

Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-

Şehriban İpek, Aşıkoğlu

İstanbul Üniversitesi/Hukuk Fakültesi/Özel Hukuk Bölümü/Avrupa Birliği Hukuk Anabilim Dalı, İstanbul, Türkiye, ipekasikoglu@istanbul.edu.tr

ORCID: orcid.org/0000-0003-4505-4048-

ÖZ

Günümüzde artan ve çeşitlenen kişisel veri işleme faaliyetleri ilgili kişilerin ve otoritelerin şeffaflık beklentilerini artırmaktadır. Kişisel verilerin korunması alanında bireylere tesis edilmiş haklar ve veri sorumlularına getirilmiş olan yükümlülükler kişisel verilerin korunması alanındaki temel enstrümanları oluşturmaktadır. Aydınlatma yükümlülüğü gerek ilgili kişilerin kişisel verilerinin üzerinde kontrolünün sağlanması gerekse veri işleme faaliyetinin hukuka uygunluğunun denetlenebilmesi için bir bel kemiği vazifesi görmektedir. Bununla birlikte iş modeli kişisel veri işlemeye dayanmayan gündelik olağan işleri kapsamında kişisel veri işleme faaliyeti yürüten küçük işletmeler bakımından ise ilgili kişinin bilgilendirilmesi ciddi bir yük oluşturmaktadır. Bu çalışmada aydınlatma yükümlülüğünün maddi ve şekli boyutu ile veri sorumlularının aydınlatma yükümlülüğünden muaf tutulduğu hâller Avrupa Birliği ve Türk hukuku bakımından ele alınmıştır. *Anahtar Sözcükler: Aydınlatma yükümlülüğü, şeffaflık ilkesi, kişisel verilerin korunması, kişisel veri*

Information Obligation of Data Controllers In European Law and Turkish Law

ABSTRACT

Nowadays increasing and diversifying of personal data processing activities increase the transparency expectations of individuals and authorities. Rights given to data subjects and obligations foreseen for data controllers are fundamental instruments of data protection area. Information obligation acts as a backbone in order to ensure control over the personal data of the data subject and to check the legality of the data processing activity. In addition to this information obligation is a heavy burden to small enterprises who have no data-driven business models and process personal data only in daily life. In this study, material and formal elements of information obligation and exceptions for data controllers' information obligation are examined in accordance with European law and Turkish law.

Keywords: Information obligation, transparency, personal data protection, personal data

Atıf Gösterme

Aşıkoğlu, Ş.İ. (2019). Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-, *Kişisel Verileri Koruma Dergisi*. 1(2), 41-65.

GİRİŞ

Kişisel verilerin korunması hukuku alanında verisi işlenen gerçek kişiye yaratılan koruma alanı içerisinde kişisel verilerinin ilgili kişi tarafından kontrolünün sağlanması, bireyin hür iradeyle hareket etmesi ve bu irade doğrultusunda kişiliğini geliştirmesi ve geleceğini belirlemesi yer almaktadır (Küzeci, 2014). Buna karşın teknolojinin gelişmesiyle beraber artan ve çeşitlenen veri işleme faaliyetleri veriye değer kazandırırken, ilgili kişilerin kişisel verileri üzerindeki hakimiyeti azalmaktadır. İlgili kişiye, kişisel verilerinin hakimiyetini tesis için büyük önem arz eden veri sorumlusunun aydınlatma yükümlülüğü AB hukuku ve Türk hukuku kapsamında bu çalışmada incelenecektir.

Veri sorumlusunun aydınlatma yükümlülüğü AB hukuku kapsamında mülga Kişisel Verilerin İşlenmesine ve Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki 95/46/AT Sayılı ve 24 Ekim 1995 Tarihli Avrupa Parlamentosu ve Avrupa Birliği Konseyi Yönergesi (“95/46/AT sayılı Yönerge”) 10 ve 11. maddelerinde, Gerçek Kişilerin Kişisel Verilerinin Korunması ve Serbest Dolaşımı ve 95/46/EC Sayılı Yönerge’nin Kaldırılmasına İlişkin 27 Nisan 2016 tarihli 2016/679 Sayılı Tüzük (“Tüzük”) 13 ve 14. maddelerinde düzenlenmiştir. Bu ölçüde detaylı olmamakla birlikte uluslararası metinler bakımından ise APEC Çerçeve Belgesi par. 15, Avrupa Komisyonu 108 sayılı Sözleşme m. 8, OECD Rehber İlkeleri par. 12, BM Genel İlkeler 3. ilke kapsamında ilgili kişinin bilgilendirilmesine ilişkin düzenlemeler yer almaktadır.

Türk hukukunda ise 24 Mart 2016 tarihinde kabul edilen ve 7 Nisan 2016 tarih ve 29677 sayılı Resmî Gazete’de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu (“KVKK”) m. 10 kapsamında veri sorumlusunun aydınlatma yükümlülüğü düzenlenmiş ve usul ve esasları 10.03.2018 tarihli 30356 sayılı Resmî Gazete’de yayımlanarak yürürlüğe giren Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ (“Aydınlatma Yükümlülüğü Tebliğ”) kapsamında belirlenmiştir. Türk hukukuna ilişkin incelemeler bu düzenlemeler ışığında yapılacaktır. Bu çalışmada AB hukuku kapsamında kişisel verilerin korunması alanında detaylı düzenlemeleri ihtiva eden ve AB üye devletleri nezdinde doğrudan uygulama alanına sahip Tüzük hükümleri Türk hukukundaki düzenlemeler ile özellikle aydınlatma yükümlülüğünün şekli ve maddi unsuru ile istisnaları bakımından karşılaştırmalı olarak incelenecektir.

AYDINLATMA YÜKÜMLÜLÜĞÜ

Kişisel verilerin korunması alanında bireylere tesis edilmiş haklar ve veri sorumlularına getirilmiş olan yükümlülükler bireylerin kişisel verilerin korunması alanındaki temel enstrümanlarını oluşturmaktadır. Bireylere tanınmış olan haklar ilgili kişiye veri işleme faaliyetinin hukuka uygunluğunu denetleme imkânı vermektedir (Çekin, 2019, s. 119). Bu hakların anahtarı niteliğinde ilgili kişiye sunulan aydınlatma metinleri ise ilgili kişinin kişisel verilerinin korunmasına ilişkin temel hak ve özgürlüklerinin merkezini oluşturmaktadır (Beyleveld, 2004; Küzeci, 2019, s. 218).

Tüzük kapsamında aydınlatma yükümlülüğü ilgili kişinin hakları bölümü altında düzenlenmiştir. İlgili kişinin Tüzük uyarınca sahip olduğu, kişisel verilerine erişim isteme, verilerinin silinmesini, düzeltilmesini talep etme gibi haklarından farklı olarak aydınlatma yükümlülüğü kapsamında ilgili kişiye sağlanacak olan bilgiler bakımından ilgili kişinin aktif bir hareketi gerekmemektedir. Aydınlatma yükümlülüğü kapsamında ilgili kişiye sağlanacak olan bilgiler gerek kişinin verilerinin kontrolünü elde etmesi gerekse veri sorumlusunun genel ilkelere uygun bir şekilde veri işleyebilmesi adına önem teşkil etmektedir.

Aydınlatma yükümlülüğünün temelinde şeffaflık ilkesi yer almaktadır. 95/46/AT sayılı Yönerge’de açıkça genel ilkeler arasında sayılmamış olan şeffaflık ilkesi sadece kişisel verilerin korunması alanında değil Avrupa Birliği Hukukunda da uzun süredir ön planda tutulan bir ilkedir. Gerek kamu gerekse şirketler hukuku bakımından hesap verilebilirlik, kamuyu aydınlatma ve şeffaflık ihtiyacı artmakta ve bu yönde düzenlemeler yapılmaktadır. Kişisel verilerin korunması alanında ise 95/46/AT sayılı Yönerge’nin yürürlük döneminde de Avrupa Birliği Adalet Divanı kararlarında şeffaflık ilkesine vurgu yapılmakta idi (AAD, C-553/07, par. 9, 60).

Günümüzde ise özellikle teknolojinin hızla gelişmesiyle birlikte gündelik hayata dahil olan nesnelere interneti, yapay zekâ uygulamaları, akıllı cihazların gerçek zamanlı olarak yürüttükleri otomatik veri işleme faaliyetleri karşısında ilgili kişilerin korunabilmesi için şeffaflık ilkesinin veri sorumluları tarafından her aşamada benimsenmesi gerekmektedir (Hildebrandt, 2012). Bu artan ve çeşitlenen veri işleme faaliyetleri karşısında şeffaflık, kullanıcı kontrolü ve hesap verilebilirlik ilkeleri teknolojik gelişmelerin merkezine yerleştirilmelidir (Aşıkoğlu, 2018, s. 149; Lynskey, 2015, s. 248). Nitekim Tüzük’ün yürürlüğe girmesine az bir süre kala, 18 Mayıs 2018’de, Avrupa Konseyi Bakanlar Komitesi tarafından kabul edilen Avrupa Konseyi 108 sayılı Kişisel Verilerin İşlenmesine İlişkin Olarak Bireylerin Korunması Sözleşmesi’ni yenileyen Protokol kapsamında da bu yaklaşım görülmektedir. Yenilenen Protokol kapsamında şeffaflık ilkesi genel ilkeler arasında kabul edilmiş, işleminin şeffaflığı başlıklı madde eklenmiştir.

Tüzük 5/1-a’da sayılarak genel ilkeler arasında yer alan şeffaflık ilkesi Tüzük’te açıkça tanımlanmamıştır. Ancak giriş bölümü 39. paragrafta şeffaflık ilkesi açıklanırken veri sorumlusu tarafından sunulan şeffaflığın ilgili kişi nezdinde sonuç doğurmasının beklendiğine işaret edilmiştir. Şeffaflık ilkesi ve gerekliliklerinin yorumunda bir madde hükmündense somut olay ve ilgili kişi önem taşımaktadır (Çalışma Grubu, 260 rev. 01, 2018).

Türk Hukuku açısından ise Anayasa’da temel bir hak olarak düzenlenen kişisel verilerin korunması hakkı kapsamında kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme sayılmıştır (Anayasa m. 20). Bu kapsamda KVKK ve Aydınlatma Yükümlülüğü Tebliği ile detaylandırılan bu yükümlülüğün Anayasa kapsamında da güvence altına alındığının altını çizmek gerekecektir. İlgili kişinin bu bilgilendirilme hakkı kişisel verilerin elde edilme anında veri sorumlusuna bir yükümlülük olarak getirilmiştir.

Tüzük kapsamında aydınlatma yükümlülüğüne ilişkin olarak şeffaflık ilkesinin vurgulandığı madde 12 hükmü de ilgili kişinin haklarının düzenlendiği Tüzük m. 13-23 hükümleri kapsamındaki etkisi itibari ile bütüncül olarak değerlendirilmelidir. İlgili kişinin haklarını kullanmasına ilişkin olarak tarafımızca benimsenmiş *Çekin* tarafından ifade edilen şekli-maddi boyut ayrımı esas alınmıştır (Çekin, 2019, s. 70). Bu kapsamda şeffaf bilgilendirme, iletişim ve yöntemler başlıklı 12. madde kapsamında aydınlatma yükümlülüğünün şekli boyutuna işaret edilirken Tüzük m. 13 ve 14’te maddi boyutu açıklanmaktadır. KVKK kapsamında ise Tüzük’te olduğu gibi aydınlatma yükümlülüğü bakımından verilerin ilgili kişiden doğrudan elde edilmesi ya da üçüncü kişi aracılığı ile elde edilmesi hâli bakımından bir ayırım yapılmamış, genel olarak aydınlatma yükümlülüğünün çerçevesi çizilmiştir. Aydınlatma yükümlülüğü kapsamında uyulacak usul ve esaslar ise Aydınlatma Yükümlülüğü Tebliği’de düzenlenmiş ve bu ayırma yer verilmiştir.

Aydınlatma yükümlülüğünün yerine getirilmesi bakımından pratik hayattaki başlıca sorunlar şu şekilde özetlenebilecektir:

- i. Özellikle iş ve ekonomik modeli kişisel verilerin işlenmesi merkezli olan ve kapsamlı, karmaşık veri işleme faaliyeti yürüten veri sorumluları bakımından aydınlatma metninin yalın, basit tutulması ilgili kişilerin yeterince bilgilenmemesine; detaylı olması hâlinde ise ilgili kişiler tarafından metnin anlaşılmasına neden olmaktadır.

- ii. Özellikle iş modeli kişisel verilerin işlenmesine dayanmayan (menfaat elde etmeyen), kişisel verileri elektronik olarak işlemeyen, hukuki yükümlülüğün yerine getirilmesi, sözleşmenin ifası gibi hukuka uygunluk sebeplerine dayanarak ve bunlarla sınırlı olarak işleyen, kurumsallaşmamış küçük ölçekteki işletmeler bakımından ise hayatın olağan akışı içerisinde aydınlatma metnine yer vermek güçlük arz edebilmektedir.

Bu sorunlardan ilki aydınlatma yükümlülüğünün şekli unsuruna ilişkindir. Gerçekten de özellikle açık rıza hukuka uygunluk sebebine dayalı veri işleme faaliyetleri bakımından ilgili kişi tarafından anlaşılabilen bir aydınlatma metni açık rızanın bilgilendirmeye dayalı olma unsurunu sağlamayacağından veri işleme faaliyetini hukuka aykırı hâle getirecektir. Aydınlatma metninde yer verilmesi gereken hususlar (maddi unsur) ise yine bu sorun kapsamında önem taşımaktadır. Veri sorumlusunun kişisel veri işleme amacına ilişkin olarak dayandığı KVKK m. 5-6 hükümlerinde yer alan veri işleme şartlarının yanlış tespit edilmesi ya da ilgili kişiye yanlış veya hatalı ya da eksik olarak bildirilmesi ilgili kişinin yanıtılmasına yol açıyorsa dürüstlük kuralına aykırılık teşkil edecektir (Yücedağ, 2019).

Ancak burada hukuki yükümlülüğün yerine getirilmesi, kanunlarda açıkça öngörülme hukuka uygunluk sebeplerinin karıştırılması ya da her somut olay bazında değerlendirme gereken, otoriteler ve Adalet Divanı tarafından da çerçevesi tartışılan meşru menfaat hukuka uygunluk sebebinin tespitinde veri sorumlusunun hatalı bir değerlendirme yaparak aydınlatma metnini buna göre kurgulamış olması hâlinde özellikle ilgili kişi nezdinde etkisine bakılması gerekecek, doğrudan dürüstlük kuralına aykırılık teşkil ettiği ifade edilemeyecektir. Buna karşın sözleşmenin ifası için gerekli olmayan verilerin aydınlatma metninde açık rıza yerine sözleşmenin ifası hukuka uygunluk sebebine dayanarak işleneceğinin ifade edilmesi dürüstlük kuralına aykırılık teşkil edecektir. Google, Facebook gibi ana faaliyet konusu kişisel veri işlemeye dayalı ve günümüz ekonomisinde ciddi pay sahibi şirketler bakımından kullanıcılarına sunulan metinlerin aydınlatma yükümlülüğünü karşılayıp karşılamadığına ilişkin denetimde şekli ve maddi boyut büyük önem taşımaktadır.

