6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI HAKKINDA KANUN'UN BIG DATA (BÜYÜK VERİ) VE İRADE SERBESTİSİ AÇISINDAN DEĞERLENDİRİLMESİ*

(AN ANALYZE OF THE NEW TURKISH CODE ON THE PROTECTION OF PERSONAL DATA NR. 6698 REGARDING BIG DATA AND FREEDOM OF WILL)

Yard. Doç. Dr./*Asst. Prof. Dr.* Mesut Serdar Çekin**

ÖZ

Elde edilen verilerin her geçen gün artması ve bu verilerin analiz edilmesi ile iktisadi açıdan değerlendirilmesi hususunda Big Data kavramı ile ifade edilen farklı teknolojik imkânlar, aynı zamanda hukuki açıdan birçok sorunları da beraberinde getirmektedir. Her ne kadar özel hukuk düzenimiz irade serbestisi ilkesine dayanmakta ise de, yaşanan bütün bu gelişmeler karşısında günümüz toplumunda irade serbestisinden bahsetmenin halen mümkün olup olmayacağı ve bu çerçevede özellikle 7 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'un nasıl bir koruma mekanizması getirdiği, getirilen bu mekanizmanın irade serbestisini Big Data'nın sunduğu imkânlar karşısında korumaya elverişli olup olmadığı sorunları ele alınmıştır.

Anahtar Kelimeler: 6698 Sayılı kişisel verilerin korunması hakkında kanun, big data (büyük veri), irade serbestisi, kişisel verilerin işlenmesi yasağı, açık rıza, amaca bağlılık

ABSTRACT

The concept of Big Data, which describes the continuous rise of data volumes and new technological possibilities regarding the analysis and economic exploitation of the collected data, brings along many challenges from the perspective of law. Although our civil law system is based upon the principle of free will, the mentioned developments raise the question of whether free will still exists or not. In this context, the aim of this paper is to analyze whether the new Code on Data Protection Nr. 6698 is able to safeguard free will against possible "threats" of Big Data.

Keywords: *Turkish code on the protection of personal data nr. 6698, big data, free will, ban on data processing, consent, initial purpose*

***

---

* Bu makale, 17.10.2016 tarihinde Editörler Kurulu'na ulaşmış olup, 28.11.2016 tarihinde birinci hakem; 04.12.2016 tarihinde ikinci hakem onayından geçmiştir.
Bu makale, 29-30 Nisan 2016 tarihinde İsviçre'nin Lozan ve Friborg şehirlerinde "Big Data and Privacy" başlığı altında gerçekleştirilen "Türk-İsviçre Hukuk Günleri" çerçevesinde "Impacts of the "Turkish (Draft) Code for the Protection of Personal Data" on Big Data from the Civil Law Perspective" başlıklı yayınlanmamış sunumun genişletilmiş halidir.

** Türk-Alman Üniversitesi Hukuk Fakültesi Medeni Hukuk Anabilim Dalı Öğretim Üyesi, cekin@tau.edu.tr

I. GİRİŞ

İnsanlık tarihinin akışını değiştiren tarım ve sanayi devrimlerinin ardından içinde bulunduğumuz dönemde yaşanan gelişmeler, bilişim devrimi olarak nitelendirilmektedir[1]. Sanayi devrimi ile birlikte artan risk kaynakları, dönemin insan topluluklarının "risk toplumu" olarak tanımlanmasına sebebiyet vermiştir[2]. Ancak günümüzde daha çok bilgiye dayalı bir toplumdan söz edilmektedir. Bu çerçevede iktisadi, siyasi ve kültürel açıdan verinin fevkalade bir öneme sahip olduğu söylenebilir.

Verilerin günümüzde hangi boyutlara ulaştığına ve hayatımızın ne kadar önemli bir parçası haline geldiğine dair *Kirk Bourne*'un şu çarpıcı tespitlerine yer vermek isabetli olacaktır: İnsanlık tarihinin başlangıcından 2003 yılına kadar kayıt altına alınmış toplam bütün veri, beş milyar gigabayt (exabayt) civarında olarak tahmin edilmektedir. 2011 yılının başlangıcında bu miktarda veri her iki gün içinde, 2013 yılında ise her 10 dakikada üretilmiştir[3]. Gerçekten de her gün kullandığımız cep telefonları, bilgisayarlar, televizyonlar, oyun konsolları ve diğer birçok elektronik cihaz, sürekli veri toplamakta ve bu verileri belirli yerlere göndermektedir. Bu sebeple öncelikle hacmi çok ciddi derecede artış gösteren verinin işlenmesi başlı başına yönetilmesi gereken bir unsurdur.

Bununla birlikte verilerin elde ediliş hızında da ciddi gelişmeler yaşanmaktadır. Hemen yukarıda işaret edildiği üzere neredeyse her elektronik cihaz günümüzde veri üretimine sebebiyet vermektedir. Verilerin elde edilişinde ulaşılan bu hızla baş etmek de bir sorun olarak karşımıza çıkmaktadır.

Verilerin sadece miktarı artmamış, aynı zamanda niteliği de değişime uğramıştır[4]. Klasik anlamda elde edilen veriler daha çok sabit şekildedir. Özellikle yazılı veriler bunun en bariz göstergesidir. Hatta elektronik veri bankaları dahi önceden elde edilmiş sabit bilgiler üzerinden işlem yapmaktadır. Oysa günümüzde özellikle cep telefonlarından, fakat bunun yanında otomobil, televizyon, bilgisayar gibi diğer birçok elektronik cihaz ve araçtan akıcı ve dinamik bilgi iletilmektedir. Dolayısıyla tek tip veriden çok farklı formatlarda birçok bilgi elde edinilmektedir. Bu farklı veri tiplerinin birbirine uyumlu hale getirilmesi de çözülmesi gereken sorunlardan biridir.

Yukarıda zikredilen sorunların Big Data ile bağlantısı ise, bu verilerin analizi sonucunda elde edilen bilgilerde kendisini göstermektedir. Nitekim günümüzde elde edilen verilerin hacmi artmış, çeşitleri çoğalmış ve veriler daha dinamik bir hale gelmiş olsa da bu verilerden elde edilen ürün bir değer teşkil etmediği takdirde iktisadi açıdan herhangi bir önem taşımayacaktır. Dolayısıyla Big Data konseptinin başlıca amacı, niteliği ve niceliği değişime uğramış olan verinin analizi sonucunda işe yarayan ve bugüne kadar klasik yöntemlerle elde edilememiş yeni sonuçların elde edilmesi, veriye bir değer katılmasıdır[5].

---

[1] Daha geniş bilgi için bkz. Frank Webster, Theories of the Information Society, Cambridge, 2002.

[2] Ulrich Beck, Risikogesellschaft – Auf dem Weg in eine andere Moderne, Frankfurt, 1986.

[3] Kirk Borne, Big Data, Small World: Kirk Borne at TEDxGeorgeMasonU, https://www.youtube.com/watch?v=Zr02fMBfuRA (08.04.2016).

[4] Kenneth Cukier, Big Data is better data, https://www.youtube.com/watch?v=8pHzROP1D-w (08.04.2016].

[5] Daha geniş bilgi için bkz. http://www.ibmbigdatahub.com/infographic/four-vs-big-data.

