

## GENEL VERİ KORUMA TÜZÜĞÜ IŞIĞINDA KİŞİSEL VERİLERİN İŞLENMESİNDE RIZA AÇIKLAMASI

DOI: <https://doi.org/10.33717/deuhfd.646330>

**Arş. Gör. Ozan SELEK\***

### Öz

*Avrupa Birliğinde kişisel verilerin korunmasına yönelik hazırlanan 95/46 sayılı Direktifin uygulanmasına 25 Mayıs 2018 tarihinden itibaren son verilmiştir. Bu tarihten itibaren Genel Veri Koruma Tüzüğü uygulanacaktır. Genel Veri Koruma Tüzüğü, veriler üzerinde sahibinin kontrol gücü prensibini benimsemiştir. Veri işleme faaliyetine rıza gösterilmesi, bahsi geçen prensip ışığında ele alınmaktadır. Rızanın geçerli olabilmesi için çeşitli şartların aranması, veri akışının engellenmesini değil, veri öznesinin korunmasını amaçlamaktadır. Gelişen noktada kişilerin özel hayatına ilişkin bilgiler, yetkisiz üçüncü kişiler arasında elden ele dolaşmaktadır. Bütün bu sürece, çoğu zaman bireyin müdahale etmesi mümkün değildir. Bu sebeple, kişisel verilerin işlenmesinde özgür iradeden kaynaklanan, konuya özel, bilgilendirilmeye dayanan, kesinlik içeren geçerli bir rıza açıklamasının önemi katlanarak artmaktadır. Kişisel veriler üzerindeki kontrol gücünün, asıl sahibine geri verilmesi gerekmektedir.*

*Amaçlanan veri trafiğini tamamen durdurmak değil, belirli kurullarla çevrelemektir. Kimlerin hangi yükümlülüklere sahip olduğunun açıkça belirlenmesi, veri ihlallerinden sorumlu olanların da tespit edilmesini kolaylaştıracaktır. Çalışmada veri sorumlusunun yükümlülüklerini kesin çizgilerle belirleyen ve geçerli bir rıza açıklamasının şartlarını makul şekilde saptayan Genel Veri Koruma Tüzüğü incelenmiş, bu şekilde uygulamaya katkı sağlamak amaçlanmıştır.*

### Anahtar Kelimeler

*Kişisel veri, Kişisel verilerin işlenmesi, Genel Veri Koruma Tüzüğü, Veri öznesi, Rıza açıklaması*

\*

Pamukkale Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı (e-posta: ozan\_selek12@hotmail.com) ORCID: <https://orcid.org/0000-0003-4049-9339> (Makalenin Geliş Tarihi: 06.09.2019) (Makale Gönderilme Tarihi: 09.09.2019/ Makale Kabul Tarihi: 30.09.2019)

## CONSENT TO PERSONAL DATA PROCESSING IN THE LIGHT OF GENERAL DATA PROTECTION REGULATION

### Abstract

*In EU, 95/46/EC Directive, which laid down with regard to protect personal data was put an end since 25 May 2018. As of this date, 2016/679/EC General Data Protection Regulation is started enforcement. General Data Protection Regulation adopts principle of control over personal data. Consent to personal data processing is dealt with in the light of mentioned principle. The purpose of conditions are being requested for valid consent is to protect data subject, rather than to prevent personal data flows. At this point, personal data with respect to private life of persons is passed from hand to hand amongst unauthorized third parties. Whole this process is not possible to be interfered by person most of the time. Therefore, the importance of freely and unambiguously given, specific, informed and valid consent is increased incrementally in the course of personal data processing. Control over this data should be returned to the original owner.*

*Original purpose is to enclose specific rules of data traffic, rather than completely stop it. Setting whose liabilities are what clearly, will make it easier to identify the responsible parties for violations of personal data. General Data Protection Regulation which designates the data controller's responsibilities with specific lines and reasonably determines the stipulations of valid consent is studied to make a contribution to practice is aimed in this essay.*

### Keywords

*Personal data, Personal data processing, General Data Protection Regulation, Data subject, Consent*

## GİRİŞ

Avrupa Birliğinde kişisel verilerin korunmasına yönelik hazırlanan 95/46 sayılı Direktifin<sup>1</sup> uygulanmasına 25 Mayıs 2018 tarihinden itibaren son verilmiştir. Çalışmada bu tarihten itibaren uygulanacak olan 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nün<sup>2</sup> rıza konusuna yaklaşımı ele alınacaktır. Direktif ile Tüzükte farklılık arz eden konulardan yeri geldiğinde söz edilecektir. 6698 Sayılı Kişisel Verilerin Korunması Kanunu<sup>3</sup> ile Direktifin rızayı ilgilendiren hükümlerinden ise genel olarak bahsedilecektir.

Kişisel veri, Tüzükte “*belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgi*” şeklinde tanımlanmıştır (m.4/1). Kişisel veriler, hassas olmayan kişisel veriler ve hassas kişisel veriler olarak ikiye ayrılabilir. Hassas kişisel veriler, taşıdıkları özellikler sebebiyle daha özel bir korumaya tabidir. Bu verilerin, belirli kurallar dışında işlenmesi, kişiler arasında haksız ayrımcılık yaratılmasına sebep olabilir<sup>4</sup>. Tüzükte “*ırksal veya etnik köken, siyasi görüş, dini veya felsefi inançlar, ticaret birliklerine üyeliği gösteren kişisel veriler ile genetik, biyometrik veriler, cinsel hayata veya cinsel tercihe ilişkin bilgiler*” hassas kişisel veri<sup>5</sup> olarak sayılmıştır (m.9/1). Tüzüğe göre, kişisel verilerin işlenmesini<sup>6</sup> hukuka uygun hâle getiren sebeplerden biri de veri öznesinin<sup>7</sup> rızasıdır (m.6/1-a). Tüzükte hassas olmayan kişisel verilerin işlenmesinde “rıza” yeterli kabul edilirken; hassas kişisel veriler için “açık rıza” aranmaktadır. Çalışmada rıza ve açık rıza kavramlarının karşılaştırılmasına yer verilecektir.

Çalışmada öncelikle, rızanın tanımına, hukuki niteliğine ve felsefi temellerine değinilecektir. Rıza, genel olarak bireyin bilgilerinin geleceğini

<sup>1</sup> Uzun adı, “Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunmasına ve Serbest Veri Akışının Sağlanmasına İlişkin Direktif” olan bu metinden çalışmada “95/46 sayılı Direktif” veya yeri geldiğinde “Direktif” olarak söz edilecektir.

<sup>2</sup> Bundan böyle “Tüzük” olarak anılacaktır.

<sup>3</sup> Bundan böyle “Kanun” olarak anılacaktır.

<sup>4</sup> **Küzeci**, Elif: Kişisel Verilerin Korunması, 2. Baskı, İstanbul 2018, s. 254 vd.

<sup>5</sup> Tüzükte “özel nitelikli kişisel veriler” kavramına yer verilse de bu çalışmada “hassas veri” kavramı kullanılacaktır.

<sup>6</sup> “*Otomatik veya otomatik olmayan vasıtalarla kişisel veriler üzerinde kaydetme, düzenleme, yapılandırma, depolama, uyarılma, değiştirme, erişme, başvurma, kullanma, yayımlama, yayma, sıralama, ifşa etme, birleştirme, sınırlama, silme veya imha etme gibi faaliyetler*” kişisel verilerin işlenmesi olarak kabul edilmektedir (Tüzük m.4/2).

<sup>7</sup> Veri öznesi, kişisel verileri işlenen gerçek kişi anlamına gelir. Çalışmada geçen “veri öznesi”, “veri ilgilisi”, “ilgili kişi”, “kullanıcı” gibi ifadeler benzer anlamları karşılayacak şekilde kullanılmıştır.

tain etme hakkı kapsamında ele alınmakta, bireyin kendisi için neyin iyi olduğuna karar verebileceği öne sürülmektedir<sup>8</sup>.

Çalışmada rıza açıklamasının geçerli kabul edilebilmesi için hangi şartları taşıması gerektiğinden söz edilecektir. Taraflar arasında güç dengesizliği mevcutsa, veri sorumlusu<sup>9</sup> tarafından rızaya dayanılmasına şüpheyle yaklaşılmaktadır. Bahsi geçen konu, “Veri İşlemenin Rızaya Dayanmasının Uygun Olmadığı Durumlar” başlığı altında ele alınacaktır.

Tüzüğe göre, veri öznesi, rızasını dilediğini zaman geri alma hakkına sahiptir (m.7/3). Geri alma hakkının nasıl kullanılacağı da çalışmada ayrıca incelenecektir. Direktifin aksine Tüzükte çocukların kişisel verilerinin işlenmesi özel olarak düzenlenmiştir. Bu özel düzenlemeye “Rıza Gösterme Ehliyeti” başlıklı bölümde değinilecektir. Tüzüğe yöneltilen eleştiriler, bu husustaki değerlendirmelerimize de yer vermek suretiyle ele alınacaktır.

Kişisel Verilerin Korunması Kanununun hazırlanmasının bir sebebi de Avrupa Birliği üyelik sürecindeki müzakere fasıllarının doğrudan kişisel verilerle ilgili olması ve AB’nin Türkiye ile ilgili ilerleme raporlarında kanun boşluğunu vurgulamasıdır<sup>10</sup>. Zaten Kanun, 95/46 sayılı Direktif esas alınarak hazırlanmıştır. Direktifi yürürlükten kaldıran Tüzük, kişisel verilerle ilgili hakları korumak noktasında daha yüksek standartlar öngörmektedir. Bu itibarla, Kanunun Tüzük esas alınarak değiştirilmesi ve geliştirilmesi önümüzdeki yıllarda gündeme gelecektir. Konu, Tüzükte daha geniş bir perspektiften ele alınsa da, temel olarak Direktifin ve Tüzüğün rıza konusuna yaklaşımları benzerdir. Bu bağlamda, Tüzüğün rızayla ilgili hükümlerine yönelik değerlendirmeler, Direktif esas alınarak hazırlanan Kanun için de büyük oranda geçerli olacaktır.

## I. RIZANIN TANIMI, HUKUKİ NİTELİĞİ, FELSEFİ TEMELLERİ

### A. Tanımı ve Hukuki Niteliği

Tüzükte rıza; *“kendisiyle ilgili kişisel verilerin işlenmesini kabul ettiğini, bir beyan veya açık onaylayıcı eylemle ortaya koyan, ilgili kişinin isteklerinin özgürce verilmiş, konuya özel, bilgilendirilmiş ve kesin bir göstergesi”* şeklinde tanımlanmıştır (m. 4/11). 95/46 sayılı Direktifte ise veri öz-

<sup>8</sup> Bkz. **Küzeci**, s. 238.

<sup>9</sup> Veri sorumlusu, *“kişisel verilerin işlenmesinin amaçlarını ve vasıtalarını tek başına veya başkalarıyla birlikte belirleyen gerçek veya tüzel kişi, kamu makamı, kurumu veya diğer bir kamu kuruluşu”* şeklinde tanımlanabilir (Tüzük m.4/7).

<sup>10</sup> Bkz. 6698 Sayılı Kişisel Verilerin Korunması Kanunu Genel Gereğe, Prg. 8.

nesinin rızası; “kendisiyle ilgili kişisel verilerin işlenmesini kabul ettiğini ortaya koyan, ilgili kişinin isteklerinin özgürce verilmiş, konuya özel ve bilgilendirilmiş bir göstergesi” olarak açıklanmıştı (m.2-h). Direktifin 7’nci maddesi ise veri işleme faaliyetini hukuka uygun kılması için rızanın “kesin olarak” verilmesini aramaktaydı. Her ne kadar rıza tanımları benzer olsa da, Tüzükte geçen “bir beyan veya onaylayıcı eylem” ibareleri, Direktifte yoktur.

6698 Sayılı Kişisel Verilerin Korunması Kanununda ise “açık rıza” ibaresine yer verilmiştir. Kanun, hassas olmayan ve hassas kişisel verilerin işlenmesinde benzer şekilde açık rızanın varlığını aramaktadır. Açık rıza Kanunda; “belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza” şeklinde tanımlanmıştır (m.3/1-a).

Rıza, tek taraflı hukuki işlem mahiyetindedir<sup>11</sup>. Birey tarafından bir hukuki sonucun doğması istenip de bu istenç, bir irade beyanıyla açığa vurulduğunda, hukuk düzeninde belirli bir hukuki sonucun doğacağı öngörülümüşse ortada bir hukuki işlem var demektir<sup>12</sup>. “Bir hakkı veya hukuki ilişkiyi kurmak, değiştirmek, devretmek, ortadan kaldırmak gibi hukuki sonuçların doğabilmesi için, tek bir irade açıklamasına gerek gösteren işlemler” ise tek taraflı hukuki işlem olarak adlandırılır<sup>13</sup>. Veri işleme faaliyetinden önce verilen rıza, işlemeye zemin hazırlayacak, hukuk düzeninde birtakım sonuçlar doğuracaktır.

Türk hukukunda rıza, failin davranışının hukuka aykırı kabul edilmesini engelleyen bir sebep olarak kabul edilmektedir<sup>14</sup>. Kişisel verilerin işlenmesine verilen rıza da veri işleme faaliyetinin hukuka aykırı olmasını engellemekte, başka bir anlatımla, faaliyeti hukuka uygun kılmaktadır<sup>15</sup>.

## B. Felsefi Temelleri

Birey, kendisini ilgilendiren veri işleme süreçlerine dâhil olma ve bu sürecin nasıl ilerleyeceği konusunda aktif şekilde söz alma haklarına sahip-

<sup>11</sup> Eren, Fikret: Borçlar Hukuku Genel Hükümler, 16. Baskı, Ankara 2014, s. 603.

<sup>12</sup> Serozan, Rona: Medeni Hukuku Genel Bölüm/Kişiler Hukuku, 6. Bası, İstanbul 2015, s. 315.

<sup>13</sup> Eren, s. 165.

<sup>14</sup> Oğuzman, M. Kemal/ Öz, M. Turgut: Borçlar Hukuku Genel Hükümler, Cilt II, 13. Bası, İstanbul 2017, s. 22; Dural, Mustafa/Öğüz, Tufan: Türk Özel Hukuku, Cilt II - Kişiler Hukuku, 19. Baskı, İstanbul 2018, s. 151.

<sup>15</sup> Çekin, Mesut Serdar: Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, İstanbul 2018, s. 57; Başalp, Nilgün: Kişisel Verilerin Korunması ve Saklanması, Ankara 2004, s. 39.

tir. Bizce bu husus, “veriler üzerinde sahibinin kontrol gücü prensibi” veya kısaca “kontrol prensibi” şeklinde ifade edilebilir. İşte bu prensibin veri öznesi bakımından önemi, rıza açıklamasıyla ortaya çıkmaktadır<sup>16</sup>.

Günümüz veri koruma sisteminde kişisel verinin nasıl yönetileceği konusunda bireyin karar almasına olanak tanıyan bir dizi hak öngörülmüştür. Veri öznesine tanınan, kişisel verilerin kim tarafından tutulduğunu bilme, verilere erişme ve yanlış olan verilerin düzeltilmesini isteme gibi haklarla kontrol prensibinin bağlantısı bulunmaktadır<sup>17</sup>. Keza veri işleme süreci hakkında veri öznesinin bilgilendirilmesi de bu bağlamda ele alınmaktadır. Zira eksik veya yanlış bilgilendirilen bir kişi, verileri üzerinde hâkimiyet kuramaz<sup>18</sup>.

Birey, kendisi için neyin iyi olduğuna karar verebilir; bu sayede hangi türde ve miktarda kişisel veriyi başkalarıyla paylaşacağı hususunda bir değerlendirme yapabilir. Bu itibarla, bireyin kendisini başkaları için erişilir kılmak veya kılmamak noktasında seçim şansına sahip olması, kontrol prensibi çerçevesinde değerlendirilir<sup>19</sup>. Temelde amaç, bireye kişisel veri üzerindeki tasarrufların yararını/zararını tartabilmesi için imkân tanımaktır<sup>20</sup>. Veri kullanımı konusunda akılcı kararların alınması, ancak kullanımın yol açacağı fayda ve zararların birey tarafından analiz edilmesiyle mümkün olabilir<sup>21</sup>.