İkinci sorun ise temel olarak veri koruma mevzuatının geniş uygulama alanından kaynaklanmaktadır. Gerçekten de kişisel verilerin korunmasına ilişkin düzenlemelerde yer alan veri sorumlusu, veri işleme ve kişisel veri kavramları son derece geniştir (bkz. AAD, C-212/13 ve C-212/13 sayılı kararları). Bu nedenle düzenlemelerin uygulama alanının gündelik hayattaki hemen her türlü veri işleme faaliyetini kapsıyor olması sebebi ile pek çok alanda aydınlatma yükümlülüğü doğmakta, ancak bu yükümlülük ihmal edilmektedir. Burada özellikle kurumsallaşmamış küçük işletmeler bakımından veri işleme süreçlerinin standart olmaması, otomasyon ve dijital süreçlerin geliştirilmemiş olması, ilgili kişi gruplarının değişkenliği gibi sebeplerle aydınlatma yükümlülüğü hiç yerine getirilememekte ya da içerik bakımından fiili durumu karşılamayan jenerik metinlere yer verilmektedir. Bu durum ise aydınlatma yükümlülüğü ile beklenen ilgili kişinin kişisel verileri üzerindeki kontrolünü sağlaması amacına hizmet etmemekte, aksine ilgili kişileri yanıltmaktadır. İkinci sorun bakımından veri işleme faaliyetinin kişisel verilerin korunması düzenlemeleri kapsamında tam istisna ya da aydınlatma yükümlülüğü bakımından getirilmiş olan bir istisna kapsamında olup olmadığının değerlendirilmesi gerekecektir.

AYDINLATMA YÜKÜMLÜLÜĞÜNÜN ŞEKİL VE MADDİ UNSURU

Şekli Unsur

Şeffaflık ilkesi uyarınca ilgili kişiyle ya da kamuyla paylaşılacak olan bilginin öz, şeffaf, anlaşılır, kolayca ulaşılabilir ve basit, sade bir dille hazırlanmış olması gerekmektedir. Tüzük'te yer alan şeffaflık ilkesinin aydınlatma yükümlülüğü ve ilgili kişinin haklarını kullanması sırasında kurulacak olan iletişimde görünümü olan öz, şeffaf, anlaşılır, kolayca ulaşılabilir ve basit, sade bir dil gerekliliği Kişisel

Verilerin Korunması Kanunu kapsamında dürüstlük kuralına uygun olma ilkesi ile bağdaşacaktır. Nitekim 95/46 sayılı Yönerge ve Kişisel Verilerin Korunması Kanunu kapsamında açıkça belirtilmeyen şeffaflık ilkesinin adil olma (dürüstlük kuralına uygun olma) ilkesinin bir görünümü olduğu kabul edilmektedir (Bygrave, 2014, s. 147; Develioğlu, 2017, s. 45; Yücedağ, 2019). Bu doğrultuda Aydınlatma Yükümlülüğü Tebliği'nde de bu yükümlülüğün yerine getirilmesinde anlaşılır, açık ve sade bir dil kullanılması; tamamen teknik bilgi, uzmanlık gerektiren bir terminoloji ile genel nitelikte ve muğlak ifadelerle yer verilmemesi gerektiği belirtilmiştir. Özellikle açıklanacak kişisel veri işleme amacının belirli, açık ve meşru olması gerekmekte, gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıran ifadeler kullanılmamalıdır. İlgili kişi bakımından erişilebilir ve kişisel verilerin toplandığı mecra ile uyumlu olması gerekmektedir.

Öz, Şeffaf ve Anlaşılır Olma

Aydınlatma metninin öz ve şeffaf olması gerekliliği, hukuki ve ağıdalı bir dilin kullanılmamasını, kişisel verilerin işlenmesi ve korunmasına ilişkin olmayan gereksiz açıklamalardan kaçınılmasını ifade eder. Genellikle avukatlar tarafından hazırlanan ve karmaşık ifadeler içeren aydınlatma metinleri örneğin açık rıza hukuka uygunluk sebebi uyarınca yürütülen bir veri işleme faaliyetinde ilgili kişinin bilgilendirilmesi şartı gerçekleşmeyeceği için hukuka aykırı veri işlemeyi gündeme getirecektir (Cate ve Mayer-Schönberger, 2013). Ayrıca bu durum her hâlükârda aydınlatma yükümlülüğünün ihlaline de sebep olacaktır.

Veri sorumlusunun kişisel verilerini işlemeyi planladığı ilgili kişi grubunu önceden belirleyerek aydınlatma metninin dilini buna göre oluşturması metnin dili ve ayrıntısı bakımından önem teşkil etmektedir. Söz konusu metnin veri işleme faaliyetinin hukuka uygunluğu için bir bel kemiği vazifesi göreceği dikkate alındığında veri sorumlusunun gerçekleştireceği veri işleme faaliyeti nezdinde doğacak hesap verilebilirlik yükümlülüğü gereği ilgili kişi grubu için anlaşılır bir metin hazırlamak için kullanıcılar nezdinde saha çalışmaları, anket çalışmaları yapmak, tüketici dernekleri ve düzenleyici otoriteler ile görüşmek gibi gerekli faaliyetleri yürüterek bu metinleri oluşturması beklenmektedir (Çalışma Grubu, 260 rev. 01, 2018). Nitekim aydınlatma metninin dilinin yalın, öz olmaması, karmaşık ifadelerle yer verilmiş olması hâlinde veri sorumlusunun hesap verilebilirlik ilkesi uyarınca neden bu dilin seçildiğini ve bu metnin dürüstlük kuralına uygun olduğunu açıklamaları gerekecektir. Burada “bilgilendirmenin basit olması hâlinde ilgili kişilerin gerçekten bilgilendirilmiş olmayacağı; detaylı olması hâlinde ise ilgili kişilerce anlaşılacak” yönünde bir paradoks olduğu ifade edilmektedir (Tene, 2013). Ancak belirtmek gerekir ki metnin öz olmasından anlaşılması gereken veri işleme faaliyetlerine ilişkin yüzeysel bilgilere yer verilmesi değildir. Bilakis veri işleme faaliyetinin hukuki sebepleri ve ilgili kişi nezdinde temel hak ve özgürlükleri bakımından doğurması muhtemel sonuçlarının açıkça ifade edilmesi, bütün bu hususların sebep ve sonuçları itibari ile ilgili kişiye sunulması gerekmektedir (Lynskey, 2015, s. 248).

Kesin olmayan belirsiz cümlelerden ve muğlak ifadelerden kaçınılması gerekmektedir. Çalışma Grubu, “belki”, “olabilir”, “bazı”, “sık sık” ve “mümkün” ifadelerin aydınlatma metinlerinde tercih edilmemesi gerektiğini, anlaşılması güç, hukuki, teknik açıklamalar ve uzmanlık gerektiren özel terimlere yer verilmemesi gerektiğini belirtmiştir (Çalışma Grubu, 260 rev. 01, 2018; Lynskey, 2015, s. 249). Nitekim, Kişisel Verilerin Korunması Kurumu tarafından hazırlanan Rehber’de de “Kişisel verilerinizi yeni hizmetler geliştirmek için kullanabiliriz” ya da “Kişisel verilerinizi araştırma amaçlı olarak kullanabiliriz” gibi ifadelerden belirsiz olmaları sebebi ile kaçınılması gerektiği ifade edilmiştir (Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, 2019).

Şeffaflık ilkesinin uygulanmasında özellikle ilgili kişi grubu da önem arz etmektedir. Bu duruma Tüzük m. 12/1’de yer alan çocuklara yönelik vurgu örnek gösterilebilecektir. Veri sorumlusu aydınlatma yükümlülüğünü yerine getirirken özellikle kişisel verilerini işlemeyi amaçladığı ilgili kişi grubunda

çocukların olup olmadığını değerlendirmek zorundadır. Yine aydınlatma yükümlülüğünün görsel ve yazın olarak yerine getirildiği hâllerde veri sorumlularının görme engelli ya da renk körü olan gerçek kişileri dikkate alması gerekecektir (Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, 2019; Çalışma Grubu, 260 rev. 01, 2018). Bu kapsamda açık bir şekilde basiretli bir veri sorumlusunun kişisel veri işlemeye başlamadan önce veri işleme faaliyetine konu olacak kişi gruplarını öngörebiliyor olması gerekmektedir. Bu doğrultuda aydınlatma yükümlülüğünü yerine getirirken tercih edeceği yolu ve dili bu kitleye göre seçmesi gerekecektir.

Erişilebilir Olma

Aydınlatma metninin çevrimiçi ortamlarda yerine getirilmesi bakımından mümkün merteye ilgili kişinin aradığı bilgiye kolayca ulaşmasına elverecek şekilde gerekli bilgilendirmenin katmanlı ve kullanıcı merkezli olarak sunulması önerilmektedir (Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, 2019; Çalışma Grubu, 260 rev. 01, 2018; European Union Agency for Fundamental Rights and Council of Europe, 2018;). İngiliz Veri Koruma Otoritesi (“ICO”) tarafından hazırlanan rehber kapsamında aydınlatmanın katmanlı olarak, kontrol paneli aracılığı ile, verinin alınma anında veri özelinde açıklamalar ile, simgeler aracılığı ile ya da mobil ve akıllı cihazların özellikleri uyarınca nasıl gerçekleştirilebileceğine ilişkin örnekler yer verilmiştir (ICO, “Are there different ways we can provide privacy information?”). Genel geçer olarak bu modellerden en iyisini seçmek mümkün değildir. Aydınlatma metninin sunulduğu mecra ve kişisel verilerin toplanma yöntemi bakımından değerlendirilerek buna en uygun modelin tercih edilmesi, geliştirilmesi gerekmektedir.

Aydınlatma yükümlülüğünün yerine getirilmesine ilişkin olarak ilgili kişiye bilgilerin sağlanması sırasında veri sorumlusu tarafından herhangi bir ücret ilgili kişiye yansıtılmayacaktır (Tüzük 12/5).

Şekil Şartı

Tüzük uyarınca aydınlatma yükümlülüğünün yerine getirilmesinde herhangi bir şekil şartı öngörülmemiştir. İlgili kişiye aydınlatma yükümlülüğü kapsamındaki bilgiler yazılı ve sözlü olarak ya da elektronik ortamda dâhil olmak üzere diğer yollarla sunulabilecektir. Ancak burada aydınlatma yükümlülüğünün yerine getirildiğine ilişkin ispat yükü veri sorumlusunda olacağından, veri sorumlusunun söz konusu aydınlatmayı kaydedilebilir, ispat edilebilir bir formatta ilgili kişiye sunmuş olması gerekmektedir. Bu noktada ilgili kişinin bilgiye kolayca erişebilir olması önem teşkil etmektedir. Nitekim Aydınlatma Yükümlülüğü Tebliği kapsamında veri sorumlusu ya da yetkilendirdiği kişi tarafından uygulanması gereken bir şekil şartı koşulmamış, örnekleme yoluyla aydınlatmanın sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle yapılabileceği belirtilmiştir. Söz konusu metotlara ilişkin örnekler, URL bağlantısı, karekod, internet sitelerinde açılan pencereler aracılığıyla bildirimlerin yapılması şeklinde çoğaltılabilecektir (Taştan, 2017, s. 159). Burada esas olarak aydınlatma metninin sözleşme hükümleri ya da genel işlem koşullarından ayrı olarak sunulması gerekmektedir (Çalışma Grubu, 260 rev. 01, 2018). Nitekim Aydınlatma Yükümlülüğü Tebliği’nde de veri işleme amacının ilgili kişinin açık rızasını gerektirmesi hâlinde aydınlatma yükümlülüğünün yerine getirilmesi ve açık rızasının alınması süreçlerinin ayrı ayrı kurgulanması gerektiği belirtilmiştir.

Veri sorumlusunun aydınlatma yükümlülüğünün yerine getirilmesi için gerekli bilgileri sunmasının yanı sıra bu bilgileri kişisel veri topladığı mecra ya da en uygun şekilde sunduğunu da açıklaması gerekecektir. Kişisel verilerin toplandığı mecra ile uyumlu olarak bu yükümlülük internet sitesinden erişilebilir olan bir yazılı metin, çağrı merkezlerinde ses kaydı, işyerlerinde duvar ya da panoya asılmış ancak ilgili kişinin kişisel verilerini verme anında dikkatini çekmesine elverişli metotlarla yerine getirilebilecektir (Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, 2019). Ancak bu durum özellikle güvenlik kameraları ya da sensörler, drone çekimleri gibi durumlar bakımından çeşitli güçlükler barındırmaktadır

(güvenlik kameraları kapsamında AB kurum ve organları tarafından aydınlatma yükümlülüğünün yerine getirilmesine ilişkin olarak öneriler için bkz. EDPS, 2010).

Yine mobil uygulamalar bakımından gerekli bilgilerin hem uygulama indirilmeden önce hem de uygulama indirildikten sonra uygulama içerisinde kolayca erişilebilir olması gerektiği belirtilmektedir. En iyi uygulama bakımından ise çevrimiçi ortamlarda yürütülen kişisel veri toplama faaliyetleri bakımından aydınlatma yükümlülüğünün verilerin toplandığı alanda yapılması önerilmektedir (Çalışma Grubu, 260 rev. 01, 2018).

Aydınlatma metninin elektronik ortamda sunulmasında muhakkak yazılı olması aranmamaktadır. Veri sorumlusu bu yükümlülüğü en açık ve kolay anlaşılabilir şekilde yerine getirmek için video, infografik, bilgi şemaları, resim ya da sesli anlatım yolunu tercih edebilecektir. Yine akıllı telefon ve akıllı cihazlar bakımından aydınlatmanın bildirim şeklinde ya da cihazın kullanımına uygun yollarla yapılabileceği ifade edilebilecektir.

Tüzük 12/1 kapsamında ilgili kişinin talebi üzerine aydınlatma da dahil olmak üzere veri sorumlusu tarafından ilgili kişinin teyit edilmesi hâlinde ilgili kişi ile iletişimin sözlü olarak yapılmasına imkân tanınmıştır. Ancak burada aydınlatma yükümlülüğü bakımından ilgili kişinin teyidi zorunluluğu aranmamalıdır. Nitekim aydınlatma kişiye özel olmayıp gelecek ilgili kişiler içinde erişilebilir ve geçerli, veri sorumlusu tarafından yürütülecek olan işleme faaliyetine ilişkindir. Bu doğrultuda aydınlatma yükümlülüğün sözlü yerine getirildiği hâllerde otomatik bir mesaj ya da önceden hazırlanmış ve veri işleme faaliyetine ilişkin bütün kullanıcılara yönelik bir metnin sesli olarak okunması söz konusu olabilecektir. Aydınlatma yükümlülüğünün sözlü olarak yerine getirilmesi hâlinde veri sorumlusu, bu talebin ilgili kişiden geldiğini ve aydınlatma yükümlülüğünü sözlü olarak yerine getirdiğini ispatla yükümlü olacaktır.

