Digital Rights Ireland and Seitlinger and Others" kararı (C:293/12) ile 2016 tarihli "Tele2 Sverige AB v Post- och telestyrelsen (C:203-15) ve Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis (C:698-15) kararına da konu olmuştur. Mahkeme, her iki kararında da bu tür verilerin, verinin ilişkin olduğu bireylerin özel yaşamları hakkında kesin sonuçlar çıkarmayı mümkün kıldığını ifade etmiştir.

Bu çalışmanın hazırlandığı dönemdeki güncel tasarı ile getirilen ve önemli tartışmalara sebep olan bir diğer mesele ise, kullanıcıların rızası aranmaksızın, servis sağlayıcıların "meşru menfaatlerinin" gerektirmesine dayanılarak üst verilerin işlenebilmesinin veya kullanıcıların terminal cihazlarına çerez ve benzeri teknolojiler yerleştirmenin mümkün olup olmayacağına ilişkindir. Zira güncel tasarı, meşru menfaat sebebiyle yapılacak bu tür veri işleme faaliyetlerine, çeşitli sınırlar ve istisnalar çerçevesinde izin vermektedir. Ancak, Avrupa Veri Koruma Kurulu'nun 25 Mayıs 2018 tarihli açıklaması ile çelişen bu düzenlemenin nihai metinde yer alıp alamayacağı tartışmalıdır. Zira, bu açıklamada Kurul, E-Gizlilik Tüzüğü'nün, "meşru menfaat" gibi açık uçlu dayanaklar ile elektronik haberleşmelerin içeriğini ve üst verileri işlenmesine izin vermemesi gerektiğini ifade etmiştir (Avrupa Veri Koruma Kurulu, 2018).

Doğrudan Dijital Pazarlama Faaliyetleri

E-Gizlilik Tüzüğü, elektronik iletişim ağları kullanılarak gerçekleştirilen doğrudan pazarlama faaliyetleri bakımından da ilgili kişilerin lehine olmak üzere, Direktif'in aradığından daha sıkı koşullar öngörmektedir. Bu bağlamda, e-posta, SMS ve telefon dahil olmak üzere, her türlü iletişim kanalı üzerinden dijital pazarlama faaliyetlerinin gerçekleştirilmesi kullanıcıların rızasına bağlanmaktadır. Bu çerçevede, rıza koşuna ilişkin istisnalar ve işletmelerin, meşru menfaat başta olmak üzere, kullanıcının rızası dışındaki veri işleme şartlarına dayanarak reklam ve tanıtım mesajları göndermesine izin verilip verilmeyeceği meselesi önemli tartışmalara sebep olmaktadır. Keza, Tüzüğün eski tasarıları incelendiğinde, Direktif'ten farklı olarak, işletmeler arasında gerçekleştirilecek (B2B) doğrudan dijital pazarlama faaliyetlerinin de Tüzük kapsamına alınmasının değerlendirildiği görülmektedir. Zira, bu gibi hallerde kişisel verilerin işlenmesi söz konusu olmadığından, gerçekleştirilen veri işleme faaliyetleri GVKT'ye de tabi olmayıp hukuki düzenlemeden yoksundur.

E- GİZLİLİK TÜZÜĞÜ'NÜN DOĞURACAĞI SONUÇLAR

Genel Olarak

E-Gizlilik Tüzüğü'nün yürürlüğe girmesi halinde hem gerçek kişilerin hem de tüzel kişilerin elektronik haberleşme alanındaki gizliliğinin, içinde bulunduğumuz dijital çağın ihtiyaçlarına daha

uygun şekilde korunacağını söylemek mümkündür. Bununla birlikte, Tüzüğün tüm taslakları, kimilerince mahremiyeti yeterince koruyamayacak kadar yumuşak olmakla suçlanırken, kimilerince de teşebbüslerin menfaatlerini göz ardı ettiği gerekçesiyle eleştirilmektedir.

E-Gizlilik Tüzüğü, elektronik haberleşme alanında faaliyet gösteren teşebbüslere önemli yükümlülükler yüklemekte ve bu yükümlülüklere aykırı hareket eden işletmelere, GVKT ile uyumlu şekilde yüksek para cezaları kesilmesi öngörülmektedir. Bu nedenle, Tüzüğün maddi ve bölgesel kapsamına giren teşebbüslerin, faaliyetlerini Tüzük ile uyumlu hale getirmeleri kaçınılmazdır. Ancak bu durum ağır eleştirileri de beraberinde getirmektedir. Zira, bu mevzuata tabi olarak faaliyet gösteren teşebbüslerin, bu mevzuata tabi olmaksızın hizmetlerini yürüten teşebbüsler ile rekabet etme gücünden mahrum kalacakları savunulmaktadır.