Belirli bir veri işleme faaliyetinin yararına olduğunu düşünen birey, bu faaliyete rıza göstererek esasen bilgilerinin geleceğini tayin eder<sup>22</sup>. Kişisel

<sup>16</sup> **Lazaro, Christophe/Le Metayer, Daniel**: “Control Over Personal Data: True Remedy of Fairy Tale”, SCRIPTed: A Journal of Law, Technology And Society, Vol. 12, I.1, 2015, s. 4. Ayrıca verinin silinmesini veya düzeltilmesini talep etme gibi aktif olarak kullanılan hakların yanı sıra veri minimizasyonu gibi daha çok veri sorumlusunun uyması gereken yükümlülükler de kontrol prensibi çerçevesinde değerlendirilir. Bilgi için bkz. **Lazaro/Le Metayer**, s. 23 vd.

<sup>17</sup> **Lazaro/Le Metayer**, s. 8.

<sup>18</sup> **Jarovsky, Luiza**: “Improving Consent in Information Privacy Through Autonomy-Preserving Protective Measures (APPMs)”, European Data Protection Law Review, Vol.4, I.4, 2018, s. 450.

<sup>19</sup> **Lazaro/Le Metayer**, s. 8.

<sup>20</sup> **Solove, Daniel J.**: “Privacy Self-Management And The Consent Dilemma”, Harvard Law Review, Symposium: Privacy And Technology, Vol.126, I.7, 2013, s. 1880.

<sup>21</sup> **Solove**, s. 1891. *Solove*, bu yaklaşımı “mahremiyetin öz-yönetimi” olarak adlandırmaktadır (**Solove**, s. 1880).

<sup>22</sup> Bkz. **Bergkamp, Lucas/Dhont, Jan**: “Data Protection in Europe And The Internet: An Analysis of The European Community’s Privacy Legislation in The Context of The World Wide Web”, The EDI Law Review, Vol.7, 2000, s. 78; **Küzeci**, s. 238. Alman

verilerin işlenmesine rıza gösterme ile bireysel özerklik düşüncesi arasında derin bir ilişki bulunmaktadır<sup>23</sup>. Kişisel verilerin işlenmesinde bireysel özerkliği koruyucu bir yaklaşımın benimsendiğinden söz edilebilmesi için şu kriterler belirleyici olacaktır<sup>24</sup>: Veri öznesi, (a) Kendisinden talep edileni ve bunun risklerini anlamış mı? (b) Kendisi için neyin en iyi olduğuna karar verebilecek durumda mı? (c) Fikirlerini açık ve kesin şekilde ifade etme olanağına sahip mi? (ç) Değişiklikler yapma ve gerektiğinde rızasını geri alma imkânlarına sahip mi?

## II. DİREKTİFİN, KANUNUN VE TÜZÜĞÜN RIZAYLA İLGİLİ HÜKÜMLERİNE GENEL BİR BAKIŞ

### A. 95/46 Sayılı Direktif

Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunmasına ve Serbest Veri Akışının Sağlanmasına İlişkin Direktif, 1995 tarihinde Avrupa Parlamentosu ve Avrupa Birliği Konseyi bünyesinde hazırlanmıştır<sup>25</sup>. Direktif, Avrupa Birliği'ne üye ülkelerin veri koruma düzenlemeleri arasındaki farklılıkların giderilmesini, asgari veri koruma ölçütlerinin belirlenmesini, bu suretle birlik içerisinde serbest veri akışının sağlanmasını hedeflemiştir<sup>26</sup>. Kişisel verilerin serbest akışı esnasında başta mahremiyet olmak üzere temel hak ve özgürlüklerin korunması da Direktifin temel amaçları arasındadır (Gerekçe, Prg. 2).

Direktifte ilgilinin veri işleme faaliyetine kesin olarak rıza göstermesi, hassas olmayan kişisel verilerin işlenmesini hukuka uygun hâle getiren sebeplerden biri olarak kabul edilmiştir (m.7-a)<sup>27</sup>. Rızanın “kesin” olmasından,

---

Hukukunda kişisel verilerin işlenmesine rıza göstermek, “bilgilerin geleceğini tayin etme” hakkıyla ilişkilendirilmektedir. Konuyla ilgili bkz. **Staben**, Julian: “Consent Under Pressure And The Right to Informational Self-Determination”, *Internet Policy Review*, Vol.1, I.4, 2012, s. 1 vd.

<sup>23</sup> **Jarovsky**, s. 451.

<sup>24</sup> **Jarovsky**, s. 448.

<sup>25</sup> <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046> (Erişim Tarihi: 17.8.2019).

<sup>26</sup> **Küzeci**, s. 166-168.

<sup>27</sup> Hassas olmayan kişisel verilerin işlenmesini hukuka uygun kılan diğer sebeplerse Direktifin 7'nci maddesinde sayılmıştır. Buna göre; “(b) ilgili kişinin tarafı olduğu bir sözleşmenin ifası için veri işlemenin gerekli olması, (c) veri sorumlusu tarafından yerine getirilmesi gereken hukuki bir yükümlülüğün mevcut olması, (d) ilgilinin hayati menfaatlerini korumak için veri işlemenin yapılması, (e) veri işlemenin kamunun menfaatine olan veya kamu gücünün icrasında gerçekleşen bir görev için gerekli olması” durumunda hassas kişisel veriler rıza aranmaksızın işlenebilir. Ayrıca bilgi için bkz. **Küzeci**, s. 258 vd.

“şüpheye yer bırakmayacak” nitelikte olması anlaşılmalıdır<sup>28</sup>. Objektif olarak değerlendirilen beyanın, içerik olarak şüpheye yer bırakmayacak ölçüde bir kesinliğe ulaşması aranmaktadır.

Direktifte kişisel veriler ve özel nitelikli (hassas) kişisel veriler ayrımı yapılmış; kişinin, “*ırksal veya etnik kökeni, siyasi görüşü, dini veya felsefi inancı, sendika üyeliği, sağlık veya cinsel yaşamına*” ilişkin bilgiler, hassas kişisel veri olarak kabul edilmiştir (m.8/1). Hassas kişisel verilere yönelik işleme faaliyetinin hangi durumlarda hukuka uygun kabul edileceği ise m.8/2’de sayılmıştır. “*İlgili kişinin açık rızası*”, hassas kişisel verilerin işlenmesini hukuka uygun kılan sebeplerden biridir (m.8/2-a)<sup>29</sup>.

Direktifin 29’uncu maddesi ile “*Kişisel Verilerin İşlenmesine Dair Bireylerin Korunması Hakkında Çalışma Grubu*” kurulmuştur. Bahsi geçen grubun danışma statüsüne sahip olduğu ve bağımsız şekilde görev yapacağı belirtilmiştir. Çalışmada “*29. Madde Veri Çalışma Grubu*” veya “*Article 29 Working Party*” olarak zikredilen bu grup, Direktifin ve Tüzüğün nasıl uygulanacağına ışık tutan raporlar hazırlamıştır. Direktifteki rıza tanımını esas almak suretiyle 13 Temmuz 2011’de yayımlanan rapor<sup>30</sup> ile Tüzükteki rıza kavramına ilişkin esasları açıklamak üzere, 10 Nisan 2018’de yayımlanan rapordan<sup>31</sup> bu çalışmada sık sık yararlanılmıştır. Keza grubun işçilerin kişisel verilerinin işlenmesine ilişkin raporları ile sağlık kayıtlarının tutulmasına ilişkin raporu da vardır. Direktifin uygulanmasına 25 Mayıs 2018’den itibaren son verilmesiyle birlikte 29. Madde Veri Çalışma Grubu, yerini Avrupa Veri Koruma Otoritesine bırakmıştır (Tüzük m.94/2).

<sup>28</sup> **Küzeci**, s. 239.

<sup>29</sup> Hassas kişisel verilerin işlenmesini hukuka uygun hâle getiren açık rıza dışındaki sebepler Direktifin 8/2’nci ve 8/3’üncü maddelerinde sayılmıştır. Direktifin 8/2’nci maddesine göre; “(b) veri işleme, veri sorumlusunun iş hukukundan kaynaklanan hak ve yükümlülüklerini yerine getirilmesi için zorunluysa, (c) veri öznesinin veya diğer bir kişinin hayati menfaatlerinin korunması için gerekliyse, (d) kar amacı gütmeyen bir kurum tarafından kanuni etkinliklerin yerine getirilebilmesi için veri işleme gerekliyse, (e) ilgili kişi tarafından kamuya açıklanan verilere ilişkin veya hakların kurulması, kullanılması ve korunması için veri işlemenin gerekli olması” durumunda açık rıza aranmaksızın veriler işlenebilir. Ayrıca Direktifin 8/3’üncü maddesine göre; “veri işlemenin önleyici hekimlik, tıbbi teşhis, tıbbi yardım veya bakım ya da sağlık hizmetlerinin idari açıdan yürütülmesi adına gerekli olması ve bu verilerin ya sağlık personeli ya da sağlık personeline benzer şekilde sır saklama yükümlülüğüne tabi kişilerce işlenmesi” hâllerinde de açık rızanın varlığına ihtiyaç yoktur.

<sup>30</sup> Bkz. Article 29 Working Party, **Opinion 15/2011 on The Definition of Consent**, 13/7/2011.

<sup>31</sup> Bkz. Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, 10/4/2018.



## B. Kişisel Verilerin Korunması Kanunu

Dünyada 1960'lı yıllardan itibaren tartışılan kişisel verilerin nasıl korunacağı meselesi, Türkiye'de ilk olarak 1989 yılında yapılan çalışmalarla gündeme gelmiş, 2000'li yıllarda ise bu konuda çeşitli kanun tasarıları hazırlanmıştır<sup>32</sup>. Nihayetinde hazırlanan tasarı, TBMM'de kabul edilerek 24 Mart 2016 tarihinde kanunlaşmıştır. 6698 Sayılı Kişisel Verilerin Korunması Kanununun yürürlüğe girmesi ise 7 Nisan 2016 tarihinde gerçekleşmiştir. Kanunun hazırlanmasında kişisel verilerin işlenmesine ilişkin usul ve esasları belirleme hedefi etkili olmuştur.

Kanun, kişisel verilerin işlenmesinde ilgili kişinin açık rızasını arar (m.5/1). Kanunun 5/2'nci maddesinde ise açık rıza aranmaksızın kişisel verilerin işlenebileceği hâller sayılmıştır<sup>33</sup>.

Kanunda hassas kişisel veriler; *“kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri”* olarak belirlenmiştir (m.6/1). Hassas kişisel verilerin işlenmesinde ilgilinin açık rızası aranmaktadır (m.6/2). Kanunun 6/3'üncü maddesinde ise açık rıza gerekmeksizin hassas kişisel verilerin işlenebileceği hâller açıklanmıştır. Burada verinin türüne göre ikili bir ayırım yapılmıştır: Sağlık ve cinsel hayat dışındaki hassas kişisel veriler, kanunlarda öngörülen hâllerde açık rıza gerekmeksizin işlenebilir (m.6/3'üncü maddenin 1'inci cümlesi). Buna karşılık, sağlık ve cinsel hayata ilişkin kişisel veriler; *“ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuru-*

<sup>32</sup> **Korkmaz**, İbrahim: Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, 2. Baskı, Ankara 2019, s. 318.

<sup>33</sup> Kişisel Verilerin Korunması Kanunu Madde 5 - *“(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür: a) Kanunlarda açıkça öngörülmesi, b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, d) İlgili kişinin kendisi tarafından alenileştirilmiş olması, e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.”*

*luşlar tarafından ilgilinin açık rızası aranmaksızın*” işlenebilir (m.6/3’üncü maddenin 2’nci cümlesi).

Kanunun hassas kişisel verilere yaklaşımı eleştiriye açıktır. Bilhassa sağlığa ve cinsel hayata ilişkin verilerin açık rıza aranmaksızın “*sağlık hizmetleri ile finansmanın planlanması ve yönetimi*” gibi amaçlarla işlenmesinin öngörülmesi yerinde olmamıştır. Zira bu tip faaliyetlerin kişinin kimliğini açığa vurmada yani anonim kayıtlarla da yürütülmesi mümkündür. Verilerin açık rıza aranmaksızın işlenebileceği durumların Kanunda bu kadar geniş tutulması, kontrol prensibinin yeteri kadar dikkate alınmadığını göstermektedir.

### C. Genel Veri Koruma Tüzüğü

Düzenleme, “direktif” değil, “tüzük” niteliğindedir. Avrupa Birliğinde direktifler, ancak üye devletin iç hukukuna aktarılsa uygulanabilir; buna karşılık tüzükler, her üye devlette doğrudan uygulama alanı bulmaktadır<sup>34</sup>. Nitekim 95/46 sayılı Direktifin hukuk sistemlerine aktarılması, her bir üye devlet açısından farklı olmuş, üye devletlerin mevzuatı arasında yeknesaklık sağlanamamıştır<sup>35</sup>. Ayrıca bilgi iletişim teknolojisinde yaşanan gelişmeler, kişisel verilerin korunması alanında daha belirli hükümlerin ihdas edilmesini gerektirmiş, nihayetinde Tüzük hazırlanmıştır<sup>36</sup>.

Rızayı ilgilendiren hükümler, genellikle Tüzüğün 4 ila 9’uncu maddelerinde yer alır<sup>37</sup>.

Tüzüğün 5/1-f maddesinde veri güvenliği ilkesi düzenlenmiştir. Veri güvenliği, internet sitelerine, veri tabanlarına, bilgisayarlara yetkisiz olarak erişilmesini engellemek için alınması gereken koruyucu tedbirleri ifade

<sup>34</sup> **Develioğlu**, Murat: 6698 Sayılı Kişisel Verilerin Korunması Kanunu İle Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, İstanbul 2017, s. 12.

<sup>35</sup> **Noujaim**, Arlette: “The Stimulus For Data Protection Laws Around The World: The Development And Anticipated Effect on The European Union’s New Data Rules”, Intellectual Property Law Bulletin, Vol.20, I.2, 2016, s. 102, 103. s. 103.

<sup>36</sup> **Avrupa Komisyonu**, Communication From The Commission to The European Parliament, The Council, The Economic And Social Committee And The Committee of The Religions, A Comprehensive Approach on Personal Data Protection in The European Union, s. 3, 4. Bkz. <http://www.beuc.eu/publications/2011-00062-01-e.pdf> (E.T. 21.05.2018).

<sup>37</sup> Konu hakkında bilgi için bkz. **Dülger**, Murat Volkan: “Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması”, Yaşar Hukuk Dergisi, C.1, S.2, Temmuz 2019, s. 111 vd.

eder<sup>38</sup>. İşlemenin rızaya dayandığı hâllerde, geçerli bir rızanın elde edilmesi tek başına yeterli değildir; veri sorumlusu, veri güvenliği ilkesi gereğince, koruyucu ve önleyici nitelikteki tedbirleri almakla yükümlüdür.

Tüzüğün 5/2'nci maddesinde yer verilen sorumluluk prensibine göre; veri sorumlusu, Tüzükte belirtilen ilkelere uygun hareket etmek ve gerektiğinde uygun hareket ettiğini ispatlamak zorundadır. Keza Tüzüğün 7/1'inci maddesine göre; veri işlemenin rızaya dayandığı durumlarda, veri öznesi tarafından rıza gösterildiğini kanıtlamak veri sorumlusuna düşmektedir. Bu hüküm, sorumluluk prensibinin bir yansımasıdır.

*“İlgili kişinin bir veya daha fazla belirli amaç için verilerin işlenmesine rıza göstermesi”*, kişisel verilerin işlenmesini hukuka uygun kılan sebeplerden biri olarak açıklanmıştır (m.6/1-a). Hassas kişisel verilerin işlenmesini hukuka uygun kılan sebepler ise; Tüzüğün 9/2'nci maddesinde belirtilmiştir. Hassas kişisel verilerin *“bir veya daha fazla belirli amaç için işlenmesine açık rıza verilmesi”* bu sebepler arasında sayılmıştır (m.9/2-a). Tüzükte *“rıza”* ve *“açık rıza”* ayrımı yapılmış, hassas kişisel verilerin işlenmesinde *“açık rıza”* aranmıştır. Açık rıza ifadesi, kişisel verilerin işlenmesinde daha yüksek bir korumaya işaret etmektedir. Rıza ve açık rıza ayrımının Tüzük bakımından önemine ileride değinilecektir.