Alternatif Metotlar: Standart Simgeler

Aydınlatma yükümlülüğünün şeffaf ve işlevsel olarak yerine getirilebilmesi adına Tüzük'te veri sorumluları tarafından planlanan işleme faaliyetine ilişkin olarak anlamlı bir genel bakışın kolayca görülebilir, anlaşılabilir ve okunaklı bir biçimde sağlanması amacı ile standart simgelerin kullanılabileceği belirtilmiştir. Veri sorumlusunun standart simgelere yer vererek elektronik olarak aydınlatma yükümlülüğünü yerine getirmeyi tercih etmesi hâlinde simgelerin makine tarafından okunabilecek şekilde olması sağlanmalıdır. Belirtmek gerekir ki Tüzük kapsamında "makine tarafından okunabilir olma" tanımı yer almamaktadır. 26 Haziran 2013 tarih ve 2003/98/EC sayılı kamu sektörü bilgilerinin tekrar kullanımına ilişkin yönergede değişiklik yapan 2013/37/AB sayılı Yönergenin giriş bölümü 21. paragrafta makine tarafından okunabilir olma bilginin bir dosya olarak biçimlendirilmiş olması hâlinde bu dosya içerisindeki bilgilerin yazılım uygulamaları ile kolayca tanımlanması, tanınması ve çıkarılmasının mümkün olması olarak açıklanmıştır. Tüzük'te standart simgelerin elektronik ortamda yer verilmesi hâlinde makine tarafından okunabilecek şekilde olması şartı koşulmuş olduğundan standart simgelere yazılı ortamlarda, cihaz ambalajlarında ve özellikle güvenlik kameralarına ilişkin fiziksel uyarılarda da yer verilebileceği anlaşılacaktır (Çalışma Grubu, 260 rev. 01, 2018). Önemle belirtmek gerekir ki kullanılacak olan standart simgelerin ilgili kişi nezdinde bir karışıklığa sebep vermemesi gerekmektedir. Aydınlatma yükümlülüğünün yerine getirilmesi adına Tüzük ile önerilen bu yol ilgili kişinin okumaktan yorulacağı bilgileri azaltarak görsel anlamda bilgilendirilmesini sağlamak ve şeffaflığı arttırmaktır. Bununla birlikte kullanılacak olan standart simgeler aydınlatma yükümlülüğünün maddi içeriğini yansıtır olmalıdır. Bu alanda veri sorumluları tarafından kullanılacak simgelerin çeşitli olmasının ilgili kişinin yanılması sebebiyet verebileceği düşüncesiyle etkin bir şeffaflık için üye devletler nezdinde kullanılan standart simgelere ihtiyaç duyulacağı açıktır (Çalışma Grubu, 260 rev. 01, 2018).

Tüzük kapsamında standart simgelere ilişkin kuralların belirlenmesi konusunda Komisyon'un sorumlu olduğu (Tüzük 12/7) ancak Avrupa Veri Koruma Kurumunun, Komisyonun talebi ya da kendi takdiri ile bu konuda Komisyon'a görüş sağlayabileceği (Tüzük 70) belirtilmiştir. Kişisel verilerin korunması alanında Avrupa Birliği kapsamında denetleyici otoritelerin veri sorumluları ile işbirliği içerisinde hareket ederek ihlalleri sadece caydırıcı cezalarla değil farkındalık yaratarak pek çok pay sahibinin fikrinin alınması ile yapılacak düzenlemelerle önlenmesi fikri yaygınlaşmaktadır (Çekin, 2019, s. 176-177). Standart simgeler bakımından da bu konuda yaratılacak kurallar bütünü hazırlanması sırasında sektör ve geniş kamu dahilinin gerçekleştiği bir araştırma standart simgelerden elde edilmek istenen menfaati gerçekleştirecektir.

Maddi Unsur

95/46/AT sayılı Yönerge'de yer alan aydınlatma yükümlülüğü uyarınca üye devletler hukukunda ilgili kişiye sunulması gereken bilgiler hususundaki çeşitlilik özellikle birlik içerisinde veri aktarımlarının olduğu durumlar bakımından problemler yaratmakta idi (üye devletler nezdindeki farklı düzenlemelere ilişkin bkz. Korff, 2002, s. 98 vd.). Bu bakımdan Tüzük ile büyük ölçüde çerçevesi netleştirilmiş ilgili kişiye sunulacak bilgi kapsamı veri koruma hukukunun amaçlarından olan verinin serbest dolaşımı prensibine de uygun düşmektedir.

Kişisel verilerin doğrudan kişinin kendisinden toplandığı hâllerde elde edilme anında veri sorumlusunun ilgili kişiye sağlaması gereken bilgiler Tüzük m. 13'de belirtilirken, madde 14'te kişisel verilerin doğrudan kişinin kendisinden toplanmadığı hâllerde sağlaması gereken bilgiler belirtilmiştir. Türk hukukunda ise KVKK 10'da sayılan aydınlatma yükümlülüğünün içeriğine ilişkin hususlar Aydınlatma Yükümlülüğü Tebliği'de aynen yer almış, bunların asgari içerik olduğu belirtilmiştir. Aydınlatma Yükümlülüğü Tebliği'de kişisel verilerin ilgili kişiden doğrudan toplanmadığı hâllerde söz konusu bilgilerin sunulmasına ilişkin süreler belirtilmiş, ancak sunulması gereken bilgilerde herhangi bir ayırım yapılmamıştır. Belirtmek gerekir ki veri sorumlusu bu bilgileri başka bir veri sorumlusundan KVKK 8-9 uyarınca, kamu kurum ve kuruluşlarından ya da kamuya açıklanmış bilgilerden elde etmiş olabilecektir. Bu doğrultuda bu hâlin "fiili imkânsızlık veya ilgili kişiye ulaşılamaması nedeniyle doğrudan ilgili kişiden elde edilememesi" (Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, 2019) hâli ile sınırlı olarak yorumlanmaması gerektiği kanaatindeyiz.

Kişisel Verilerin Doğrudan İlgili Kişiden Toplanması

Tüzük 13 kapsamında veri sorumlularının kişisel verilerin ilgili kişiden elde edilme anında sağlamak zorunda olduğu bilgilerin çerçevesi çizilmiştir. Buna göre veri sorumlusu:

- a. Veri sorumlusu ve varsa temsilcisinin kimliği ve iletişim bilgileri,
- b. Varsa, veri koruma görevlisinin iletişim bilgileri,
- c. Kişisel verilerin işleme amacı ve özellikle hukuki dayanağı,
- d. Kişisel verilerin meşru menfaat hukuka uygunluk sebebine dayanarak işlenmesi hâlinde veri sorumlusu ya da üçüncü taraf tarafından ileri sürülen meşru menfaat,
- e. Varsa, kişisel verilerin alıcıları ya da alıcı kategorileri,
- f. Kişisel verilerin birlik dışına aktarılması hâlinde yeterli ve uygun güvenlik önlemlerine ilişkin bilgiler ve bu bilgilerin bir kopyası ya da bu bilgilerin erişilebilir olduğu yere ilişkin bilgileri ilgili kişiye sunmakla yükümlüdür.

Yukarıda sayılan bilgilere ek olarak veri işleme faaliyetinin dürüstlük kuralına uygun ve şeffaf olması için gerekli olması hâlinde veri sorumlusu aşağıdaki bilgileri de sunmakla yükümlüdür:

- a. Kişisel verilerin saklanma süresi ya da mümkün olmaması hâlinde bu sürenin belirlenmesine ilişkin kriterler,
- b. İlgili kişinin kişisel verilere erişim ve kişisel verilerin düzeltilmesi ya da silinmesini veya ilgili işleme faaliyetinin kısıtlanmasını talep etme ve işleme faaliyetine itiraz etme hakkının yanı sıra verilerin taşınabilirliği hakkının olduğuna ilişkin bilgi,
- c. Kişisel verilerin rıza/açık rıza uygunluk sebebine dayanarak işlenmesi hâlinde ilgili kişinin her zaman vermiş olduğu rıza/açık rızayı geri alabileceğine ilişkin bilgi (bu hâlde rıza/açık rıza hukuka uygunluk sebebine dayanılarak yürütülen önceki veri işleme faaliyetleri etkilenmeyecektir),
- d. Denetleyici otoriteye şikâyet hakkı,
- e. Kişisel verilerin sözleşmenin kurulması ya da sözleşme gereğince işlenmesinin gerekmesi veya yasal bir zorunluluk uyarınca gerekli olması hâlinde bu duruma ilişkin bilgiler ve verilerin sağlanmamasının muhtemel sonuçları,
- f. Profillemeye dahil olmak üzere otomatik bir karar mekanizmasının varlığı hâlinde yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin ilgili kişi açısından önemi ve öngörülen sonuçları.

Şekli unsur bakımından ifade edilmiş olduğu gibi bu bilgilerin ilgili kişi tarafından anlaşılabilir şekilde sunulması büyük önem arz etmektedir. İlgili kişi, bu bilgileri edindikten sonra veri işleme faaliyetinin kendisi nezdindeki sonuçlarını bütünsel olarak öngörebilir ve kişisel verilerinin işlenmesine ilişkin olarak riskler, kurallar, tedbirler ve haklar konusunda farkındalığa sahip olmalıdır (Lynskey, 2015, s. 249; Tüzük giriş bölümü par. 39). Özellikle karmaşık, ilgili kişi için bilinmez ve beklenmedik veri işleme faaliyetleri bakımından veri sorumlusu ayrıca işlemin önemli sonuçları bakımından ilgili kişiyi tereddütte mahal vermeyecek şekilde bilgilendirmelidir (Çalışma Grubu, 260 rev. 01, 2018). Aksi hâlde ilgili kişinin kişisel verileri üzerinde kontrolünün devamından bahsedilemeyecektir (Lynskey, 2015, s. 250). Bu husus özellikle ilgili kişinin profillemeye de dahil olmak üzere otomatik karar mekanizmalarına konu olduğu hâller bakımından önem teşkil etmektedir.

Tüzük'te teknolojinin gelişmesi ile beraber artan ve bireyler üzerinde yoğun olarak etkileri bulunan profillemeye de dahil olmak üzere otomatik karar mekanizmalarına ilişkin olarak müstakil hükümler yer almaktadır. Bu doğrultuda tanımlar maddesinde yer alan profillemeye faaliyetinin ve Tüzük 21, 22 kapsamında profillemeye de dâhil olmak üzere otomatik karar mekanizmalarının veri işleme faaliyetinde yer alması hâlinde veri sorumlusunun ek yükümlülükleri bulunmaktadır. Veri sorumlusu işleme faaliyetinin altında yürütülen mantığa ilişkin anlamlı bilgileri, işleme faaliyetinin ilgili kişi açısından önemi (riski) ve öngörülen sonuçlarını da aydınlatma yükümlülüğü kapsamında ilgili kişiye sunmalıdır (Gutwirt, Leenes ve de Hert, 2015, s. 29, 31). Ayrıca bireylerin otomatik karar mekanizmalarına konu olmama -itiraz- hakkının en geç ilgili kişi ile ilk kez iletişime geçildiği zaman ayrıca belirtilmesi gerektiği düzenlenmiştir (Tüzük 21/4). Doğrudan pazarlamaya ilişkin olarak ise özel bir düzenleme öngörülmüş olup, kişisel verilerin doğrudan pazarlama amaçlı olarak işlenmesi hâlinde ilgili kişinin bunu reddetme imkânının bulunduğunu da veri sorumlusu ayrıca bildirmekle yükümlüdür (Tüzük 21/2).

Aydınlatma yükümlülüğü kapsamında “planlanan” veri işleme faaliyetleri hakkında ilgili kişi bilgilendirilmektedir. Veri işleme süreçlerine ilişkin profillemeye de dâhil olmak üzere otomatik karar mekanizmalarının kullanıldığı bilgisi ile mekanizmaların genel olarak çalışma mantığı, anlamı ve sonuçları hakkında otomatik bir karar elde edilmeden önce ilgili kişi bilgilendirilmektedir (Malgieri ve Comandé, 2017; Wachter, Mittelstadt ve Floridi, 2017). Bu noktada henüz kişiye ilişkin belirli bir karar ya da profil çıkarılmamış durumdadır. Aydınlatma yükümlülüğü kapsamındaki bilgilendirme özellikle belirli bir kararın nasıl verildiğine veya ulaşıldığına dair herhangi bir bilgiyi içermemekte, bunun yerine mekanizmanın nasıl çalıştığını açıklamaktadır. Bu kapsamda örneğin; karar ağacı veya kuralların ya da girdilerin nasıl işleneceği hakkında tahminlerin veri sorumlusu tarafından ilgili kişiye sunulması beklenmektedir (Wachter, Mittelstadt ve Floridi, 2017). Yürütülen veri işleme faaliyetinin ilgili kişiye

yönelik etkilerinin aydınlatma metninden anlaşılabilir olması gerekmektedir (Gutwirt, Leenes ve de Hert, 2015, s. 136).

Metninde yer alan “mekanizmanın altında yatan mantık hakkında anlamlı bilgiler” ifadesi ise sunulacak bilgilerin kapsamı ve dili bakımından önemli rol oynamaktadır. Algoritma ya da mekanizmaya ilişkin hangi bilgilerin “anlamlı” olarak değerlendirileceği tartışmalı bir konu teşkil etmektedir. Çalışma Grubu tarafından yayımlanan otomatik karar mekanizmaları ve profillemeye faaliyetlerine ilişkin rehberde, öğrenilebilir makinaların büyüklüğünün ve karmaşıklığının otomatik karar mekanizmaları ve profillemeye kapsamında çeşitli zorluklar doğurduğu belirtilmiştir. Ancak yine de veri sorumluları algoritmalara ilişkin karmaşık ya da algoritmayı olduğu gibi anlatan açıklamalardan kaçınarak basit bir şekilde ilgili kişiyi bilgilendirmekle yükümlü kılınmıştır (Çalışma Grubu, 2018 rev. 01, 2018; ICO, What do we need to think about if we use Artificial Intelligence (AI)). Bu çerçevede akla gelen büyük veri uygulamaları bakımından ise ilgili kişinin tamamen bilgilendirilmesinin güçlüğüne öğretilmiştir (Çekin, 2016; Sydow, 2018, par. 14). *Wachter* ise otomatik karar mekanizmaları bakımından Tüzük uyarınca öngörülen aydınlatma yükümlülüğü kapsamını yeterli olmadığı gerekçesiyle eleştirmektedir (Kaminski ve Maligneri, 2019; Wachter, Mittelstadt ve Floridi, 2017).

