Araştırma Makalesi/Research Article **Doi: 10.55009/bilisimhukukudergisi.1230809**

KİŞİSEL VERİ KAVRAMININ TÜKETİCİ AÇISINDAN İNCELENMESİ VE TÜKETİCİ VERİLERİNİ TEKNİK ANLAMDA KORUMAYA YÖNELİK UYGULAMALAR*

Examination of the Concept of Personal Data from the Perspective of the Consumer and Applications to Protect Consumer Data Technically

Dila Nur Halaçoğlu**

Öz

Kişisel veri, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" dir. Kişisel verinin sahip olduğu bilgi unsurunun, geniş bir alanı içine alması, farklı işlemler aracılığıyla ve kişiler farklı konumlardayken, kişisel veri üretiminin önünü açar. Bu durumlardan bir tanesi de kişilerin tüketici konumundayken kişisel veri üretmesidir. Teknolojinin gelişmesi ile tüketiciler farklı nitelikte kişisel veri oluşturmaya başlamıştır. Ayrıca kişisel verinin kaynakları da çoğalmıştır. Bu durum kişisel verilerin korunmasına teknik anlamda yaklaşılmasını gerekli kılmıştır. Kişisel verilerin teknik anlamda

---

* Bu makale Baskent Üniversitesi Sosyal Bilimler Enstitüsü, Prof. Dr. Kudret Güven danışmanlığında Dila Nur Halaçoğlu tarafından yazılan " Mesafeli Elektronik Sözleşmelerde Tüketicilerin Kişisel Verilerinin Korunması" başlıklı Yüksek Lisans tezinden türetilmiştir.

** Email: halacoglu96@gmail.com, ORCID: 0000-0003-1001-9373.

Makale Gönderim Tarihi/Received: 07.01.2023.

Makale Kabul Tarihi/Accepted: 06.04.2023.

Atıf/Citation: Halaçoğlu, Dila Nur. "Kişisel Veri Kavramının Tüketici Açısından İncelenmesi Ve Tüketici Verilerini Teknik Anlamda Korumaya Yönelik Uygulamalar." *Bilişim Hukuku Dergisi* 5, no. 1 (2023): 37- 74.

korunması bilgilendirme temelinde işleyen opt-in sistem çerçevesinde incelenebilir. Çünkü bu sistemde tüketiciler hem kişisel verileri üzerinde denetime sahip olurlar hem de veri işleme faaliyetinin meşru amaçlar için gerçekleştirildiğinden emin olabilirler. Bu anlamda makalenin amacı, kişisel veri kavramının tüketiciler açısından incelenmesi ve teknik anlamda verilerin ne tür uygulamalarla korunabileceğinin değerlendirilmesidir.

Anahtar Kelimeler: Kişisel Veri, Tüketici, Büyük Veri, Profilleme, Çerez Teknolojisi

Abstract

Personal data is "any information relating to an identified or identifiable natural person". The fact that personal data includes a wide area of information, paves the way for the production of personal data through different processes and when people are in different locations. One of these situations is when people produce personal data while they are consumers. With the development of technology, consumers have started to create different types of personal data. In addition, the sources of personal data have increased. This situation necessitated a technical approach to the protection of personal data. The technical protection of personal data can be examined within the framework of the opt-in system, which operates on the basis of information. Because in this system, consumers both have control over their personal data and can be sure that data processing is carried out for legitimate purposes. The purpose of this comprehensive article is to examine the perspectives of the concept of personal data and to evaluate what kind of applications can protect technical data.

Key Words: Personal Data, Consumer, Big Data, Profiling, Cookies

GİRİŞ

Tüketici, 6502 sayılı Kanun'da verilen tanımı ile "*ticari veya mesleki olmayan amaçlarla hareket eden gerçek veya tüzel kişiyi"* ifade eder. Bu anlamda tüketiciler, mal veya hizmeti özel kullanımları için edinen kişilerdir ve hukukumuzda özel olarak korunurlar.[1] Bunun sebebi tüketicilerin, ticari hayatın içindeki güçsüz taraf olmasıdır.[2] Tüketiciler, sadece tüketici işlemleri açısından değil, özellikle teknolojik gelişmeler ile birlikte gelişen elektronik ticaret işlemlerinde kişisel verilerin işlenmesi açısından da güçsüz konumdadırlar. Çünkü tüketiciler, dijital ortamda işlem gerçekleştirirken deneyimsizlik ve bilgisizlikten kaynaklı olarak irade dışı işlemler gerçekleştirebilmektedirler ya da gerçekleştirdikleri işlemlerin anlam ve önemini anlayamamaktadırlar.