E-Gizlilik Tüzüğü'ne yöneltilen bir diğer eleştiri, E-Gizlilik Tüzüğü'nün teknolojik gelişmenin önünde engel teşkil edebileceğidir[9]. Tüzüğün, özellikle çerezlere ilişkin hükümlerinin yürürlüğe girmesi ile birlikte kullanıcılar hakkında bilgi toplamak ve onlara kişiselleştirilmiş reklamlar sunmak güçleşecektir. Bu bağlamda, reklama dayalı olarak, böylelikle de kullanıcılardan herhangi bir ücret talep etmeksizin hizmet sunan teşebbüs ve uygulamaların akıbetinden endişe edilmektedir[10].

E-Gizlilik Tüzüğü'nün çocuk pornosu, çocuk istismarı ve diğer suçlarla mücadele üzerindeki olası etkisi de önemli tartışmalara yol açmaktadır. Örneğin, Ekim 2018'de Facebook, çocuk istismarı teşkil eden 8.7 milyon görselin, şirketin kullandığı özel bir yazılım sayesinde tespit edilerek silindiğini bildirmiştir. Geliştirilen yazılım, söz konusu fotoğrafların %99'unu, herhangi bir kullanıcı tarafından rapor edilmeksizin tespit etmiştir[11]. Ancak, rızaya dayalı sistemi benimseyen Tüzüğün yürürlüğe girmesi halinde, çocukların cinsel istismarını teşkil eden görselleri tarayan özel yazılımların kullanılmasının önünün kapanacağından endişe edilmektedir[12].

Kanımızca, GVKT'nin kişisel verilerin korunması odaklı bir düzenleme olması, E-Gizlilik Direktifi'nin ise elektronik haberleşme alanındaki teknolojik gelişmeler ile bunlardan kaynaklanan sorun ve ihtiyaçlara uzak olması nedeniyle yeni bir yasal düzenleme yapılması gerektiği açıktır. Keza, bu düzenlemenin her bir maddesinin, çağın gerektirdiği ihtiyaçlar göz önünde tutularak kaleme alınması ve AB üye ülkeleri arasındaki uygulama farklılıklarının önüne geçilebilmesi amacıyla tüzük şeklinde yapılması da son derece faydalı olacaktır. Yukarıda anılan endişe ve eleştirilerin ise tamamının haklılık payı bulunmaktadır. Ancak, Tüzük metni hala taslak halinde olup tüm bu eleştiriler doğrultusunda geliştirilmeye açıktır. Ortaya çıkacak sonuç, özü itibariyle kişilerin elektronik haberleşme alanındaki gizliliğini korurken, diğer yandan teşebbüs özgürlüğü inovasyonu da baltalamamalıdır. Nitekim, AB'nin yetkili karar organlarının yıllardır süren çalışmalara rağmen E-Gizlilik Tüzüğü'nü yürürlüğe sokamamalarının sebebi de -elde edilmesi son derece güç olan- bu dengenin sağlanmasına ilişkin ısrarlı gayretleridir.

Türk Hukuku Bakımından

E-Gizlilik Tüzüğü'nün Türk hukuku bakımından doğuracağı sonuçları iki temel başlık altında gruplamak mümkündür. İlk olarak, Tüzüğün sınır ötesi etkisi, Türkiye'de kurulu olarak faaliyet gösteren birçok teşebbüsün veri işleme politikalarını AB mevzuatı ile uyumlaştırmalarını zorunlu kılacaktır. İkinci olarak, çağın gerisinde kalmaması için, elektronik haberleşme alanındaki Türk mevzuatının, Tüzük'te yer alan düzenlemeler de dikkate alınarak güncellenmesi gerekecektir. Bu çerçevede Tüzük, Türk mevzuatının eksiklerine ışık tutacak ve yol gösterici bir nitelik taşıyacaktır. Bununla birlikte, Tüzük henüz taslak halinde olduğundan, bu bölümde Türk mevzuatının Tüzük ile uyumlaştırılmasına ilişkin detaylı önerilerde bulunulmayacaktır. Bunun yerine, Tüzüğe ilişkin çalışmaların ışığında, dijital çağın gereklerine ayak uydurabilmek bakımından, Türk mevzuatında

düzenlenmesi gereken kimi meseleler ortaya konulacaktır. Bu meselelerin her birinin ne şekilde düzenlenmesi gerektiği ise ayrı bir çalışma konusudur.