Big Data'nın sunduğu imkânlara örnek olarak Google tarafından geliştirilen ve şoförsüz gidebilen araç ya da internette her gün kullandığımız ve kendiliğinden bize öneriler sunan arama motorları gösterilebilir. Diğer bir güncel örnek, yine Google tarafından geliştirilen *Deepmind* isimli bilgisayardır. Bu bilgisayar, Dünya Go şampiyonu Lee Se-dol'u 4-1'lik bir skorla yenmeyi başarmıştır[6]. Bütün bu örneklerin ortak yanı ise, "makine öğrenimi" olarak adlandırılan bilgisayarların verilere dayalı olarak öğrenimini mümkün kılan bilim alanıyla olan bağlantısıdır. Gerçekten de makine öğrenimi çerçevesinde geliştirilen algoritmalar, bilgisayarların kendilerine sunulan veriler sayesinde kendi kendilerine karar verme ve yeni şeyler öğrenme kabiliyetlerini geliştirmelerini amaçlamaktadır. Bu sayede algoritmalar, kendilerine sunulan veri sayesinde geleceğe dair tahminlerde bulunup karar alabilmektedir. Nitekim Google'ın *Deepmind* bilgisayarı, amatörler tarafından oynanan 700 civarında "go" oyununun verileri ile beslenmiş, sırf bu verilere dayanarak bilgisayar, dünya şampiyonu Lee Se-dol'u yenmeyi başarmıştır. Dolayısıyla en basit anlatımla değişik alanlardan toplanan veriler ve bunlar vasıtasıyla geliştirilmiş algoritmalar sayesinde artık bilgisayarlar kendi kendilerine nasıl davranacaklarını öngörebilmektedirler.

Büyük hacimli verinin işlenip analiz edilmesi sadece teknolojik hayata değil, bizzat siyasetin gidişatına da yön vermektedir. Mesela ABD Başkanı Barack Obama'nın 2012 yılındaki seçimlerde Big Data sayesinde birçok seçmene ulaştığı, bu çerçevede farklı kaynaklardan birçok verinin analiz edilip elde edilen sonuçlar doğrultusunda seçmenlerle iletişim kurulduğu belirtilmiştir[7]. Aynı durum, 2016 yılındaki seçimler açısından da söz konusu olmuş, bu çerçevede özellikle kişisel verilerin büyük çapta işlenmesi ve kişilere özel psikogramların oluşturulması alanında uzmanlaşmış olan Cambridge Analytica kuruluşu öne çıkmıştır[8].

Fakat yukarıda izah edilen gelişimin olumsuz sonuçlarını da her geçen gün gözlemlemek mümkündür. Örneğin Facebook tarafından kullanılan bir algoritma, arkadaş listesinde kullanıcının dünya görüşüne en uygun düşen yorum ve bildirimleri seçip göstermeyi amaçlamaktadır[9]. Diğer bir örnekte kullanıcılara ırkına ya da ten rengine göre farklı reklamlar gösterilmektedir[10]. Benzer şekilde Google, kişinin profiline göre farklı sonuçlar sunmaktadır[11]. Başka bir örnekte Microsoft tarafından geliştirilen ve Twitter kullanıcılarından bir insan gibi düşünmeyi ve konuşmayı öğrenmesi amaçlanan Tay, hayata geçiril-

---

[6] "Google DeepMind computer beats Go champion Lee Se-dol in shock 4-1 victory", The Independent, 15.03.2016.

[7] Bkz. How Obama's data crunchers helped him win, http://edition.cnn.com/2012/11/07/tech/web/obama-campaign-tech-team/ [Erişim: Ağustos 2016].

[8] Daha geniş bilgi için bkz. The Power of Big Data and Psychographics, https://www.youtube.com/watch?v=n8Dd5aVXLCc [Erişim: Ağustos 2016].

[9] "Facebook fängt den Nutzer in seiner eigenen Weltanschauung ein", Süddeutsche Zeitung, 03 Şubat 2016; Facebook ve Google'ın kullanıcı profiline göre farklı sonuçlar gösterdiğine dair bkz. TED Talks: Eli Pariser, What FACEBOOK And GOOGLE Are Hiding From The World, https://www.youtube.com/watch?v=aAMP1Wu_M2U [Erişim: Ağustos 2016].

[10] "Schwarze sehen bei Facebook andere Werbung als Weiße", JETZT, 21 Şubat 2016.

[11] Bkz. dn. 6.

diği ilk 24 saat içinde cinsiyetçi ve Nazi hayranı bir kişiliğe bürünmüş, ardından kapatılmıştır[12].

Yukarıda verilen örneklerden de görüldüğü gibi büyük çapta toplanan ve her geçen gün hacmi artan veriler, algoritmaların hayatımıza dair birçok hususu öngörmelerini mümkün kılmaktadır. Ancak bu tür bir analizin, hukuk düzenimizin en temellerine dahi etki ettiği gerçeği de göz ardı edilmemelidir. Nitekim söz konusu algoritmalar, kullanıcının geçmişini analiz edip geleceğini yönlendirmeye de çalışabilmektedir. Bunun en basit görünümü, kullanıcının yazdığı e-posta içeriğine göre reklam görmesi, daha karmaşık örnekleri ise yukarıda zikredilen Facebook'un kullanıcının dünya görüşüne göre göreceği bildirimleri uyarlaması olarak karşımıza çıkmaktadır. Oysa Kıta Avrupası ve Türk özel hukukunda da benimsenen en temel ilkelerden birisi irade serbestisidir. İradenin hür olmadığı, serbest bir şekilde oluşmadığı, hatta dışarıdan hiçbir etken olmaksızın yanılmadan ötürü sıhhatli bir şekilde meydana gelmediği durumlarda dahi hukuk düzeni, iradesi sakatlanan kişiye farklı imkânlar tanımaktadır. Bu netice dahi başlı başına hukuk düzeninin, özellikle özel hukukun irade serbestisine atfettiği önemi açıkça gözler önüne sermektedir.

Dolayısıyla verilerin büyük çapta kullanılıp işlendiği günümüz toplumunda irade serbestisinden bahsetmenin halen mümkün olup olmayacağı ve bu çerçevede özellikle 7 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'un nasıl bir koruma mekanizması getirdiği sorularına cevap aranması icap etmektedir. Zira Big Data'nın öncülerinden olan *Kenneth Cukier*'in de belirttiği gibi küçük veri çağında esas olan mahremiyet iken büyük veri çağında özellikle hür iradenin ve ahlaki seçimde bulunabilme hürriyetinin bütün tehditlere karşı savunulması gerekmektedir[13].

Her ne kadar geçmişte de iradenin yönlendirilmesi amaçlanmış olsa da Big Data'nın sunduğu farklı imkanlar, manipülasyon ihtimalini de farklı boyutlara taşımıştır. Misal olarak geçmişte insanların fikirlerine yön vermek isteyen gazete ya da televizyon kuruluşlarının az ya da çok hangi dünya görüşüne sahip olduklarını kestirmek mümkün olmuştur. Kişi de buna göre ilgili medya üzerinden bilgi edinip edinmeyeceği hususunda seçim yapma imkânına sahiptir. Oysa yukarıda açıklanan yöntemler, kişi farkında olmadan onun seçim yapma imkânını elinden almaktadır. Kuşkusuz bu çerçevede bireyin tamamiyle sosyal medya araçlarından uzak durarak söz konusu manipülasyondan kurtulma imkânının pekâlâ mevcut olduğu, kimsenin kişiyi sosyal medya araçlarını kullanmaya zorlamadığı savunulabilir. Fakat aynı zamanda unutulmamalıdır ki günümüzde kamuoyu, televizyon ya da gazete vesilesiyle değil, bizzat sosyal medya üzerinden şekillenmektedir.

Bu bağlamda her ne kadar Kişisel Verilerin Korunması Hakkında Kanun ile ilgili bugüne kadar birçok çalışma yapılmış olsa da, ilgili düzenlemenin Big Data sorunsalı kapsamında irade serbestisini ne derece müdafaa etmeye elverişli olduğu hususunda görüldüğü kadarıyla herhangi bir değerlendirme mevcut değildir. Dolayısıyla çalışmamızın amacı, bilişim sektöründe yaşanan bütün gelişmelere, özellikle Big Data'nın sunduğu imkânlara rağmen irade serbestisi-

---

[12] "Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter", The Guardian, 24 Mart 2016, https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter [Erişim: Ağustos 2016].