Tüketicilerin sahip olduğu cihazların internete bağlanabilme özelliğinin artmasına paralel olarak çevrimiçi insan etkileşimlerinde de artma yaşanmıştır. Özellikle günümüzde elektronik ticaret işlemlerinin tüketiciler tarafından fazlasıyla tercih edilmesi ile dijital ortama veri aktarımı her geçen gün fazlalaşmaktadır. Tüketici verilerinin algoritmik sistemler aracılığıyla analiz edilmesi ile profil oluşturmaya yönelik işlemlerin şirketler tarafından ekonomik çıkar sağlama aracı kullanılmaya başlaması karşısında tüketicinin çevrimiçi ortam ile ilgili bilinçsizliği, tüketiciler açısından yeni bir sömürü alanı oluşturmuştur. Bu durum tüketiciler açısında mahremiyet kaygısını güçlendirmektedir.

Kişisel verilerin korunması için normatif alanda çeşitli düzenlemeler yapılmıştır. Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ve ülkemizde 2016 yılında yürürlüğe giren 6698

---

1 Aydın Zevkliler ve Çağlar Özel, *Tüketicinin Korunması Hukuku,* (Ankara: Seçkin Yayınları, 2016), 94.

2 Zevkliler ve Özel, *Tüketicinin,* 44.

sayılı Kişisel Verilerin Korunması Kanunu kişisel verilerin korunmasına yönelik kapsamlı düzenlemeler içerir. Bu düzenlemeler ile özellikle veri işleme faaliyetine şeffaflık ve öngörülebilirlik kazandırma hedeflenmektedir. Ancak günümüzde veri kavramının değerinde yaşanan değişim, veri elde yöntemlerinde yaşanan artış ve veri üretme kapasitesinin ulaştığı boyut gözetildiğinde kişisel verilerin sadece normatif alanda korunmasının yeterli olup olmayacağı tartışmalı bir konu haline gelmiştir. Özellikle biliçsiz ve sosyal yönden zayıf konumda bulunan tüketiciler açısından, teknolojinin tüketicilere adapte edilmesi ve bu şekilde veri dostu sistemler üretilme ihtiyacı doğmaktadır.

Çalışmamızın ilk bölümünde kişisel veri kavramının tüketiciler açısından incelenmesi yapılacaktır. Bu kapsamda özellikle dijital ortamda tüketici verilerinin edilmesine ve algoritmik sistemler vasıtasıyla yapılan profilleme işlemleri ile büyük veri kavramına değinilecektir. Ayrıca çerez teknolojisinin kişisel veri alanına ilişkin olan özelliklerine ilişkin açıklamalar yapılıp tüketicilerin çerez teknolojisindeki yeri değerlendirilecektir.

Çalışmamızın ikinci bölümünde tüketici verilerinin korunması için dijital ortamın teknik anlamda nasıl şekillenmesi gerektiği incelenecektir. Bu kapsamda "*Privacy by Design*" ve "*Privacy by Default*" kavramları ile "*Opt-in*" ve "*Opt-out*" sistemlere yönelik açıklamalar yapılıp kişisel verilerin ve tüketicilerin korunması bakımından incelemeler yapılacaktır. Özellikle opt-in sistemin veri odaklı ve tüketici için en verimli şekilde nasıl uygulanabileceği ve uygulaması esnasında ne tür kriterlere dikkat edilmesi gerektiği konusunda değerlendirmeler yapılarak normatif alana ek olarak teknik alanda da kişisel verilerin ne şekilde korunabileceği açıklanacaktır.