Rızanın geçerlilik şartlarına ilişkin bir diğer hüküm, Tüzüğün 7'nci maddesidir. Tüzüğün 7/2'nci maddesine göre, *“ilgili kişinin rızası, başka konuları da kapsayan yazılı bir beyan hâlinde verilecekse, rıza talebi, diğer konulardan açıkça ayırt edilebilecek şekilde sunulmalı, anlaşılır ve kolaylıkla erişilebilir olmalı, talepte açık ve basit bir dil kullanılmalıdır.”*

Tüzüğün 7/3'üncü maddesi, rızanın geri alınmasına ilişkindir. Buna göre; *“ilgili kişi, her zaman rızasını geri alma hakkına sahiptir. Rızanın geri alınması, o ana kadar gerçekleştirilen işleme faaliyetlerinin hukuka uygunluğunu etkilemez. İlgili kişi rıza vermeden önce bu konuda bilgilendirilmiştir. Rızanın geri alınması, rızanın verilmesi kadar kolay olmalıdır.”*

Tüzüğün 7/4'üncü maddesine göre; sözleşmenin ifası veya bir hizmetin sunulması için gerekli olmayan bir veri işleme faaliyetine rıza gösterilmesi sözleşmenin ifa edilmesi veya hizmetin sunulması için şart koşuluyorsa, bu husus, rızanın serbestçe verilip verilmediğinin değerlendirilmesinde bir ölçüttür. Taraflar arasında hiyerarşi ve güç dengesizliği bulunan durumlarda bahsi geçen hüküm devreye girmektedir<sup>39</sup>.

<sup>38</sup> **Bozkurt Yüksel**, Armağan Ebru: Bulut Bilişimde Kişisel Verilerin Korunması, Ankara 2016, s. 175.

<sup>39</sup> Bkz. **Çekin**, s. 61.

Tüzük, çocukların kişisel verilerinin işlenmesinde özel bir düzenlemeye yer vermiştir (m.8). Tüzüğün 8/1'inci maddesine göre, bir çocuğa doğrudan bilgi toplumu hizmetlerinin<sup>40</sup> sağlanması söz konusu olduğunda, kişisel verilerin işlenebilmesi için çocuğun en az 16 yaşında olması gerekmektedir. Çocuğun 16 yaşından küçük olması hâlinde ise, işleme faaliyeti, sadece çocuk üzerinde velayet hakkı bulunan yasal temsilcinin rıza göstermesi veya çocuğun rızasını onaylaması durumunda mümkündür. Aksi takdirde, işleme faaliyeti hukuka aykırı olacaktır. Yine sorumluluk prensibi gereğince, velayet sorumlusunun yetki veya izin verdiğini ispat etmek, veri sorumlusuna düşmektedir (m.8/2). Tüzükteki bu hüküm, rıza gösterme ehliyetinin tespiti bakımından önemlidir.

### III. GENEL VERİ KORUMA TÜZÜĞÜ BAĞLAMINDA RIZA AÇIKLAMASI

#### A. Geçerli Bir Rıza Açıklamasının Şartları

Tüzüğün 4/11'inci maddesinde rıza; *“kendisiyle ilgili kişisel verilerin işlenmesini kabul ettiğini, bir beyanla veya açık onaylayıcı eylemle ortaya koyan, ilgili kişinin isteklerinin özgürce verilmiş, konuya özel, bilgilendirilmiş ve kesin bir göstergesi”* şeklinde tanımlanmıştır. Tanımdan yararlanarak geçerli bir rıza açıklamasının şartlarını saptamak mümkündür. Buna göre rıza; (a) özgür iradeye dayanmalı, (b) konuya özel olmalı, (c) bilgilendirilmiş olmalı ve (ç) veri öznesinin isteklerinin kesin bir göstergesi olmalıdır. Çalışmanın bu bölümünde bahsi geçen şartlar inceleme konusu yapılacaktır.

#### 1. Özgür İradeye Dayanmalı

Veri öznesine gerçek bir seçim şansının tanındığı durumlarda ancak, özgür iradenin varlığından söz edilebilir (Tüzük, Giriş Kısmı, Prg. 42). Rıza göstermeyen veri öznesi, olumsuz sonuçlara katlanmak zorunda kalacaksa veyahut gösterilen rıza baskının bir sonucuysa “gerçek bir seçim” imkânı tanınmamıştır<sup>41</sup>. Rızaya ilişkin şartlar tartışmaya açık olmayan özellikler taşıyorsa, özgür iradeyle verilen bir rıza mevcut değildir. Sadece veri özne-

<sup>40</sup> Bilgi toplumu hizmetleri ile elektronik araçlarla belirli bir mesafeden sunulan, bireysel bir taleple ve genellikle bir bedel karşılığında verilen hizmetler kastedilmektedir. Tanım için bkz. EU Directive 2015/1535 of The European Parliament And of The Council of 9 September Lations And of Rules on Information Society Services, m. 1/1-b.

<sup>41</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, 10/4/2018, s. 5.

sinin herhangi bir etki altında kalmadan aldığı kararların özgür iradeye dayandığı söylenebilir<sup>42</sup>.

Bir zarara uğramadan rıza göstermeyi reddetmek veya rızayı geri almak mümkün değilse, baştan itibaren geçerli bir beyandan söz edilemez (Tüzük, Giriş Kısmı, Prg. 42). Gözdağı verme, zorlama, yıldırma, aldatma gibi bireyin iradesini dışarıdan etkileyen durumlarda<sup>43</sup> veya rıza göstermeyen bireye doğrudan bir yaptırımın uygulanacağı hâllerde<sup>44</sup>, özgür irade mevcut değildir.

Bir şirket, doğa sporlarında göz için kullanılan aksesuarları, müşterilerin ihtiyaçlarını dikkate alarak üretmektedir. Uzağı görme konusunda sıkıntı yaşayan müşterilere özellikli kar gözlüğü hazırlanması için sağlık bilgilerine ihtiyaç duyulmakta, müşteriden elektronik reçetenin paylaşılması talep edilmektedir. Bu bilgiler olmadan, özellikli kar gözlüklerinin üretilmesi de olanaklı değildir. Şirket, ek olarak, sağlık bilgilerini paylaşmak istemeyen müşteriler için standart kar gözlüğü göndermeyi teklif etmektedir. Örnekte rıza açıklaması, özgür iradeye dayanmaktadır<sup>45</sup>.

Bir yerel belediye yol bakım çalışması yapmayı planlar. Bu esnada bir süre trafikte aksamalar yaşanması muhtemeldir. Beklenen aksamalardan ve çalışma saatlerinden haberdar olabilmeleri için o bölgede yaşayan insanlar, bir e-posta listesine abone olmaya davet edilir. Ayrıca belediye, e-postaların sadece bu amaç için kullanılacağını ve listeye abone olma gibi bir zorunluluğun bulunmadığını açıklar. Bu örnekte, rıza göstermeyen bir vatandaş, belediyenin sağladığı herhangi bir hizmetten mahrum kalacak değildir. Zira yol çalışmalarıyla ilgili bilgiler, halihazırda belediyenin internet sitesinde de yer almaktadır. Örnekte, özgür iradeye dayanan bir beyan bulunmaktadır. Bir devlet okulu, magazin dergisinde yayımlamak üzere öğrencilere fotoğrafları konusunda rıza verip vermeyeceklerini sormaktadır. Bir zarara uğramadan rıza vermeyi reddetmek mümkünse, gerçek bir seçim şansı mevcuttur, alınan beyan geçerlidir<sup>46</sup>.

<sup>42</sup> Korkmaz, s. 149.

<sup>43</sup> Misek, Jakub: "Consent to Personal Data Processing- The Panacea or The Dead End", Masaryk University Journal of Law and Technology, Vol.8, I.1, 2014, s. 72; Benzer Staben, s. 3; Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 10.

<sup>44</sup> Bergkamp/Dohnt, s. 77, 78.

<sup>45</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 19, 20.

<sup>46</sup> Her iki örnek için bkz. Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 6, 7.

Sahip olduğu arazi üzerinde bir kişi, hem belediyeden hem de hükümetten ruhsat izni talep eder. Her iki kurum da izin konusunu değerlendirebilmek için benzer bilgiler talep eder, kurumlar birbirlerinin veri tabanlarına erişim yetkisini haiz değildir. Kişi, her iki kuruma da bilgilerini gönderir. Belediye ve hükümet yetkilileri, yazışmaların tekrar etmesinden kaçınmak için her iki kurumdaki dosyaların birleştirilmesi konusunda kişiden rıza talebinde bulunurlar. Rıza gösterilmesinin isteğe bağlı olduğunu belirterek kişinin seçiminin, ruhsat izni hakkında verilecek kararı etkilemeyeceğini garanti ederler. Dosyaların birleştirilmesine gösterilen rıza, özgür iradeye dayanmaktadır<sup>47</sup>.

Doktrinde rızanın gösterilmemesi hâlinde uygulanacak yaptırımın çok hafif olduğu durumlarda rızanın özgür iradeye dayandığı savunulmaktadır<sup>48</sup>. Bu görüşe göre, ücretsiz olarak sunulan e-posta hizmetinin çerezler olmadan kullanılmasının mümkün olmadığı durumlarda, kullanıcı eşdeğer ve ücretsiz şekilde başka bir yerden hizmeti temin etmekle hafif bir külfet altına girdiği için elde edilen rıza geçerlidir<sup>49</sup>. Bizce veri öznesi, ya bir zarara uğramıştır ya da uğramamıştır. Veri öznesinin baştan rıza göstermediği veya sonradan rızasını geri aldığı durumlarda hafif bir yaptırıma dahi maruz bırakılması, rızanın özgür iradeye dayanmadığını göstermektedir.

## 2. Bilgilendirilmiş Olmalı

Geçerli bir rıza beyanının varlığı, hiç şüphesiz, veri öznesinin doğru olarak bilgilendirilmesiyle yakından ilişkilidir. Bireyin geleceği öngörebilmesi ve veri işleme sürecini bütün olarak kavrayabilmesi için veri sorumlusu tarafından bilgilendirme yükümlülüğü eksiksiz yerine getirilmelidir<sup>50</sup>. Öncelikle birey, verilerin nasıl işleneceği hakkında bilgilendirilir, ardından veri işlemeyi kabul edip etmemek konusunda bir seçim imkânıyla donatılır<sup>51</sup>.

Veri işleme süreci ne kadar karmaşıklaştıkça veri sorumlusunun bilgilendirme yükümlülüğü aynı oranda ciddileşir<sup>52</sup>. Değerlendirme, objektif olarak değil, sübjektif olarak; yani, veri öznesinin şahsına göre yapılmalıdır. Veri

<sup>47</sup> Örnek için bkz. Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 6.

<sup>48</sup> Görüşler için bkz. **Küzeci**, s. 241; **Korkmaz**, s. 149; **Bergkamp/Dohnt**, s. 78.

<sup>49</sup> Örnek için bkz. **Bergkamp/Dohnt**, s. 77, 78.

<sup>50</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 21.

<sup>51</sup> Doktrinde bu husus, “fark et ve seç” şeklinde adlandırılmaktadır (Bkz. **Solove**, s. 1883).

<sup>52</sup> Article 29 Working Party, **Opinion 15/2011 on The Definition of Consent**, 13/7/2011, s. 20.

öznesi, neye rıza göstereceğini tam olarak kavrayabilmelidir. Bu kavrayışın kazanılması, veri öznesinin şahsına özgü bir bilgilendirme süreci yürütülmesine bağlıdır. Veri sorumlusu tarafından verilecek bilgi, kişiliğinden kaynaklı olarak farklı özellikler arz eden veri öznesi için anlaşılabilir olmalıdır.

Neye rıza gösterildiği, kişisel verilerin nasıl kullanılacağı, hangi amaçlarla verilerin işlendiği veya verilere erişim yetkisini kimlerin haiz olduğu gibi hususlarda veri öznesi bilgilendirilmelidir<sup>53</sup>. Keza, veri öznesi, rıza göstermenin sonuçlarını değerlendirme olanağına da sahip olmalıdır<sup>54</sup>. Veri öznesi, rızasını dilediği zaman geri alabileceği noktada da aydınlatılmalıdır. Zira sırf rızasını geri alma hakkı olmadığı zannıyla veri işleme sürecine müdahale etmeyen veri öznesinden<sup>55</sup> geçerli bir rıza alındığını söylemek pek mümkün değildir.

Bilgilendirme yükümlülüğünün ifa edildiğinden söz edilebilmesi için şu şartların yerine getirilmesi gerekir: (a) Hazırlanan metinde, normal bir insanın kolaylıkla anlayabileceği ölçüde açık ve anlaşılabilir bir dil kullanılmalı, (b) Metin kolayca ulaşılabilir olmalı, hangi konuda rıza talebinde bulunduğu diğer konulardan ayırt edilebilir şekilde anlatılmalı, (c) Gizlilik politikasına<sup>56</sup> ilişkin metinler uzun olmamalı, metinlerde tamamen belirli bir bölgeye özgü jargon kullanılmamalıdır<sup>57</sup>.

<sup>53</sup> **Misek**, s. 73.

<sup>54</sup> **Custers, Bart/van der Hof, Simone/Schermer, Bart/Appleby-Arnold, Sandra/Brockdorff, Noellie**: “Informed Consent in Social Media Use- The Gap Between User Expectations And EU Personal Data Protection Law”, *SCRIPTed: A Journal of Law, Technology And Society*, Vol. 10, I.3, 2013, s. 437.

<sup>55</sup> Veri öznesinin aydınlatıldığından söz edilebilmesi için şu hususlar ölçüt alınabilir: (a) Veri öznesi, neye rıza göstereceğini anlama noktasında yetkinliğe sahip bir yetişkin mi, değilse yasal temsilcisi mevcut mu? (b) Rıza, yazılı olarak alınmış mı? (c) Rıza, akla uygun ve inandırıcı mı? (ç) Rıza, bağımsız bir karar verme sürecinin ürünü mü? (d) Rıza, güncel mi? (e) Hangi verilerin toplanacağı, kullanılacağı ve paylaşılacağı açıkça belirtilmiş mi? (f) Veriler belirli bir amacı gerçekleştirmek üzere toplanmış mı? g) Verileri korumaya yönelik hangi önlemlerin alınacağı açıkça belirtilmiş mi? (h) Verileri işleyen ve verilerin işlenmesinden sorumlu olan kişiler belirli mi? (ı) Veri öznesine tanınan hakların nasıl kullanılacağı belirli mi? (i) Veri öznesine konuya özel ve detaylı bilgi verilmiş mi? (j) Veri öznesine sağlanan bilgi, anlaşılabilir, erişilebilir ve doğru mu? (**Custers/van der Hof/Schermer/Appleby-Arnold/Brockdorff**, s. 438).

<sup>56</sup> Gizlilik politikaları, kişisel verilerin nasıl ve niçin toplanacağı, depolanacağı, kullanılacağı ve ifşa edileceği gibi konularda kullanıcıyı aydınlatan metinlerdir. Bu metinler, veri güvenliği çerçevesinde alınan önlemler ve veri öznesinin hakları gibi konularda bilgiler içermektedir. Temelde amaç, verilerin kullanılmasının yararlarını ve zararlarını tartılabilmek için veri öznesine tanımadır (**Monteleone**, Shara: “Adressing The ‘Failure’ of Informed Consent in Online Data Protection: Learning The Lessons From Behaviour-

Tüzük, bilgilendirme yükümlülüğüne ilişkin olarak ikili bir ayırım yaparak kişisel verilerin “ilgili kişiden elde edildiği” ve “ilgili kişiden elde edilmediği” hâlleri birbirinden farklı düzenlemiştir<sup>58</sup>.