[13] "Privacy was the central challenge in a small data-era; in the big-data age, the challenge will be safeguarding free-will, moral choice, human volition, human agency", bkz. dn. 3.

nin nasıl söz konusu olabileceği sorusuna cevap aramaktır. Ancak kanunun diğer düzenlemelerine değinilmeyecek, sadece Big Data ve irade serbestisi hususları açısından incelemelerde bulunulacaktır. Ayrıca belirtelim ki Big Data, sadece irade serbestisinden ve dolayısıyla kişilik hakkından ibaret değildir. Bilakis kişilik hakkı, Big Data'nın sadece bir boyutunu ilgilendirmektedir[14]. Dolayısıyla çalışmamızda Big Data'nın sadece kişilik hakkını ilgilendiren boyutu ele alınacak, kişilik hakkıyla alakalı olmayan diğer boyutlar[15] ise çalışma kapsamı dışında bırakılacaktır.

II. BİG DATA'NIN KİŞİSEL VERİLERİN KORUNMASI HAKKINDA KANUN ÇERÇEVESİNDE DEĞERLENDİRİLMESİ

1. Başlangıç Noktası: Anayasa md. 20 f. 3'te Düzenlenen Kişisel Verilerin Korunmasını İsteme Hakkı

Big Data ile kişisel verilerin korunması ve dolaylı olarak irade serbestisi arasındaki ilişki değerlendirilirken öncelikle bu sorunun anayasal temellerinin incelenmesi isabetli olacaktır. Anayasa'nın 20. maddesine 2010 yılında eklenen üçüncü fıkraya göre "*[h]erkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar*". Kişilik hakkının bir türü olarak kabul edilen söz konusu temel hak[16], bireyin modern hayatta verilerin işlenmesinden doğan tehlikelere karşı korunmasını amaçlamaktadır. Nitekim kendine ait kişisel verilerin nerede, nasıl ve ne amaçla işlendiği ya da muhafaza edildiği hususunda bilgi sahibi olmayan bireyin bu yolla hareket serbestisinin sınırlanması söz konusu olabilir. Örneğin bireyin özel hayatına dair yazışmalara, alışveriş bilgilerine ya da seyahat bilgilerine sahip olan kurum ya da kuruluş, bu bilgileri pekâlâ kötü amaçları için kullanabilir[17]. Bu tehdit, sadece kişinin hareket serbestisini sınırlandırmakla kalmayıp, toplumu bir bütün halinde olumsuz şekilde etkileme potansiyeline sahiptir. Zira hür ve demokratik bir toplumun temelini kendi geleceğini kendisi belirleyebilecek nitelikte bireyler oluşturmaktadır[18]. Kişinin mahrem bilgilerinin bir başkası tarafından ele geçirilmesi, kişinin onayı olmadan işlenmesi ya da üçüncü şahıslara devredilmesi ise bireyin kendi geleceğini serbestçe belirleme imkânını ciddi derecede sınırlamaya elverişlidir.

Diğer taraftan yukarıda zikredilen temel hak, diğer temel haklarla korunan menfaatlerle çatıştığı takdirde, özüne dokunulmaması kaydıyla pekâlâ

---

[14] Wilhelm Hackenburg, in T. Hoeren & U. Sieber & B. Holznagel (eds.), Multimedia-Recht, 42. Ergänzungsband, München 2015, Teil 16.7 Big Data, kn. 10.

[15] Bunlar özellikle, Internet of Things olarak adlandırılan ve belirli bir kişi ya da kişiler ile bağlantısı olmayan verilerdir. Örneğin hava sıcaklığı, su hacmi gibi bilgiler bu kategoriye dâhil edilmektedir.

[16] Bkz. Alman Federal Mahkemesi'nin Volkszählungsurteil kararı: BVerfG vom 15.12.1983, 1 BvR 209/83 u. a. – Volkszählung –, BVerfGE 65, p. 1 ve Integritätsgrundrecht kararı, BVerfG, 1 BvR 370/07 ve 1 BvR 595/07.

[17] Örneğin Ashley Madison skandalı çerçevesinde eşlerini aldatan binlerce kişinin kişisel bilgileri ifşa edilmiştir, daha geniş bilgi için bkz. "Hackers Finally Post Stolen Ashley Madison Data", https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/ [Erişim: Ağustos 2016].

[18] Bkz. yukarıda zikredilen Alman Federal Mahkemesi'nin Volkszählungsurteil kararı.

sınırlandırılabilir. Özellikle verilerin işlenmesi ve üçüncü şahıslara devredilmesi bağlamında düşünceyi açıklama ve yayma hürriyetini esas alan Anayasa'nın 26. maddesinde belirtilen "resmi makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliği" hususu önem kazanmaktadır. Bu iki temel hak ve özgürlüğün çakışmasına bir diğer örnek de AB Temel Haklar Şartı'nın 8. maddesi çerçevesinde kişisel verilerin korunmasını esas alan düzenleme ile resmi kuruluşların müdahalesi olmaksızın bilgi edinme hakkını esas alan hükümdür[19]. Benzer şekilde Avrupa Birliği Kişisel Verilerin Korunması Tüzüğü'nde (Tüzük) de bu ihtilafa yer verilmiştir. Tüzüğün 3a numaralı gerekçesinde açıkça "*enformasyonel self-determinasyon*"[20] hakkının sınırlandırılamaz bir hak niteliğinde olmadığı, "toplum nezdindeki işlevi dikkate alınarak ve diğer temel hak ve özgürlükler gözetilerek ölçülülük ilkesine uygun olarak değerlendirilmesi" gerektiği vurgulanmıştır[21].

Bu sebeple Anayasa md. 20 f. 3'te düzenlenen kişisel verilerin korunmasını esas alan temel hakkın ve Kişisel Verilerin Korunması Hakkında Kanun'un ilgili hükümlerini yorumlarken daima yukarıda zikredilen hususların dikkate alınması gerekecektir. Her ne kadar temel hak ve özgürlükler yatay ilişki çerçevesinde doğrudan uygulama alanı bulamasa da, kanun koyucu, yargı ve idarenin bu temel hak ve özgürlükleri esas alması gereği yadırganamaz[22]. Dolayısıyla çatışan farklı menfaatler arasında bir denge kurulması gerekmektedir.

2. Kişisel Verilerin Korunması Hakkında Kanun'un Esas Aldığı Temel İlkeler ve Big Data'ya Etkileri

a. Kişisel Verilerin Korunması Hakkında Kanuna Dair Genel Bilgiler

Kişisel Verilerin Korunması Hakkında Kanun md. 4 f. 2'de kişisel verilerin işlenmesi çerçevesinde dikkate alınması gereken ilkeler, "*a) hukuka ve dürüstlük kurallarına uygun olma; b) doğru ve gerektiğinde güncel olma; c) belirli, açık ve meşru amaçlar için işlenme; ç) işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve d) ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme*" olarak tanımlanmıştır[23].

Ayrıca kanunda kişisel veriler ile özel nitelikli kişisel veriler arasında bir ayırım yapmaktadır. Md. 3 f. 1 b. d)'de yapılan tanıma göre kişisel veri, "*[k]imliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi*" esas almaktadır. Dolayısıyla kişisel veri kavramının çok geniş bir uygulama alanına sahip olduğu söylenebilir. Özel nitelikli kişisel veri ise, md. 6 f. 1'e göre "*[k]işilerin 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*

---

[19] Hackenburg, Multimedia-Recht, kn. 16.