I. KİŞİSEL VERİ VE PROFİLLEME

A. Kişisel Veri Kavramı ve Tüketici Verileri

Kişisel veri kavramına ilişkin tanım, 6698 sayılı Kişisel Verilerin Korunması Kanun'u ve Avrupa Birliği Genel Veri Koruma Tüzüğü'nde (GDPR) verilmiştir. Buna göre kişisel veri, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" dir. Görüldüğü üzere kişisel veri, değerlendirme yapılırken bazı kriterlerin gözönünde bulundurulmasını gerektiren bir kavramdır. Bu kriterler Çalışma Grubu'nun (Article 29 Data Protection Working Party) ilgili raporunda detaylı bir şekilde açıklanmıştır.[3]

Kişisel verinin ortaya çıkmasında birbirine sıkı sıkıya bağlı ve birbirini besleyen dört kavram etkilidir. Bunlardan ilki "bilgi" (*any information)* kavramıdır. Kişisel verinin ana unsuru olarak bilgi esasen çok geniş bir çerçevede ifade bulmuştur. Çünkü bilginin kabulüne ilişkin bir sınırlandırma yapılmamıştır. Şöyle ki bilginin diğer kriterler birlikte kişisel veri oluşturabilmesi için objektif olması, doğruluğunun kanıtlanmış olması, kağıt üzerinde ya da sanal ortamda bulunması gerekmez. Başka bir anlatımla kişiye ilişkin sübjektif, doğruluğu kanıtlanmamış ve herhangi bir somut ortamda bulunmayan bilgiler de diğer kriterleri sağlamak koşuluyla kişisel veri oluşturabilir.[4] Bilginin gerçek bir kişiye (*natural person*) ilişkin *(relating to*) olması ve bu bilginin bir kişiyi tanımlaması ya da tanımlanabilir (*an identified or indentifiable*) kılması gerekir.

---

[3] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, erişim tarihi Aralık 21, 2022, 12251/03/EN (clinicalstudydatarequest.com.

[4] Opinion 4/2007 on the concept of personal data, 6-8.

Kişisel verinin sahip olduğu bilgi unsurunun, geniş bir alanı içine alması, farklı işlemler aracılığıyla ve kişiler, farklı konumlardayken kişisel veri üretiminin önünü açar. Bu durumlardan bir tanesi de kişilerin tüketici konumundayken kişisel veri üretmesidir. Tüketici kişisel verisi, kişiler (tüketiciler) ticari bir ilişkinin parçasıyken toplanan verilerdir.[5] Kişiler tüketici konumunda işlemlerde bulunurken birçok kişisel veri üretirler. Üretilen bu kişisel verilerin geleneksel kişisel veriler ve elektronik ticaretin gelişmesi ile ortaya çıkan kişisel veriler olarak sınıflandırılması mümkündür. Geleneksel kişisel veriler, internetin ortaya çıkmasından ve yaygınlaşmasından önce, tüketicilerin genellikle kağıt üzerinde oluşturduğu kişisel verileridir. Buna göre tüketicilerin kimlik bilgileri, adresleri, çeşitli demografik bilgileri (yaş, cinsiyet vb.) bu kapsamda sayılabilir. Bazı kişisel veriler ise internetin ve elektronik ticaretin yaygınlaşıp yeni teknolojilerin kullanılması ile oluşmaya başlamıştır. Bu tür kişisel verilerin geleneksel kişisel verilerden farkı, kişisel verinin öznesi olarak tüketicinin rızası ve beyanı dışında da ortaya çıkabilecek olması ve bir sözleşme ilişkisinde edimin yerine getirilmesine hizmet etmekten çok tüketicinin analiz edilip yönlendirilmesi amacına hizmet ediyor olmasıdır.

Yeni tür kişisel verilerin ortaya çıkmasının sebebi esasen bilginin elde edilme yöntemlerinin değişmiş olmasıdır.[6] Buna göre veri öznesi olarak tüketiciler, aktif davranışlarıyla kişisel veri üretebilecekleri gibi pasif konumda bulunurlarken de kişisel veri üretebilecek konuma gelmişlerdir. OECD'nin ilgili raporunda tüketici kişisel verileri, verilerin ortaya çıkma durumu esas alınarak gruplandırılmış ve dört kategoriye

---

5 OECD, Consumer Data Rights and Competition - Background note, (2020): 7, erişim tarihi Aralık 21, 2022, https://www.oecd.org/competition/consumer-data-rights-and-competition.htm.