Öncelikle söz konusu bilgi teknik bir uzmanlığı bulunmasa bile ilgili kişi tarafından anlamlı bulunmalıdır (Gutwirt, Leenes ve de Hert, 2015, s. 84-85). Ancak veri sorumlusu tarafından yapılacak açıklamanın anlamlı olabilmesi adına unsurların somutlaştırılması gerekmektedir. Bu doğrultuda veri sorumlusu tarafından yapılacak açıklamanın ilgili kişinin özgür iradesini korumaya ve verileri üzerindeki kontrolünü tesise yönelik olması gerektiği kabul edilebilecektir (Selbst ve Powles, 2017, s. 236). Ancak bu beklentinin sınırlarının belirlenmesi aşamasında sorunlar meydana gelmektedir. İlgili kişinin özgür iradesini kurma ve kontrolünün tesisi subjektif kavramlar olarak her bir ilgili kişi nezdinde farklılık arz edebilmektedir. Bu da farklı uzmanlık seviyelerindeki ilgili kişiler bakımından birbirinden farklı açıklamaları gündeme getirebilmekte ve farklılaşan açıklamalar veri sorumlusunun somut menfaat savunması ile çatışabilecektir. Ancak yine de asgari düzeyde ilgili kişinin veri koruma mevzuatı ve insan hakları hukuku çerçevesinde tanınmış olan haklarını kullanmaya elverişli ve etkin bir bilgilendirmenin sağlanması için veri sorumlusunun hesap verilebilirlik ilkesi gereğince sarf ettiği çabayı ortaya koyması gerekmektedir (Çekin, 2016). Bu da doğal olmaktadır ki her bir veri sorumlusu ve hatta veri işleme faaliyeti bakımından farklı bir test gerektirecektir.

Türk hukuku açısından gerek KVKK gerekse Aydınlatma Yükümlülüğü Tebliği’de aydınlatma yükümlülüğünün maddi unsuruna ilişkin detaylı düzenlemeler yer almamaktadır. Veri sorumlusu veya yetkilendirdiği kişi, aydınlatma yükümlülüğü kapsamında; veri sorumlusunun ve varsa temsilcisinin kimliği, veri işleme amacı, verilerin kimlere ve hangi amaçla aktarılabileceği, veri toplamanın yöntemi ve hukuki sebebi ile KVKK 11’de sayılan diğer hakları konusunda ilgili kişiyi bilgilendirme yükümlülüğü altındadır. Veri sorumlusu özellikle açık rıza hukuka uygunluk sebebine dayanması hâlinde geçerli bir açık rızanın söz konusu olması için işlemeye ilişkin her türlü bilgiliyi ilgili kişiye sunmalıdır. Bu kapsamda gerekli bilgilerin KVKK 10 ve 11 kapsamında daha geniş olabileceği öğretilmiştir (Yücedağ, 2017).

Aydınlatma yükümlülüğüne ilişkin hükümler bir çerçeve çizerek asgari içeriği belirlemiştir. Özellikle Tüzük ile profillemeye ve otomatik karar mekanizmaları göz önünde bulundurularak bilgilendirme kapsamına dâhil edilmiş detaylı hususların KVKK kapsamında olmaması bir eksiklik olarak değerlendirilebilecektir. Ancak KVKK 10/1-ç uyarınca toplama yöntemi ve hukuki sebebine ilişkin bilgileri sunan veri sorumlusunun KVKK kapsamında özel olarak belirtilmemiş olsa dahi profillemeye de dahil olmak üzere otomatik karar mekanizmalarının varlığı hakkında ilgili kişiyi bilgilendirmesi dürüstlük kuralı ilkesiyle de bağdaşacaktır. Bu durum ise aydınlatma yükümlülüğünün somut içeriğinin farklı veri işleme faaliyetleri yürüten veri sorumluları bakımından objektif olarak kesin bir şekilde belirlenememesinden kaynaklanmaktadır.

Kişisel Verilerin Doğrudan İlgili Kişiden Toplanmaması

Kişisel verilerin doğrudan ilgili kişiden toplanmadığı hâller bakımından sağlanacak bilgiler büyük ölçüde kişisel verilerin doğrudan ilgili kişilerden elde edildiği hâllerle örtüşmektedir. Tüzük 14/1 kapsamında veri sorumlusunun ayrıca elde ettiği ilgili veri kategorilerini de ilgili kişiye açıklama yükümlülüğü bulunmaktadır. Buna karşın Tüzük 13/1 de sayılan ve zorunlu içeriğe dâhil olan, kişisel verilerin meşru menfaat hukuka uygunluk sebebine dayanarak işlenmesi hâlinde veri sorumlusu ya da üçüncü tarafça ileri sürülen meşru menfaatin açıklanması Tüzük 14/2’de veri işleme faaliyetinin dürüstlük kuralına uygun ve şeffaf olması için gerekli olması hâlinde sağlanması gereken ek bilgiler arasında sayılmıştır. Yine bu kapsamda kişisel verilerin sözleşmenin kurulması ya da sözleşme gereğince işlenmesinin gerekmesi veya yasal bir zorunluluk uyarınca gerekli olması hâlinde bu duruma ilişkin bilgiler ve verilerin sağlanmamasının muhtemel sonuçlarını açıklama Tüzük 14’de yer almamaktadır.

Verilerin doğrudan ilgili kişiden elde edilmediği hâllerde bu verilerin kamuya açık kaynaklardan elde edilmiş olması özellikle profillemeye de dahil olmak üzere otomatik karar mekanizması ve büyük veri uygulamaları bakımından sık rastlanabilecek bir durumdur. Tüzük 14/2’de bu durum gözetilerek, veri sorumlusunun ilgili kişinin verilerini elde ettiği kaynağı açıklama yükümlülüğü ek bilgiler arasında sayılmıştır. Ancak bu kaynakların çok çeşitli olması ve doğrudan belirtilememesi hâlinde genel bilgilerin sağlanması gerektiği Tüzük gerekçelerinde ifade edilmiştir (Tüzük Giriş Bölümü, par. 61). Özellikle büyük veri uygulamaları bakımından bu yaklaşım önem teşkil etmektedir. Gerek öğretilerde gerekse endüstride üzerinde uzlaşmış, net bir büyük veri tanımı bulunmamakla birlikte çeşitli kaynaklarda büyük veri; genel olarak bilgi, teknoloji, yöntem ve etki kavramları ile ilişkilendirilmektedir (Mauro, Greco ve Grimald, 2014). Ayrıca büyük veriyi tanımlayabilmek için kullanılan hız, verinin gerçek zamanlı olması; çeşitlilik, verinin farklı kaynaklardan elde edilebilir olması; hacim, verinin büyük veri kümelerinden oluşması ve değer ise kullanımının bir fayda yaratması şeklinde açıklanmaktadır (Aşikoğlu, 2018, s. 21). Gerçekten de özellikle profillemeye amaçlı kullanılan büyük veri uygulamaları kesin ve gerçeğe yakın sonuçlar elde edebilmek için pek çok kaynaktan veri toplamaktadır. Bunlar kamuya açık –alenileştirilmiş- veriler olabileceği gibi üçüncü taraf uygulamalardan, nesnelerin interneti, RFID ve sensörler gibi çeşitli teknolojiler aracılığıyla da toplanabilmektedir. Büyük veri uygulamaları bakımından genellikle kullanılan verilerin üçüncü taraf uygulamalardan sağlanıyor olması veya veri sorumlularının büyük veri uygulamalarında çalıştırdıkları algoritmaların çalışma prensiplerini tam olarak açıklayamamaları, uygulamaların şeffaflık ve hesap verilebilirlik ilkesi ile ters düşmesine sebep olmaktadır (Lynskey, 2015, s. 247-248). Nitekim özellikle üçüncü taraf ve kamuya açık kaynaklardan toplanacak veriler bakımından ilgili kişiler nezdinde farklılık doğabilecektir. Örnek olarak uygulama kapsamında sosyal medya verilerinin kullanılmasına aydınlatma metninde hukuka uygunluk sebeplerine uygun olarak yer verilebilir, ancak kişinin sosyal medya hesaplarının olmaması, tespit edilememesi hâlinde bu kişi özelinde bu kaynaklardan veri sağlanamayacaktır. Gerekçede yer alan ifadenin bu şekilde anlaşılması gerektiği belirtilmektedir (Çalışma Grubu, 260 rev. 01, 2018). Yoksa veri sorumlusuna veri işleme sürecini, toplama kanalları ve işleme amaçlarını belirlemeden genel ifadelerle aydınlatma metni hazırlama imkânı vermemektedir. Nitekim hesap verilebilirlik ve şeffaflık ilkesi uyarınca veri sorumlusunun tasarımdan itibaren veri koruma ve tasarımla veri koruma yükümlülüğü bulunmaktadır. Bu doğrultuda veri sorumlusu veri işleme süreçlerinin hepsi için veri toplama kaynaklarını belirli ve izlenebilir kılmalıdır. Belirtmek gerekir ki bu genel ifadeler ilgili kişinin haklarını kullanarak veri sorumlusuna başvurması hâlinde kullanılamayacaktır. Aydınlatma yükümlülüğünün bütün ilgili kişilere yönelik olması sebebi ile söz konusu olabilecek olan bu durum ilgili kişinin tamamen kendi nezdinde işlenen verilerin nereden, kimler aracılığıyla, ne amaçla toplandığını sorması hâlinde somut olarak belirli olacağından veri sorumlusunun kişisel verileri edindiği üçüncü kişileri açıklaması gerekecektir.

Burada belirtmek gerekir ki KVKK açısından ilgili kişi tarafından alenileştirilmiş verilerin aydınlatma yükümlülüğünden istisna tutulması sebebi ile ilgili kişinin kamuya açıklamış olduğu verileri bu

açıklama amacına uygun şekilde elde eden veri sorumlusunun kişiyi ayrıca aydınlatma yükümlülüğü bulunmamaktadır (KVKK 28/2-a).

Yapay zekâ ve öğrenilebilir algoritmalar kullanılan veri işleme faaliyetleri bakımından veri işleme süreçlerinin başında öngörülemediği olan ve ilgili kişiye ilişkin kişisel veriler (örn. profiller) ortaya çıkabilmektedir. Bu mekanizmaların kendi içinde farklı kaynaklardan beslenirken yarattığı korelasyonların sonucunda elde edilen bu veri, veri sorumlusu tarafından kullanılacak ise yine Tüzük 14 hükmü gündeme gelecektir (ICO, What do we need to think about if we use Artificial Intelligence (AI)).

Veri sorumlusunun Tüzük 14 kapsamındaki aydınlatma yükümlülüğünü kişisel verilerin elde edilmesinden itibaren makul süre içerisinde ancak her hâlikârda en geç bir ay içerisinde; söz konusu verilerin iletişim amaçlı olarak kullanılması hâlinde en geç ilgili kişi ile iletişime geçilen anda; söz konusu verilerin diğer alıcılara açıklanması hâlinde en geç ilk açıklama anında yerine getirilmesi gerekmektedir. Türk hukuku açısından bilgilendirmenin ilgili kişiye iletilmesine ilişkin süreler yukarıda açıklanmıştır.

Burada önemle belirtmek gerekir ki kişisel verileri bir başka veri sorumlusundan elde eden veri sorumlusunun aydınlatma yükümlülüğü ilk veri sorumlusunun yükümlülüğünden bağımsızdır. Her hâlikârda ikinci veri sorumlusu söz konusu verileri elde etmesi için ilgili kişinin bilgilendirilmesine dayalı bir hukuka uygunluk sebebine ihtiyaç duymak ve bunun varlığını sorgulamakla yükümlü olacaktır. Tüzük 14 kapsamında düzenlenen ise kendi yürüteceği veri işleme faaliyetleri bakımından ayrıca ilgili kişiyi bilgilendirmesi gereğidir. Bu yönde bir yorum Türk hukuku açısından da geçerli olacaktır. Örneğin bir kariyer sitesi üzerinden ilgili kişilerin özgeçmişlerini ve diğer bilgilerini elde eden veri sorumlusunun internet sitesinden ayrı olarak da aydınlatma yükümlülüğü bulunmaktadır. Nitekim Aydınlatma Yükümlülüğü Tebliğ kapsamında kişisel verilerin ilgili kişiden elde edilmemesi hâlinde aydınlatma yükümlülüğünün yerine getirilmesi için öngörülen süreler belirtilmiştir. Tebliğ’de kişisel verileri doğrudan ilgili kişinin kendisinden elde etmemiş olan veri sorumlusunun aydınlatma yükümlülüğünün maddi içerik olarak değiştirilmediği görülmektedir. KVKK m. 10 ve Aydınlatma Yükümlülüğü Tebliğ m. 4’de yer alan hususları içeren ve madde 5’te belirtilen usul ve esaslara uygun bir aydınlatmayı veri sorumlusunun ilgili kişiye madde 6’da öngörülen sürelerle riayet ederek ulaştırması gerekecektir. Ancak burada veri sorumlusunun aydınlatma metninde yer vereceği “kişisel veri toplama yöntemi ve hukuki sebebi” kapsamında yapacağı açıklamalarda söz konusu verileri elde etmesine ilişkin ilişkileri ve hukuki sebepleri açıklarken verileri elde ettiği başka bir veri sorumlusu var ise buna ilişkin açıklamaları yapması gerekebilecektir.

Aydınlatma Metninin Güncellenmesi

Şeffaflık ilkesinin, sadece veri toplama anında değil bir bütün olarak bütün veri işleme süreçleri bakımından da geçerli olması gerekmektedir. Aydınlatma metninin güncellenmesi ve bu güncellenmenin ilgili kişiye bildirilmesi maddi ve şekli unsur kapsamında değerlendirilmelidir.

Veri sorumlusunun aydınlatma metninin içeriğinde yapacağı herhangi bir değişikliğin hâli hazırda aydınlatma metni sağlanmış ilgili kişilere de bildirilmesi önem arz etmektedir. Özellikle yapılan değişikliklerin veri işleme faaliyeti bakımından ve ilgili kişi nezdindeki etkilerinin iletilmesi gerekmektedir. Özellikle veri işleme amacının, veri sorumlusu kimliğinin, ilgili kişinin haklarını kullanma yollarının değişmesi hâlinde bu değişiklikler aydınlatmanın yapıldığı yol ile uyumlu şekilde ya da teknolojik imkânlar doğrultusunda (e-posta, uygulama içi bildirim, internet sitesi bildirim gibi) ilgili kişinin bu değişikliklerin kendisi nezdinde sonuçlarına anlam vermesine imkân verir şekilde bildirilmelidir.