[20] Bu terimi "kişinin kendisiyle ilgili kişisel verileri üzerindeki tasarruf hakkı" olarak nitelendirmek mümkündür.

[21] The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality.

[22] Claus-Wilhelm Canaris, Grundrechte und Privatrecht, Archiv für die civilistische Praxis (AcP), 184 (1984), s. 202, 222.

[23] İsviçre Kişisel Verilerin Korunması Kanunu için bkz. Nicole Beranek Zanon, Big Data und Datensicherheit, in: Rolf H. Weber & Florent Thouvenin (eds.) Big Data und Datensicherheit – Gegenseitige Herausforderungen, Zürich, 2014, s. 85, 92 vd.

ve genetik verileri"dir. Özel nitelikli verilerin işlenmesi, bir takım özel şartlara bağlanmıştır. Burada da ölçülülük ilkesinin bir yansımasını görmek mümkündür. Gerçekten de özel nitelikli kişisel veri, kişilik hakkının doğrudan özüyle bağlantılı olduğu için bu hakka yapılan müdahale için de özel şartlar getirilmiş, bir diğer ifade ile müdahalenin meşru dayanağının şartları ağırlaştırılmıştır.

Çalışmanın başlangıcında kişisel verilerin korunması ile kişilik hakkı arasındaki bağlantıya işaret edilmiş, kişisel verilerin korunmasının kişilik hakkının bir görünümü niteliğinde olduğu tespit edilmiştir. Dolayısıyla Kişisel Verilerin Korunması Hakkında Kanun md. 3 f. 1 b. d)'de yapılan tanımın uygulama alanına giren her verinin, aynı zamanda kişilik hakkının bir parçası olarak korunacağını söylemek isabetli olacaktır. Bunun sonucu olarak ilgili tanımda belirtilen unsurları taşıyan verilerin korunması da, bir mutlak hak niteliği taşıyacaktır. Ancak hemen belirtelim ki kanun koyucu, söz konusu mutlak hakkın derecesine göre bir ayırıma gitmiş, "basit" kişisel verilerin işlenmesini haklı kılacak şartları ve "nitelikli" kişisel verilerin işlenmesini meşru kılacak sebepleri ayrı ayrı belirtmiştir.

Yine md. 11 uyarınca herkes, ilgili veri sorumlusuna başvurarak kendisiyle alakalı kişisel verilerin işlenip işlenmediği hususunda bilgi alma hakkına sahiptir. Aynı hüküm çerçevesinde birey, işlenme amacını, verilerin bu amaca uygun şekilde işlenip işlenmediğini, verilerin üçüncü kişilere aktarılıp aktarılmadığını sorma ve bunların düzeltilmesini talep etme hakkına sahiptir. İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkması halinde bireye itiraz hakkı tanınmakta ve nihayet kanuna aykırı olarak işlenen kişisel veriler sebebiyle zarar meydana geldiğinde zararın giderilmesi talep edilebilmektedir.

b. Kural: Kişisel Verilerin İşlenmesi Yasağı

Birçok hukuk düzeninde olduğu gibi Kişisel Verilerin Korunması Hakkında Kanun da kural olarak kişisel verilerin işlenmesini yasaklamıştır (bkz. md. 4). Ancak kişinin rızası (kişisel verilerin işlenmesiyle alakalı olarak md. 5 f. 1; nitelikli kişisel verilerin işlenmesi hususunda md. 6 f. 2, verilerin aktarılması hususunda md. 8 ve kişisel verilerin yabancı bir ülkeye aktarımı konusunda md. 9 f. 1 çerçevesinde düzenlemeler öngörülmüştür) ya da kanuni bir dayanak (md. 5 f. 2, md. 6 f. 3, md. 8 f. 2 ve md. 9 f. 2 ve 5) söz konusu olduğu takdirde kişisel verilerin işlenmesi mümkün kılınmıştır. Uluslararası sözleşmelerden doğan yükümlülükler de benzer şekilde kişisel verilerin işlenmesi için meşru bir dayanak niteliği taşımaktadır.

Oysa Big Data, niteliği itibariyle verilerin çokluğundan beslenmektedir. Zira yukarıda da belirtildiği gibi Big Data'nın temel karakteristik özelliklerinden biri verilerin hacmidir. Verilerin çokluğu sayesinde yeni ve daha kaliteli sonuçların elde edilmesi amaçlanmaktadır. Nitekim uygulamaya bakıldığında da verilerin toplanması ve işlenmesinin istisna değil, bilakis kural olduğu bir hakikattir[24]. Bu sebeple söz konusu kuralın nasıl uygulanacağı ve kural ihlallerinin nasıl müeyyide altına alacağı sorusu önem kazanacaktır.

Bu bağlamda öncelikle belirtelim ki, verilerin anonim hale getirilmesi kanaatimizce yeterli değildir. Zira büyük çapta veriler anonim hale getirilse dahi, verilerin çapı büyüdükçe kişilerin kimliğinin saptanması da kolaylaşacaktır.

[24] Bkz. Hackenburg, Multimedia-Recht, N 15-17.

Özellikle AOL ve Netflix örnekleri, bu bulguyu desteklemektedir. İki şirket milyonlara varan kullanıcı bilgilerini anonim hale getirerek internete sunmuş, bunun üzerine bazı kullanıcıların kimliği, veri uzmanları tarafından tespit edilebilmiştir[25].

Dolayısıyla kişisel verilerin işlenmesinin kural olarak yasaklanması, kanaatimizce uygulamada istisna hükümlerinin önemini artıracaktır. Bir diğer ifade ile ilgili istisna hükümlerine geniş bir uygulama alanı kazandırma girişimleri artacaktır. Özellikle özel hukuk alanında iki hükme değinmekte fayda vardır. Bunlardan birincisi, md. 5 f. 2 b. c)'de belirtilen istisna hükmüdür. Buna göre *"[b]ir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması"* halinde kişisel veriler işlenebilecektir. Dolayısıyla Big Data'nın olanaklarından istifade etmek amacıyla veri işleyen tarafın bu hükümden hareketle kendisine meşru bir dayanak arama girişiminde bulunması beklenebilir. Benzer şekilde aynı hükmün f) bendine göre *"[i]lgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması"* halinde verinin işlenmesi mümkündür. Bu bağlamda başlangıçta zikredilen menfaat çatışmasına değinmek isabetli olacaktır. Nitekim her iki istisnai hüküm yorumlanırken bir menfaat çatışmasının söz konusu olduğu söylenebilecektir. Hatta f) bendinde açıkça "ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla" denilmekle, çatışan farklı menfaatlerin bir dengeye oturtulması zorunluluğuna bizzat işaret edilmektedir. Dolayısıyla kişisel verilerin korunmasına dair temel hakkın diğer temel hak ve özgürlüklerle çatışması halinde sınırlandırılabileceğini bir kez daha vurgulamakta fayda vardır. Bu hak, veri işleyen gerçek ya da tüzel kişinin haklı menfaatleri dolayısıyla sınırlandırılabilir. Kuşkusuz bu sınırlandırma, somut olay şartlarına göre değerlendirilecektir. Ancak şu kadarını ifade edelim ki kişisel verinin kişilik hakkının özüne yaklaştığı derece ve ölçüde veriyi işleyen kişinin söz konusu veriyi işlemekte menfaati bulunmalıdır ki bu durum kişilik hakkının ihlal edilmesini meşru kılabilsin. Nitekim bu husus, bizzat kanun tarafından benimsenmiştir. Kişisel veri ile özel nitelikli kişisel veri arasında bir ayırıma giden kanun koyucu, kişilik hakkının ihlal derecesi arttıkça veri işlenmesi için daha ağır şartlar aramıştır.

c. İlgili Kişinin Açık Rızası

Md. 3 f. 1 b. a)'da açık rıza, "belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza" olarak tanımlanmıştır. Gerek md. 5 f. 1, gerek ise md. 6 f. 2'ye göre kişisel verilerin ve özel nitelikli kişisel verilerin işlenmesi için kişinin açık rızası gerekmektedir. Nihayet kişisel verilerin aktarımı için de açık rıza şartı öngörülmüştür.