6 OECD, Consumer Data Rights and Competition, 9.

ayrılmıştır. Buna göre kaynakları bakımından kişisel veriler şu şekildedir: "gönüllü veri" (*volunteered data*), "gözlemlenmiş veri" *(observed data*), "türetilmiş veri" (*derived data*), "edinilmiş ya da satın alınmış veri" (*acquired (purchased or licenced) data*). Gönüllü veriler, kişilerin aktif eylemleri ile oluşturulan verilerdir. Gözlemlenmiş veriler ve türetilen veriler ise bireyler pasif konumdayken, bireylerin takip edilip gözlemlenmesi ya da bireylerin eylemlerinin analiz edilmesi sonucunda ortaya çıkan kişisel verilerdir.[7] Belirtilen kişisel veri kaynaklarından anlaşıldığı üzere üç kademede gerçekleştirilen bir veri oluşum aşaması vardır ve bu aşamalarda veri bazen oluşturulmakta bazen ise sadece toplanmaktadır.[8] Ayrıca bazı tüketici verileri, kişisel veri işleme eyleminden önce mevcutken, profil oluşturmaya yönelik kişisel veriler önceden mevcut değildir; verinin elde edilmesinden sonra analiz edilmesi ile türetilirler.[9] İlk aşamada tüketicilerin kişisel verileri, onların aktif ya da pasif davranışları ile elde edilir.[10] Sonrasıda bilişim çağının araçları aracılığıyla analiz edilen veriler üçüncü aşamada, üçüncü aşama veri kontrolörlerine aktarılır.[11]

Kişisel veriler üzerinde gerçekleştirilecek her işlem, tüketicilerin verileri üzerindeki denetimini biraz daha azalır.

---

7 OECD, Consumer Data Rights and Competition, 9.

8 Francesco Banterle, "The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database *sui generis* Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis", Personal Data in Competition, Consumer Protection and Intellectual Property Law, Ed. Mor Bakhoum · Beatriz Conde Gallego Mark-Oliver Mackenrodt Gintarė Surblytė-Namavičienė, no: 28 (2018): 411-443.

9 Banterle, The Interface, s. 426.

10 I. Van Ooijen, Helena U Vrabec., "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective", *Journal of Consumer Policy*, (Aralık, 2018): 91-107.

11 Ooijen and Vrabec, Does the GDPR, 101.

Özellikle dijital ortamda ortaya çıkan kişisel verilerin soyut yapısı gereğince, tüketiciler tarafından deneyimlenmesi çok daha zordur[12]. Teknolojinin gelişmesi ve verinin kullanım alanlarının coğalması ile tüketicilerin kişisel verileri üzerinde kontol sahibi olması gitgide zorlaşmaktadır.[13] Ayrıca kişisel verilerin soyut yapısı, verilerin kolayca çoğlatılıp paylaşılmasına da neden olmaktadır.[14]

Tüketiciler kişisel verilerin sanal ortama aktarılması hususunda çok daha bilinçsizlerdir ve genellikle somut durumlara, soyut durumlara oranla daha fazla değer atfetme eğilimindedirler.[15] Bu nedenle dijital ortamda veri paylaşımına ilişkin eylemlerinde, gizlilik açısından kaygıları olsa dahi, bilinçsizce hareket edebilirler.[16] Örneğin bir tüketici bir sözleşmeye imza atma eylemini sorgularken web sitelerinin kişisel verilerinin işlenmesi için kendisinden alması gereken rızayı sorgulamadan (gizlilik açısından endişeleri olsa dahi) tek bir işlemle gerçekleştirir. Özellikle şirketlerin tüketici verilerinin elde edilmesi bakımından gösterdiği saldırgan tavır ve dijital ortamda bulunan verilere yönelik sızıntılar tüketicilerin veri

---

12 Ooijen and Vrabec, Does the GDPR, 101.

13 Ooijen and Vrabec, Does the GDPR, 91.

14 Ooijen and Vrabec, Does the GDPR, 101.

15 Tüketiciler nezdinde dijital olanın fiziksel olandan daha az değerli olmasına ilişkin olarak detaylı bilgi için bakınız: Atasoy, Özgün/Morewedge, Carey K., "Digital Goods Are Valued Less Than Physical Goods", *Journal of Consumer Research*, 2017.