Veri öznesinin bilgilendirilmesinden sonra rıza talebinde bulunulur. Yeni bir veri işleme amacı ortaya çıkarsa, rıza talebinde bulunmadan önce tekrardan bilgilendirme yükümlülüğü ifa edilmelidir<sup>59</sup>.

İnternet ortamında sunulan hizmetler bakımından kullanıcının hizmetten yararlanmasını önemli ölçüde güçleştirecek şekilde rıza talebinde bulunamaz (Tüzük, Giriş Kısmı, Prg. 32). Kullanıcının hizmetlerden faydalandığı esnada aniden ekranda beliren, tüm sayfayı kaplayan, kullanıcıda rahatsızlık uyandıran, hizmetin kalitesini ve verimini düşüren gizlilik politikaları bu konuda olumsuz bir örnektir. Gereğinden fazla uzun ve karmaşık olan bu metinler<sup>60</sup>, kullanıcının kavramasını zorlaştıracak bir formatta sunulmaktadır<sup>61</sup>. Bu yönüyle süreçle ilgili olarak veri öznesine farkındalık kazandırmaktan da oldukça uzaktırlar<sup>62</sup>.

Gizlilik politikalarının uzun ve karmaşık yapısı, veri koruma alanında olumsuz sonuçların doğmasına sebep olmaktadır. Bu metinlerin içeriği, servisi ilk olarak kullanmaya başlayan kullanıcı tarafından ya hiç anlaşılammakta ya da güçlükle anlaşılabilir. Verilerin ne tür amaçlarla kullanılacağını anlayanların sayısı ise gerçekte çok azdır<sup>63</sup>. Bir diğer sorun, bu

---

Aware Regulation”, Syracuse Journal of International Law And Commerce, Vol. 43, I.1, 2015, s. 79).

<sup>57</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 14.

<sup>58</sup> Tüzüğün 13’üncü maddesinde kişisel verilerin ilgili kişiden elde edildiği hâllerde sağlanacak bilgiler, 14’üncü maddesinde ise ilgili kişiden elde edilmediği hâllerde sağlanacak bilgiler gösterilmiştir.

<sup>59</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 17, 18.

<sup>60</sup> **Monteleone**, s. 80; **Solove**, s. 1885. Bir araştırmaya göre, bir akıllı telefondaki 33 tane uygulamanın toplamda 250 bin kelimedenden oluşan gizlilik politikasının bir kullanıcı tarafından okunabilmesi, 24 saati aşan bir süreyi gerektirmektedir. Açık ki, bu tarz metinler, kullanıcıların temel haklarını ve mahremiyetlerini korumaktan oldukça uzaktır (**Lopez**, Santiago Ramirez: “Informing Consent Giving Control Back to The Data Subject From a Behavioral Economics Perspective”, Journal of Intellectual Property, Vol.9, I.1, 2018, s. 39).

<sup>61</sup> **Jarovsky**, s. 448.

<sup>62</sup> **Kuner**, Christopher: European Data Protection Law Corporate Compliance And Regulation, Second Edition, New York 2007, s. 68.

<sup>63</sup> **Staben**, s. 2.



metinlerde gelecekte verilerin nasıl kullanılacağına ilişkin bilgilere yer verilmemesidir<sup>64</sup>.

Veri koruma alanındaki belirsiz düzenlemelerin ve karmaşık metinlerin doğurduğu<sup>65</sup> sonuçlar şunlardır: Kullanıcılar, internette edindikleri kulaktan dolma bilgilerle, karanlıkta yol almaya çalışırlar. Keza, hangi kişisel verinin ne tür amaçla kullanıldığı, kullanıcılar için genellikle karanlıkta kalan bir husustur<sup>66</sup>. Veri koruma hukukundaki spesifik düzenlemeler, bu alandaki terminolojiye hâkim olmayan yeni nesil kullanıcılar tarafından anlaşılabilir<sup>67</sup>.

Tüzüğün 7/2'nci maddesine göre; “*ilgili kişinin rızası başka hususları da kapsayan yazılı bir beyan şeklinde alınacaksa, rıza talebi diğer hususlardan açıkça ayırt edilebilecek şekilde sunulmalı, anlaşılır ve kolayca erişilebilir bir şekilde olmalı, açık ve basit bir dil kullanılmalıdır.*” Tarafların yükümlülüklerine yer veren bir metinde, rıza talebi de yer alıyorsa, bu talebin ilişkili olduğu bölümün diğer bölümlerden açıkça ayırt edilebilecek şekilde sunulması gerekmektedir.

### 3. Konuya Özel Olmalı

Verilerin birden fazla amaçla işlendiği durumlarda bu ölçüt önem kazanmaktadır. Konuya özel bir rızadan söz edilebilmesi için amaçların her biri için veri öznesinden rıza alınması gerekmektedir. Keza gösterilen rıza, veri işleme faaliyetlerini ve amaçlarını tamamen kapsamalı, amaçların her birine nüfuz etmelidir. Farklı faaliyetler ve amaçlar ayrı ayrı değerlendirilmeli, veri öznesi bunlardan bir kısmına rıza gösterip, diğerlerine rıza göstermekten kaçınabilmelidir<sup>68</sup>. Rıza gösterilmesi talep edilen husus, somut bir şekilde tanımlanmış olmalıdır. Kişisel verilerin tamamının işlenmesine sınırsız olarak rıza gösterilmesi geçersizdir<sup>69</sup>.

Bir şirket, film izleme alışkanlıklarına dayalı olarak yeni film önerileri sunmak için abonelerinin kişisel verilerini, rızaları dâhilinde toplamaktadır.

<sup>64</sup> Solove, s. 1885.

<sup>65</sup> Gizlilik politikasına ilişkin metinlerin sadeleştirilmesi tavsiye edilmektedir. Ancak Solove'a göre, bu tavsiyeler, temel bir çelişkiyi gözden kaçırmaktadır. Önemli olan, süreç hakkında veri öznesinin derin bir anlayışa ulaşmasını sağlamaktır, oysa metinleri sadeleştirmek bu amacın gerçekleştirilmesini zorlaştıracaktır (Solove, s. 1885, 1886).

<sup>66</sup> Staben, s. 2.

<sup>67</sup> Staben, s. 2, 3. Yine, kullanım şartlarına ilişkin metinleri okumak konusundaki tembelik de buna eklenince bireyin bilgilerinin geleceğini belirlemesi mümkün olmamaktadır (Staben, s. 2, 3).

<sup>68</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 10.

<sup>69</sup> Misek, s. 73; Küzeci, s. 241.

Daha sonra şirket, reklamcılık faaliyetlerinde kullanılması için üçüncü kişilere bu film tercihlerini göndermek ister. Yeni amaç dikkate alındığında, yeni bir rıza talep edilmesi zorunludur<sup>70</sup>. Verilerin üçüncü kişilerle paylaşılması sonradan gündeme geldiğinde, veri öznesinden ayrı ve ek bir rıza talep edilmesi gerekmektedir<sup>71</sup>.

Rızanın konuya özel olması ile özgür iradeye dayanması, bir zincirin halkalarını oluşturmaktadır. Bazı durumlarda veri sorumlusu, birden fazla faaliyet ve süreç için veri öznesini toptan bir rıza açıklamasına zorlayabilir<sup>72</sup>. Tüzüğe göre, farklı veri işleme faaliyetlerine ayrı ayrı rıza gösterme imkânı tanınmamışsa, rızanın özgür iradeye dayanmadığı söylenebilir (Tüzük, Giriş Kısmı, Prg. 43). Bu tip durumlarda, rıza açıklamasının konuya özel olduğundan da söz edilemez. Örneğin, kişisel verileri, ticari ortaklarıyla paylaşmak isteyen veri sorumlusunun toptan bir rıza talebinde bulunması, Tüzük hükümlerine uygun değildir. Her bir ticari ortağın kimliğine ilişkin bilgiler, veriler toplanmadan önce müşteri ile paylaşılmalı, veriler her bir ortağa benzer amaçlarla aktarılmalıdır<sup>73</sup>.

Kişisel veriler, belirli amaçlar için toplanmalı ve bu amaçlara uygun olmayacak şekillerde işlenmemelidir (Tüzük m.5/1-b). Konuya özel olma şartı da bu çerçevede ele alınmalıdır. Bedava akaryakıt kampanyası için e-posta bilgilerini toplayan bir akaryakıt şirketi, bu bilgileri kampanya konusuyla sınırlı olarak kullanabilir. Üçüncü kişilerle bu bilgileri paylaşmak arzusunda olan şirket, müşterilerden ayrıca bir rıza talep etmelidir. Zira müşteriler, bilgilerini kampanya amacıyla sınırlı olarak vermişlerdir. Hemen belirtelim ki, verilerin işlenmesini “konu” yönünden sınırlamak, işleme faaliyetinin süresini de belirleyecektir. Yukarıdaki örnek özelinde, veri işleme faaliyeti, kampanyanın bitimiyle beraber sona erecektir. Taraflar arasında belirlenmemiş olsa dahi, kişisel verilerin işlenmesinde belirli sürelerin bulunması kaçınılmazdır.

Kaç kilometre koştuğunu veya kaç kalori yaktığını öğrenmek isteyen kullanıcılara hitap eden çeşitli uygulamalar bulunmaktadır. Bunlar, genellikle Quantified-self (QS) olarak adlandırılmaktadır<sup>74</sup>. QS uygulamaları,

<sup>70</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 12.

<sup>71</sup> Article 29 Working Party, **Opinion 15/2011 on The Definition of Consent**, s. 18.

<sup>72</sup> **Çekin**, s. 60.

<sup>73</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 10.

<sup>74</sup> Quantified Self, özetle “*sayılar vasıtasıyla kendini tanıma*” olarak tanımlanabilir. QS uygulamaları, bireylerin sağlığına, ruhsal durumuna ve kişisel amaçlarına hitap eden çeşitli yöntemler kullanmaktadır. (Reijneveld, Minke D.: “Quantified Self, Freedom,

kullanıcıların birbirlerini kıyaslamalarına imkân veren bir yapıya sahiptir; bu yönüyle söz gelimi, bir kullanıcının kaç kilometre koştuğu bilgisi, diğer kullanıcılarla paylaşılmaktadır. Bu husus da “konuya özel olma” şartı bakımından sakıncalar doğurmaktadır. QS uygulamasını kullanan kişi, sırf bu sebeple, verilerinin kıyaslama veya reklamcılık gibi amaçlarla işlenmesine rıza göstermiş değildir<sup>75</sup>. Uygulamanın verilerin hangi amaçlarla işleneceği hususunda kullanıcıyı bilgilendirmesi, ardından her bir amaca ilişkin olarak ayrı bir rıza talebinde bulunması gerekmektedir.

#### 4. Veri Öznesinin İsteklerinin Kesin Bir Göstergesi Olmalı

Veri öznesinin kesin olarak rıza gösterdiğinden söz edilebilmesi için öncelikle beyanın nasıl açığa vurulduğu incelenmelidir. Tüzük, bu noktada “beyan” ve “açık onaylayıcı eylem” şeklinde ikili bir ayırım yapmıştır: Beyanın niteliğine ilişkin Tüzükte bir hüküm olmadığından, “sözlü” beyan da geçerli kabul edilebilir. Önemli olan, rıza açıklamasının veri öznesinin isteklerini, belirsizlik içermeyecek biçimde açığa vurmasıdır. Otel görevlisi, promosyonlarla ilgili bilgi vermek için müşteriden e-posta adresini talep eder. Görevli tarafından yeterince bilgilendirildikten sonra e-posta adresini paylaşan müşteri, sözlü olarak geçerli bir rıza açıklamasında bulunmuştur<sup>76</sup>. Ancak veri sorumlusu, rıza verildiğini kanıtlamakla yükümlüdür (m.7). Bu sebeple kanıtlamanın daha kolay olacağı mekanizmaları seçebilir.

Bilinçli şekilde gerçekleştirdiği davranışlar sonucunda, belirli bir veri işleme faaliyetine rıza gösterdiği anlaşılan veri öznesi, “onaylayıcı eylem” ile iradesini göstermiş demektir. Onaylayıcı eylemin, sözlü veya yazılı beyan niteliği taşımayan davranışlar olarak anlaşılması gerekmektedir. Kullanıcının açık ve aktif bir hareketi, rızanın kesin olarak gösterildiğini ortaya koymalıdır. Bilgisayara bir yazılım yüklendiğinde, uygulama, çökme raporlarını (crash reports), yazılımı geliştirmek amacıyla kullanmak ister. Veri öznesi, kendisine sunulan kutucuktaki “rıza gösteriyorum” ifadesini işaretlediği zaman, onaylayıcı eylemle rıza göstermiştir<sup>77</sup>.

Belirli bir hareketin yapılmasının onaylayıcı eylem olarak kabul edileceği veri sorumlusu tarafından pekâlâ belirlenebilir. Ancak bu hareketlerin,

---

And The GDPR”, SCRIPTed: A Journal of Law, Technology And Society, Vol. 14, I.2, 2017, s. 291 vd).

<sup>75</sup> Reijneveld, s. 302.

<sup>76</sup> Örnek için bkz. Article 29 Working Party, **Opinion 15/2011 on The Definition of Consent**, s. 22.

<sup>77</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 16.

karişıklığa yer vermeyecek özellikler içermesi, Tüzük hükümleri gereğince şarttır. Söz gelimi, kullanıcının sadece ekran üzerinde parmağını hareket ettirmesi, her durumda rıza anlamına gelmeyebilir. Zira akıllı telefon kullanıcısının bu hareketi, başka bir amaçla yapması da imkân dâhilindedir. Bu tarz eylemler, yanlış anlaşılmaya müsait yapıları sebebiyle “belirsizliğe mahal vermeme” şartı bakımından sakıncalar doğurabilir. Veri öznesi için “anlaşılabilir ve açık olma”, onaylayıcı eylem belirlemek noktasında veri sorumlusuna tanınan serbestliğin sınırını çizmektedir<sup>78</sup>.

Sadece bir internet sitesinin kullanılması, bir sitede uzun süre kalınması ya da salt bir servis üzerinde işlem yapılması, belirli bir veri işleme faaliyetine rıza gösterildiği şeklinde yorumlanamaz<sup>79</sup>. Örneğin, canlı olarak oynanan bir oyuna giriş yapan kullanıcılardan, ad, yaş, adres gibi bilgilerini paylaşması talep edilir. İnternet sitesi bir bağlantı vasıtasıyla erişilebilen bir bildiri yayımlar. Bildiride siteyi kullanan kişilerin üçüncü kişilere ve oyunun servis sağlayıcılarına pazarlama amacıyla kişisel veri gönderilmesine rıza göstermiş sayılacakları açıklanır. Bir oyuna katılmak, bunun dışındaki amaçlar için rıza gösterildiği anlamına gelmez. Örnekte, şüpheye yer vermeyecek kesinlikte bir rıza alınmış değildir<sup>80</sup>.

Uygulamada opt-in ve opt-out yöntemleri kullanılarak kullanıcıdan rıza talep edildiği görülmektedir. Bu yöntemlere pek çok şirketten pazarlama faaliyetleri kapsamında gönderilen e-postalar örnek verilebilir. E-postada “*bu iletileri istemiyorsanız aşağıdaki kutuyu işaretleyiniz*” şeklindeki bir ibare varsa, bu “opt-out” yöntemine örnek oluşturabilir. Şirketler günümüzde veri alışveriş yaparak çeşitli menfaatler elde etmeyi amaçlamaktadır. Bir şirket; “*sizin tercihlerinize uygun fırsat ve seçenekler sunması için bilgilerinizi X şirketi ile paylaşmamıza izin veriyorsanız aşağıdaki kutucuğu işaretleyiniz*” şeklinde bir e-posta gönderiyorsa “opt-in” yöntemi uygulamıştır<sup>81</sup>.

İşleme faaliyetine rıza göstermek istemeyen kullanıcının halihazırda işaretli olan kutucuktaki işareti kaldırması bekleniyorsa, bu da opt-out yöntemi uygulandığının göstergesidir<sup>82</sup>. Rıza göstermeyen kullanıcıyı aktif bir

<sup>78</sup> Benzer Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 17.

<sup>79</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 16, 17.

<sup>80</sup> Örnek için bkz. Article 29 Working Party, **Opinion 15/2011 on The Definition of Consent**, s. 23.