Tüzük'te veri sorumlusunun kişisel verilerin toplandığı anda belirtmiş olduğu amaçtan başka bir amaçla kişisel verileri işleme yönünde bir niyetinin olması hâlinde sonraki amaç uyarınca kişisel verileri işlemeyen önce bu hususa ilişkin bilgileri ilgili kişiye sağlaması gerektiği özel olarak düzenlenmiştir. Bu düzenleme esas olarak amaçla bağlılık ilkesine ilişkindir (sonraki amaca ilişkin olarak açıklamalar için bkz. Çekin, 2019, s. 66; Yücedağ, 2019). Tüzük 5/1-b uyarınca kişisel veriler “*belirli, açık ve meşru amaçlara yönelik olarak toplanır ve bu amaçlara uygun olmayan bir şekilde işlenemez*”. Burada sonraki amacın, kişisel verilerin toplandığı anda ilgili kişiye belirtilmiş olan amaç ile uyumlu olması yani ilgili kişi tarafından öngörülebilir, beklenebilir bir amaç olması hâlinde bu bağlantılı amacın da ilgili kişiye bildirilmesi gerektiği hatta veri sorumlusunun sonraki amacın ilk amaçla uyumluluğuna ilişkin açıklamaları da ilgili kişiye sunması gerektiği Çalışma Grubu tarafından belirtilmektedir (Çalışma Grubu, 260 rev. 01, 2018). Tüzük aksine KVKK'da sonraki amaca ilişkin olarak bir düzenleme yer almamakla birlikte buna uyumlu şekilde sonraki amaca ilişkin önceki amaç doğrultusunda herhangi bir uyumluluk testi öngörülmesizin yeni amaçlarla kişisel verinin işlenecek olması hâlinde veri sorumlusunun ilgili kişiyi tekrardan bilgilendirmekle yükümlü olduğu hüküm altına alınmıştır.

Ancak Tüzük kapsamında bu değişikliklerin bildirilmesinde herhangi bir süre öngörülmemiştir. Yalnızca yeni ortaya çıkan amaç bakımından amaç uyarınca işleme faaliyetine başlamadan önce bilgilerin iletilmesi gerektiği hüküm altına alınmış ancak veri sorumlusunun değişmesi, güvenlik tedbirlerinin değişmesi gibi aydınlatma metninin diğer hususlarındaki güncellemelerin bildirim için özel bir düzenleme getirilmemiştir. Bu doğrultuda yapılan değişikliğin niteliğine göre ilgili kişinin herhangi bir hak kaybına uğramamasını sağlayacak, ilgili kişinin yapılan değişikliğe ilişkin olarak kendisi üzerindeki etkilerini değerlendirmesine ve değişikliğe ilişkin olarak Tüzük uyarınca sahip olduğu hakları kullanmasına elverişli bir süre tanınmalıdır (Çalışma Grubu, 260 rev. 01, 2018). Bu noktada veri sorumlusunun şeffaflık ve hesap verilebilirlik ilkesi uyarınca özellikle önemli değişiklikler bakımından sadece değişikliği bildirmesi değil ek olarak bu değişikliğin ilgili kişi nezdinde bir etkisi olacak ise bunu da açıklaması gerekecektir.

Aydınlatma Yükümlülüğünün Şekli ve Maddi Unsuruna İlişkin Sorunlar

Tüzük'ün yürürlüğe girmesiyle beraber pek çok şirket aydınlatma metinlerini (privacy policy) güncelleyerek kullanıcılarına tekrar iletmiştir. Avukatlar tarafından hazırlanan ve çoğu zaman ağdalı ifadeler içeren bu metinler ilgili kişiler için anlaşılabilir ve uzun olabilmektedir (Yücedağ, 2019). Aydınlatma yükümlülüğü ilgili kişinin kişisel verilerinin akıbeti hakkında karar vermesi, bilgilenebilmesi, haklarının farkında olması bakımından büyük önem taşımaktadır. Bu bakımdan aydınlatma yükümlülüğü bir formalitenin yerine getirilmesi değil, ilgili kişi nezdinde faydanın gerçekleşmesine hizmet etmelidir.

Avrupa Tüketici Organizasyonu (BEUC) destekli proje kapsamında büyük şirketlerin aydınlatma metinleri yapay zekâ tarafından değerlendirilmiştir (Contissa ve diğerleri 2018). Proje kapsamında Google, Facebook, Instagram, Amazon, Apple, Microsoft, WhatsApp, Twitter gibi dünyada çok fazla kullanıcısı olan 14 uygulama seçilerek çalışma bu uygulamaların aydınlatma metinleri üzerinden yürütülmüştür. Tam bilgi, yetersiz bilgi, açık olmayan dil ve sorunlu veri işleme faaliyeti olarak 4 kategori altında cümle cümle değerlendirilen aydınlatma metinlerinde pek çok eksik olduğu ve Tüzük beklentilerinin karşılanmadığı ortaya konmuştur. Yine Digital World Market Watch tarafından yayınlanan çalışmada 8 sosyal medya uygulaması üzerinden yapılan incelemede aydınlatma metinlerinden kullanıcıların hangi verilerinin, hangi amaçla ve hangi hukuka uygunluk sebebine dayanılarak toplandığını anlamalarının güç olduğu ifade edilmiştir (Digital World Market Watch, 2018, s. 2).

Bir yıldır yürürlükte olan Tüzük'ün uygulamasına ilişkin olarak çok paydaşlı uzmanlar grubu tarafından Komisyon'a sunulan 13 Haziran 2019 tarihli raporda, pek çok organizasyonun aydınlatma metinlerinin

güncellenmesi için büyük ölçüde yatırım yaptığı ve iş gücü ayırdığı ifade edilmiştir (Multistakeholder Expert Group, 2019). Raporda aydınlatma yükümlülüğünün kapsamının belirlenmesinde teknik ve karışık süreçlerin açık ve sade bir dille açıklanmasına ilişkin güçlükler değinilmiştir. Özellikle Çalışma Grubu tarafından hazırlanan ve çalışmada açıklanan rehberde yer alan örneklerin uygulama bakımından kimi belirsizliklere ve sorunlara neden olduğu ifade edilmiştir. Örneğin kişisel verilerin aktarılacağı kişilerin ve ülkelerin adının paylaşılması ve güncel tutulmasının zor olduğu ve kullanıcı için de anlamlı olup olmadığının tartışmaya açık olduğu ifade edilmiştir. Özellikle sözleşme öncesi veri işleme faaliyetleri bakımından yüz yüze iletişimde bilgilerin sağlanmasındaki güçlüğü değinilmiştir.

Fransız Veri Koruma Otoritesinin Google Kararı

Tüzük uyarınca uygulanan idari para cezaları arasında Fransız Veri Koruma Otoritesi CNIL’ın Google aleyhine vermiş olduğu 50.000.000 Euro idari para cezası ise hem kişisel verilerin korunması alanında uygulanan en yüksek para cezası olması hem de aydınlatma yükümlülüğüne ilişkin olarak değerlendirmeler içermesi sebebi ile önem arz etmektedir (CNIL Restricted Committee, 2019).

Tüzük’ün yürürlüğe girdiği günlerde yapılan başvuru uyarınca CNIL hiç vakit kaybetmeden 1 Haziran 2018’de soruşturma başlatmış ve iki ihlal tespit etmiştir: şeffaflık ilkesi ve aydınlatma yükümlülüğünün ihlali, kişiselleştirilmiş reklamlara yönelik veri işlemenin hukuka uygunluk sebebinin açık olmaması (CNIL Restricted Committee, 2019, par. 6-8). Aydınlatma yükümlülüğü ve şeffaflık ilkesi uyarınca yapılan incelemede ilk olarak Google tarafından ilgili kişilere sunulan aydınlatma metninin kolay ulaşılabilir olmadığı tespiti yapılmıştır (CNIL Restricted Committee, 2019, par. 88, 96). Aydınlatma metni için önemlilik arz eden veri işleme amacı, veri saklama periyodu, kişiselleştirilmiş reklamlar için işlenen veri kategorilerine ilişkin bilgilerin, erişmek için tıklama gerektiren buton ve linkler aracılığıyla birkaç dokümanda dağınık olarak yer aldığı ve gerekli bilgilere ulaşmak için 5-6 adımın gerekli olduğu belirtilmiştir (CNIL Restricted Committee, 2019, par. 97 vd.). Google tarafından sunulan hizmet sayısının çok ve çeşitli olmasına rağmen yürütülen işleme faaliyetinin kullanıcılar için anlaşılır olmadığı, bilgilendirmenin açık ve kapsayıcı olmadığı, belirtilen veri işleme amaçlarının (“kişiselleştirilmiş reklam ve içerik hizmet sunma”, “ürün ve servislerin güvenliğinden emin olma”, “hizmetlerin sağlanması ve geliştirilmesi” vb.) oldukça basma kalıp ve geniş şekilde ifade edildiği ve kullanıcıların hukuki dayanağın veri sorumlusunun meşru menfaati değil de açık rızalarını olduğunu anlayamadıkları tespiti yapılmıştır. Belirtmek gerekir ki CNIL, Google’ın ürün ve hizmetleri içerisinde sunmuş olduğu “gizlilik kontrol” ve “yönetim paneli” özelliklerini ve açılan pencere uyarılarını soruşturma kapsamında gözetmiş ancak bu özelliklerin Tüzük 13 kapsamındaki gerekli bilgilerin ilgili kişiye sunulduğunu ispat için uygun bulmamıştır.

CNIL, kişiselleştirilmiş reklamlar doğrultusunda veri işleme amacının hukuki dayanağı olan rızanın geçerli olmadığı tespitini yaparken de şeffaflık ilkesi ve aydınlatma metni üzerinden incelemesini sürdürmüştür. Rızanın geçerliliği incelemesinde bilgilendirmeye dayalı, açık, spesifik olma ve tereddütte yer bırakmama şartlarının sağlanmadığı belirtilirken, yapılan bilgilendirmenin özellikle ilgili kişilerin kişiselleştirilmiş reklamlara ilişkin ayarlarını yapmak üzere açtıkları sayfa üzerinden kişisel verilerinin işlendiği Google hizmetlerinin, internet sitelerinin ve uygulamaların çeşitliliği ve sayısı konusunda açık olmadığı ifade edilmiştir (CNIL Restricted Committee, 2019, par. 141 vd).

Bu tespitler ışığında CNIL, Google’ın hizmet çeşitliliği, yürüttüğü veri işleme faaliyetinin bireyler üzerinde etkisi, kullanıcı sayısının fazla olması, söz konusu ihlalin bir kerelik olmayıp, sürekli olması sebebi ile 50.000.000 Euro idari para cezasına hükmetmiştir. CNIL özellikle ekonomik modeli veri işleme ve kişisel reklamcılık üzerine kurulu olan Google’ın bu yükümlülükleri yerine getirmek konusunda en üst seviyede sorumlu olduğunu belirtmiştir.

Değerlendirme

Karar kapsamında yapılan değerlendirme ve uygulanan idari para cezasının miktarı bakımından CNIL'in özellikle iş ve ekonomik modeli veri işlemeyle dayalı veri sorumluları bakımından şeffaflık beklentisinin yüksek olduğu ifade edilebilecektir. Karar özellikle yapılan aydınlatmanın içeriği ile birlikte bilgilendirmenin ilgili kişilere sunuluş biçimi ve ilgili kullanıcılar tarafından erişilmesi bakımından özel olarak yapılan test uygulamalarıyla buna ilişkin değerlendirmeler bakımından da önem arz etmektedir. Aydınlatma metinlerinden beklenen açık ve öz olma ile yürütülen veri işleme faaliyetlerini hukuka uygunluk sebepleri ile ilgili kişiye detaylı olarak açıklama ikilemi kararda görülmektedir. Aydınlatma metninin katmanlı ve basit tutulması adına yapılan sayfa yönlendirmeleri CNIL tarafından bilgilendirmeye erişimi zorlaştırma olarak yorumlanmıştır.

Profilleme de dahil olmak üzere otomatik karar mekanizmalarının yer aldığı, bunların öğrenilebilir algoritmalarla desteklendiği veri işleme faaliyetleri bakımından yürütülen veri faaliyetini açıklamakta veri sorumluları zorlanmaktadır. Korunması gereken menfaatin özüne inerek değerlendirme yapıldığında öğretide hesap verilebilirlik ilkesinin öne çıkardığı *self-regulation* odaklı bir model önerilmektedir. *Malgieri* ve *Comandé* tarafından "Legibility test" olarak getirilen bu öneri ile aydınlatma yükümlülüğünün özellikle karmaşık algoritmalar kapsamında hukuka uygun şekilde yerine getirilebilmesi adına çözüm olarak sunulmaktadır. Okunabilirlik testi olarak Türkçeleştirilebilecek olan bu kavram ile temelde algoritmaların önyargılarından ve bireylerin ayrımcılığa uğramamaları riskine odaklanarak mekanizmaların ön değerlendirmeye tabi tutulması öngörülmektedir. Önerilen test algoritmanın kendisi ve çalışmaları, geçmişi, öğrenme yöntemleri, veri setleri ve çıktıları ile ilgili çok çeşitli sorular içermektedir. Ancak bu yöntem şeffaflık ilkesini barındırmamakta, ilgili kişilere sadece üçüncü taraflar tarafından onaylanmış bir taahhüt sunmaktadır. Bu bakımdan bilgi alma hakkının barındırdığı şeffaflık ilkesini yerine getirmediği için eleştirilmektedir (Gunst, 2017, s. 78-79).

Google gibi büyük ölçek ve geniş ilgili kişi grubu nezdinde etkileri olan veri işleme faaliyeti yürüten veri sorumluları bakımından işleme süreçlerinin şeffaf bir şekilde ilgili kişiye bildirilmesi gerektiği açıktır. Yine bu metinlerin kullanıcılar bakımından okunabilirliğine ilişkin denetim bir başka deyişle aydınlatma metninin şekli unsuru veri işleme faaliyetinin de genel ilkelere uyumluluğu bakımından büyük önem teşkil etmektedir. Ancak özellikle profilleme ve otomatik karar mekanizmaları, öğrenilebilir algoritmalar ve büyük veri uygulamaları bakımından aydınlatma yükümlülüğünün maddi unsurlarına ilişkin sınıra yönelik kriter ve unsurlar belirlenmemektedir. Bu ise veri işleme faaliyeti ve iş modellerinin çeşitliliği ve öngörülebilir olmamasından kaynaklanmaktadır.

AYDINLATMA YÜKÜMLÜLÜĞÜNÜN İSTİSNALARI

Hem Tüzük hem de KVKK kapsamında genel olarak istisna tutulmuş hâller ve özel olarak aydınlatma yükümlülüğünden istisna tutulan hâllere yer verilmiştir. KVKK'da istisnalar başlıklı 28. madde kapsamında kanunun uygulanmayacağı hâller ve özel olarak aydınlatma yükümlülüğünü düzenleyen KVKK 10, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen KVKK 11 ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen KVKK 16'nın uygulanmayacağı hâller belirtilmiştir. Bu doğrultuda aşağıda sayılan hâllerde kanun hükümleri uygulama alanı bulmayacağından aydınlatma yükümlülüğü söz konusu olmayacaktır:

- Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi,
- Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi,
- Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi,
- Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbarî faaliyetler kapsamında işlenmesi,
- Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

Yukarıda sayılanların yanı sıra KVKK amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünün bulunmadığı hâller ise şunlardır (detaylı bilgi ve değerlendirmeler için bkz. Küzeci, 2019, s. 328):

- Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması,
- İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi,
- Kişisel veri işleminin kanunun verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması,
- Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

Tüzük kapsamında ise genel istisna hâllere (Tüzük 2/2, 85-91) ek olarak ilgili kişinin hâlihazırda söz konusu bilgilere sahip olduğu durumlarda aydınlatma yükümlülüğünün ayrıca yerine getirilmesine gerek bulunmamaktadır. Bununla birlikte kişisel verilerin ilgili kişinin doğrudan kendisinden toplanmadığı durumlar için doğrudan ilgili kişinin kendisinden toplanan durumlardan daha farklı istisnalar öngörülmüştür. Tüzük 14/5-a uyarınca:

- Özellikle kamu yararı doğrultusunda arşiv amaçlı, bilimsel, tarihsel araştırma amaçlı ya da istatistiksel amaçlı veri işleme faaliyetleri bakımından aydınlatma yapmanın imkânsız olması veya ölçüsüz bir çaba gerektirmesi hâli veya aydınlatma yükümlülüğünün yerine getirilmesi ile işleme faaliyetinin hedefinin gerçekleşmesinin imkânsız olması ya da ciddi şekilde zarar görmesi hâli,
- Veri sorumlusunun ulusal hukuk ya da AB hukuku uyarınca açıkça kişisel verileri elde etme ya da açıklama yükümlülüğünün olması,
- Kişisel verilerin yasal bir gizlilik yükümlülüğü de dâhil olmak üzere AB ya da üye devlet hukuku ile düzenlenen bir mesleki sır saklama yükümlülüğüne tabi olarak gizli kalmasının gerekmesi hâllerinde kişisel verileri doğrudan ilgili kişiden toplamayan veri sorumlusu aydınlatma yükümlülüğünden muaf tutulmuştur.