16 OECD, tavsiye kararlarının yer aldığı raporunda hükümetler ile şirketlerin, tüketicilerin bilinçli kararlar almasını sağlamaya yönelik eğitilmesi için birlikte çalışması gerektiğini belirtmiştir. Tüketicilerin elektronik ticaret kapsamında kişisel veri güvenliği ile alakalı olarak da bilgilendirilmeleri gerektiği düşüncesindeyiz. OECD, Consumer Protection in E-commerce, OECD Recommendation, (2016): 18, erişim tarihi Aralık 22, 2022, https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf.

paylaşımına ilişkin endişelerini artırmaktadır. Ancak bu durum tüketicilerin dijital ortama veri aktarma kapasitesi etkilememektedir. Bu anlamda tüketiciler mahremiyetlerine ilişkin endişlere sahip olsalar dahi veri aktarımını azaltmaya yönelik eylemlerde bulunmamaktadırlar. Bu duruma "gizlilik paradoksu" denmektedir.[17]

Tüketicilerin kişisel verilerinin artık tüketicilerden bağımsız bir ticari değer haline dönüşmesi ile tüketiciler özellikle büyük şirketler nezdinde, çeşitli alanlarda profil oluşturulmasını sağlayan nesneler olarak görülmeye başlanmıştır. Tüketicilerin özellikle sanal ortamda gerçekleştirdiği eylemler, şirketlerin ticari amaçlarla kullandıkları çok geniş yelpazede kişisel verinin ortaya çıkmasına neden olmaktadır.[18] Tüketici verilerinin içerik bakımından yedi başlık altında gruplandırılması mümkündür. Bunlardan ilki "kullanıcı tarafından oluşturulan içerik" *(user generated content*) dir. Bu kategoriye tüketicilerin dijital ortamda yaptığı yorumlar, paylaştığı fotoğraf ve videolar girer. İkinci kategori, "aktiviteleri ve davranışsal verileri" (*activity or behavioural data*) dir. Tüketicilerin internette neler arattıkları, hangi web sitelerini kullandıkları ve hangi ürünü internet vasıtası ile ne kadar aldıkları gibi hususlar bu kapsamda değerlendirilir. Üçüncü kategori, "konum verileri" (*locational data*) dir. Tüketicilerin yerleşim yeri adresleri, IP adresleri ve coğrafi konum bilgileri, konum bilgisi kapsamında tüketici kişisel verilerini oluşturur. Dördüncü kategori demografik verilerdir. Tüketicinin yaşı, cinsiyeti, cinsel tercihi, politik

---

17 CMA, The Commercial Use of Consumer Data, (2015): 129, erişim tarihi Aralık 21, 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf.

18 CMA, The Commercial Use of Consumer Data, 23.

görüşü vb hususlar demografik veri kategorisinde yer alır. Beşinci kategori resmi nitelik taşıyan veriler *(identifying data of an official nature*) dir. Tüketicinin ismi, finansal durumu, hesap numarası, T.C. kimlik numarası tüketicinin resmi verileridir. Altıncı kategori, tüketicilerin parmak izleri gibi verilerinin yer aldığı "biyometrik veriler" dir. Son kategori ise "sosyal veriler" (*social data*) dir. Sosyal paylaşım sitelerinden başkaları ile kurulan iletişim bu kapsamda değerlendirilir.[19]

Çağımızda tüketicilere ait kişisel veriler, şirketler nezdinde ekonomik bir değer ifade etmektedir. Çünkü şirketler farklı içerikteki çok sayıda tüketici verisini analiz ederek, bu veriler doğrulanmamış olsa bile, faaliyetlerini yönlendirme imkanı bulmaktadırlar[20]. Bu doğrultuda ham halde bulunan verilerin tek başına fazla bir değeri yoktur ve verilerin ekonomik değeri esas olarak verilerin analiz edilmesi ile ortaya çıkar.[21] Verinin analiz edilmesi ile şirketler, pazarlama yeteneklerini geliştirerek müşterilere hitap etme noktasında reklam maliyetlerini düşürebilirler.[22] Ancak bu durum, şirketlerin ekonomik kaygıları ile tüketicilerin kişisel verileri üzerindeki egemenlik hakları noktasında bir çatışmanın doğmasına sebep olur. Bu çatışma nedeniyle gerek ulusal gerek uluslararası düzenlemeler ile veri işlenmesi belirli şartlara tabi kılınmıştır.