<sup>81</sup> Örnek için bkz. **Küzeci**, s. 243.

<sup>82</sup> **Çekin**, s.55-56, dn. 133; Benzer **Korkmaz**, s. 151, 152.

harekete zorlayan opt-out yöntemi, kişisel verilerin korunmasını zayıflatan bir niteliğe sahiptir<sup>83</sup>. Zira opt-out yönteminde sessiz kalan kullanıcı, verilerin işlenmesine rıza göstermiş demektir.

Tüzükte internet ortamında da rıza verilmesinin mümkün olduğu ifade edilmiş, bu bağlamda, kutucukların tıklanması yeterli kabul edilmiş, ancak önceden tıklanmış kutucuktaki işareti kaldırmayarak hareketsiz kalmanın rıza anlamına gelmeyeceği belirtilmiştir (Giriş Kısmı, Prg. 32). Başka bir deyişle, Tüzük, opt-out yöntemine kapıları kapatmıştır. Keza, opt-out yöntemi, onaylayıcı eylem kabul ederek veri öznesinin rıza gösterdiği sonucuna ulaşmak da mümkün değildir<sup>84</sup>. Opt-out yönteminde veri öznesi, rıza gösteriyorsa değil, rıza göstermiyorsa bilinçli, aktif bir harekette bulunmalıdır. Esasen rıza göstermek istemeyen, belki de rıza göstermek gibi bir düşüncesi hiç olmayan veri öznesine aktif bir hareket adeta dayatılmaktadır.

Doktrinde *Solove*'a göre, opt-in yöntemi, uzun vadede başarısız olacaktır. Opt-in yönteminde daha fazla "tıklama" faaliyeti ve form doldurma işlemi gerçekleştirilecek, ancak verilerin daha makul şekilde korunması mümkün olmayacaktır. Yazara göre, opt-in yöntemi ve onaylayıcı eylemle rıza talebinde bulunulması oldukça maliyetli olduğundan, uzun vadede şirketleri veri işleme faaliyetlerinden uzak durmaya yöneltecektir. Opt-in ve onaylayıcı eylem vb. faaliyetlerin şekilci yaklaşımı, yararlı/zararlı veri kullanımlarını birbirinden ayırt etmeyi oldukça zorlaştırmaktadır. Yazar, daha az veri toplamayı ve kullanmayı her durumda başarı olarak görenleri, veri kullanımının faydalı olduğu durumlarda ortada bir başarı bulunmadığını savunarak eleştirmektedir. Keza, yazara göre, opt-in yönteminin masraflı olduğunu gözeten veri sorumluları, verilerin gelecekte nasıl kullanılacağına ilişkin belirsiz ve açık uçlu bilgiler vererek tekrar tekrar rıza istemekten sakınmayı da tercih edebilir<sup>85</sup>.

Öte yandan, *Solove*, opt-out yönteminin de seçenekler konusundaki farkındalığı azalttığına işaret etmektedir. Yazara göre, opt-out, meşru olmayan bir yöntem olmamakla birlikte belirsizliğe mahal veren bir yapıya sahiptir. Nihayetinde yazar, opt-in yönteminin verilerin nasıl kullanılacağı ve ifşa edileceği gibi konularda veri öznesini daha farkında olmaya sevk ettiğini, opt-out yönteminin ise böyle bir etkiye sahip olmadığını kabul etmektedir<sup>86</sup>.

<sup>83</sup> **Küzeci**, s. 243, 244.

<sup>84</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 16.

<sup>85</sup> **Solove**, s. 1898, 1899.

<sup>86</sup> **Solove**, s. 1899.

Rızanın geçerli kabul edilebilmesi için aranan şartlar, Direktife nazaran, Tüzükte daha katı bir perspektifle ele alınmıştır. Rızanın tanımlandığı 2'nci madde göz önüne alındığında; Direktifin genel olarak opt-in mi yoksa opt-out mu yönteminin benimsenmesi gerektiğine ilişkin bir düzenlemeye yer vermediği anlaşılmaktadır<sup>87</sup>. Ancak Direktifin 14'üncü maddesi bu konuda istisnadır. Buna göre, doğrudan pazarlamaya ilişkin konularda “opt-out” yöntemi standart olarak benimsenmiştir. Bütün bu düzenlemeler, Direktifin genel hususlarda, opt-in yöntemini bir gereklilik olarak görmediğini ortaya koymaktadır<sup>88</sup>.

Veri öznesi, rıza gösterme iradesini aktif şekilde ifade etmedikçe, geçerli bir rıza beyanından söz edilemez. Örneğin, iş hayatında işçinin elektronik cihazlarında varsayılan ayarların bulunması veya işçi tarafından bir yazılımın yüklenmesi, tek başına rızanın varlığını göstermez<sup>89</sup>.

Susma, kural olarak talebin reddi anlamına gelse de, mevzuat tarafından ilgili kişinin susmasının kabul olarak değerlendirildiği durumlar bulunmaktadır. Ancak salt susmanın kabul olarak yorumlanması, kişisel veri hukukuna yabancıdır<sup>90</sup>. Sosyal medyada kullanıcının müdahalesi olmaksızın belirlenen varsayılan gizlilik ayarlarında “arkadaşların arkadaşları” kutucuğu işaretliyse, kişisel veriler, bu kişiler tarafından görülebilir. Bu seçenekten memnun olmayan veri öznesinin kutucuğu değiştirmek suretiyle ayarlara müdahale etmesi mümkündür. Ancak kendisinin katılımı olmaksızın belirlenen ayarlara müdahale etmeyen kullanıcının rıza gösterdiği varsayılmaktadır. Aktif bir davranış söz konusu olmadığı için bu husus, Tüzük hükümlerine aykırıdır<sup>91</sup>.

## B. Açık Rıza İle Rıza Kavramlarının Karşılaştırılması

Direktifte ve Tüzükte açık rıza ve rıza kavramlarının kullanılması, yerine göre farklı sonuçların doğmasına sebep olmaktadır. Direktifte hassas olmayan kişisel veriler için rıza yeterli kabul edilirken; hassas kişisel veriler için açık rıza aranmaktadır (m.8/2). Direktif kapsamında ele alındığında; “açık rıza” ile “rıza” arasındaki birtakım farklar bulunmaktadır. Söz gelimi,

<sup>87</sup> Kuner, s. 68.

<sup>88</sup> Kuner, s. 68.

<sup>89</sup> Bkz. Article 29 Working Party, **Opinion 2/2017 on Data Processing at Work**, 8/6/2017, s. 7.

<sup>90</sup> Kuner, s. 69.

<sup>91</sup> Örnek için bkz. Article 29 Working Party, **Opinion 15/2011 on The Definition of Consent**, s. 24.

kullanıcının hareketsiz kalmasına bir sonuç bağlayan opt-out yöntemi, Direktifte rızanın arandığı durumlar bakımından geçerli kabul edilirken; açık rızanın arandığı hassas kişisel verilerin işlenmesinde ise opt-out yönteminin kabul edilemeyeceği belirtilmektedir<sup>92</sup>. Buna karşılık, Tüzük, hassas olmayan kişisel veri/hassas kişisel veri ayrımı yapmadan, opt-out yöntemini reddetmektedir (Giriş Kısmı, Prg. 32).

Çalışmada belirtildiği üzere, veri öznesinin susması, belirli bir veri işleme faaliyetine rıza gösterdiği şeklinde yorumlanamaz. Ancak susmayı destekleyen birtakım emarelerin bulunması durumunda geçerli bir rıza açıklamasının bulunduğu söylenebilir mi? Bu konuda rızanın veya açık rızanın arandığı durumlar için Direktif kapsamında bir ayırım yapılması mümkündür.

Doktrinde Direktifi değerlendiren yazarlar, tek başına susma veya hareketsizliğin rıza olarak yorumlanamayacağını, ancak susmayı destekleyen birtakım emarelerin var olması durumunda geçerli bir rızanın mevcut olabileceğini ifade etmişlerdir. Bu görüşe göre, halihazırda sessiz kalan veri öznesi, önceden bazı aktif hareketler gerçekleştirerek rıza gösterdiğini ortaya koymuşsa, geçerli bir rızadan söz edilebilir<sup>93</sup>. Bir görüş ise, açık rıza aranan hassas kişisel verilerin işlenmesinde rızanın açık bir şekilde ortaya koyulması gerektiğini, örtülü şekilde ifade edilen rızanın geçerli kabul edilemeyeceğini savunmaktadır<sup>94</sup>.

Kanaatimizce, Direktif bakımından bu görüşler geçerli kabul edilebilirse de Tüzük bakımından aynısını söylemek güçtür. Direktif ile benzer şekilde Tüzük, hassas olmayan kişisel verilerin işlenmesinde rızayı yeterli kabul ederken (m. 6/1-a), hassas kişisel verilerin işlenmesinde ise açık rızanın varlığını aramaktadır (m.9/2- a). Buna karşılık Direktiften farklı olarak Tüzükte rızanın “*beyan veya açık onaylayıcı eylemle*” açıklanabileceği ifade edilmiştir. Açık onaylayıcı eylem, sözlü veya yazılı beyan dışında kalan, aktif hareketler şeklinde anlaşılmalıdır. Her ne kadar, beyanın açık olması gerektiğine ilişkin bir ifadeye yer verilmese de, onaylayıcı eylemin “açık” olması aranmaktadır. Onaylayıcı eylem için geçerli olan bu hususun beyan için geçerli olmadığını söylemek mümkün değildir.

Tüzük, veri öznesinin aktif şekilde rıza açıklamasında bulunmasını aramaktadır. Direktiften farklı olarak Tüzükte opt-out yöntemine kapıların kapatılması, bu hususu doğrulamaktadır. Halihazırda sessiz kalan veri özne-

<sup>92</sup> Article 29 Working Party, **Working Document on The Processing of Personal Data Relating to Health in Electronic Health Records**, 15/2/2007, s. 9.

<sup>93</sup> **Kuner**, s. 69.

<sup>94</sup> Bkz. **Başalp**, s. 40.

sinin önceden birtakım aktif hareketler gerçekleştirdiğinden bahisle rıza gösterdiğini söylemek de güçtür. Bu konuda şu örnek verilebilir: Telefon numarasının işlenmesine başta rıza gösteren kullanıcıya iki ay sonra aynı talep iletilir, ancak kullanıcı sessiz kalır. Tüzük esas alındığında; bu noktada susmayı destekleyen birtakım emareler bulunduğundan bahisle rıza gösterildiği sonucuna ulaşılamaz.

Direktifte açık rızanın arandığı durumlarda açık bir irade beyanının var olması gerektiği ve opt-out yönteminin uygulanamayacağı belirtilmişti. Rızanın arandığı durumlarda ise böyle bir sınırlamaya gidilmemiştir. Tüzük ise her durumda opt-out yöntemini reddetmekte, veri öznesinin aktif ve açık şekilde rıza açıklamasını beklemektedir. Özetle, Tüzükte ve Direktifte açık rıza ve rıza kavramlarına yüklenen anlam ve bu ayrımın doğurduğu sonuçlar birbirinden farklıdır.

Kanaatimizce, Tüzük koyucu, açık rıza kavramını kişisel verilerin işlenmesinde daha yüksek bir korumaya işaret etmek için kullanmıştır. Açık rızanın arandığı durumlarda Tüzük, verileri işleyen veya veri ihlallerini değerlendiren makamları dikkatli olmaya sevk etmekte, bu makamların titiz davranmasını beklemektedir.

### C. Rıza İle Diğer Hukuka Uygunluk Sebepleri Arasındaki İlişki

Kişisel verilerin işlenmesini hukuka uygun kılan tek sebep, rıza değildir. Rıza dışındaki sebeplerin uygulama alanı varsa, ayrıca rızaya dayanılması gerekmez. Ancak rıza dışında pek çok sebebin bulunması, bunların geniş olarak uygulanmaya imkân veren yapısı rızanın uygulama alanını oldukça sınırlandırmaktadır<sup>95</sup>. Diğer hukuka uygunluk sebeplerinin geniş olarak yorumlanması, rızaya dayanmadan verilerin işlenmesini mümkün kılarak kontrol prensibinin göz ardı edilmesine sebep olmaktadır. Keza veri sorumlusu, rıza dışındaki hukuka uygunluk sebeplerini tercih etmeye eğilimlidir.

Veri işlemek, bir sözleşmenin ifası için gerekliyse, veri sorumlusu Tüzük m.6/1-b'ye dayanabilir, ayrıca rıza talebinde bulunması şart değildir. Örneğin, sınır aşan para transferinde bankalara verilen havale emrinin yerine getirilmesi için kişisel verilerin işlenmesi zorunluluk arz eder<sup>96</sup>. Banka hesap numarası, ad ve soyad gibi kişisel verilerinin üçüncü kişilerle paylaşılmasını istemeyen bir kişi, bankadan para gönderemeyecektir.

<sup>95</sup> Küzeci, s. 238.

<sup>96</sup> Başalp, s. 39.



Sözleşmenin ifası için veri işlemek gerekliyse, veri sorumlusunun ayrıca rıza talebinde bulunmasının gereksiz olduğu savunulmaktadır. Keza bu görüşe göre, olayda başka bir hukuka uygunluk sebebi bulunduğundan, veri öznesi, rızasını geri alabileceğini düşünüp yanılabilir<sup>97</sup>. Bizce, taraflar arasında güç dengesizliği yoksa, başkaca hukuka uygunluk sebepleri bulunsa dahi, rızaya dayanılmasında olağandışı bir durum yoktur. Rızaya dayanılmasının gerekli olması ile zorunlu olması birbirinden farklı konulardır. Söz gelimi iki tane hukuka uygunluk sebebi varsa, veri sorumlusu tercihen bunlardan birine dayanabilir. Ancak, veri sorumlusu, hangi hukuka uygunluk sebebine dayanmışsa, bunun şartlarının oluştuğunu gözetmeli ve yeri geldiğinde hukuka uygun bir işleme faaliyeti bulunduğunu kanıtlamalıdır (Tüzük m.7). Örneğin, sözleşmenin ifası için gerekli olan bir işleme faaliyeti bulunsa dahi, veri sorumlusu, işleme faaliyetini sağlam bir zemine oturtmak ve zamanı geldiğinde hesap verebilmek için veri öznesinden rıza talep edebilir. Hemen belirtelim ki, hukuka uygunluk sebeplerinin var olup olmadığı sırayla değerlendirilmelidir. Rızaya dayanan veri sorumlusu, konuya özel, aydınlatılmış, özgür iradeye dayanan bir rıza elde etmelidir. Rıza gösterildikten sonra rızanın geri alınmasına da engel bir durum yoktur. Her nasılsa, veri öznesi, başta verdiği rızayı geri alırsa, veri sorumlusu, uygulama alanı bulunan diğer sebepleri gözetip verileri işleyebilir. Özetle, veri öznesi rızasını geri alabileceği gibi veri sorumlusu da diğer hukuka uygunluk sebeplerine dayanabilir. Rızasını geri alan veri öznesi, bazen veri sorumlusunu, işlemenin hukuka uygunluğu konusunda düşünmeye sevk eder, veri sorumlusunun özdenetim gerçekleştirilmesini sağlayabilir.

Hassas kişisel verilerin işlenmesini hukuka uygun kılan tek sebep de açık rıza değildir. Örneğin, komada olduğu için sağlık bilgilerinin başka bir yere gönderilmesine rıza gösteremeyen kişinin hayatı menfaatlerini korumak için işleme gerekliyse, rızaya dayanılması şart değildir (Tüzük m.9/2-c).

Veri öznesi tarafından açıkça aleni hâle getirilen kişisel veriler<sup>98</sup>, açık rıza gerekmeksizin işlenebilir (Tüzük m.9/2-e). Bizce bu hukuka uygunluk sebebi, rızadan ayrı olarak düşünülemez. Esasen bilgilerini bizzat aleni hâle

<sup>97</sup> Görüşler hakkında bilgi için bkz. **Çekin**, s. 64.