E-Gizlilik Tüzüğü'nün Sınır Ötesi Etkisinin Doğuracağı Sonuçlar

Kişisel veri işleyen teşebbüslere önemli yükümlülükler yükleyen ve bunların ihlali halinde ağır yaptırımlar öngören GVKT'nin yürürlüğe girmesiyle, merkezi AB sınırları dışında bulunan pek çok kuruluş da faaliyetlerini GVKT ile uyumlu hale getirmek zorunda kalmıştır. Nitekim, GVKT madde 3/2 incelendiğinde, Tüzüğün, merkezi AB'de bulunsun veya bulunmasın, AB vatandaşlarına hizmet sunan veya bu kapsamda AB vatandaşlarını dijital olarak izleyen şirketlerin, bu amaçlarla işleyecekleri kişisel veriler bakımından GVKT'nin kapsamına girecekleri ve GVKT altında sorumlu olacakları düzenlenmektedir. Bu bağlamda, GVKT hükümleri Avrupa Birliği dışındaki ülkelerde gerçekleşen faaliyetlere de uygulanabilir niteliktedir (Kiss ve Szoke, 2014)[13].

GVKT'nin sınır ötesi etkisi, düzenlemenin yürürlüğe girdiği 2016 yılından itibaren tüm dünyada etkisini göstermiş olup bu düzenleme ile birlikte, AB, veri koruma alanında öncü toplum haline gelmiştir. Öyle ki, GVKT düzenlemelerinin izdüşümlerini, dünyadaki pek çok ülkenin düzenlemelerinde ve içtihatlarında görmek mümkündür. 1 Ocak 2020 tarihinde yürürlüğe giren ve ABD'nin kişisel verilerin korunması konusundaki bakış açısını baştan aşağı yenileyen Kaliforniya Tüketici Gizlilik Yasası, bu etki kapsamında verilebilecek en güzel örneklerdendir. Yine, Kişisel Verileri Koruma Kurumu'nun vermiş olduğu bazı kararlarda GVKT'ye atıfta bulunduğu veya GVKT düzenlemeleri ile 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndaki boşlukları doldurduğu görülmektedir[14].

GVKT yalnızca ülkelerin kanuni düzenlemelerini etkilememiş; AB'de kurulu olmayan ancak GVKT m. 3/2 kapsamında değerlendirilebilecek şirketlerin faaliyetlerini de değiştirmiştir. Bu düzenleme kapsamına giren Türk şirketler de dahil olmak üzere, dünyanın farklı ülkelerinde kurulu pek çok şirket, şirket içi veri koruma politikalarını GVKT ile uyumlaştırmıştır. Bu etkiyi, şirketlerin web sitelerinde, şirket faaliyetlerinde veya gizlilik politikalarında görmek mümkündür.

Tıpkı GVKT gibi, E-Gizlilik Tüzüğü'nün de sınır ötesi etkisi olması planlanmaktadır. GVKT'nin sınır ötesi özelliğinin yarattığı sonuçlar dikkate alındığında, E-Gizlilik Tüzüğü'nün yürürlüğe girmesi halinde elektronik haberleşme sektöründe (OTT'ler ve elektronik ticaret faaliyetinde bulunan şirketler de dahil olmak üzere) benzer bir etkinin meydana gelmesi olası gözükmektedir. Daha açık bir ifadeyle, E-Gizlilik Tüzüğü'nün yürürlüğe girmesi ile birlikte, dünyanın çeşitli ülkelerinde faaliyet gösteren birçok şirketin politikalarını Tüzük ile uyumlu hale getirmek zorunda kalacağı kesindir. Ayrıca, Türkiye dahil olmak üzere AB dışındaki ülkelerin de Tüzükte yer alan düzenlemelerden etkilenerek, iç hukuklarında benzer düzenlemeler yapma yoluna gitmeleri olası görünmektedir.

Elektronik Haberleşmeye İlişkin Mevzuat ve Yeni Düzenleme İhtiyacı

Türk hukukunda, doğrudan ve özel olarak elektronik haberleşmede dijital gizliliğin sağlanması ve kişisel verilerin korunmasını konu alan bir düzenleme bulunmamaktadır. Nitekim, bu konuda, Türk hukuku bakımından en ilgili düzenlemeler, 5809 sayılı Elektronik Haberleşme Kanunu ve ikincil mevzuatı, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve 6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun ile Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik'tir. Ancak, hiçbir düzenleme özel olarak elektronik haberleşmede dijital gizliliğin sağlanması ve kişisel verilerin korunması hedefine yönelmemiştir.

Elektronik Haberleşme Kanunu ve İkincil Mevzuat

5809 sayılı Elektronik Haberleşme Kanunu'nun "Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması" başlıklı 51. maddesi altında, elektronik haberleşme sektörü bakımından işlenen kişisel verilerin gizliliğinin sağlanmasına yönelik düzenlemeler bulunmaktadır. Esasen, 2010 yılında Anayasa'da yapılan ve kişisel verilerin işlenmesine ilişkin hususların kanunla düzenlenmesinin anayasal bir prensip olarak kabul edilmesine yönelik değişiklikten sonra, 5809 sayılı Elektronik Haberleşme Kanunu'nun 51. maddesi ve 4, 6, 12. maddelerine dayanılarak, "*Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik*" hazırlanmış ve 24/07/2012 tarihli ve 28363 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Ancak, Danıştay İdari Dava Daireleri Kurulu'nun 5809 sayılı Elektronik Haberleşme Kanunu'nun 51 inci maddesinin iptaline ve yürürlüğünün durdurulmasına ilişkin olarak Anayasa Mahkemesi'ne başvurması ve Anayasa Mahkemesi'nin 2013/122 Esas ve 2014/74 Karar numaralı ve 09/04/2014 tarihli kararı ile ilgili maddenin iptaline karar verilmiştir (Anayasa Mahkemesi, 2014). Bu karar sonrasında, "*Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik*" maddeleri de hükümsüz hale gelmiştir.