---

19 OECD, "Consumer Data Rights and Competition", 7-8.

20 Alessandro Acquisti, "The Economics of Personal Data and the Economics of Privacy", The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines, (2010): 9, erişim Tarihi Aralık 21, 2022, https://www.oecd.org/sti/ieconomy/46968784.pdf.

21 Zhijun Chen, "Privacy Costs and Consumer Data Acquisition: An Economic Analysis of Data Privacy Regulation", (2022): 3, erişim tarihi Aralık 22, 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4085923.

22 Acquisti, The Economics, 8.

Doktrinde şirketlerin kişisel verileri bu şekilde kullanmasının, dijital işlemlerde tüketicilere dayatılan nesnel bir işlem maliyeti olduğunu belirten görüşler[23] olsa da tüketici verilerinin yalnızca ekonomik değeri üzerinden metalaştırılarak yapılacak bir yorumun ticari hayatın güçsüz aktörü konumunda bulunan tüketicilerin korunması mantığı ile bağdaşmayacağı düşüncesindeyiz. Ayrıca şirketlerin tüketici verilerini kullanmasına yönelik olarak getirilecek bu şekilde bir yorum en başta, sadece gerekli olan kadar verinin işlenmesini gerekli kılan "veri minimizasyonu" ilkesine aykırılık oluşturur. Çünkü verinin bir işlem bedeli olarak görülmesi demek, yapılan işlemin artması ile bedelin yani veri işleme kapasitesinin artırılması demektir.

B. Profilleme ve Çerez Teknolojisi

Veri toplama, yorumlama ve verileri bir araya getirme işlemleri insanlar için her zaman bir arzu ve hedef olmuştur. Ancak teknoloji ve internet çağında gerçekleştirilen veri edinimini insanlık tarihinin diğer dönemlerinden ayırmak gerekir. Çünkü internetin ve internete bağlanabilen araçların yaygınlaşması ile kişilerin veri üretme kapasitesinde büyük bir değişim meydana gelmiştir.[24]

Veri oluşturma kapasitesindeki dramatik artış, "Büyük Veri" (*Big Data*) kavramının oluşturmuştur. Büyük veri, şirketler, yetkililer ve büyük kuruluşlar tarafından kontrol

---

[23] Katharine Kemp, "Concealed data practices and competition law: why privacy matters", European Competition Journal", (2020): 628-672, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3432769.

[24] Nikolaus Forgó, Stefanie Hänold ve Benjamin Schütze, "The Principle of Purpose Limitation and Big Data", *New Technology, Big Data and the Law*, Ed: Marcelo Corrales, Mark Fenwick, Nikolaus Forgó, (Singapore, part of Springer Nature, 2017): 17-42.

edilen, kapsamlı bir analize tabi tutulmuş, bilgi varlıklarıdır.[25] Kavram olarak bakıldığında büyük verinin sadece veri miktarını (*volume*) kapsadığı ve veri miktarının fazlalığını ifade ettiği düşünülmemelidir. Bu anlamda büyük veri, çok boyutlu bir kavramdır. Doktrinde büyük verinin boyutları "3V" (*volume, velocity, variety*) olarak ifade edilmiştir.[26]Veri miktarının yanında, veri çeşitliliği (*data variety*) ve veri hızı (*data velocity*) da büyük verinin boyutlarıdır. Buna göre büyük veri, büyük miktarda ve farklı türde, farklı kaynaklardan beslenen ve hızla biriken verilerdir.

Büyük veri uygulamalarındaki değişim ve ilerleme ile birlikte büyük veri kavramı da farklı boyutlar kazanmaktadır. Şöyle ki teknolojik gelişmelere ve artan veri işleme kapasitesine bağlı olarak verinin doğruluğu ve değeri sorgulanmaya başlanmıştır. Artık doktrinde büyük veri, "5V" ile ifade edilmektedir.[27] Belirtilenlere ek olarak veri doğruluğu (*data veracity*) ve veri değeri (*data value*) de artık büyük veri kapsamında bulunması gerekli unsurlar arasındadır. Buna göre veri güvenliğinin garanti edilmesi ile veri doğruluğunun; biriken verilerin analiz edilmesi yoluyla veri değerinin ortaya çıkarılması gerekir.[28]

Büyük verinin, veri toplama, veri depolama, veri analizi ve analiz sonuçlarını içeren dört temel aşamadan oluşan bir "değer zinciri" (*value chain*) olarak değerlendirilmesi de mümkündür.[29]

---

[25] Nancy J. King, Jay Forder , "Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data", *Computer Law & Security Review*, no:32, (2016): 696-714.