<sup>98</sup> Hassas olmayan kişisel verilerin veri sahibi tarafından alenileştirilmesi, Kanunda hukuka uygunluk sebebi olarak düzenlenmiştir (m.5/2-d). Söz gelimi, sosyal medya profilinde kullanılan herkese açık bir fotoğrafın başkaları tarafından görülmesinde bir sakınca yoktur. Bununla birlikte, alenileşen bilginin farklı şekillerde kullanılması, bazı durumlarda, kişilik haklarına aykırılık teşkil eder. Yukarıdaki örnekte, fotoğraf üzerinde birtakım değişiklikler yapılması veri öznesinin kişilik haklarını ihlal edebilir. Bkz. **Develioğlu**, s.59.

getiren kişinin belirli işleme faaliyetlerine rıza gösterdiği varsayılmakta, bu husus da ayrı bir hukuka uygunluk sebebi kabul edilmektedir. Söz gelimi, kişinin cinsel eğilimlerini yansıtan bilgiler, hassas kişisel veri teşkil eder (Tüzük m.9/1). Cinsel eğilime ilişkin bir bilgiyi, sosyal medyada herkese açık profilden edinen üçüncü bir kişinin, bunu bir başkasına aktarmasında Tüzük m.9/2-e'ye göre bir hukuka aykırılık yoktur. Ancak aleni hâle getirilen bir bilginin her türlü amaçla kullanılması hukuka uygun olmayabilir. Rıza gösterildiği varsayılan işleme faaliyetlerinin sınırı iyi çizilmelidir. Bizce bizzat sahibi tarafından alenileştirilen cinsel eğilime ilişkin bilgilerin, devlet arşivlerinde veya şirket kayıtlarında tutulması, kamuya ilişkin bir menfaatle bağdaşmaz, veri öznesinin kişilik hakkını da ihlal edebilir.

#### D. Veri İşlemenin Rızaya Dayanmasının Uygun Olmadığı Durumlar

Tüzüğün 7/4'üncü maddesine göre; sözleşmenin ifası veya bir hizmetin sunulması için gerekli olmayan bir veri işleme faaliyetine rıza gösterilmesi, sözleşmenin ifa edilmesi veya hizmetin sunulması için şart koşuluyorsa, rızanın serbestçe verilip verilmediği değerlendirilirken bu konu da dikkate alınmalıdır. Tüzük, veri ihlallerini değerlendiren makamın bu hususta “*azami dikkat*” göstermesini bekler (m.7/4). Sağlık hizmetlerinin sunulması için gerekli olmamasına rağmen, cinsel bilgilerin işlenmesi için hastadan rıza talep edilirse, rızanın özgür iradeye dayandığı tespit edilirken bu konu özellikle araştırılmalıdır. Zira hekim-hasta arasında bir nevi, bağımlılık ilişkisi vardır; rıza göstermeyen hasta, sağlık hizmetlerinden gereği gibi yararlanamayacağından endişe edebilir.

Taraflar arasında hiyerarşinin ve güç dengesizliğinin bulunduğu durumlarda, (söz gelimi veri sorumlusu kamu kurumuyorsa) rızanın özgür iradeye dayandığını söylemek pek mümkün değildir (Tüzük, Giriş Kısmı, Prg. 43)<sup>99</sup>. Bu tip durumlarda, veri sorumlusu, genellikle şartları varsa, rıza dışındaki hukuka uygunluk sebeplerine dayanmalıdır.

Veri öznesi ile veri sorumlusu arasındaki güç dengesizliğine, işçi-işveren ilişkileri örnek verilebilir. İşçi ve işveren arasındaki bağımlılık ilişkisi, rıza beyanına şüpheyle yaklaşılmasına sebep olabilir<sup>100</sup>. İşçi, rıza göstermeyi reddettiğinde bu hususun aleyhine kullanılacağından endişe edebilir<sup>101</sup>. İşverenin işçiye karşı tutumunun değerlendirilmesine ilişkin bir form, işçi

<sup>99</sup> Ayrıca bkz. **Develioğlu**, s. 54; **Çekin**, s. 61.

<sup>100</sup> **Kuner**, s. 68.

<sup>101</sup> **Bergkamp/Dohnt**, s. 77.

tarafından genellikle baskıya maruz kalmadan, korkusuz bir şekilde doldurulamaz. Keza işyerinde gözetleme sistemlerinin kurulmasına rıza gösteren bir işçinin özgür iradesiyle hareket ettiğini söylemek çoğu zaman mümkün olmayacaktır<sup>102</sup>.

Belirttiğimiz sebeplerle, işçi-işveren ilişkilerinin çoğunda işverenin rıza dışındaki hukuka uygunluk sebeplerine dayanması tavsiye edilmektedir<sup>103</sup>. İşveren, şartlarının oluşması durumunda, sözleşmenin ifası için gerekli olma (Tüzük m.7-b), işveren tarafından uygulanması gereken yasal zorunlulukların veri işlemeyi gerektirmesi (Tüzük m.7-c) ve işverenin meşru menfaatlerinin varlığı (Tüzük m.7-f) hukuka uygunluk sebeplerine dayanabilir<sup>104</sup>. Söz gelimi işçinin maaşının ödenmesi için banka hesap bilgilerinin işlenmesi, sözleşmenin ifası için gereklidir, ayrıca işçiden rıza alınması gerekmez<sup>105</sup>.

İşveren, mevzuat tarafından işe giriş-çıkış bildirgeleri hazırlamak ve özlük dosyası tutmakla yükümlü tutulmuş olabilir. Özlük dosyasında genel olarak, işçinin işyerinde çalışması için gerekli olan belgeler ile<sup>106</sup> işçinin işe yatkınlığı ve verimiyle ilgili bilgiler yer alır. Veri sorumlusunun tabi olduğu hukuki bir yükümlülüğe uyulması veyahut sözleşmenin ifa edilmesi için<sup>107</sup> gerekliyse rıza aranmaksızın veriler işlenebilir. İşçinin ikametgâh belgesi, askerlik durum belgesi, sürücü belgesi, personel evliyse eş ve çocuklarına ilişkin nüfus cüzdanı örneği, vergi numarası gibi belgelerin özlük dosyasında yer alması gerekmektedir<sup>108</sup>. İşveren tarafından bu bilgi ve belgelere dosyada yer verilmesi, veri sorumlusunun tabi olduğu bir yükümlülüğe uyulmasıyla yakından ilişkilidir.

İşverenin kendi dünya görüşüne uygun olmayanları işten çıkarmak amacıyla, siyasi görüşlere veya cinsel eğilimlere ilişkin bilgileri toplaması

<sup>102</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 7.

<sup>103</sup> Küzeci, s. 240; Article 29 Working Party, **Opinion 2/2017 on Data Processing at Work**, s. 6, 7.

<sup>104</sup> Bilgi için bkz. Article 29 Working Party, **Opinion 2/2017 on Data Processing at Work**, s. 6 vd.

<sup>105</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 8. Sözleşmenin ifası ile verilerin işlenmesi arasında doğrudan ve objektif bir bağlantı bulunmalıdır (Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 8).

<sup>106</sup> Aydın, **Ufuk: “İşverenin İşçi Özlük Dosyası Tutma Yükümü”**, İş Hukuku ve Sosyal Güvenlik Hukuku Türk Milli Komitesi 30. Yıl Armağanı, Ankara 2006, s. 494.

<sup>107</sup> Tüzükte “sözleşmenin ifası için veri işlemenin gerekli olması”, hassas kişisel verilerin işlenmesinde bir hukuka uygunluk sebebi olarak düzenlenmemiştir. Bkz. Tüzük m.9.

<sup>108</sup> Aydın, s. 493.

ise hukuka uygun değildir. “İşleme faaliyeti, veri sorumlusunun, iş ve sosyal sigorta ve güvenlik hukuku alanlarındaki yükümlülüklerinin yerine getirilmesi ve belirli haklarının kullanılması için gerekliyse” bahsi geçen verilerin işlenebileceğini öngören<sup>109</sup> hukuka uygunluk sebebinin şartları bu örnekte oluşmamıştır. İşte, işleme faaliyetini hukuka uygun kılan sebeplerin gerçekleşmediğini fark eden işveren, hiyerarşisini kötüye kullanarak işçinin rıza göstermesini sağlayabilir. Bu örnek özelinde de rızadan kaynaklı olarak verilerin işlenmesi, işçinin aleyhinedir.

İş ilişkilerinde, ancak işçinin gerçek bir seçim şansına sahip olduğu ve herhangi bir zarara uğramadan rızasını geri alabileceği durumlarda rızaya dayanılması gerektiği ifade edilmektedir<sup>110</sup>. Rızanın geçerliliği irdelenirken, bir zarara maruz kalıp kalmama ölçütünün özellikle göz önünde tutulması gerekmektedir. Zayıf konumda olan tarafa zarara uğramayacağı konusunda birtakım ek güvenceler verilmesi, rızanın geçerliliği için şart olabilir<sup>111</sup>. İşini kaybetmeyeceği veya çalışma koşulları daha ağır bir bölüme gönderilmeyeceği konularında işçiye garanti verilebilir.

Film çekiminde çalışan personelin ekranın arka planında görünmesi muhtemel olduğu için, işveren çekime katılanlardan bu hususta rıza talep eder. Rıza göstermeyenler, herhangi bir şekilde cezalandırılmaz; film çekimi sürerken eşdeğer başka bir bölümde çalıştırılır. Örnekte geçerli bir rıza beyanı bulunmaktadır<sup>112</sup>.

Kamuya ilişkin menfaatlerin ağır bastığı hâller, bir diğer örnektir. Söz gelimi yetkilerle donatılmış kamusal otoritelerin işlemede rızaya dayanması, kural olarak meşru kabul edilmez<sup>113</sup>. Örneğin, şüphelilerin vücudundan hangi hâllerde örnek alınabileceği mevzuatta gösterilmiştir. Hemen belirtelim ki, adli makamın bu noktada dayanması gereken hukuka uygunluk sebebi rıza değildir. Tüzüğün “Cezai Hükümler ve Suçlarla İlgili Kişisel Verilerin İşlenmesi” başlıklı 10’uncu maddesinde bu konuda özel bir düzenleme yer almaktadır. Buna göre, üye devlet, ilgili kişinin hak ve özgürlük-

<sup>109</sup> Siyasi görüşlere ve cinsel eğilimlere ilişkin bilgiler, Tüzükte hassas kişisel veri kategorisinde sayılmıştır. Bu verilerin hangi şartlarda işlenebileceğini tespit etmek için Tüzüğün 9-b maddesine gidilmelidir.

<sup>110</sup> Article 29 Working Party, **Opinion on The Processing of Personal Data in The Employment Context**, 13/9/2001, s. 23.

<sup>111</sup> **Bergkamp/Dohnt**, s. 77 vd.

<sup>112</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 7. Türk hukukunda işçinin çalıştığı yerin değiştirilmesi, esaslı değişiklik kabul ediliyorsa, ayrıca 4857 Sayılı İş Kanununun 22’nci maddesi de dikkate alınmalıdır.

<sup>113</sup> Article 29 Working Party, **Opinion 15/2011 on The Definition of Consent**, s. 15, 16.

lerinin korunmasına yönelik uygun güvenceler getiren birtakım düzenlemeler ile resmi makamlara cezai hükümler veya suçlarla ilgili verileri işleme yetkisi verebilecektir. Dolayısıyla vücuttan örnek alınması, üye devletin mevzuatında öngörülen şartlar gerçekleştiğinde mümkün olabilir, ilgilinin rızası hukuka uygunluk sebeplerinden biri değildir. Bu örnek bakımından rızayı hukuka uygunluk sebebi olarak kabul etmek veri öznesinin aleyhinedir. Mevzuatta öngörülen şartlar gerçekleşmediği hâlde, rızaya dayanarak verilerin işlenmesi, emredici kuralların dolanılması demektir. Geniş yetkilerle donatılmış kamusal makamın, baskı uygulamak suretiyle rıza elde etmesi de kuvvetle muhtemeldir.

Önemli ölçüde bağımlılık içeren hasta-hekim ilişkileri bakımından da rızanın özgür iradeye dayanıp dayanmadığı hususu bilhassa incelenmelidir<sup>114</sup>. Sağlık konusunda yeterince bilgi sahibi olmayan birey, çözümü hastanelerde arar. Öncelikli olarak sorunun çözümüne odaklandığı için hekim veya görevli diğer kişiler tarafından yapılan bir işleme itiraz ettiğinde sağlık hizmetlerinin aksayacağını düşünebilir. Bu açıdan taraflar arasında güç dengesizliği ve bir bağımlılık ilişkisi mevcuttur. Özetle, hasta-hekim ilişkilerinde de rızaya ancak sınırlı durumlarda dayanılması gerektiği ifade edilmektedir. Rızaya dayanılması, hastanın gerçek bir seçim şansına sahip olduğu ve herhangi bir zarara uğramadan rızasını geri alabileceği durumlarla sınırlandırılmalıdır<sup>115</sup>. Söz gelimi, rıza göstermemesi hâlinde sırf bu sebeple sağlık hizmetlerinin aksamayacağı konusunda hastaya garanti verilmesi durumunda rıza geçerlidir<sup>116</sup>.

İşçi-işveren, resmi makam-vatandaş veya hekim-hasta örneklerinde rızaya dayanılmaması, veri sorumlusunun da lehinedir. Zira özgür iradeye dayanan, bilgilendirilmiş ve konuya özel bir rıza verildiğini ispat yükü, veri sorumlusunun omuzlarına yüklenmiştir (Tüzük m.7/1). Taraflar arasındaki hiyerarşinin kötüye kullanılması suretiyle sözleşmenin ifası için gerekli olmayan veriler işlendiğinde, veri koruma hukukunun temel ilkeleri ihlal edilmiştir. “Belirli, açık ve meşru amaçlar için toplanma (Tüzük m.5/1-b)” ve “yeterli, alakalı ve işlendikleri amaçlarla bağlantılı olarak sınırlı olarak işlenme (Tüzük m.5/1-c)” ilkeleri ihlal edildiğinden işleme faaliyeti hukuka aykırı olacaktır. Nihayet veri sorumlusu, ihlal iddialarına karşı sorumluluk prensibi gereğince hesap vermekte zorlanacaktır.

<sup>114</sup> Korkmaz, s. 149.

<sup>115</sup> Article 29 Working Party, **Working Document on The Processing of Personal Data Relating to Health in Electronic Health Records**, s. 8.

<sup>116</sup> Bergkamp/Dohnt, s. 77.

Örneklerde belirtildiği üzere, rızaya rağmen belirli durumlarda verilerin işlenmesini engellemek, esasen veri öznesini korumayı amaçlamaktadır. Bu itibarla, Tüzüğün kontrol prensibini göz ardı ettiği yönündeki eleştirilere katılmıyoruz<sup>117</sup>.

### E. Rızanın Geri Alınması

Belirli bir veri işleme faaliyetine rıza göstermek ve rızayı geri almak birbirinden ayrı olarak düşünülemez. Tüzüğün 7/3'üncü maddesine göre; *“ilgili kişi, her zaman rızasını geri alma hakkına sahiptir. Rızanın geri alınması, o ana kadar gerçekleştirilen işleme faaliyetlerinin hukuka uygunluğunu etkilemez. İlgili kişi rıza vermeden önce bu konuda bilgilendirilmelidir. Rızanın geri alınması, rızanın verilmesi kadar kolay olmalıdır”*.

Tüzüğe göre, rıza geri alınırken, rıza verilmesinde uygulanandan daha zor bir sürecin izlenmesi mümkün değildir (m.7/3). Klavyede bir tuşa basılması ya da ekrana dokunulması gibi şekillerde rıza alınmışsa, rızanın geri alınması da aynı ölçüde kolay olmalıdır.

Pazarlama faaliyetleri için iletişim bilgilerini toplamayı amaçlayan bir bilet şirketi, internette “Evet” veya “Hayır” kutucuğunun işaretlenmesini isteyerek rıza talep eder. İşgünlerinde ve mesai saatlerinde çağrı merkezini aramak suretiyle rızanın ücretsiz olarak geri alınabileceği konusunda müşteriler bilgilendirilir. Tek bir tıklama faaliyetiyle rıza elde eden veri sorumlusunun rızanın geri alınmasında müşteriler için daha külfetli bir yöntem uygulaması, Tüzüğün 7/3'üncü maddesine aykırıdır<sup>118</sup>. Yine bu hükme göre, çevrimiçi ortamda kolaylıkla rıza verilmesine imkân tanınmışsa, rızanın geri alınması için yazılı bir bildirim talep edilemez<sup>119</sup>.