Bu bağlamda önemle belirtelim ki kişisel verilerin işlenmesine dair açıklanacak alelade bir rıza, kanunda öngörülen şartları karşılayacak nitelikte değildir. Bilakis kanun, açık, belirli bir konuyla bağlantılı ve bilgilendirmeye da-

---

[25] New York Times gazetecileri, AOL tarafından alenileştirilip internete konulan kullanıcı bilgileri üzerinden kullanıcıların bazılarının kimliğini tespit etmeyi başarmışlardır, bkz. Michael Barbaro/Tom Zeller, A face is exposed for AOL searcher Nr. 441749, New York Times, 09.08.2008. Benzer bir örnek için bkz. Ryan Singel, Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims, where a re-identification of Netflix-User's data was possible although data was anonymized by Netflix before.

yanan özgür bir rıza koşulu getirmektedir. Dolayısıyla uygulamada sıkça rastlanan kişisel verilerin işlenmesine dair genel ve geniş çaplı bir rıza yeterli olmayacaktır. Rızanın açıklandığı esnada ilgili kişinin hangi amaç için rızasını açıkladığı belirli olmalıdır. Kanunda öngörülen bir diğer koşul ise bilgilendirmeye dayanan rızadır. Ancak yine uygulamada durumun çok farklı olduğunu tespit etmek mümkündür. Gerçekten de şirketler, çok uzun ve karmaşık şekilde sundukları bilgilendirme formlarıyla ilgili kişinin rızasını almaya çalışmaktadırlar. Son olarak ilgili rızanın özgür iradeyle açıklanması şartı getirilmiştir. Bu çerçevede de özellikle bir hizmetin ya da ürünün satın alınmasını, kişinin onayına bağımlı kılan hükümler sorun teşkil etmektedir.

d. Amaçla Sınırlı Olma

Rıza ilkesi doğrudan amaçla sınırlı olma ilkesiyle bağlantılıdır. Amaçla sınırlı olma ilkesine göre belirli bir amaç için elde edilen kişisel veri, bu amaç dışında kullanılmamalıdır. Nitekim md. 4 f. 2 b. ç)'ye göre " kişisel verilerin işlenmesi, *"[i]şlendikleri amaçla bağlantılı, sınırlı ve ölçülü"* olmaları şartına bağlanmıştır. Dolayısıyla kişisel verilerin işlenmesi, başlangıçta açık rızanın açıklandığı amaca uygun şekilde gerçekleştirilmeli, bu amaçla bağdaşmayan işlemler için ise yeniden açık rıza aranmalıdır[26]. Özellikle bu son husus, veri minimizasyonu (asgarilik) ve amaçla sınırlı olma ilkelerinin bir göstergesidir.

Kanunun bu çerçevede güttüğü amaç, verilerin depolanmasının önüne geçilmesidir. Ayrıca ölçülülük ilkesi sayesinde toplanan veri miktarının asgari miktara çekilmesi amaçlanmaktadır. Mesela cep telefonlarında kullanılan "el feneri" uygulaması, kurulum için bütün kişiler listesine, resimlere, videolara, maillere ve diğer kişisel bilgilere ulaşım talebinde bulunduğunda bu şekilde geniş çaplı verinin ilgili uygulamanın kurulumu için gerçekten de gerekli olup olmadığı sorusuna cevap aramak gerekecektir. Özellikle ölçülülük ilkesi dikkate alındığında bu denli geniş çapta verilere ulaşımın gerekli olmayacağı sonucuna varmak mümkün olacaktır[27]. Dolayısıyla her somut olayda çatışan menfaatlerin makul bir dengeye oturtulması gerekecektir. Bu netice de başlangıçta işaret edilen farklı temel hak ve özgürlüklerin çatışması konusunu hatırlatmaktadır.

Yukarıda zikredilen hususlar göstermektedir ki kanunun öngördüğü koşullar, Big Data'nın kullanımını imkânsız hale getirebilecek niteliktedir. Nitekim olabildiğince büyük miktarda veriden beslenen Big Data ile verilerin toplanması ve işlenmesini belirli amaçlara bağlı kılarak minimize etmeye çalışan kanuni düzenleme birbiriyle bağdaşmamaktadır. Bu çerçevede karşılaşılacak en temel sorun, verilerin toplandığı ve rızanın açıklandığı esnada verilerin işleneceği her amacın öngörülebilir olmamasıdır. Öte yandan geniş ve genel anlamda kaleme alınan rıza beyanları da TBK md. 20 vd. hükümleri çerçevesinde özellikle içerik denetimi çerçevesinde sorunlara sebebiyet verecek niteliktedir[28].

---

[26] İsviçre Kişisel Verilerin Korunması Kanunu md. 4 daha esnek bir mekanizma öngörmektedir.

[27] Örneğin kişinin mahrem fotoğraflarının belirli bir uygulamanın daha da iyi hale gelmesine hizmet edeceği hususunda ciddi tereddütler mevcuttur.

[28] Peter Katko/Ayda Babaei-Beigi, Accountability statt Einwilligung? Führt Big Data zum Paradigmenwechsel im Datenschutz? MultiMedia und Recht (MMR) 2014, s. 360, 362; Rolf H. Weber, Big Data: Rechtliche Perspektive, in: Rolf H. Weber & Florent Thouvenin (eds.) Big Data und Datensicherheit – Gegenseitige Herausforderungen, Zürich, 2014, s. 17, 25.

Nihayet verilerin asgari seviyeye indirilmesi ilkesi, Big Data konseptine büsbütün aykırılık teşkil etmektedir.

e. Sorumluluk İlkesi

Yukarıda da belirtildiği üzere herkes, md. 11 doğrultusunda kendisiyle alakalı kişisel verilerin işlenip işlenmediği hususunda bilgi alma, işlenme amacını, bu amaca uygun şekilde işlenip işlenmediğini, üçüncü kişilere aktarılıp aktarılmadığını sorma ve bunların düzeltilmesini talep etme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkması halinde itiraz etme hakkına sahip olmakla birlikte[29] kanuna aykırı olarak işlenen kişisel veriler sebebiyle zarar meydana geldiğinde zararın giderilmesini de talep etme hakkına sahiptir.

Öncelikle tazminat hususuna bakıldığında kanunda öngörülen mekanizmanın bir kusur sorumluluğu hali olduğunu kabul etmek bir hayli zor olacaktır. Nitekim kanun koyucu kusur şartını aramamıştır. Kanaatimizce ilgili hükümde öngörülen tazminat yükümlülüğünün bir sebep sorumluluğu niteliği taşıdığını kabul etmek daha isabetli olacaktır. Zira veri sorumlusu, md.12'de öngörülen şartları yerine getirdiği takdirde ilgili kişiyi hala mesul kılmanın bir anlamı olmayacaktır. Bu sebeple kural olarak zarar meydana geldiğinde veri sorumlusunun md. 12'de öngörülen yükümlülüklerini yerine getirmediği kabul edilmeli, ancak veri sorumlusunun ilgili hükümde öngörülen bütün koşulları yerine getirdiğini ispat etmesi halinde kendisine kurtuluş imkânı tanınmalıdır.