İlgili Kişinin Hâlihazırda Söz Konusu Bilgilere Sahip Olması

Kişisel verilerin doğrudan ilgili kişinin kendisinden toplandığı ya da toplanmadığı durumlar için aydınlatma yükümlülüğüne ilişkin olarak tek bir ortak istisnaya yer verilmiştir. Bu da ilgili kişinin hâlihazırda söz konusu bilgilere sahip olmasıdır (Tüzük 13/4, 14/5-a). Veri sorumlusunun bu istisnadan

yararlanması hâlinde hesap verilebilirlik ilkesi uyarınca ilgili kişinin söz konusu bilgilerden haberdar olduğunu ispatlaması, belgelendirmesi gerekmektedir. Bu noktada veri sorumlusunun ilgili kişinin tam olarak hangi bilgileri, ne zaman ve nasıl edindiği konusunda gerekli olması hâlinde açıklama yapabiliyor olması, ilgili kişinin sahip olduğu bilgiler nezdinde herhangi bir değişikliğin olmadığını ortaya koyuyor olması gerekmektedir. Yine ilgili kişinin bu bilgilerin bir kısmından haberdar olması hâlinde veri sorumlusu eksik bilgileri tamamlamalıdır (Çalışma Grubu, 260 rev. 01, 2018). ICO tarafından ise aydınlatma yükümlülüğüne ilişkin hazırlanan rehber kapsamında ilgili kişinin söz konusu bilgilere sahip olduğu “bariz” (obvious) ise veri sorumlusunun ayrıca aydınlatma yükümlülüğünün bulunmadığı ifade edilmiştir (ICO, “What are the exceptions in the GDPR?”). Ancak veri sorumlusunun ilgili kişinin hangi bilgilere sahip olduğunu bilmemesi ya da emin olmaması hâlinde ilgili kişilere gerekli bilgilerin hepsinin sağlanması gerektiği belirtilmiştir. Bu hâlde ise ilgili kişinin tekrar tekrar aynı/benzer bilgilere maruz kalması ile kişinin bu bilgilere karşı duyarsızlaşması söz konusu olabilecektir (Ehmann/Selmayr, 2018, par. 68; Yücedağ, 2017). Bununla birlikte ilgili kişinin kişisel verilerinin elde edildiği koşullar altında, ilgili kişinin verilerinin hakkaniyet çerçevesinde işlenmesi için aydınlatma yapılmasının gerekli olmaması hâlinde veri sorumlusunun aydınlatma yükümlülüğünden muaf olacağı uygulamada özellikle yüz yüze iletişim bakımından ve aydınlatma metnini o an için sağlamanın güçlüğü sebebi ile ileri sürülmektedir (Çekin, 2019, s. 142). Gerçekten de kişisel verilerin korunmasına ilişkin düzenlemelerde yer alan veri sorumlusu, veri işleme ve kişisel veri kavramlarının son derece geniş ve düzenlemelerin uygulama alanının gündelik hayattaki hemen her türlü veri işleme faaliyetini kapsıyor olması sebebi ile aydınlatma yükümlülüğünün yerine getirilmesine ilişkin zorunluluk pek çok yerde karşılanamamaktadır.

Kişisel verilerin doğrudan ilgili kişiden toplandığı hâller bakımından hem Tüzük hem KVKK uyarınca özel sektör bakımından hayatın olağan akışına uygun ve ilgili kişinin temel hak ve özgürlüklerine zarar getirmeyen veri işleme faaliyetleri için açık bir muafiyet öngörülmemiştir. Öngörülen istisnaların kişisel amaç ve hane halkına ilişkin olma (Tüzük 2/2-c, KVKK 28/1-a) gibi çok sınırlı olması sebebi ile iş modeli kişisel veri işlemeye dayanmayan, kişisel veriler üzerinden herhangi bir menfaat elde etmeyen, hatta sadece hukuki yükümlülüğü ile sınırlı olan veri sorumluları bakımından da aydınlatma yükümlülüğü doğmaktadır. Özellikle ticari hayatta işletmeler arası ilişkiler kapsamında çalışan ve yönetici verilerinin paylaşılması, tanışma toplantılarındaki kartvizit alışverişleri ve dijital ortamlar harici küçük işletmelerin günlük olağan müşteri ilişkileri bakımından doğan aydınlatma yükümlülüğünün yerine getirilmesinde birtakım zorluklar gündeme gelmektedir. Ancak burada düzenlemede açıkça bir muafiyet getirilmediğinden aydınlatmanın her hâlükârda veri sorumlusu tarafından erişilebilir olarak bulundurulması, o an için sağlanamaması hâlinde makul süre içerisinde iletilmesinin de uygun olacağı *de lege feranda* olmasa da *de lege lata* olarak söylenebilecektir (bu konuda ayrıca bkz. BDSG § 32/3). Nitekim bu eleştiri ve yorumlar üye devlet temsilcileri tarafından da Tüzük’e ilişkin değerlendirme ve görüşler kapsamında Delegasyon’a iletilmiştir (Council of the European Union, 12756/1/19 rev. 1).

Aydınlatma yükümlülüğüne ilişkin olarak ayrıca söz konusu bilgilerin ilgili kişiye subjektif olarak sağlanmış olmasının aranmayacağı, objektif olarak makul koşullarda söz konusu bilgilerin veri sorumlusu tarafından erişilebilir kılınmış olmasının yükümlülüğün yerine getirilmesi bakımından yeterli sayılacağına ilişkin görüşler ileri sürülmektedir (Kühling ve Buchner, 2018, par 86). Özellikle taraflar arasında uzun süreli iş ilişkisi olduğu durumlarda kişisel verilerin toplanmış olduğu ilk anda sağlanmış olan aydınlatma metninin ilişki süresince tekrar tekrar iletilmesi gerekmemekle birlikte ancak somut olayın gerektirdiği ölçüde güncellenmesi gerekecektir (Kühling ve Buchner, 2018, par 87). Buna karşılık Çalışma Grubu görüşüne göre ise ilgili kişinin uzun süre aldığı bir hizmet bakımından veri sorumlusu tarafından aydınlatma metni üzerine herhangi bir değişiklik yapılmaması hâlinde dahi veri sorumlusu erişilebilir kıldığı aydınlatma metnini hatırlatmalıdır (Çalışma Grubu, 260 rev. 01, 2018).

Türk hukuku açısından ise bu istisnaya yer verilmemiş olması öğretilerde eleştirilmektedir (Çekin, 2019, s. 142). Ancak kanaatimizce ilgili kişiye veri sorumlusu tarafından kişisel verilerin elde edilme anında aydınlatma yükümlülüğü yerine getirilerek birtakım bilgiler özellikle veri sorumlusunun kimliği, ilgili

kişinin hakları ve veri sorumlusuna başvuru yöntemi gibi hususlar bildirilmiş ise sonraki süreçte bu bilgilerin her seferinde aranmasında ilgili kişinin menfaati bulunmayacaktır. Nitekim özellikle sonraki amaç bakımından veri sorumlusunun ilgili kişiyi söz konusu amaç için bilgilendirmesi hâlinde hâlihazırda sunmuş olduğu bilgileri ilgili kişiye tekrar sunması ilgili kişi açısından da karmaşık ve anlaşılması güç bir duruma neden olmaktadır. Burada ilgili kişinin makul koşullar altında kendisine sağlanması gereken bilgileri bilmesi gerektiğinin kabul edilip edilemeyeceği tartışmalı bir alan oluşturmaktadır. Örneğin alışveriş karşılığında e-fatura düzenlenmesi için kişisel verilerin paylaşılması ve sadece bu amaçla kullanılarak veri sorumlusunun hukuki yükümlülüğünün yerine getirilmesi ile sınırlı olarak işlenmesi, saklanması hâlinde hayatın olağan akışında ilgili kişinin veri sorumlusunun kimliğini, işleme amacını, kişisel verilerin toplanma yöntem ve hukuki sebebinin bilebilecek durumda olduğu ifade edilebilecektir (diğer örnekler için bkz. Çekin, 2019, s. 142). Ancak kanuni düzenlemenin ilgili kişinin hakları ile birlikte diğer bilebilecek durumda olduğu hususlara ilişkin her hâlükârda bir aydınlatma yapılmasını araması sebebi ile veri toplama anında bu yükümlülüğün kısaca da olsa kasa arkasında yer verilen metin ya da toplama anında sözlü olarak yerine getirilmesi kimi zaman hayatın olağan akışına ters düşse de aranmaktadır. Burada bilgilendirilmiş olma varsayımı, makul bir kişinin göstermesi gereken makul özen üzerine temellendirilmelidir (Yücedağ, 2017).

“İmkânsız Olma”, “Ölçüsüz Çaba Gerektirme”, “Veri İşleme Faaliyetinin Amacının Gerçekleşmesi İçin İmkânsız” ya da “Ciddi Zarar İçerme”

Kişisel verileri doğrudan ilgili kişiden elde etmemiş olan veri sorumlusunun söz konusu istisnalar kapsamında aydınlatma yükümlülüğünü yerine getirmemesi hâlinde, “imkânsız olma”, “ölçüsüz çaba gerektirme”, “veri işleme faaliyetinin amacının gerçekleşmesi için imkânsız” ya da “ciddi zarar içerme” unsurlarını ve gerekliliğini hesap verilebilirlik ilkesi uyarınca ispat zorunluluğu bulunmaktadır.

Çalışma Grubu tarafından verilen örnekte özellikle kamu yararı doğrultusunda arşiv amaçlı, bilimsel, tarihsel araştırma amaçlı ya da istatistiksel amaçlı veri işleme faaliyetleri dışında aydınlatma yükümlülüğünün yerine getirilmesinin imkânsız olmasına ilişkin verilen örneğin çok istisnai bir durum olduğu görülmektedir (Çalışma Grubu, 260 rev. 01, 2018; Simitis, Hornung ve Spiecker, 2019, par. 21). Söz konusu örnekte, çevrimiçi bir abonelik sözleşmesinin kurulması kapsamında ilgili kişinin ödeme yeterliliğine ilişkin kredi raporlama kuruluşundan veri alınması hâlinde veri sorumlusunun bu verileri işlemeden önce ilgili kişiye yapması gereken aydınlatmayı ilgili kişinin adresinin olmaması ya da e-posta adresinin geçerli olmaması durumunda imkânsızlık istisnası kapsamında yerine getirmeksizin veriyi işleyerek abonelik işlemlerini tamamlayıp tamamlayamayacağı tartışılmıştır. Veri sorumlusunun ilgili kişiye ulaşamıyor olması hâli en başta internet sitesinde yer alan ve kayıt anında ilgili kişiye sunacağı aydınlatma metninde bu duruma yer vermesi gerekeceği belirtilerek imkânsızlık istisnası kapsamında değerlendirilmemiştir. ICO’da söz konusu durumun ancak ilgili kişinin iletişim bilgilerinin olmadığı hâllerde söz konusu olabileceğini ifade ederek bir kütüphanenin yapacağı proje kapsamında aktif olmayan kulüp ve topluluklardan çeşitli kayıtları alması ve bu kayıtların ilgili kişinin iletişim bilgisini içermemesi hâlinde veri sorumlusu olan kütüphanenin imkânsız olma istisnasına dayanabileceğini örnek olarak vermiştir (ICO, When can we rely on impossibility?). Ancak her hâlükârda veri koruma etki analizi yaparak aydınlatma metnini yerel gazete ya da internet sitesi aracılığı ile duyurması gerektiği belirtilmiştir. Bu doğrultuda açıkça belirtilmemiş olmakla birlikte söz konusu kulüp ve toplulukların bu veri aktarımı sebebi ile Tüzük 13/3 uyarınca aydınlatma yükümlülüğü saklıdır.

Aydınlatma yükümlülüğünün yerine getirilmesinin imkânsız olması durumu ile benzer şekilde ölçüsüz çaba gerektirmesi hâlinin de belirtilen hususlar haricinde uygulanmasının istisnai olacağı Çalışma Grubu tarafından ifade edilmiştir (Çalışma Grubu, 260 rev. 01, 2018). Bu hâlde ilgili kişi sayısı, verilerin güncelliği ve alınan güvenlik tedbirlerinin göz önünde bulundurulması gerekmektedir (Tüzük Giriş Bölümü, par. 62). Çalışma Grubu tarafından büyük şehir hastanelerinin hastadan, hasta yakınlarına ilişkin bilgi talep etmesi hâlinde her seferinde kişisel verilerini doğrudan kendisinden almadığı ilgili kişi

konumundaki hasta yakınına Tüzük 14 uyarınca gerekli aydınlatmayı iletmesinin ölçüsüz çaba gerektirebileceği ifade edilmiştir. Verilerin güncelliğine ilişkin olarak ise tarihsel araştırma yapan kişilerin erişmiş olduğu veri tabanında çok fazla kişinin bulunması ve bu veri tabanının 50 yıl önce herhangi bir iletişim bilgisi olmaksızın oluşturulmuş olması hâli örnek verilmiştir. Burada veri sorumlusunun bu kişilere ulaşarak Tüzük 14 uyarınca gerekli bilgileri sunması ölçüsüz çaba gerektirmektedir. Önemle belirtmek gerekir ki hesap verilebilirlik ilkesi uyarınca veri sorumlusunun Tüzük 14 uyarınca gerekli bilgileri imkânsız olması ya da ölçüsüz çaba gerektirmesi gerekçesiyle sunmaktan kaçındığı hâllerde bir denge testi yapması gerekmektedir. Burada özellikle veri işleme faaliyetinin ilgili kişi bakımından sonuç ve etkileri büyük önem arz etmektedir. Veri sorumlusu söz konusu işleme faaliyetinin ilgili kişinin temel hak ve özgürlükleri ile menfaatlerini koruyan uygun tedbirleri aldığı ortaya koyabilmeli; kendisine ait bir internet sitesi ya da medya aracılığı ile kamuya açık bir bilgilendirme sunmalıdır.