İlgili Anayasa Mahkemesi kararını takiben, Elektronik Haberleşme Kanunu'nun 51. maddesi yeniden düzenlenmiş ve elektronik haberleşme sektörüne özgü kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik hususlara ilişkin çerçeve yeniden oluşturulmuştur. Her ne kadar hazırlanan kanun maddesi, Direktif ve Tüzük düzenlemesi içeriğinde de bulunan trafik verileri, konum verileri ve terminal cihazlarda bulunan verilerin gizliliğini kapsamakta ise de çerezler, üst veri işleme ve veri gözetleme faaliyetleri ile spam uygulamaları gibi hususlar karşısında kullanıcıların gizliliğinin sağlanmasına ilişkin olarak AB standartlarında bir düzenlemenin varlığından söz edilemez. Dijital dünyada bu hususlara yönelik olarak kullanıcıların kişisel verilerinin korunması ve gizliliğinin tesis edilmesi bir zorunluluktur. Bu bağlamda, Elektronik Haberleşme Kanunu'nun 51. maddesi, AB düzenlemeleri ile karşılaştırıldığında eksiktir.

Bu süreçte, ikincil düzenleme olarak Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik yeniden hazırlanmış ve söz konusu yönetmelik 04.12.2020 tarihinde yürürlüğe girmiştir. İlgili Yönetmelik de tıpkı Elektronik Haberleşme Kanunu'nun 51. Maddesi gibi, konum verilerine ve saklama sürelerine ilişkin belirli düzenlemeler içermekte ise de bu yönetmelik, E-Gizlilik Direktifi ve E-Gizlilik Tüzüğü taslağında yer alan, kullanıcının rızası olmaksızın gerçekleşen iletişim ('spam') ve çerezler gibi önemli konu başlıklarında herhangi bir düzenleme barındırmamaktadır. Kanımızca bu önemli bir eksikliktir. Türk hukuk mevzuatı, e-gizlilik kuralları açısından AB düzenlemesinin gerisinde kalmaya devam etmektedir.

Son olarak, 30224 sayılı ve 28 Ekim 2017 tarihli Resmi Gazete'de yayınlanan Elektronik Haberleşme Sektörüne İlişkin Tüketici Hakları Yönetmeliği de elektronik haberleşmede gizlilik hakkının temini kapsamında değerlendirilebilecek ikincil bir düzenlemedir. Ancak, bu düzenleme de elektronik haberleşme sektöründe tüketici hak ve menfaatlerini korumaya yönelik usul ve esasları belirlemeyi amaçladığından, özel olarak gizliliğin korunması amacına yönelik düzenlemeler ihtiva etmemektedir.

Kişisel Verilerin Koruması Kanunu

Tüm dünyadaki teknolojik gelişmelere paralel olarak, ülkemizdeki veri işleme faaliyetleri de özellikle 2000'li yıllardan itibaren hız kazanmakla birlikte, bu denetimden uzak ve kontrolsüz veri akışı, veri işleme sürecinde kişisel verilerin korunması açısından büyük bir güvenlik zafiyetine sebep olmuştur. Bununla birlikte, kişisel verilerin bir temel hak olarak korunması düşüncesi; e-ticaret ve diğer ekonomik etkinlik ve eylemde ülkemizin geride kalmaması amacı ve ekonomi dışındaki sektörlerde de kişisel verilerin korunmasına duyulan ihtiyaç ile birlikte, Türkiye'de kişisel verilerin korunmasına

yönelik olarak kapsayıcı ve dağınık olmayan bir kanuni düzenleme yapılması zorunlu hale gelmiştir (Küzeci, 2018). Yine, kişisel verilerin korunmasındaki eksiklik sebebiyle AB üye devletleri arasında bilgi akışında da aksaklıklar yaşanmış olup bu hususta düzenleme yapma zorunluluğu ülkemizin AB üyelik süreci bakımından da bir gereklilik halini almıştır (Küzeci, 2018). Bu gelişmelerin sonucunda ve 2010 Anayasa değişikliğine uygun olarak, "6698 sayılı Kişisel Verilerin Korunması Kanunu" (KVKK), 07.04.2016 tarihi itibariyle yürürlüğe girmiştir. Ancak, KVKK da tıpkı GVKT gibi genel anlamda kişisel verilerin korunmasını düzenleyen bir kanun olup elektronik haberleşme sektörü özelinde herhangi bir düzenlemeyi ihtiva etmemektedir.