Rızanın geri alınması, veri öznesini bir zarara uğratmamalıdır; rızasını geri alan kullanıcı, hizmet seviyesinde bir düşüş yaşamamalı veyahut rızasını geri alırken ek ücret ödemek zorunda kalmamalıdır<sup>120</sup>.

Kullanıcı, indirimde olan bir moda dergisine abone olur. Moda dergisi, kullanıcıların alışveriş alışkanlıklarını tespit etmek ve tekliflerini kullanıcıların tercihlerine uygun hâle getirmek üzere, doldurulması gönüllülük esasına bağlı olan bir anketle bazı kişisel veriler toplamaktadır. Sonradan rızasını geri alan kullanıcı, tercihlerine göre kişiselleştirilmemiş dergiyi, aynı indirim oranıyla almaya devam eder. Bu örnekte, rızasını geri alan veri

<sup>117</sup> Karşı görüş için bkz. Solove, s. 1897.

<sup>118</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 22.

<sup>119</sup> Çekin, s. 62.

<sup>120</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 21.

öznesi, bir zarara maruz kalmış değildir. Akıllı telefon uygulaması, telefonun ivmeölçerine (accelerometer) erişmek için kullanıcıdan izin talep eder. Bir süre sonra, rızasını geri alan kullanıcı, uygulamayı artık sınırlı olarak kullanabildiğini fark eder. Rızasını geri alan veri öznesi bir zarara uğratıldığından, bu örnek özelinde geçerli bir rıza talebi yoktur<sup>121</sup>.

Rızanın geri alınmasının ardından veri sorumlusu, saklamasını gerektiren başkaca yasal zorunluluklar bulunmadığı takdirde, elde ettiği verileri silmek zorundadır<sup>122</sup>. Verilerin silinmesi talep edilmese dahi, veri sorumlusu kendiliğinden bu konuyu değerlendirmelidir. Buna karşılık, mevzuatta verilerin belirli bir süre daha saklanması öngörülmüş olabilir. Söz gelimi kullanıcının internet sitesindeki üyeliği sona erse dahi, çevrimiçi gezinme işlem bilgisi, IP adresi, aktarılan veri miktarı gibi kişisel veriler, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun gereğince belirli bir süre daha saklanmalıdır (m.5/3).

## F. Rıza Gösterme Ehliyeti

Fiziksel ve psikolojik olarak yeterli olgunluğa sahip olmayan çocuklar, yetişkinlere kıyasla daha çok korunmalıdır. Aynı koruma, çocukların kişisel verileri bakımından da sağlanmalıdır. Konunun uluslararası sözleşmelerde sıklıkla adı geçen “çocuğun üstün yararı” ilkesiyle<sup>123</sup> de bağlantısı bulunmaktadır. Türkiye’nin de taraf olduğu, 1989 tarihli Birleşmiş Milletler Çocuk Hakları Sözleşmesi’nin 3’üncü maddesine göre; kamu kurum ve kuruluşları, özel kuruluşlar, mahkemeler, idari makamlar ve yasama organı tarafından gerçekleştirilen ve çocukları ilgilendiren bütün faaliyetlerde çocuğun yararı ilkesi gözetilmelidir.

Çocukların sosyal medya paylaşımları da bu ilke ışığında ele alınmalıdır. Küçük yaşta yapılan bir paylaşım, yeri geldiğinde kişiyi hayatı boyunca

<sup>121</sup> Her iki örnek için bkz. Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 11.

<sup>122</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 22.

<sup>123</sup> Çocuğun üstün yararı ilkesi ile çocuğun mahremiyet hakkı bazı durumlarda yarış içinde olabilir. Örneğin, çocuk ile velinin menfaatleri çatışırsa kişisel verilerin işlenmesine veli tarafından gösterilen rıza geçersiz kabul edilebilir. Keza bir öğretmen, çocuğun fail/ mağdur olduğu bir suçtan ötürü fiziksel ve psikolojik olarak korunabilmesi için sosyal hizmet görevlisine çocuğun bazı kişisel verilerini açıklayabilir. Çocuğun üstün yararı ilkesi bunu gerektirir. Ek olarak, çocuğun istismara veya kötü muameleye maruz kalıp kalmadığını tespit edebilmek için sağlık mensubu görevlilerine bazı bilgilerin açıklanmasında da aynı durum söz konusudur (Article 29 Working Party, **Opinion 2/2009 on The Protection of Children’s Personal Data**, 11/2/2009, s. 5, 6).

takip ederek onun gelişimi üzerinde olumsuz sonuçlar doğurabilir<sup>124</sup>. Çocukların özellikle sosyal medya paylaşımlarında “bilinçli” bir bireyin izlerini görmek her zaman mümkün değildir<sup>125</sup>. Çocuklar adına yasal temsilcilerin rıza göstermesi, kişisel veri hukukunda da gündeme gelebilecektir.

Çocuk, haklarını kullanabilmek için yasal olarak temsil edilmek isteyebilir. Yasal temsilcinin çocuk üzerinde mutlak ve koşulsuz bir egemenliği bulunmadığı gibi bazı durumlarda çocuğun üstün yararı ilkesi, yasal temsilcinin isteklerinin göz ardı edilmesini gerektirebilir<sup>126</sup>.

Belirli bir yaştan sonra çocuk, yasal temsilcisine danışmadan kararlar alabilir. Çocuğa ilişkin bir kişisel veri, başlangıçta yasal temsilcinin rızasıyla işlenmişse, daha sonra ehil olan birey, bu rızayı geri alabilir. Çocukla ilgili bir ameliyata başta yasal temsilci açık rıza göstermiş, ancak çocuk sonradan ehil olmuşsa, veri sorumlusu ehil olan bireyin rıza göstermeyi sürdürdüğünden emin olmalıdır, zira bu örnekte, hassas kişisel veri teşkil eden bilgiler işlenmektedir<sup>127</sup>. Her durumda korunan yasal temsilcinin değil, çocuğun menfaattir; kişisel verilerin korunması hakkı, bizatihi çocuğun kendisine aittir<sup>128</sup>.

Veri sorumlusu, sunduğu hizmetin kimlere hitap ettiğine, veri öznesinin yaşına ve kim olduğuna dikkat etmelidir. Söz gelimi, rıza ehliyetine sahip olmayan kimselerin de kişisel verileri işleniyorsa, veri sorumlusu bu kişilere özgü bir bilgilendirme süreci yürütmek zorundadır<sup>129</sup>.

Verilerin işlenmesinde ne zaman rıza ehliyetinin mevcut olduğu tartışmalı bir husustur. Ancak mevzuatta açıkça belirli bir yaşın üstü ehliyetli

<sup>124</sup> Çekin, s. 63.

<sup>125</sup> Keza yetişkinlerin de sosyal medya paylaşımları için aynı yorum pekâlâ yapılabilir. Yetişkin veya çocuk olsun, bugün itibariyle geline nokta da bireylerin kişisel veriler konusunda yeterince hassas olmadığı ortadadır. Teknolojik gelişmeler ve bilginin serbest dolaşımı, kişisel verilerin korunması noktasında vurdumduymaz bir sosyal algı doğmasına sebep olmaktadır (Lopez, s. 38). Gizlilik politikasını düzenli olarak okuyan bireylerin dahi çoğu zaman, veri kullanımının ve ifşasının sonuçlarını sağlıklı bir şekilde değerlendiremedikleri gözlenmektedir. Bu bireyler, genelde çok küçük yararlar karşılıklı kişisel verilerini devredebilmektedir. Araştırmalara göre, yetişkinler ve küçükler, verilerin işlenmesi konusunda benzer şekilde duyarsız davranmaktadır (Solove, s. 1886).

<sup>126</sup> Article 29 Working Party, **Opinion 2/2009 on The Protection of Children’s Personal Data**, s. 5.

<sup>127</sup> Article 29 Working Party, **Opinion 2/2009 on The Protection of Children’s Personal Data**, s. 5.

<sup>128</sup> Benzer Küzeci, s. 245.

<sup>129</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 14.



olarak belirlenmişse, bu hususun tespiti kolaylaşır<sup>130</sup>. Direktiften ve Kanundan farklı olarak, Tüzükte çocukların kişisel verilerine yönelik açık bir düzenleme mevcuttur. Tüzüğe göre, bir çocuğa doğrudan bilgi toplumu hizmetlerinin sağlanması söz konusu olduğunda, kişisel verilerin işlenebilmesi için çocuğun en az 16 yaşında olması gerekmektedir. Çocuğun 16 yaşından küçük olması hâlinde ise, işleme faaliyeti, sadece çocuk üzerinde velayet hakkı bulunan yasal temsilci rıza gösterir veya çocuğun rızasını onaylarsa, mümkündür. Sayılan koşullar yoksa, işleme faaliyeti hukuka aykırı olacaktır (Tüzük m.8/1). Tüzüğe göre, üye devlet, 13 yaşından az olmamak üzere mevzuatında başka bir yaş sınırı belirleyebilir (m.8/1). Tüzük, bireyin ergin olmasını değil, ayırt etme gücünün varlığını ölçüt olarak kabul etmiştir<sup>131</sup>. Önleyici veya bilgilendirici hizmetlerin sunulmasında velayet sorumlusunun rızası gerekmez. Buna karşılık pazarlama veya profileme amaçlarıyla veriler işleniyorsa, veli ya da vasiye rıza gösterip göstermeyeceği sorulmalıdır (Tüzük, Giriş Kısmı, Prg. 38).

Bilgi toplumu hizmetleri ile elektronik araçlarla belirli bir mesafeden sunulan, bireysel bir taleple ve genellikle bir bedel karşılığında verilen hizmetler kastedilmektedir<sup>132</sup>. “*Genellikle bir bedel karşılığı*” ibaresi, bilgi toplumu hizmetlerinin kapsamını sınırlamış görünse de bu kavramın oldukça geniş yorumlanması gerekmektedir. Zira, çocukların sıklıkla kullandığı canlı oyunlar, eğlence siteleri, e-posta ve sosyal medya bedelsiz olarak hizmet vermektedir<sup>133</sup>. Tanımda “*genellikle*” ifadesi kullanıldığı için bedelsiz olarak hizmet veren bu platformlar da hükmün kapsamına girer. Kaldı ki, “*bir bedel karşılığı*” şartının sağlanması için bedelin hizmet sağlayana ödenmesinin zorunlu olduğu, ancak mutlaka hizmeti alan tarafından ödenmesinin gerekmediği, bedelin üçüncü bir kişi, söz gelimi reklamcılar tarafından ödenmesinin de yeterli olduğu kabul edilmektedir<sup>134</sup>.

Ülkeler arasındaki tarihi, kültürel ve sosyal farklılıklar, çocukların karar alma becerilerini etkiler<sup>135</sup>. Bu farklılık dikkate alınarak üye devletlerin yaş

<sup>130</sup> Korkmaz, s. 152.

<sup>131</sup> Çekin, s. 63.

<sup>132</sup> Tanım için bkz. EU Directive 2015/1535 of The European Parliament And of The Council of 9 September Lations And of Rules on Information Society Services, m.1/1-b.

<sup>133</sup> Macenaite, Milda/Kosta, Eleni: “Consent For Processing Children’s Personal Data in The EU: Following in US Footsteps?”, Information & Communications Technology Law, Vol.26, I.2, 2017, s. 170.

<sup>134</sup> Macenaite/Kosta, s. 170, 171.

<sup>135</sup> Macenaite/Kosta, s. 151.

sınırını aşığıya çekmesine imkân tanınmıştır. Doktrinde bu husus eleştirilmiş, üye devletlere verilen bu yetki sebebiyle birlik içinde ortak bir yaş sınırı belirlemenin zorlaşacağı ifade edilmiştir<sup>136</sup>.

Tüzüğe göre, çocuk adına hareket eden velayet yetkisine sahip kişinin rıza gösterdiğini kanıtlama yükümlülüğü, veri sorumlusunun omuzlarındadır (m.8/2). Şüpheleri ortadan kaldırmak ve ispat kolaylığı sağlamak için velayet sorumlusundan yazılı rıza alınması tavsiye edilmektedir<sup>137</sup>.

Çocuğun rıza açıklamasının sonuçlarını değerlendirebilme yeteneğine sahip olup olmadığı incelenmelidir<sup>138</sup>. Zira görüşlerini oluşturma yeteneğine sahip çocuk, kendisini ilgilendiren bütün hususlarda görüşlerini serbestçe ifade etme hakkına sahiptir (BM Çocuk Hakları Sözleşmesi, m.12). Belirli bir olgunluğa sahip çocuklar, kendilerini doğrudan ilgilendiren veri işleme sürecinde aktif olarak yer alma hakkına sahiptirler. Çocuğun görüntülerinin kullanılması, coğrafi olarak konumunun belirlenmesi gibi konularda çocuğun kararlara katılımı önem kazanmaktadır<sup>139</sup>.

### G. Tüzüğün Rızayla İlgili Hükümlerine Yöneltilen Eleştiriler ve Değerlendirmelerimiz

Tüzüğe yöneltilen eleştiriler; “Tüzük hükümlerinin<sup>140</sup> rızaya dayanan işleme faaliyetlerini bile kısıtlayarak verilerin serbest akışını engellediği, bu şekilde bireyin karar alma serbestisini sınırladığı, Tüzüğün paternalist<sup>141</sup> bir yaklaşımla hareket ettiği” noktalarında toplanmaktadır.

*Solove*, hukuk sisteminin yeri geldiğinde tehlikeli faaliyetlere verilen rızayı dahi geçerli kabul ettiğini, hukukun genellikle bir işlemin rızaya aykırı olarak gerçekleştirildiğini kabul etmeden önce, önemli ölçüde manipülasyonu, hatta baskıyı hoş gördüğünü belirtmektedir. Yazara göre, birey, ken-

<sup>136</sup> Görüş için bkz. **van der Hof**, Simone: “I Agree, or Do I: A Rights-Based Analysis of The Law on Children’s Consent in Digital World”, *Wisconsin International Law Journal*, Vol.34, 2016, s. 425.

<sup>137</sup> Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, s. 18.

<sup>138</sup> **Çekin**, s. 63.

<sup>139</sup> Article 29 Working Party, **Opinion 2/2009 on The Protection of Children’s Personal Data**, s. 6.

<sup>140</sup> Teknolojinin yükselişi karşısında Tüzüğün kişisel verileri koruma konusunda yetersiz kaldığına ilişkin görüşler için bkz. **Lopez**, s. 36.

<sup>141</sup> Paternalizm, devlet idaresinde görev yapan kişilerin tecrübelerini ve bilgilerini kullanarak yeri geldiğinde toplumdaki bireylerin rızasına aykırı şekilde kararlar alabilmelerini öngören sistem olarak tanımlanabilir Bilgi için bkz. <https://www.bilgiustam.com/paternalizm-nedir/> (Erişim Tarihi: 19.08.2019).

disinin yüksek menfaatine uygun olmayan kararları, dilediği zaman alabilir, haklarından vazgeçebilir, riskler alabilir ve hukuk sistemi bireylere müdahale etmez. Buradan hareketle yazara göre, Tüzük, rızaya dayanan işleme faaliyetlerini dahi kısıtlamak suretiyle kontrol prensibini göz ardı etmektedir<sup>142</sup>. Yazar, bireysel özerkliği geliştirme vizyonuyla hareket eden Tüzüğün<sup>143</sup> paternalist bir yaklaşımla bireyin karar alma özgürlüğünü sınırlamasını çelişkili bulmaktadır<sup>144</sup>.

*Solove*, kişisel verinin kullanılma şekliyle ilgili bireyin maliyet-fayda analizi yaparak anlamlı kararlar alabilmesini mümkün kılan bir sistemin Tüzükte var olmadığını savunmaktadır. Yazara göre, Tüzükteki kısıtlayıcı prensipler, bir zararın doğmasını aramadan verilerin işlenmesini engellemekte, yeri geldiğinde faydalı bilgi akışları dahi Tüzük hükümlerinin engeline takılmaktadır<sup>145</sup>.