Yukarıda açıklanan koruma mekanizmasının zayıf noktası ise, kişisel veri sahibi ile kişisel veri işleyen kişi arasında interaktif bir iletişimin olmayışıdır. Gerçekten de kişisel veri sahibi sadece bilgi talebinde bulunabilmekte, oysa kendisine sunulan bilginin doğru ve tastamam olup olmadığını kontrol etme imkânından mahrum bırakılmaktadır. Mesela veriyi işleyen kişi kişisel verileri yabancı bir ülkeye aktardığında ve bu hususu talepte bulunan kişiye ifşa etmediğinde verisi aktarılan kişinin yabancı ülkede kişisel verilerinin peşine düşmesi çok zor olacaktır.

III. ÇÖZÜM ÖNERİLERİ

Yukarıda kısaca işaret edildiği üzere Kişisel Verilerin Korunması Hakkında Kanun'un temel ilkeleri, özellikle açık rıza ve amaca bağlı kalma hususları ile devasa çapta verilerin işlenmesi ve analizini esas alan Big Data konsepti birbiriyle uyum halinde gözükmemektedir. Öte yandan kanunda benimsenen koruma ve özellikle tazminat mekanizması proaktif, yani henüz zarar meydana gelmeden müdahale etmeye elverişli olmamakta, ancak zarar meydana geldikten sonra devreye girmektedir. Kişisel verisi işlenen kişi bütün sürecin aktif bir parçası değildir. Dolayısıyla bir sonraki aşamada işaret edilen sorunların yeni kanun çerçevesinde nasıl çözüme ulaştırılabileceği hususunda muhtemel çözüm önerileri sunulacaktır.

---

[29] Ayrıca md. 19 GDPRP'ye göre bireyin kişisel verilerinin işlenmesine itiraz etme hakkı mevcuttur. İtirazın ardından veri işleyen ancak meşru ve özellikle verisi işlenen kişinin menfaatlerinden daha ağır bir sebep sunduktan sonra verileri işleyebilecektir.

1. Açık Rıza ve Amaca Bağlı Kalma

a. Öneriler

Yukarıda da işaret edildiği üzere yeni kanun, iki temel ilkeye dayanmaktadır. Bunlar, kişisel verisi toplanan ve işlenen kişinin açık rızası ve verinin toplandığı esnada belirtilen amaca bağlılıktır. Oysa uygulamaya bakıldığında karmaşık ve aşırı uzunlukta olan rıza beyanlarına rastlamak mümkündür. Amerika Birleşik Devletleri'nde yapılan bir araştırmaya göre ortalama bir vatandaş internet ortamında kişisel verilerin işlenmesiyle alakalı karşısına çıkan her bilgilendirmeyi okumak istemesi halinde yılda 200 saatini bu işe ayırmak zorunda kalacaktır[30]. Dolayısıyla açık rıza ve amaca bağlılık ilkeleri, hayatın gerçeklerinden uzak olduğu gerekçesiyle eleştirilmekte, hatta açık rıza kıstasının tamamiyle terkedilmesi gerektiği savunulmaktadır[31]. "Kişisel Verilerin Yeniden Değerlendirilmesi"[32] başlığı altında Dünya Ekonomik Forumu çerçevesinde de açık rıza kıstasının terk edilmesi, bunun yerine sorumluluk ilkesine ağırlık verilmesi önerisi getirilmiştir[33].

AB Tüzüğü'nde de amaca bağlılık hususu ele alınmıştır. Tüzüğün 2012 yılında yayınlanan ilk halinde kişisel verinin toplandığı esnada belirtilen koşulların mevcut olması halinde amacın değiştirilebileceği belirtilmişken[34] (ki bu düzenleme Alman Kişisel Verilerin Korunması Kanunu § 28[35] düzenlemesiyle örtüşmektedir) Tüzüğün nihai halinde veri işleyen kişi, çatışan menfaatleri dengeye oturtmakla mükellef kılınmıştır[36]. İlgili düzenlemeye göre kişisel veri işleyen kişi ya da kuruluş, kişisel verinin toplanması esnasında belirtilen amacın, sonradan ortaya çıkan amaçla örtüşüp örtüşmediğini kendi kendine denetlemekle yükümlüdür. Bu çerçevede veri işleyen özellikle önceki amaç ile sonradan ortaya çıkan amaç arasındaki her türlü bağlantıyı tespit etmek, veri sahibi ile veri işleyen arasındaki ilişkiyi dikkate alarak verinin hangi bağlamda toplandığını göz önünde bulundurmak, kişisel verinin niteliğini dikkate almak, öngörülen amaç değişikliğinin muhtemel sonuçlarını değerlendirmek ve mevcut koruma mekanizmalarını (şifreleme ve anonim hale getirme imkânları) göz önünde bulundurmakla mükelleftir. Bu da ilgili düzenlemenin sorumluluk ilkesine verdiği önemi açıkça gözler önüne sermektedir.

---

[30] Aleecia M. McDonald/Lorrie Faith Cranor, The cost of reading privacy policies, available at lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf [Erişim: Ağustos 2016].

[31] Fred H. Cate/Peter Cullen/Viktor Mayer-Schönberger, Data Protection Principles for the 21st Century; Florent Thouvenin, Erkennbarkeit und Zweckbindung, s. 61, 78.

[32] Rethinking Personal Data.

[33] World Economic Forum, Unlocking the Economic Value of Personal Data, s. 11.

[34] Md. 6 f. 4: "Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract."

[35] (1) The collection, storage, modification or transfer of personal data or their use as a means of fulfilling one's own business purposes shall be admissible

1. when needed to create, carry out or terminate a legal obligation or quasi-legal obligation with the data subject [...].

(2) Transfer or use for another purpose shall be admissible:

1. under the conditions given in sub-Section 1 first sentence No. 2 or No. 3, [...].

[36] Bkz. Tüzük md. 6 f. 3a.

b. Kanaatimiz

Uzun ve karmaşık bilgilendirme beyanlarının ancak şekli bir öneme sahip olduğu gerçeği yadsınamaz. Gerçekten de uzun ve karmaşık bilgilendirme notlarının hukukçular tarafından dahi sonuna kadar okunmadığı hususunda tereddüt etmemek gerekecektir. Ancak bu demek değildir ki kişisel verilerin işlenebilmesi için ilgili kişinin açık rızasına başvurulmasın. Bilakis; kişisel verilerin işlenmesi, bizzat Anayasa tarafından koruma altına alınmış olan bir temel hak ve özgürlük ile doğrudan alakalıdır. Dolayısıyla, kanunda açıkça öngörülen istisnalar dışında, temel hak ve özgürlüğüne müdahalede bulunulan kişinin iradesi açıkça beyan edilmeden bu hakkın kısıtlanması mümkün olmamalıdır. Bilakis, şayet Kişisel Verilerin Korunması Hakkında Kanun çerçevesinde düzenlenen istisnai hükümler saklı kalmak kaydıyla, tam bu açık irade ifadesi, temel hak ve özgürlüğe yapılan müdahaleyi meşru kılacak yegâne unsurdur. Yukarıda verilen örnekler de göstermektedir ki içinde bulunduğumuz bilişim çağında ve özellikle Big Data'nın sunduğu imkânlar karşısında kişinin iradesi halen esas alınmak isteniyorsa, açık rıza konseptinin muhafaza edilmesi zorunludur. Nitekim hür irade, irade serbestisi ilkesine dayanan özel hukuk sistemimizin de yegâne unsurudur. Dolayısıyla temel hak ve özgürlüğe yapılan müdahaleyi meşru kılacak bir irade yok ise, özel hukuk düzeninin esas aldığı bir serbestiden de bahsetmek imkân dâhilinde olmayacaktır.