6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun ile Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik

6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun ile Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik, ticari iletişime ilişkin temel esasları, hizmet sağlayıcılar ile aracı hizmet sağlayıcıların sorumluluklarını, elektronik iletişim araçları vasıtasıyla kurulan sözleşmeleri, elektronik ticaret kapsamında söz konusu olan bilgi verme yükümlülüklerini ve bu yükümlülüklerin ihlali durumunda uygulanacak yaptırımları düzenlemektedir. Bu bağlamda, kişisel verilerin korunması hususu, bu düzenlemelerin ilgili maddelerine de sirayet etmiş olup bu düzenlemelere göre gerek hizmet sağlayıcı gerekse aracı hizmet sağlayıcı, faaliyet ve hizmetleri çerçevesinde elde ettiği verilerin korunmasından ve bu koruma için gerekli tedbirlerin alınmasından sorumludur. Ayrıca, bu kapsamda elde edilen kişisel verilerin üçüncü kişilerle paylaşılabilmesi ve elde edilme amacı dışındaki amaçlarla kullanılabilmesi de ilgili kişinin onayına tabidir.

Genel anlamda kişisel verilerin korunmasına ilişkin bu düzenlemeler de tıpkı Kişisel Verilerin Korunması Kanunu gibi doğrudan doğruya elektronik haberleşmede gizliliğin korunması amacı taşımamaktadırlar. Oysa daha önce de ifade ettiğimiz üzere, elektronik haberleşmede kişisel verilerin korunması ile gizliliğin korunması farklı meselelerdir. Genel olarak hizmet sağlayıcıların yükümlülüklerini konu alan bu düzenlemelerde, özellikle çerez uygulamalarına yönelik kapsamlı hükümler bulunmamaktadır.

E-Gizlilik Tüzüğü Işığında Türk Hukukunda Yeni Bir Düzenlenme Yapılması İhtiyacı

Kişisel Verilerin Korunması Kanunu başta olmak üzere, yukarıda açıklanan çeşitli yasal düzenlemeler, elektronik haberleşme servisleri kapsamında işlenen kişisel verilerin gizliliğini de konu alan hükümler ihtiva etmektedir. Bu bağlamda, söz konusu mevzuatta, E-Gizlilik Direktifi'nin içeriğinde yer alan (i) veri işleme güvenliği, (ii) iletişimin gizliliği, (iii) veri saklama ve (iv) trafik ve konum verilerinin işlenme usulleri gibi konuların düzenlendiği anlaşılmakta ise de bu düzenlemelerin güncel AB düzenlemeleri ve dijitalleşmedeki yeni akımlar dikkate alındığında pek çok eksik yönünün bulunduğu görülmektedir.

İlk olarak, bu düzenlemeler kapsamında, kullanıcının rızası olmaksızın gerçekleşen iletişimler (spam) ve çerezler bakımından açık ve ayrıntılı hükümlere yer verilmemiş olması, Türk elektronik haberleşme sektöründe kişisel verilerin gizliliğinin sağlanması açısından büyük bir eksikliktir. Bununla birlikte, Kişisel Verileri Koruma Kurulu (Kurul), Amazon Türkiye'ye 1.200.000 TL idari para cezası uyguladığı 27/02/2020 tarihli ve 2020/173 sayılı kararında, 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[15]. Her ne kadar söz konusu para cezasının yalnızca 100.000 TL'lik kısmı çerezlerle ilgili aydınlatma yükümlülüklerinin yerine getirilmemesi nedeniyle verilmiş ise de bu karar, çerez kullanımını konusunun Kurul'un radarına girdiğini ve bu meselenin giderek daha fazla önem kazanacağını göstermektedir. Türkiye'deki internet kullanıcı sayısının nüfusa oranla yüksek olduğu[16] da dikkate

alındığında, ne kadar fazla kişinin elektronik haberleşme servisi sağlayıcıları ve/veya internet sitesi operatörleri tarafından sıklıkla başvurulan bu uygulamalardan etkilendiği de göz önüne serilecektir. Yine bu nedenle, kullanıcının rızası olmaksızın gerçekleşen iletişimler ile çerezler konusunda ayrıntılı yasal düzenlemelere ihtiyaç vardır.