*Schwartz*, ABD ile Avrupa'daki veri koruma kurallarını karşılaştırdığı eserinde; ABD'de önlemler alınmasını gerektiren güçlü kanıtlar bulunmadığı sürece, mevzuatın veri akışına müdahale etmekten imtina ettiğini, buna karşılık Avrupa'da veri akışını sınırlayan, katı bir sistemin mevcut olduğunu ifade etmektedir. Söz gelimi, ABD'de verilerin işlenmesi için bir veri koruma otoritesinin varlığına ihtiyaç duyulmazken, Avrupa'daki veri koruma sisteminde bu kurumun varlığı zorunludur. Yazar, veri işlemenin ABD'de mevzuat tarafından "yasaklanmadığı sürece" serbest olduğunu vurgulamaktadır<sup>146</sup>.

Kanaatimizce, Tüzüğe yöneltilen bu eleştiriler haksızdır. Tüzük, mahremiyet ihlallerinin artmasının yarattığı farkındalıkla hareket ederek kişisel verilerin korunmasında yüksek standartlar öngörmektedir. Veri sorumlusunu disiplinize etmek için öngörülen yükümlülüklerin paternalist bir yaklaşım olarak tarif edilmesi yerinde olmamıştır. Zira gelinen noktada, son derece kırılğan hâle gelen veri işleme faaliyetlerinin belirli kurullarla çevrelenmesi, belirli bir zemine oturtulması kaçınılmaz hâle gelmiştir.

<sup>142</sup> Bkz. *Solove*, s. 1897.

<sup>143</sup> Tüzükte kontrol prensibi benimsenmiştir (Tüzük, Giriş Kısmı, Prg.7).

<sup>144</sup> *Solove*, s. 1894. Yazar, problem olarak gördüğü bu hususu, "Rıza İkilemi" olarak adlandırmaktadır (*Solove*, s. 1894). Yazara göre, böyle bir problem mevcut olmasına rağmen, mahremiyetin öz-yönetimi yaklaşımının terk edilmesi yerinde olmaz. Ancak, paternalist bir yaklaşım da benimsenmemelidir (*Solove*, s. 1903).

<sup>145</sup> Görüş için bkz. *Solove*, s. 1897.

<sup>146</sup> *Schwartz*, Paul M.: "The EU-U.S. Privacy Collision: A Turn to Institutions And Procedures", Harvard Law Review, Vol. 126, I.7, 2013, s. 1976.

Veri sorumlusunun denetlenmesi, kişisel veri hukukunda ayrı bir önem taşımaktadır. Hakkı olarak Tüzük, rızaya dayanan veri işleme faaliyetlerinde dahi, veri sorumlusunun bazı ek yükümlülüklerine uymasını aramaktadır. Söz gelimi, veri güvenliği ilkesi gereğince, veri sorumlusu, yetkisiz kişilerin veriye erişimini engellemeye yönelik teknolojik ve idari tedbirleri almakla yükümlüdür. Keza şeffaflık, anlaşılabilirlik, erişilebilirlik gibi temel veri koruma prensiplerine Tüzükte yer verilmesi aynı amaçlara hizmet eder.

İşlemenin rızaya dayandığı durumlarda, veri sorumlusu, rızanın geçerliliği için aranan şartlara ve diğer yükümlülüklerine aynen riayet etmelidir. Salt rızanın sağlanması, her durumda yeterli kabul edilirse, rıza beyanı, prensiplere aykırı veri işleme faaliyetleri için bir kalkan olarak kullanılır. Bu durumda, veri sorumlusunun kaliteli bir veri işleme faaliyeti yürüttüğünden söz edilemez. Verilerin belirli kurallara göre işlenmesi, modern toplumda sadece veri öznesini değil, bütün bireyleri ilgilendirir. Veriler düzenli ve belirli kurallara göre işlenirse, toplumsal faaliyetler de sağlıklı yürütülecektir. Özetle, veri işleme faaliyeti, başlı başına sosyal faydayı da ilgilendiren bir konudur.

## SONUÇ

Veri işlemenin devasa boyutlara ulaştığı günümüzde Tüzüğe aykırı olan veri işleme faaliyetlerine sıklıkla rastlanmaktadır. Veri işleme vasıtalarının çeşitliliği, süreci, veri öznesi için belirsiz hâle getirmiştir. Tüzüğün amacı, bu süreci, veri öznesi için anlaşılabilir ve algılanabilir kılmaktır. Tüzüğün paternalist olduğu yönündeki eleştirilere katılmak mümkün değildir. Verilerin belirli kurallara ve esaslara göre işlenmesi, işin doğasından kaynaklanır. Keza rızanın geçerliliği için belirli şartların öngörülmesi, veri sorumlusuna çeşitli yükümlülükler yükleyerek veri öznesinin korunmasını amaçlamaktadır.

Verilerin işlenmesi sadece bireysel çıkarları değil, aynı zamanda sosyal faydayı da ilgilendiren bir konudur. Verilerin işlenmesinde belirli kuralların öngörülmesi, düzenli veri akışının sağlanmasını ve işlemlerin sağlıklı yürütülmesini amaçlar. İşlemlerin sağlıklı yürütülmesi de bütün bireyleri ilgilendirir. İşte, sosyal faydanın gözetilmesi, bazı veri işleme faaliyetlerinde daha titiz davranılmasını gerektirir. Zayıf tarafı korumak ihtiyacı doğabilir. Bilhassa taraflar arasında güç dengesizliğinin bulunduğu hâllerde veri işlemenin rızaya dayanması çoğu zaman uygun değildir. Zira güçlü taraf, üstünlüğünü kötüye kullanarak ve zayıf üzerinde baskı kurmak suretiyle rıza elde edebilir. Bu tip durumlarda zayıf tarafın karar alma serbestisi, taraflar arasındaki ilişkinin doğası gereği sınırlıdır. Söz gelimi, 2559 Sayılı Polis Vazife ve

Salahiyet Kanunu, polisin “gönüllü” olarak tabir edilen kimselerden parmak izi almasına imkân tanımaktadır (m.5). Bahsettiğimiz üzere, taraflar arasında açık bir güç dengesizliğinin var olduğu bu gibi durumlarda birey, kendisini baskı altında hissedip rıza gösterebilir, bu yönüyle rızanın özgür iradeye dayandığı hususu şüpheli hâle gelir.

Rıza, veri işlemeyi hukuka uygun kılan tek sebep değildir. Diğer hukuka uygunluk sebeplerinin koşulları oluşmuşsa, ayrıca veri öznesinden rıza alınması gerekmez. Ancak rıza dışında pek çok sebebin varlığı ve bunların geniş olarak uygulanmaya imkân veren yapısı, rızanın uygulama alanını oldukça sınırlar. Aslolan veri işleme faaliyetlerinin rızaya dayalı olarak yapılmasıdır. Diğer hukuka uygunluk sebepleri, ancak istisnai durumlarda uygulanmalıdır. Ancak gelinen noktada, istisna aslolanın yerini almıştır.

Rızanın geri alınmasının ardından saklanmasını gerektiren başka yasal zorunluluklar yoksa, toplanan veriler silinmelidir. Verilerin her şartta belirli bir süre saklanması mevzuatta öngörülmüş olabilir. Esasen rızasını geri alan veri öznesi, verileriyle ilgili gelecekteki işlemleri engellemeyi amaçlamaktadır. Dolayısıyla açıkça verilerin silinmesi talep edilmese dahi, veri sorumlusu bu konuda bir değerlendirme yapmalıdır. Veri öznesine rağmen verilerin saklanmaya devam edilmesi ve bu sürece veri öznesi tarafından müdahale edilememesi kontrol prensibinin yeteri kadar dikkate alınmadığını gösterir. Hemen belirtelim ki, asıl olan veri işleme faaliyetlerinin kontrol prensibi ışığında ele alınmasıdır. Bu kurala bir istisna öngörülmesi, ancak çok sınırlı durumlarda mümkün olmalıdır. Söz gelimi, kullanıcı, internet sitesindeki üyeliğini sona erdirse dahi, çevrimiçi gezinme işlem bilgisi, IP adresi, aktarılan veri miktarı gibi kişisel veriler, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun gereğince belirli bir süre daha saklanmalıdır (m.5/3). Her koşulda verilerin saklanmasını öngören bu hükmün, kontrol prensibi ışığında tekrardan ele alınması gerekmektedir.

Yasal temsilci, kişisel verilerin işlenmesi konusunda çocuk adına birtakım kararlar alma yetkisine sahip olsa da esasen kişisel verilerin korunması hakkı bizatihi çocuğun kendisine aittir. Bu sebeple konuyla ilgili kararlara çocuğun katılımı önem kazanmaktadır. Veriler üzerindeki tasarrufların sonuçlarını anlama yetkinliğine sahip olan çocuğun görüşlerini serbestçe ifade etmesine olanak tanınmalıdır. Bazı durumlarda çocuğun üstün yararı ilkesi, çocuğa rağmen kararlar alınmasını gerektirir. Buna karşılık, bazen yasal temsilci tarafından çocuğa rağmen kararlar alınması, bahsi geçen ilkeyle bağdaşmaz. Aksi takdirde çocuk açısından kontrol prensibi göz ardı edilmiş

olur. Zira veriler üzerinde hâkimiyet kurması gereken, hakkın gerçek sahibi olan çocuktur.

Kanunda çocukların kişisel verilerinin korunmasına ve rızanın geri alınmasına ilişkin bir düzenlemeye yer verilmemesi eksikliklerdir. Kanunun Tüzükteki hükümler esas alınarak değiştirilmesi gerekmektedir. Keza Kanunda opt-out yöntemine ilişkin herhangi bir açıklamaya yer verilmemiştir. Buna karşılık Kanunda her türlü kişisel verinin ancak “açık rıza” ile işlenebileceği ifade edilmiştir. Tüzük ve Direktif için yapılan değerlendirmeler dikkate alındığında; opt-out yönteminin Kanun bakımından da geçerli kabul edilemeyeceği sonucuna ulaşılır.

## KAYNAKÇA

### Basılı Kaynaklar

- Aydın, Ufuk:** “İşverenin İşçi Özlük Dosyası Tutma Yükümü”, İş Hukuku ve Sosyal Güvenlik Hukuku Türk Milli Komitesi 30. Yıl Armağanı, Ankara 2006, s. 491-505.
- Başalp, Nilgün:** Kişisel Verilerin Korunması ve Saklanması, Ankara 2004.
- Bergkamp, Lucas/Dhont, Jan:** “Data Protection in Europe And The Internet: An Analysis of The European Community’s Privacy Legislation in The Context of The World Wide Web”, The EDI Law Review, Vol.7, 2000, s. 71-114.
- Bozkurt Yüksel, Armağan Ebru:** Bulut Bilişimde Kişisel Verilerin Korunması, Ankara 2016.
- Custers, Bart/van der Hof, Simone/Schermer, Bart/Appleby-Arnold, Sandra/Brockdorff, Noellie:** “Informed Consent in Social Media Use-The Gap Between User Expectations And EU Personal Data Protection Law”, SCRIPTed: A Journal of Law, Technology And Society, Vol. 10, I.3, 2013, s. 435-457.
- Çekin, Mesut Serdar:** Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, İstanbul 2018.
- Develioğlu, Murat:** 6698 Sayılı Kişisel Verilerin Korunması Kanunu İle Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, İstanbul 2017.
- Dural, Mustafa/Öğüz, Tufan:** Türk Özel Hukuku, Cilt II - Kişiler Hukuku, 19. Baskı, İstanbul 2018.
- Dülger, Murat Volkan:** “Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması”, Yaşar Hukuk Dergisi, C.1, S.2, Temmuz 2019, s. 71-175.
- Eren, Fikret:** Borçlar Hukuku Genel Hükümler, 16. Baskı, Ankara 2014.
- Jarovsky, Luiza:** “Improving Consent in Information Privacy Through Autonomy-Preserving Protective Measures (APPMs)”, European Data Protection Law Review, Vol.4, I.4, 2018, s. 447-458.
- Korkmaz, İbrahim:** Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, 2. Baskı, Ankara 2019.
- Kuner, Christopher:** European Data Protection Law Corporate Compliance And Regulation, Second Edition, New York 2007.

- Küzeci**, Elif: *Kişisel Verilerin Korunması*, 2. Baskı, İstanbul 2018.
- Lazaro**, Christophe/**Le Metayer**, Daniel: “*Control Over Personal Data: True Remedy of Fairy Tale*”, *SCRIPTed: A Journal of Law, Technology And Society*, Vol. 12, I. 1, 2015, s. 3-34.
- Lopez**, Santiago Ramirez: “*Informing Consent Giving Control Back to The Data Subject From a Behavioral Economics Perspective*”, *Journal of Intellectual Property*, Vol.9, I.1, 2018, s. 35-50.
- Macenaite**, Milda/**Kosta**, Eleni: “*Consent For Processing Children’s Personal Data in The EU: Following in US Footsteps?*”, *Information & Communications Technology Law*, Vol.26, I.2, 2017, s.146-197.
- Misek**, Jakub: “*Consent to Personal Data Proccessing- The Panacea or The Dead End*”, *Masaryk University Journal of Law and Technology*, Vol.8, I.1, 2014, s. 69-84.
- Monteleone**, Shara: “*Adressing The ‘Failure’ of Informed Consent in Online Data Protection: Learning The Lessons From Behaviour-Aware Regulation*”, *Syracuse Journal of International Law And Commerce*, Vol. 43, I.1, 2015, s. 69-120.
- Noujaim**, Arlette: “*The Stimulus For Data Protection Laws Around The World: The Development And Anticipated Effect on The European Union’s New Data Rules*”, *Intellectual Property Law Bulletin*, Vol.20, I.2, 2016, s. 99-118.
- Oğuzman**, M. Kemal/**Öz**, M. Turgut: *Borçlar Hukuku Genel Hükümler*, Cilt II, 13. Bası, İstanbul 2017.
- Reijneveld**, Minke D.: “*Quantified Self, Freedom, And The GDPR*”, *SCRIPTed: A Journal of Law, Technology And Society*, Vol. 14, I.2, 2017, s. 285-325.
- Schwartz**, Paul M.: “*The EU-U.S. Privacy Collision: A Turn to Institutions And Procedures*”, *Harvard Law Review*, Vol.126, I.7, 2013, s. 1966-2009.
- Serozan**, Rona: *Medeni Hukuku Genel Bölüm/ Kişiler Hukuku*, 6. Bası, İstanbul 2015.
- Solove**, Daniel J.: “*Privacy Self-Management And The Consent Dilemma*”, *Harvard Law Review*, Symposium: Privacy And Technology, Vol.126, I.7, 2013, s. 1880-1903.
- Staben**, Julian: “*Consent Under Pressure And The Right to Informational Self-Determination*”, *Internet Policy Review*, Vol.1, I.4, 2012, s. 1-6.



**van der Hof, Simone:** “*I Agree, or Do I: A Rights-Based Analysis of The Law on Children’s Consent in Digital World*”, Wisconsin International Law Journal, Vol.34, 2016, s. 409-445.

### **Raporlar**

Article 29 Working Party, **Opinion on The Processing of Personal Data in The Employment Context**, 13/9/2001.

Article 29 Working Party, **Working Document on The Processing of Personal Data Relating to Health in Electronic Health Records**, 15/2/2007.

Article 29 Working Party, **Opinion 2/2009 on The Protection of Children’s Personal Data**, 11/2/2009.

Article 29 Working Party, **Opinion 15/2011 on The Definition of Consent**, 13/7/2011.

Article 29 Working Party, **Opinion 2/2017 on Data Processing at Work**, 8/6/2017.

Article 29 Working Party, **Guidelines on Consent Under Regulation 2016/679**, 10/4/2018.

### **İnternet Kaynakları**

<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046>  
(E.T. 17.8.2019).

<http://www.beuc.eu/publications/2011-00062-01-e.pdf> (E.T.21.5.2018).

<https://www.bilgiustam.com/paternalizm-nedir/> (E.T. 19.08.2019).