Tüzük 14 kapsamındaki aydınlatma yükümlülüğünün yerine getirilmesinde veri işleme faaliyeti ile elde edilmek istenen menfaatin ciddi şekilde etkilenmesi hâli de yine istisnai bir durum teşkil etmektedir. Burada örnek olarak bir bankanın (A bankası) müşterisinin şüpheli işlemine ilişkin bilgileri diğer bir bankadan (B bankası) edininip bir soruşturma başlatmak üzere ilgili kamu otoritesi ile paylaşması hâlinde ilgili kişinin bilgilendirilmesi soruşmanın gizliliğini etkileyebilecektir (Çalışma Grubu, 260 rev. 01, 2018). Bu durumda her iki bankanın da hesap açılırken ilgili kişiyi şüpheli işlemler bakımından farklı bankalar ve otoritelerle veri paylaşımı yapabileceğine ilişkin bilgilendirmesi gerekmele birlikte kişisel verileri B bankasından edinen A bankasının Tüzük 14 uyarınca gerekli bilgileri sunmaktan imtina etmesi hukuka uygun olacaktır. Ancak bu hâlde sadece Tüzük 14 kapsamında bir istisnadan bahsetmek mümkün olup, ölçülülük, gereklilik başta olmak üzere genel veri koruma ilkeleri gözetilmelidir.

Burada belirtmek gerekir ki Türk hukuku açısından söz konusu durumun KVKK 28/2-a kapsamı ile örtüştüğü ancak özünde farklılık taşıdığı değerlendirilebilecektir. Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması halinde herhangi bir veri sorumlusu grubuna daraltılmaksızın bu istisna getirilmiştir. Ancak KVKK 28/2-a'da yer alan istisna bakımından 3 husus önem arz eder: i. Bu istisna sadece KVKK 10, 11 ve 16'ya ilişkindir, ii. veri sorumlusunun kişisel verileri doğrudan ilgili kişiden elde edip etmemesi bakımından bir ayırım getirmemiştir, iii. açıkça kamu – özel sektör ayırımı yapılmamıştır. Burada özellikle bu istisnanın kamu – özel sektör ayırımı yapılmaksızın getirilmiş olması sebebi ile dar yorumlanması bir başka deyişle veri sorumlusunun veri işlemenin hukuka uygunluk sebebi olan suçun önlenmesi veya soruşturulması konusunda kanunlarda açıkça öngörülmüş bir hukuki yükümlülüğünün bulunması aranmalıdır. Nitekim bu madde hükmünden KVKK 4 ve 5 istisna değildir.

Kanunlarda Açıkça Öngörülen Bir Yükümlülük Olması

Kanunda açıkça öngörülme hâlinde ise kişisel verileri doğrudan ilgili kişiden toplamayan veri sorumlusunun Tüzük 14 kapsamındaki bilgileri ilgili kişiye sunma zorunluluğu istisna tutulmuştur. Bu kapsamda kanunda açıkça öngörülmeden kasıt birlik ya da üye devlet hukukunda veri sorumlusunun doğrudan söz konusu verileri elde etme veya açıklama zorunluluğu düzenlenmiş olmalıdır. Örneğin vergi mevzuatı uyarınca vergi dairesinin işverenden çalışanına ilişkin genel ilkeler uyarınca ölçülü ve gereklilik kıstası gözetilerek bilgi toplaması hâlinde vergi dairesinin Tüzük 14 uyarınca çalışana bilgilendirmede bulunması gerekmecektir (Çalışma Grubu, 260 rev. 01, 2018). Ancak tekrar ifade etmek gerekir ki işverenin çalışana yapacağı aydınlatma kapsamında kişisel verilerin vergi daireleri ile hukuki yükümlülüğün yerine getirilmesi amacıyla paylaşılacağı ifade edilmiş olmalıdır.

Türk hukuku bakımından ise benzer bir istisna KVKK 28/2-c kapsamında düzenlenmiş ancak kanunun yetki verdiği kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarına bu istisna sadece denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması

için gerekli olması hali ile sınırlı olarak getirilmiştir. Bir başka deyişle, kanunlarda açıkça öngörülme hukuka uygunluk sebebine dayanarak olağan bir şekilde işverenden bilgi alan kamu kurum ve kuruluşları söz konusu verileri elde ettikten sonra ilgili kişiye bildirimde bulunmakla yükümlüdür.

Sır Saklama Yükümlülüğü Altındaki Kişiler

Birlik ya da üye devlet hukuku uyarınca sır saklama yükümlülüğü altındaki kişilerin de söz konusu verileri ilgili kişiden doğrudan almadıkları hâllerde sır saklama yükümlülükleri kapsamındaki veri işleme faaliyetleri için edindikleri kişisel veriler nezdinde ilgili kişiye Tüzük 14 uyarınca bilgilendirmede bulunması gerekmemektedir. Örneğin hastanın sır saklama yükümlülüğü altındaki doktora muayene sırasında kendisinde görülebilecek genetik hastalıklara ilişkin olarak akrabalarına ilişkin verdiği bilgiler nezdinde doktorun Tüzük 14 uyarınca hasta akrabalarına gerekli bilgileri sunma yükümlülüğü söz konusu olamayacaktır (Çalışma Grubu, 260 rev. 01, 2018). Türk hukuku açısından ise KVKK kapsamında sağlık ve cinsel hayata ilişkin kişisel verilerin belirtilen şartlarda sır saklama yükümlülüğü altında bulunan kişilerce işlenmesi bir hukuka uygunluk sebebi sayılmış olmakla birlikte bu kişiler aydınlatma yükümlülüğünden muaf tutulmamıştır. Bu ise özellikle sır saklama yükümlülüğü altındaki kişilerin üçüncü kişiler hakkında elde ettikleri veriler bakımından aydınlatma yükümlülüklerinin doğmasına sebebiyet vermektedir.

İlgili Kişinin Haklarına İlişkin Olarak Üye Devletlerce Getirilen Ek Sınırlamalar

Tüzük, yürürlüğe girmesiyle beraber üye devletlerin doğrudan iç hukuklarının bir parçası olmuş, ancak ihtiva ettiği çeşitli hükümlerde üye devletlere iç hukuklarında çeşitli düzenleme yapma imkânı getirmiştir. Bu doğrultuda üye devlet hukuklarında yürürlükte olan kişisel verilerin korunmasına ilişkin düzenlemeler doğrudan kadük hâle gelmemiş Tüzük'ün 2 yıllık geçiş hükmü doğrultusunda bir uyumlulaştırma süreci geçirmiştir.

Tüzük 23 uyarınca veri sorumlusu ya da veri işleyenlerin tabi olduğu birlik ya da üye devlet hukukunca yükümlülüklerine ve ilgili kişinin haklarına ilişkin Tüzük'te düzenlenen hususlara (Tüzük 5, 12-22, 34) sınırlamaların getirilebileceği hüküm altına alınmıştır. Ancak bu sınırlamaların tesisinde temel hakların ve demokratik toplum gereği ölçütünün nazara alınması gerekmektedir. Ayrıca söz konusu sınırlandırmaların dar yorumlanması esastır.

Tüzük kapsamında söz konusu sınırlandırmanın çerçevesinin kesin bir şekilde belirlenerek yapılması gerektiği düzenlenmiştir (Tüzük 23/2). Üye devletler tarafından yapılacak olan sınırlamanın milli güvenlik, savunma, kamu güvenliği, kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dâhil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesi, başta birliğin veya bir üye devletin önemli ekonomik veya finansal çıkarı olmak üzere mali, bütçe ve vergilendirmeye ilişkin hususlar ile halk sağlığı ve sosyal güvenliğe ilişkin birlik ya da bir üye devletin genel kamu yararına yönelik diğer önemli hedefler, yargı bağımsızlığının ve adli süreçlerin korunması, düzenlenmiş meslek gruplarına ilişkin etik kuralları ihlalinin önlenmesi, soruşturulması, tespiti ve kovuşturulması, istisnai olarak resmi bir yetkinin kullanımı ile bağlantılı bir izleme, denetleme veya düzenleme, ilgili kişinin veya başkalarının haklarının ve özgürlüklerinin korunması, medeni hukuktan kaynaklanan taleplere ilişkin kararların icrası ile bağlantılı ve gereğince olması gerekmektedir.

Bu doğrultuda üye devletler bu kıstaslara bağlı olarak iç hukuklarında çeşitli sınırlamalar getirmiştir. Örneğin, Birleşik Krallık'ta kişisel veri içeren yönetim planlama ve tahminleri, müzakere kayıtları, eğitim ve iş amaçlı gizli referanslar ile sınav metinleri ve notları bakımından da aydınlatma yükümlülüğü istisna tutulmuştur (UK Data Protection Act 2018, Schedule 2, Part 4, 22, 23, 24, 25; diğer istisna hâlleri için bkz. ICO, Exemptions).

Almanya ise Tüzük 13/4 kapsamında düzenlenen sonraki amaç istisnasına ilişkin olarak ek düzenlemeler getirmiştir. Özellikle dijital ortamda saklanmayan ve hâli hazırda aralarında bir sözleşme bulunan veri sorumlusu – ilgili kişi ilişkisi bakımından ilgili kişi ile yazışmaların dijital ortamda yapılmadığı ve ilgili kişinin bilgilendirilmesinde menfaatinin çok düşük olması hâlinde söz konusu istisnanın uygulama alanı bulacağı hüküm altına alınmıştır (BDSG § 32). Bununla birlikte kişisel verilerin elde edilme anında aydınlatma yükümlülüğünün geçici bir mazeret sebebi ile gerçekleştirilememesi hâlinde, veri işleme faaliyetinin özel durumu gözetilerek veri sorumlusunun söz konusu mazeretin ortadan kalmasından itibaren makul süre her hâlükârda iki hafta içerisinde bu yükümlülüğünü yerine getirmesi gerektiği hüküm altına alınmıştır (BDSG § 32/3). Bu duruma örneğin yüz yüze iletişimde aydınlatmanın yapılamaması hâlinde kişinin iletişim bilgilerinin alınması durumunda aydınlatmanın iletişime geçilen anda sağlanması örnek olarak verilebilecektir. Kişisel verileri üçüncü kişiler aracılığı ile elde eden veri sorumlusu bakımından ise kişisel verilerin bir özel hukuk sözleşmesi kapsamında işlenmesi hâlinde ilgili kişiyi bilgilendirme yükümlülüğü ilgili kişinin bu bilgileri edinmekte üstün menfaati olmama koşulu ile istisna tutulmuştur (BDSG § 33/2-a).

Aydınlatma Yükümlülüğünün İstisnalarına İlişkin Sorunlar

Gerek Tüzük ve Tüzük kapsamında getirilen imkân uyarınca üye devletler gerekse KVKK kapsamında getirilen istisnaların ağırlıklı olarak kamu düzeni ve güvenliğine yöneliktir. Gerçek kişinin kendisiyle veya aynı konutta yaşayan aile bireyleri ile ilgili faaliyetler kapsamında işlemesine ilişkin istisna ise Tüzük düzenlemesi ile farklılık taşımaktadır. AB düzenlemelerinde ilgili istisna “kişisel amaç” ve “aynı konutta yaşayan bireyler” unsurlarını barındırmaktadır. Bu halde KVKK’da öngörülen istisnanın daha dar olduğu, örneğin gerçek kişilerin kişisel amaçlı olarak oluşturdukları telefon rehberleri, fotoğraf albümleri bakımından veri sorumlusu sıfatı söz konusu olabilecektir (Küzeci, 2019, s. 329). Yine aile ferdi olmayan kişilerle birlikte yaşanması (paylaşımlı evler, ev arkadaşlığı gibi) halinde istisna uygulama alanı bulamayacaktır. Bununla birlikte KVKK’da ilgili kişi tarafından alenileştirilmiş kişisel verilerin elde edilmesi de aydınlatma yükümlülüğünden istisna tutulmuştur. Ancak KVKK’nın tamamı kapsamında istisna tutulmayan bu veriler uyarınca veri sorumlusunun ilgili kişinin alenileştirme amacına uygun olarak söz konusu verileri işlemesi hâlinde hukuka uygunluk söz konusu olacaktır. Öğretide bu durumun kişisel verilerin işlendikleri amaçla bağlantılı ve sınırlı olma ilkesinin gereği olduğu ifade edilmektedir (Küzeci, 2019, s. 346). Bununla birlikte ilgili kişinin alenileştirme amacı her zaman veri sorumlusu bakımından anlaşılır olmayabilir. Ayrıca özellikle kamuya açık kaynaklardan veri toplayan algoritmalar bakımından da alenileştirilmiş verilerin kamuya açıklanma amacı ile örtülü şekilde kullanılması ve işlenmesi güçlük arz edebilmektedir.

Tüzük’te genel olarak ilgili kişinin söz konusu bilgilere hâlihazırda sahip olması hâli ile sadece veri sorumlusunun söz konusu verileri doğrudan ilgili kişiden elde etmediği hâllerde uygulama alanı olan aydınlatma yükümlülüğünü yerine getirmenin “imkânsız olması”, “ölçüsüz çaba gerektirmesi”, “veri işleme faaliyetinin amacının gerçekleşmesi için imkânsız olma” ya da “ciddi zarar içerme” gibi istisnaların ise uygulama alanının son derece dar olduğu görülmektedir. Belirtmek gerekir ki “imkânsız olma”, “ölçüsüz çaba gerektirme”, “veri işleme faaliyetinin amacının gerçekleşmesi için imkânsız” ya da “ciddi zarar içerme” hâlleri bakımından kriterlerin getirilmesi gerekmektedir.

Polonya Veri Koruma Otoritesi Kararı

Polonya veri koruma otoritesinin kamuya açık kaynaklardan kişisel veri elde eden ancak Tüzük 14 uyarınca ilgili kişiye gerekli bilgileri sunmayan veri sorumlusu hakkında hükmettiği PLN 943,000 (yaklaşık 220.000 Euro) tutarında idari para cezası yaptırımına ilişkin kararda “ölçüsüz çaba gerektirme” hâlini çok dar yorumladığı görülmektedir (Urzęd Ochrony Danych Osobowych, 2019). İhlale konu olayda veri sorumlusu olan şirket, Polonya Ekonomik Hareketlilik Bilgi ve Kayıt Merkezi

(Polish Central Electronic Register and Information on Economic Activity) gibi kamuya açık sicillerden ticari rapor ve kişi listesi oluşturma ile müşterilerine işletme ve yönetim danışmanlığı hizmetleri sunma amacı ile kişisel verileri elde etmiştir. Şirket tarafından yaklaşık olarak gerçek kişilere ait 7,6 milyon kişisel veri toplanmıştır. Şirket 2018 Nisan ayında elinde e-posta adresi bulunan kişilere aydınlatma metni ileterek bu bilgilendirmeyi internet sitesinde de yayınlamış ancak sadece telefon numarası ya da posta adresi bulunan kişilere sms ya da posta yolu ile herhangi bir bilgilendirmede bulunmamıştır. Şirket bu kişilere sms ya da posta yolu ile ulaşmasının maliyetli olacağı ve iş gücü gerektireceği iddiasıyla aydınlatma yükümlülüğünün yerine getirilmemesinin Tüzük 14/5-b’de yer alan “ölçüsüz çaba” istisnası kapsamında değerlendirilmesi gerektiğini savunmuştur. Polonya Veri Koruma Otoritesi ise gerek internet sitesinde yer alan aydınlatma metninin yetersiz oluşu gerekse ilgili kişilere telefon ya da posta yolu ile bu metnin iletilmesinin ölçüsüz bir çaba gerektirmeyeceği gerekçesiyle idari para cezası yaptırımına hükmetmiştir. Otorite, şirketin ancak elinde telefon numarası ya da adresi olmayan kişilere ulaşmak için bu bilgileri diğer veri tabanlarında aramasının gerekmesi hâlinde “ölçüsüz bir çaba” hâlinin söz konusu olacağını belirtmiş ve bilgilendirmelerin yapılması için şirkete 3 aylık süre tanımıştır.