İkinci olarak, yürürlükteki mevzuatta bulunan "elektronik haberleşme" kavramının, teknolojik gelişmelere bağlı olarak güncellenmesi ve AB'de kısa süre önce yürürlüğe giren Elektronik Haberleşme Yasası'ndaki (2018/1972 sayılı Direktif) tanıma uygun olarak ve anlık mesajlaşma, IP üzerinden görüşme ve web tabanlı e-posta uygulamalarındaki haberleşmeyi ("Şebekeler Üstü Hizmet") de kapsayacak şekilde yeni bir tanımın oluşturulması isabetli olacaktır. Ayrıca, Türkiye'de elektronik iletişim servisleri sunan şirketlerin "veri gözetimi" (data surveillance) faaliyetleri ve otomatik veri işleme yöntemleri kullanımı da son yıllarda artış göstermiş olup yukarıda ifade edilen kanuni düzenlemeler, bu iş modellerinin doğurdukları riskleri bertaraf etmek bakımından da yetersiz kalmakta ve kullanıcıların kişisel verileri yeterli düzeyde korunamamaktadır.

Üçüncü olarak, 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'un 6(2) maddesi ile Yönetmeliğin ise 6(3) maddesi, esnaf ve tacirlerin elektronik iletişim adreslerine, kendilerinden önceden onay alınmaksızın ticari iletiler gönderilebileceğini ifade etmektedir. Bu bağlamda, söz konusu kuralının E-Gizlilik Tüzüğü'ne ilişkin tartışmalar doğrultusunda gözden geçirilmesi faydalı olabilir.

Son olarak belirtmek gerekir ki, mevcut kanuni düzenlemeler, elektronik haberleşme servisi sağlayan geleneksel haberleşme servisi sağlayıcıları dikkate alınarak kaleme alınmış düzenlemelerdir. Ancak, pek çok ülkede olduğu gibi Türkiye'de de elektronik iletişim servisleri dijitalleşme ile birlikte önemli ölçüde değişmiştir. Anlık mesajlaşma, IP üzerinden görüşme ve web tabanlı e-posta uygulamalar, Türkiye'de de kullanıcılar tarafından yaygın olarak tercih edilen ve sıklıkla kullanılan uygulamalardır. Mevcut düzenlemeler, bu uygulamaları kapsar nitelikte hükümler ihtiva etmemektedir.

Tüm bu sebeplerle, Türk hukukundaki mevcut düzenlemelerin, elektronik haberleşme servisleri kapsamında gerçekleştirilen kişisel veri işleme faaliyetleri bakımından ilgili kişileri etkin bir şekilde koruyabilecek nitelikte düzenlemeler olmadığı görülmektedir. Özellikle değişen elektronik iletişim yöntemleri ve bu alanda AB hukukundaki güncel gelişmeler dikkate alındığında, bu eksiklik AB'ye uyum sürecini de olumsuz yönde etkilemekte olup bu husus, Avrupa Komisyonu'nun hazırlamış olduğu ilerleme raporunda da ayrıca ifade edilmiştir (Avrupa Komisyonu, 2019b). Bu bağlamda, Türk hukukunda, doğrudan e-gizliliği konu alan bir yasal düzenlemeye ihtiyaç olduğu da açıktır. Nitekim, Türkiye Cumhuriyeti Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı'nın "On Birinci Kalkınma Planı (2019-2023)" ve Bilgi Teknolojileri ve İletişim Kurumu "2019-2023 Stratejik Planı"nda, dijital dönüşüm ve teknolojik gelişmelere özel olarak yer verilmiş olması da e-gizlilik kuralları bakımından güncel bir düzenleme yapılmasının önemini ortaya koymaktadır. Ayrıca, Bilgi Teknolojileri ve İletişim Kurumu "2019-2023 Stratejik Planı"nın dördüncü alt başlığında ifade edilen 5G, yapay zekâ, makineler arası haberleşme ve nesnelerin interneti gibi teknolojilere yapılacak yatırımların artacağı ve bu alandaki gelişmeleri Türkiye'nin de takip edeceği dikkate alındığında, ulusal mevzuatın güncellenmesi ihtiyacı bir zorunluluk haline dönüşmektedir. Keza ilgili 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 edilmiştir (Bilgi Teknolojileri ve İletişim Kurumu, 2018; Türkiye Cumhuriyeti Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, 2018).

SONUÇ

Türk mevzuatı, elektronik haberleşme sektöründe gizliliğin korunması bakımından AB mevzuatının gerisinde kalmıştır. Kişisel Verileri Koruma Kurumu ve Bilgi Teknolojileri ve İletişim Kurumu kararları ile, elektronik haberleşme sektöründe kişisel verilerin korunması ile ilgili dünyadaki modern düzenleme ve uygulamalar takip edilmeye çalışılmakta ve Türk hukuku uygulaması dünyadaki benzerlerine yaklaştırılmaya çalışılmaktaysa da gerekli ve nitelikli mevzuat değişikliğinin yapılmaması durumunda, bu çabanın etkili bir sonuç doğurması güç gözükmektedir. Bu bağlamda, Türk hukukunda, doğrudan elektronik haberleşme sektöründe gizliliği korumaya yönelik düzenlemeler yapılmalıdır. Bu değişiklik, veri akışının önemli ölçüde arttığı ve dijitalleşmenin çığ gibi büyüdüğü dünyamızda, Türkiye'nin AB ve diğer dünya ülkeleri ile sağlam ve sürdürülebilir ekonomik ve politik ilişkiler kurabilmesi açısından zorunlu olup Türkiye'nin stratejik planları da bu değişimin aciliyetini gözler önüne sermektedir.