[26] Nikolaus, Hänold and Schütze, The Principle, 20.

[27] Emre Cihan Ateş, Erkan Bostancı ve Mehmet Serdar Güzel, "Big Data, Data Mining, Machine Learning, and Deep Learning Concepts in Crime Data", *Ceza Hukuku ve Kriminoloji Dergisi*, no:2, (2021): 293-319.

[28] Ateş, Bostancı ve Güzel, Big Data, 297.

[29] King, Forder, Data analytics, 698.

Bu değer zincirinde büyük veriyi etkili kılarak bir bakıma onu canlandıran şey toplanan verilerin analiz edilmesidir.[30] Başka bir anlatımla elde edilen veriler ile ekonomik, sosyal veya yasal bir değer yaratılmasını sağlayan işlem, verinin analiz edilmesidir. Çünkü analiz işlemi, veriler arasındaki bağıntının ortaya çıkmasını sağlayarak verileri etkili kılar.[31]

Elektronik ticaret işlemlerinde tüketiciler farklı nitelikte çok sayıda verisini dijital ortama aktararak bir tüketici işlemi gerçekleştirmeyi amaçlar. Bu anlamda web sitesinde üyelik oluşturarak isim ve soyadı başta olmak üzere, e-mail adresi, yerleşim yeri adresi, telefon numarası, ödeme bilgileri gibi sözleşmeden beklenen faydanın elde edilmesi için gerekli olan bilgilerini web sitesi ile paylaşır. Ancak oluşturulan kişisel veriler, sözleşmenin kuruluş aşamalarında tüketicinin doğrudan dijital ortama aktardığı veriler ile sınırlandırılamaz. Tüketiciler arama motoru üzerinden gerçekleştirecekleri her aramada ve web sitesine verecekleri her bir komutta kişisel veri oluştururlar. Bunu sağlayan teknoloji, çerez teknolojisidir ve bu teknolojinin kullanılması ile tüketicilerin "davranışsal verileri"ne (*behavioural data*) ulaşılır.

Çerez, web sitesi kullanıcılarının verilerini depolamak için çeşitli cihazlarda saklanan küçük yazılım parçalarıdır.[32] Çerezlerin birçok türü ve çerez teknolojisinin birçok fonksiyonu bulunur.[33] Bu fonksiyonlardan bazıları tüketicilerin web

---

30 King, Forder, Data analytics, 698.

31 Giovanni De Gregorio, Digital Constitutionalism in Europe, (Cambridge University Press, 2022), 228.

32 Marilyn Lavin, "Cookies: What do consumers know and what can they learn?", *Journal of Targeting, Measurement and Analysis for Marketing*, no: 14, (2006): 279-288.

33 Kişisel Verileri Koruma Kurumu, Haziran 2022'de çerez uygulamaları hakkında bir rehber yayınladı. Rehberde özellikle farklı çerez türlerine

sitelerini kullanım deneyimlerini kolaylaştırmaya yöneliktir.[34] Örneğin bazı çerezler web sitelerinin daha hızlı yüklenmesine, kullanıcı bilgilerinin ya da sepete eklenen ürünlerin hatırlanmasına yardımcı olur. Bazı çerezler ise tüketicilerin web sitesindeki komutlarını takip ederek profil oluşturmayı amaçlar.[35] Bu tür çerezler, "kullanımı için tüketicinin açık rızası gerekli olan çerezler" olarak da ifade edilebilir.[36] Çünkü bu tür çerezler aracılığıyla elde edilen verilerin, verilere sahip olanlar tarafından ne şekilde kullanılacağı gizlilik endişesi oluşturur.[37] Nitekim çerez kullanımı ile tüketicilerin farklı web sitelerindeki aktiviteleri analiz edilerek tüketici tercihlerine ulaşılması mümkün olsa da tüketicilerin sağlık verilerine, cinsel tercihlerine, dini inançlarına vb. ilişkin son derece hasas verilere ulaşılması da mümkündür.[38]

---

ilişkin detaylı açıklamalar yer almaktadır. Ancak biz çerezleri yalnızca profilleme işlemi ile alakalı olduğu kadar ele alacağız. Çerez türleri hakkında detaylı bilgi için bakınız: Kişisel Verileri Koruma Kurumu, Çerez Uygulamaları Hakkında Rehber, Haziran 2022, erişim tarihi Aralık 23, 2022, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/fb193dbb-b159-4221-8a7b-3addc083d33f.pdf.