Değerlendirme

Karara konu olay kapsamında Polonya veri koruma otoritesinin “ölçüsüz bir çaba” kıstasını oldukça dar yorumladığı görülmektedir. Veri sorumlusu Tüzük 14/1,2 uyarınca gerekli bilgileri internet sitesi üzerinden duyurduğuna ancak ilgili kişilere doğrudan bilgilendirme için yapması gereken masrafların yüksek olmasına ilişkin savunmaları dahi otorite tarafından nazara alınmamıştır. “Ölçüsüz bir çaba” kıstası ilgili kişinin iletişim verilerine ulaşılması için harcanması gereken çaba olarak yorumlanması kanaatimizce eksiktir. Nitekim veri sorumlusunun elinde ilgili kişinin iletişim bilgilerinin olmaması halinde bu bilgilere ulaşması ölçülülük ilkesi ile bağdaşmayacağından “imkânsızlık” kapsamında değerlendirilmelidir. Otoritenin önüne gelen olayda ise ilgili kişilere ulaşılacak iletişim bilgileri bulunmakla birlikte bu iletişim kanalları üzerinde ilgili kişilerin bilgilendirilmesi eğer veri sorumlusunun ekonomik olarak mahvına yol açacak ya da telafisi güç bir zarar verecek ise ölçüsüz bir çaba olarak değerlendirilmelidir. Ancak veri sorumlusu tarafından ölçüsüz olma istisnasına dayanılarak yapılacak diğer aydınlatma yollarının içeriğine ve ilgili kişilerin nezdinde veri işleme faaliyetinin sonuçlarına ilişkin denge testine ilişkin değerlendirme gerekliliği saklıdır.

İdari para cezası uygulanan şirketin iç hukukta itiraz yollarını izleyerek konuyu Avrupa Adalet Divanı önüne gelmesi hâlinde özellikle mahkemenin yapacağı “ölçüsüz bir çaba” değerlendirmesi ve ortaya koyacağı kıstaslar büyük önem taşıyacaktır. Nitekim sadece ölçüsüz olma değil, imkânsızlık hâli bakımından da objektif kriterlerin belirlenmesi gerekmektedir. İstisnaların dar yorumlanması gerektiği ilkesinden hareketle de belirlenecek olan kriterler gerek kişisel verilerin korunması alanına gerekse verinin serbest dolaşımına hizmet edecektir.

DEĞERLENDİRME VE SONUÇ

Tüzük uyarınca ilgili kişilerin Tüzük 12 ile 22 arasında düzenlenen haklarına ilişkin olarak bir ihlal söz konusu olması hâlinde 20.000.000 Euro’ya kadar veya şirketin bir önceki mali yılın yıllık dünya çapındaki cirosunun %4’üne kadar idari para cezalarına hükmedilmesi söz konusu olabilecektir. Tüzük’ün yürürlüğe girmesi ile birlikte üye devletler nezdindeki veri koruma otoriteleri hem şikâyete bağlı olarak hem de re’sen soruşturmalar başlatmış ve idari para cezası yaptırımları uygulamıştır. Avrupa Komisyonu tarafından 22 Mayıs 2019 tarihinde yayımlanan istatistiklere göre Tüzük’ün yürürlüğe girmesinden itibaren 1 yıl içerisinde 144.376 şikâyet veri koruma otoritelerine iletilmiştir

(Avrupa Komisyonu, GDPR in Numbers, 2019). Bu çalışmada değinilmiş olan aydınlatma yükümlülüğünün ihlaline ilişkin CNIL tarafından uygulanan idari para cezası yaptırımını ise Tüzük'ün yürürlüğü sonrasında uygulanmış yüksek miktartlı idari para cezası olma özelliğini haizdir.

Aydınlatma yükümlülüğünün yerine getirilmesine ilişkin zorluklar sektör ve üye devlet temsilcileri tarafından da dile getirilmektedir. Tüzük kapsamında aydınlatma yükümlülüğüne getirilen istisnaların açık ve hayatın olağan akışı için uygulanabilir olmadığı ifade edilmektedir. İlgili kişinin kişisel verilerinin kontrolünü elinde bulundurması adına büyük önem taşıyan aydınlatma yükümlülüğüne ilişkin çerçevenin otoritelerce genişletilmesi ve -yoğun veri işleme faaliyetleri bakımından çoğu zaman haklı- artan beklentileri veri sorumluları bakımından karışıklığa yol açmaktadır. Nitekim hesap verilebilirlik ve şeffaflık ilkesi uyarınca veri koruma hukuku aktörü olan ilgili kişi nezdinde söz konusu aydınlatmanın açıklığının değerlendirilmesi ve menfaat dengesinin bu şekilde kurulması gerekmektedir. Türkiye açısından ise veri sorumlularının aydınlatma yükümlülüğü KVKK'nın yayımından altı ay sonra yürürlüğe girmiş olup üç senedir uygulama alanı bulmaktadır. Tüzük'te yer alan ilgili kişinin söz konusu bilgilere hâli hazırda sahip olması, bilgileri sağlamanın "imkânsız olması", "ölçüsüz çaba gerektirmesi", "veri işleme faaliyetinin amacının gerçekleşmesi için imkânsız olma" ya da "ciddi zarar içerme" gibi istisnalar ile sır saklama yükümlülüğü bulunan kişiler için öngörülen muafiyete yer verilmemesi sebebiyle KVKK uyarınca daha geniş bir veri sorumlusu grubunun daha geniş bir alanda bu yükümlülüğü yerine getirmesi gerekmektedir. Buna karşın veri sorumlularının aydınlatma metinleri ile ilgili kişileri bilgilendirmekten ziyade birbirini tekrar eden, veri işleme amacı ve hukuki sebeplerini yeterince açık bir dil ile açıklamadıkları metinleri formalite olarak yayınladığı görülmektedir. Belirtmek gerekir ki veri sorumluları bakımından aydınlatma metinleri yürüttükleri veri işleme faaliyetlerinin hukuka uygunluğunu ispat açısından da önem teşkil etmektedir. Burada özellikle ekonomik modeli veri işlemeye dayalı olan, kapsamlı ve ilgili kişiler nezdinde etkisi olan veri işleme faaliyeti yürüten veri sorumluları ile sadece bir alım satım sözleşmesinin kurulması ve ifası kapsamında veri işleyen veri sorumluları bakımından aydınlatma yükümlülüğü ve gerekliliği eş derecede vardır. Ancak burada ilgili kişiler nezdindeki makul beklenti gözetilerek aydınlatma metninin şekli ve maddi unsurlarının denetlenmesi gerekecektir.

Aydınlatma yükümlülüğünün ilgili kişinin talebine bağlı olmaksızın veri sorumlusu tarafından yerine getirilmesi gereken bir husus olduğu konusunda tereddüt bulunmamakla birlikte bu metinlerin işlevsel olması esasen kültürel bir değişimi de gerektirmektedir. İlgili kişilerin kişisel verilerinin korunmasına ilişkin duyarlılığı arttıkça söz konusu metinlerin işlevlerine uygunluğundan bahsedilebilecektir.

KAYNAKLAR

- AAD. (6 Kasım 2003). C-101/01 sayılı Lindquist kararı. <http://curia.europa.eu/juris/liste.jsf?num=C-101/01> adresinden 29.09.19 tarihinde alınmıştır.
- AAD. (22 Aralık 2008). C-553/07 sayılı Rijkeboer kararı. <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-553/07> adresinden 29.09.19 tarihinde alınmıştır.
- AAD. (11 Aralık 2014). C-212/13 sayılı Rynes kararı. <http://curia.europa.eu/juris/liste.jsf?num=C-212/13> adresinden 29.09.19 tarihinde alınmıştır.
- Aşıkoğlu, İ.Ş. (2018). *Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri*. İstanbul Üniversitesi Hukuk Fakültesi Özel Hukuk Yüksek Lisans Tezleri Dizisi No:5. İstanbul: On İki Levha Yayıncılık.
- Avrupa Komisyonu. (2019). *GDPR in Numbers*. https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf adresinden 29.09.19 tarihinde alınmıştır.

- Avrupa Konseyi. (2019). Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR), 12756/1/19 Rev 1. <https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf> adresinden 29.09.19 tarihinde alınmıştır.
- Bacher, M. (2018). *Datenschutz-Grundverordnung / BDSG*. Kühling/Buchner, (Ed.). München: C.H. Beck. 2. Auflage.
- Beyleveld, D. (2004). 'The duty to provide information to the data subject: Articles 10 and 11 of Directive 95/46/EC'. *The Data Protection Directive and medical research across Europe*. Aldershot: Ashgate, s. 69-88.
- Bygrave, L. A. (2014). *Data Privacy Law, an International Perspective*, Oxford, Oxford University Press,
- Cate, F. H., Mayer-Schönberger, V. (2013). Notice and Consent in a World of Big Data. *International Data Privacy Law*, 3(2) s. 67-73.
- CNIL Restricted Committee. (2019). *Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC*. <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf> adresinden 29.09.19 tarihinde alınmıştır.
- Contissa, C., Docter, K., Lagioia, F., Lippi, M., Micklitz, H. W., Palka, P., Sartor, G., Torroni, P. (2018). *CLAUDETTE meets GDPR Automating the Evaluation of Privacy Policies using Artificial Intelligence*.
- Çalışma Grubu. (2018) Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251 rev.01.
- Çalışma Grubu. (2018) Guidelines on Transparency under Regulation 2016/679, WP260 rev.01.
- Çekin, M. S. (2016). 6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi. *İÜHFİM*, LXXIV(2), s. 629-644.
- Çekin, M. S. (2019). *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*. İstanbul: On İki Levha Yayıncılık.
- Develioğlu, M. (2017). *6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku*. İstanbul: On İki Levha Yayıncılık.
- Digital World Market Watch. (2018). *Social Media and The Gdpr: Consumers Should Expect Better*.
- Dix, A. (2019). *Datenschutzrecht*. Simitis/Hornung/Spiecker, (Ed.). 1. Auflage.
- EDPS. (2010). *The EDPS Video-Surveillance Guidelines*, https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf adresinden 29.09.19 tarihinde alınmıştır.
- European Union Agency for Fundamental Rights and Council of Europe. (2018). *Hanbook of European Data Protection Law*. Luxembourg: Publications Office of the European Union.
- Gunst, H. (2017). *The Right to Explanation and the Right to Secrecy*. Helsinki: University of Helsinki.
- Gutwirt, S., Leenes, R. ve de Hert, P. (2015). *Reforming European Data Protection Law*. Springer.
- Hildebrandt, M. (2012). The Dawn of a Critical Transparency Right for the Profiling Era. *Digital Enlightenment Yearbook*.
- ICO . *Are there different ways we can provide privacy information?*. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/> adresinden 29.09.19 tarihinde alınmıştır.
- ICO. *Exemptions*. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/> adresinden 29.09.19 tarihinde alınmıştır.
- ICO. *What are the exceptions in the GDPR?*. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/are-there-any-exceptions/> adresinden 29.09.19 tarihinde alınmıştır.
- ICO. *What do we need to think about if we use Artificial Intelligence (AI)*. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-common-issues-might-come-up-in-practice/> adresinden 29.09.19 tarihinde alınmıştır.
- ICO. *When can we rely on impossibility?*. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/are-there-any-exceptions/> adresinden 29.09.19 tarihinde alınmıştır.
- Ingold, A. (2018). *Europäische Datenschutzgrundverordnung*. Sydow, (Ed.). 2. Auflage.
- Kaminski, M. E. ve Malgieri, G. (2019). Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations. *U of Colorado Law Legal Studies Research Paper No. 19-28*.
- Kişisel Verileri Koruma Kurumu. (2018), *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi*.
- Kişisel Verileri Koruma Kurumu. (2019), *Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi*.

- Knyrim, R. (2018). *DS-GVO: Datenschutz-Grundverordnung*. Ehmann/Selmayr (Ed.). München: C.H. Beck. 2. Auflage.
- Korff, D. (2002). *EC Study on Implementation of Data Protection Directive Comparative Summary of National laws*. Cambridge.
- Küzeci, E. (2014). İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı. *İnsan Hakları Yıllığı*, 32, s.53-75.
- Küzeci, E. (2019). *Kişisel Verilerin Korunması*. Ankara: Turhan Kitapevi.
- Lynskey, O. (2015). *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press.
- Malgieri, G. ve Comandé, G. (2017). Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. *International Data Privacy Law*, 7(4), s. 243-265.
- Mauro, A., Greco, M., Grimaldi, M. (2014). What is Big Data? A Consensual Definition and a Review of Key Research Topics. *4th International Conference on Integrated Information*, AIP Proceedings.
- Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679. (2019). Report – Contribution From The Multistakeholder Expert Group to the Stocktaking Exercise of June 2019 on one Year of GDPR Application. https://ec.europa.eu/commission/sites/beta-political/files/report_from_multistakeholder_expert_group_on_gdpr_application.pdf adresinden 29.09.19 tarihinde alınmıştır.
- Selbst, A. D., Powles, J. (2017). Meaningful information and the right to explanation. *International Data Privacy Law*, 7(4), s. 233-242.
- Taştan, F. G. (2017). *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*. İstanbul: On İki Levha Yayıncılık.
- Tene, O. (2013). Privacy Law's Midlife Crisis'. *Ohio State Law Journal*, 74(6), s. 1217-1262.
- Urzędu Ochrony Danych Osobowych. (2019). *The first fine imposed by the President of the Personal Data Protection Office*. https://uodo.gov.pl/en/553/1009_adresinden 29.09.19 tarihinde alınmıştır.
- Wachter, S., Mittelstadt, B., Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*.
- Yücedağ, N. (2017). Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı Ve Genel Hukuka Uygunluk Sebepleri. *İÜHFEM*, LXXV (2), s. 765-790.
- Yücedağ, N. (2019). Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler. *Kişisel Verileri Koruma Dergisi*, 1(1), s. 47-63.