KAYNAKLAR

Ascroft, L. (2020). *New Draft of ePrivacy Regulation*. Protecture.org.uk. https://protecture.org.uk/new-draft-of-eprivacy-regulation/ adresinden 09.04.2020 tarihinde alınmıştır.

Avrupa Komisyonu. (1988). *Green Paper on Copyright and the Challenge of Technology* (No: C0M (88) 172). Brüksel. http://aei.pitt.edu/1209/1/COM_(88)_172_final.pdf adresinden 13.04.2020 tarihinde alınmıştır.

Avrupa Komisyonu. (2001). *Use of EC Competition Rules in the Liberalisation of the European Union's Telecommunications Sector* (No: COMP / C / 2 / HU/ rdu). Brüksel. https://ec.europa.eu/competition/speeches/text/sp2001_009_en.pdf adresinden 07.04.2020 tarihinde alınmıştır.

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 02.05.2020 tarihinde alınmıştır.

Avrupa Komisyonu. (2016). *Online Platforms and the Digital Single Market Opportunities and Challenges for Europe* (No: COM(2016) 288). Brüksel. https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX%3A52016DC0288 adresinden 10.05.2020 tarihinde alınmıştır.

Avrupa Komisyonu. (2017). *Data Protection Reform Package*. http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm adresinden 10.04.2020 tarihinde alınmıştır.

Avrupa Komisyonu. (2019a). *Data protection rules as a trust-enabler in the EU and beyond – taking stock* (No: COM(2019) 374). Brüksel. https://ec.europa.eu/commission/sites/beta-political/files/communication_from_the_commission_to_the_european_parliament_and_the_council.pdf adresinden 23.04.2020 tarihinde alınmıştır.

Avrupa Komisyonu. (2019b). *Turkey 2019 Report* (Progression Report No: SWD(2019) 220). https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-turkey-report.pdf adresinden 14.04.2020 tarihinde alınmıştır.

Avrupa Veri Koruma Kurulu. (2018). *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/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf adresinden 13.04.2020 tarihinde alınmıştır.

Avrupa Veri Koruma Kurulu. (2019). *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*. Brüksel. https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf adresinden 10.05.2020 tarihinde alınmıştır.

Avrupa Veri Koruma Kurulu. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679*. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf adresinden 10.05.2020 tarihinde alınmıştır.

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 12.05.2020 tarihinde alınmıştır.

Buttarelli, G. (2017). The Commission Proposal for a Regulation on ePrivacy: Why Do We Need a Regulation Dedicated to ePrivacy in the European Union? *European Data Protection Law Review, 3*(2), 155-159.

Buttarelli, G. (2018). *The urgent case for a new ePrivacy law*. https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en adresinden 19.04.2020 tarihinde alınmıştır.

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

DLA Piper UK LLP. (2016). *Study on the revision of the ePrivacy Directive*. https://etno.eu/datas/publications/studies/DPTS_Study_DLA_04082016_ePrivacy_Final.pdf.

Dülger, M. V. (2019). *Kişisel Verilerin Korunması Hukuku* (1. bs.). İstanbul: Hukuk Akademisi.

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

Gonzalez, E. G., De Hert, P. ve Papakonstantinou, V. (2020). The proposed ePrivacy regulation: The commission's and the parliament's drafts at a crossroads? *Data Protection and Privacy: Data Protection and Democracy* (ss. 267-298). Oxford: Hart Publishing.

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

Kiss, A. ve Szoke, G. L. (2014). Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation. *Privacy and Data Protection*, 20, 311-333.

Küzeci, E. (2018). Kişisel Verilerin Korunması (2. bs.). Ankara: Turhan Kitabevi.

Lambert, P. (2017). *Understanding the New European Data Protection Rules* (1. bs.). Amerika Birleşik Devletleri: CRC Press.

Libert, T., Graves, L. ve Nielsen, R. K. (2018). *Changes in Third-Party Content on European News Websites after GDPR*. Reuters Institute and University of Oxford. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-08/Changes%20in%20Third-Party%20Content%20on%20European%20News%20Websites%20after%20GDPR_0_0.pdf adresinden 10.05.2020 tarihinde alınmıştır.

Marcus, J. S., Petropoulos, G. ve Yeung, T. (2019). *Contribution to Growth: The European Digital Single Market Delivering economic benefits for citizens and businesses* (No: PE 631.044). Brüksel: Avrupa Parlamentosu. https://www.bruegel.org/wp-content/uploads/2019/02/IPOL_STU2019631044_EN.pdf adresinden 03.05.2020 tarihinde alınmıştır.