Öte yandan kişisel verilerin korunmasına dair temel hak ve özgürlüğün sınırlandırılamaz nitelikte olmadığını bir kez daha tekrar etmekte fayda vardır. Dolayısıyla diğer tarafın menfaatlerinin, özellikle temel hak ve özgürlüklerinin ihlal edildiği durumlarda bu temel hak ve özgürlüğün sınırlarının belirlenmesi gerekecektir. Dolayısıyla bu hususu da açık rıza ilkesi çerçevesinde dikkate almak gerekecektir.

Çözüm yolu olarak açık rıza ilkesinden feragat edilmemesi gerektiği, fakat aynı zamanda açıklanan rızanın niteliğinin, kalitesinin artırılması gerektiği söylenebilir. Bir diğer söyleyişle açık rıza beyanı, sadece bir formalite, şekli bir unsur olmakla kalmamalı, açıklanan rıza gerçekten de ilgili kişinin rızasını yansıtır nitelikte olmalıdır. Dolayısıyla açık rıza şartından tamamiyle feragat etmek yerine çatışan menfaatler arasında bir denge kurmayı amaçlayan 29. Madde Çalışma Grubu'nun (Art. 29 Data Protection Working Party[37]) önerilerini esas almak daha isabetli gözükmektedir. Bu öneriler özetle 1) kişisel verilere sunulan bilgilerin basit ve anlaşılabilir formatta olması[38]; 2) kişisel verisi işlenen kişi için çok aşamalı bilgilendirme beyanlarının sunulması[39] ve bütünüyle kanuna uygun, fakat çok aşamalı konsepte uygun olacak şekilde kısa ve anlaşılır bilgilendirme notlarının esas alınmasıdır. Dolayısıyla kanunun esas aldığı açık rıza kıstası yukarıda belirtilen unsurlar dikkate alınarak yorumlandığında açık rıza sadece bir formalite olmaktan çıkarak kişinin iradesini ifade eden,

---

[37] ARTICLE 29 Data Protection Working Party, Opinion 10/2004 on More Harmonised Information Provisions.

[38] Veri sahibinin bilinçli tercihte bulunabilmesi için neye onay verdiğini daha iyi anlaması, büyük önem taşımaktadır. Bu sayede veri işleyenin davranışlarını da etkileme imkânı doğacaktır. Dolayısıyla kişilerin (özellikle çocukların) şartlarına uygun bilginin sunulması gerekmektedir.

[39] Çok aşamalı bilgilendirmeler sayesinde kişi ihtiyaç duyduğu aşamaya daha iyi yoğunlaşıp daha kaliteli bilgi edinme imkânına sahip olacaktır. Zaman ve mekân darlığı dikkate alındığında çok aşamalı bilgi notları okunurluğu da artırmaktadır.

açıklanan iradenin gerçekten de bilgilendirmeye dayandığını temin eden bir unsur haline gelecektir.

2. Şeffaflık

Kanunun 10. maddesine göre veri sorumlusu ilgili kişilere *"a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi ve d) 11 inci maddede sayılan diğer hakları konusunda bilgi vermekle yükümlüdür."* İlgili hükümden de görüleceği üzere bu çerçevede güdülen amacının şeffaflık sağlamak olduğu söylenebilir. Ancak bazı eksikliklerin de olduğu şüphesizdir. Özellikle Big Data sebebiyle bireyin ilgili düzenleme çerçevesinde tamamiyle bilgilendirilmesi imkânsız olabilir. Gerçekten de günümüz teknolojisinin sunduğu olanaklar, örneğin "profiling" olarak nitelendirilen ve en menfi tercümesiyle "fişleme" olarak açıklayabileceğimiz teknoloji dikkate alındığında kişinin kişisel verisinin kullanılıp kullanılmadığı ve hangi amaçla kullanıldığı hususunda bilgi sahibi olması yeterli değildir[40]. Mesela Facebook farklı ırktan olan kişilere farklı bilgi sunan bir algoritma geliştirdiğinde Facebook tarafından ilgili kişiye kişisel bilgilerinin reklam amacıyla işlendiği bilgisinin verilmesi yetersiz kalacaktır.

Dolayısıyla münhasıran otomatik sistemler vasıtasıyla elde edilen neticeler çerçevesinde ilgili kişiye sunulacak bilgi, "ilgili sistemin mantığına dair bilgileri, kişisel verilerin işlenmesinin ilgili kişi açısından ne derece önem taşıdığını ve amaçlanan sonuçları" içermelidir. Nitekim AB Tüzüğü, md. 14 f. 1a b. h) çerçevesinde bilgilendirme yükümlülüğünü yukarıda zikredilen hususlarla genişletmiştir. Bu sayede ilgili kişi, açıkladığı rızanın sonuçlarını öngörebilecek bir konuma sahip olacaktır. Bu da aynı zamanda açıklanan rızanın daha kaliteli olmasına sebebiyet verecek ve şeffaflığı da artıracaktır. Önemle belirtelim ki elbette ilgili kişinin kendisine sunulan bu bilgileri hiçbir şekilde dikkate almadan rızasını açıklaması ihtimal dâhilindedir. Ancak kanunun amacı en azından kişilere böyle bir imkânın sunulmasını sağlamak olmalıdır. Dolayısıyla kişisel verilerin algoritmalar sayesinde işlenmesi halinde kanaatimizce md. 10 yorumlanırken AB Tüzüğü md. 14 f. 1a b. h)'de belirtilen unsurların da dikkate alınması isabetli olacaktır[41].

3. Mahremiyetin Tasarım Aşamasında Dikkate Alınması ve Sorumluluk İlkesi

Geçtiğimiz yıllarda seçim özgürlüğü ve hür iradeyi muhafaza etmek amacıyla Mahremiyetin Tasarım Aşamasında Dikkate Alınması olarak tercüme edebileceğimiz "Privacy by Design" isimli bir konsept ortaya atılmıştır. Buna göre mahremiyet, hukuki, teknik ve organizasyonel açıdan daha henüz gelişim aşamasında temel bir unsur olarak esas alınmaktadır[42]. İlgili konseptin temel ilkeleri ise reaktif değil proaktif davranılması, mahremiyetin tasarım aşamasında ve temel bir unsur olarak dikkate alınarak tatbik edilmesi sayesinde esas bir

---

[40] İsviçre Hukuku için bkz. Thouvenin, Erkennbarkeit und Zweckbindung, s. 61, 63 vd.

[41] İsviçre Kişisel Veriler Kanunu md. 4 f. 4'ün geniş uygulama alanı olması doğrultusunda bkz. Thouvenin, Erkennbarkeit und Zweckbindung, s. 61, 63, 66.

[42] İsviçre Hukuku için bkz. Rehana Harasgama/Aurelia Tamò, Smart Metering und Privacy by Design im Big-Data-Zeitalter, s. 117 vd.

unsur ve sistemin vazgeçilmez bir parçası haline gelmesi ve bu sayede mahremiyetin diğer ilkelerle çatışması yerine uyumlu hale getirilmesi, verinin bütün yaşam süreci esnasında mahremiyetin dikkate alınması, görülebilirlik ve şeffaflık olarak özetlenebilir[43].

AB Tüzüğü md. 23 de benzer düzenlemeler içermektedir. Buna göre veri sorumlusu, kişisel verilerin korunmasına dair ilkelerin uygulanabilmesi için gerekli ve uygun teknik ve organizasyonel önlemleri almak zorundadır. İlgili hükmün devamında veri sorumlusunun elde ettiği kişisel verilerin ancak belirtilen amaç doğrultusunda kullanılması için gerekli önlemleri almak zorunda olduğu, bu kaidenin de verilerin hacmini, işlenmesinin kapsamını, muhafaza edilme süresini ve ulaşılabilirliği hususlarını kapsadığı belirtilmektedir. Bu önlemler sayesinde özellikle kişinin haberi ve müdahalesi olmaksızın kişisel verilerinin sayısı ve kimliği belirlenemeyen bir kitleye aktarılmasının önüne geçilmesi amaçlanmaktadır.

Bu sebeple her ne kadar Kişisel Verilerin Korunması Hakkında Kanun çerçevesinde pozitif bir düzenleme öngörülmemiş olsa da mahremiyet hususunun henüz algoritmalar yazılırken ve bilgi ya da veri işleme ve depolama sistemleri oluşturulurken dikkate alınması, hür iradenin korunması amacına hizmet edecek nitelikte olacaktır.

Esasen sorumluluk ilkesi de yukarıda zikredilen ilkeyle bağlantılıdır. Zira kontrol etmek yerine karar verme yetkisini ve sorumluluğunu veri sorumlusuna yüklemekle veri sorumlusu kendi kendine gerekli adımları atmaya gayret edecektir[44]. Ancak bu sistem elbette bir taraftan yaptırımların dikkate alınmasını, diğer yandan dikkate alınmadığında da öngörülen müeyyideyi kati surette uygulayan bir mekanizma gerektirmektedir.

Yukarıda zikredilen ilkeler ışığında yeni kanuna bakıldığında 12. madde f. 1 çerçevesinde sorumluluk ilkesinin dikkate alındığını, ancak "Privacy by Design" ilkesinin pozitif bir dayanak bulmadığını tespit etmek mümkündür. Maalesef kanunumuzun en temel eksikliklerinden birisi de burada yatmaktadır.

IV. SONUÇ

Önemle belirtelim ki yeni çıkan bir kanunu değerlendirmek, o kanunu yapmaktan daima daha kolaydır. Dolayısıyla Kişisel Verilerin Korunması Hakkında Kanun'un büyük ve önemli bir adım olduğu hususunda tereddüt etmemek gerekir. Özellikle Türk toplumunun kişisel veriler konusunda henüz gerekli özeni göstermediği dikkate alındığında yeni kanunun bir "paradigma kayması" olarak nitelendirilmesi dahi mümkündür. Özellikle kişilik hakkının bir görünümü olarak nitelendirilebilecek olan açık rıza kıstasının öngörülmüş olması özel hukuk açısından sevindiricidir. Sorumluluk ilkesi çerçevesinde veri sorumlularının daha dikkatli davranacağı ümidi de mevcuttur.

Öte yandan uluslararası platformlarda sürekli zikredilen veri işleyen ile kişisel veri sahibinin arasındaki iletişimi teşvik eden bir mekanizmanın öngörülmemiş olması üzücüdür. Bireyin kişisel verileri üzerindeki hâkimiyetini tamamiyle kaybetme riski çok yüksektir ve kanunun getirdiği koruma mekaniz-

---

[43] Daha geniş bilgi için bkz. Ann Cavoukian, Privacy by Design The 7 Foundational Principles, https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf [Erişim: Ağustos 2016].

[44] Weber, Big Data: Rechtliche Perspektive, s. 17, 27.

masında veri sorumlusu ile verisi işlenen kişi arasında interaktif bir ilişkinin kurulmasını öngören düzenlemeler mevcut değildir. Dolayısıyla söz konusu risk dikkate alınarak kişisel verisi işlenen kişinin bütün süreç boyunca sürece dâhil edilmesini teşvik eden bir mekanizma kanaatimizce günümüz teknolojisinin sunduğu imkânlar ışığında daha isabetli gözükmektedir.

KAYNAKÇA

ARTICLE 29 Data Protection Workıng Party, Opinion 10/2004 on More Harmonised Information Provisions, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf (08.04.2016).

Barbaro, M. & Zeller, T., A face is exposed for AOL searcher Nr. 441749, New York Times, 09.08.2008., available at www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all&_r=0 (08.04.2016).

Borne, K., Big Data, Small World: Kirk Borne at TEDxGeorgeMasonU, available at https://www.youtube.com/watch?v=Zr02fMBfuRA (08.04.2016).

Canarıs, C.-W., Grundrechte und Privatrecht, Archiv für die civilistische Praxis (AcP), 184 (1984), p. 202.

Cate, F.H. & Cullen, P. & Mayer-Schönberger, V., Data Protection Principles for the 21st Century; available at https://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiEjZyM4oHMAhWkJ5oKHS7GBzYQFggbMAA&url=http%3A%2F%2Fwww.oii.ox.ac.uk%2Fpublications%2FData_Protection_Principles_for_the_21st_Century.pdf&usg=AFQjCNFKf66M4OmJ-hxctbA8hxsEFlf0Og&cad=rja (08.04.2016).

Cavoukıan, A., Privacy by Design The 7 Foundational Principles, https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf (08.04.2016).

Cukıer, K., Big Data is better data, available at https://www.youtube.com/watch?v=8pHzROP1D-w (08.04.2016].

"Facebook fängt den Nutzer in seiner eigenen Weltanschauung ein", available at http://www.sueddeutsche.de/digital/algorithmen-wie-facebook-den-nutzer-in-seiner-eigenen-weltanschauung-einfaengt-1.2845656 (08.04.2016).

"Google DeepMind computer beats Go champion Lee Se-dol in shock 4-1 victory", available at http://www.independent.co.uk/life-style/gadgets-and-tech/news/google-deepmind-computer-beats-go-champion-lee-se-dol-in-shock-4-1-victory-a6931876.html (08.04.2016).

Hackenburg, W., Teil 16.7: Big Data, in T. Hoeren & U. Sieber & B. Holznagel (eds.), Multimedia-Recht, 42. Ergänzungsband, München 2015.

Harasgama, R. & Tamò A., Smart Metering und Privacy by Design im Big-Data-Zeitalter: Ein Blick in die Schweiz, in: R. H. Weber & F. Thouvenin (eds.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, p. 117.

Katko, P. & Babaeı-Beıgı, A., Accountability statt Einwilligung? Führt Big Data zum Paradigmenwechsel im Datenschutz? MultiMedia und Recht (MMR) 2014, p. 360.

McDonald, A. M. & Faıth Cranor, L., The cost of reading privacy policies, available at lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf (08.04.2016).

"Schwarze sehen bei Facebook andere Werbung als Weiße", available at http://www.jetzt.de/facebook/facebook-werbung-fuer-ethnien (08.04.2016).

Sıngel, R., Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims, 17.12.2009, available at http://www.wired.com/2009/12/netflix-privacy-lawsuit (08.04.2016).

Thouvenın, F., Erkennbarkeit und Zweckbindung: Grundprinzipien des Datenschutzrechts auf dem Prüfstand von Big Data, in: Rolf H. Weber & Florent Thouvenin (eds.) Big Data und Datensicherheit – Gegenseitige Herausforderungen, Zürich 2014, p. 61,

Weber, R. H., Big Data: Rechtliche Perspektive, in: Rolf H. Weber & Florent Thouvenin (eds.) Big Data und Datensicherheit – Gegenseitige Herausforderungen, Zürich 2014, p. 17.

World Economıc Forum, Unlocking the Economic Value of Personal Data: Balancing Growth and Protection, 2012, available at http://www3.weforum.org/docs/WEF_IT_UnlockingValueData_BalancingGrowthProtection_SessionSummary.pdf (08.04.2016).

Zanon, N.B., Big Data und Datensicherheit, in: Rolf H. Weber & Florent Thouvenin (eds.) Big Data und Datensicherheit – Gegenseitige Herausforderungen, Zürich 2014, p. 85.