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

National Information Standards Organization. (2004). *Understanding Metadata. NISO Press*. https://www.lter.uaf.edu/metadata_files/UnderstandingMetadata.pdf adresinden 10.04.2020 tarihinde alınmıştır.

Türkiye Cumhuriyeti Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı. (2018.). *On Birinci Kalkınma Planı (2019-2023)*. http://www.sbb.gov.tr/wp-content/uploads/2019/07/OnbirinciKalkinmaPlani.pdf adresinden 11.05.2020 tarihinde alınmıştır.

Voigt, P. ve Von Dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. İsviçre: Springer.

Voss, W. G. (2017). First the GDPR, Now the Proposed ePrivacy Regulation. *Journal of Internet Law*, *21*(1), 3-11.

EK NOTLAR

1. Ayrıca, çalışmamız bakımından önem arz eden "konum verileri"ne yönelik düzenlemeler de Direktif ile düzenlenen konular arasındadır.
2. 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 olup bu tarih itibariyle direktifin tüm hükümleri üye ülkelerin iç hukuklarına aktarılmış olacaktır. (Ayrıntılı bilgi için bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN, E.T: 11.04.2020)
3. ABAD'ın söz konusu kararlarıyla, kişilerin elektronik haberleşme sektöründeki gizlilik ve kişisel verilerin korunması hakları güçlendirilmiş ve insan hakları odaklı kararlar AB'nin konuya ilişkin içtihatlarında hakim kılınmıştır.
4. Avrupa Komisyonu'nun ilgili teklifine dair ayrıntılı bilgi için bkz. Commission proposes a comprehensive Reform of Data Protection Rules. (https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46 , E.T.: 01.04.2020)

5. Avrupa Birliği'nde gerçekleştirilen yasama tasarruflarına ilişkin ayrıntılı bilgi için bkz. Regulations, Directives and other acts. (https://europa.eu/european-union/eu-law/legal-acts_en) [E.T.: 16.03.2020]
6. Bkz. GVKT Gerekçe 1.
7. Bu husus, E-Gizlilik Tüzüğü'nün gerekçe kısmı dahil olmak üzere çeşitli maddelerinde ifade edilmektedir.
8. Avrupa Adalet Divanı, 1 Ekim 2019 tarihinde yayınladığı ve çerez kullanımına ilişkin kullanıcı rızalarını Direktif açısından ele aldığı Planet49 kararında (C-673/17), bu rızaların, önceden işaretlenmiş halde sunulan kutucuklar yoluyla alınamayacağını ifade etmiştir. E-Gizlilik Tüzüğü'nün önceki tarihli taslakları hakkındaki düşünceler ve özellikle rıza kavramına ilişkin bilgi ve değerlendirmeler için bkz. (Keser Berber, Atabey ve Mert, 2019)
9. Ayrıntılı bilgi için bkz. https://www.enpa.eu/news/cross-industry-open-letter-e-privacy-europe-cannot-afford-miss-data-revolution
10. Ayrıntılı bilgi için bkz. https://siteimprove.com/en/gdpr/eprivacy-regulation-rethinks-cookies/
11. Ayrıntılı bilgi için bkz. https://www.bbc.com/news/technology-45967301
12. Ayrıntılı bilgi için bkz. https://www.ecpat.org/wp-content/uploads/2018/12/Letter-to-EU.pdf
13. GVKT'nin bu özelliği, "sınır ötesi" etki olarak tanımlanmakta olup bu perspektiften bakıldığında, GVKT'nin bazı kaynaklarda "bulaşıcı bir hastalık" olarak tanımlandığı görülmektedir (Kiss ve Szoke, 2014).
14. Örneğin, "Spor salonu servisi sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar Özeti". Bu karar hk. ayrıntılı bilgi için bkz. "https://www.kvkk.gov.tr/Icerik/5496/2019-81-165" (E.T: 16.03.2020); Ayrıca, Kurum'un 10.04.2020 tarihinde yayınlamış olduğu ve kişisel verilerin yurtdışına aktarımına ilişkin "bağlayıcı şirket kuralları"nı düzenleyen belgede de bu etkiyi görmek mümkündür. Bu belge hk. ayrıntılı bilgi için bkz. "https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU" (E.T: 11.04.2020)
15. Kişisel Verileri Koruma Kurulu'nun ilgili "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: 08.05.2020)
16. İnternet Dünya İstatistikleri raporuna göre Türkiye'de 46,282,850 kişi internet kullanmakta olup bu rakama Türkiye toplam nüfusunun yaklaşık %60'ına denk gelmektedir. Türkiye'de internet kullanıcı sayısına dair istatistikler için bkz. https://internet.btk.gov.tr/istatistikler (E.T: 08.04.2020)