34 Lavin, Cookies, 280

35 Lavin, Cookies, 280.

36 Article 29 Data Proteciton Working Party, Opinion 04/2012 on Cookie Consent Exemption, (2012): 2, erişim tarihi Aralık 23, 2022, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

37 Hüseyin Can Aksoy, Halıcıoğlu, Mesut, "AB ve Türk Hukuklarında Çerezler: Kişisel Verilerin Korunması Açısından Karşılaştırmalı Bir Değerlendirme", *Kişisel Verileri Koruma Dergisi*, no: 1, (2021): 63.

38 Anca D. Chrita, "The Rise of Big Data and the Loss of Privacy", *Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?,* Ed. Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt, Gintarė Surblytė-Namavičienė, (Germany, part of Springer Nature, 2018): 153-189.

Esasen çerez teknolojisinin kullanımı için açık rızanın gerekli olup olmaması hususunda değerlendirme kriterleri Çalışma Grubu tarafından belirlenmiştir. "Kriter A" ve "Kriter B" şeklinde ifade edilen durumlara dahil olan çerezler onau gerekliliğinden muaf kabul edilir. Kriter A, çerezlerin yalnızca elektronik iletişim ağı üzerinden bir bilginin iletimini gerçekleştirmek amacıyla kullanılmasıdır. Kriter B ise, çerez kullanımının bilgi sağlayıcısının fonksiyonunu gerçekleştirmek için kullanılmasının kesinlikle zorunlu olmasıdır.[39] Belirtilen kriterleri sağlamayan "sosyal eklenti takip çerezleri" (*Social plug-in tracking cookies*) ile "üçüncü taraf reklamcılık çerezleri" (*Third party advertising*) açık rıza kapsamındaki çerezlerdir.[40] Tüketicileri profilleme hedefi genellikle belirtilen çerezler aracılığıyla gerçekleştirilir.

Tüketicilerin dijital ortama aktardıkları verilerinin analiz edilmesi sonucunda tüketici profilleri oluşturulur. Oluşturulan profiller ile tüketiciler cinsiyetleri, yaşlarına, konumlarına ve hatta yaşam tarzları ve olası gelirleri gibi konularda gruplandırılır.[41] Bu profiller, özellikle tüketici davranışlarını etkilemek ve "gruplandırmaya dayalı fiyatlandırma"[42] oluşturmak için kullanılır.[43] Başka bir anlatımla tüketicilerin tercihleri ve sahip oldukları alışkanlıklar, onların tüketim alışkanlıklarının yönlendirilmesinde etkili olur. Ayrıca

---

39 Article 29 Data Proteciton Working Party, Opinion 04/2012 on Cookie Consent Exemption, 2.

40 Article 29 Data Proteciton Working Party, Opinion 04/2012 on Cookie Consent Exemption, 9.

41 Etye Steinberg, "Big Data and Personalized Pricing", *Business Ethics Quaterly*, no: 1, (2019): 97-117.

42 Steinberg, Big Data, 98.

43 Michael Nagenborg, "Surveillance and persuasion", *Ethics and Information Technology*, (2014): 43-49.

tüketicilerin özellikle ekonomik gelirleri gözetilerek gruplandırılması, fiyat ayrımcılığının oluşmasına neden olabilir.[44]

Doktrinde veri analizini gerçekleştiren otomatik teknolojilerin "dijital kapitalizm"i[45] ortaya çıkardığı belirtilmektedir.[46] Ortaya çıkan bu yeni ekonominin hammaddesi ise dijital alandaki faaliyetlerin sonucu olan verilerin analiz edilmesi ile ortaya çıkan kişisel verilerdir.[47] Bu durumdan yola çıkarak günümüzde tüketicilerin, dijital kapitalizmin esas unsuru konumunda olduğu söylenebilir. Çünkü elde edilen verilerle oluşturulan algoritmik sistemler, tüketicileri ikna etmek ya da bireysel kararlarını etkilemek için donatılmıştır.[48] Tüketiciler bu şekilde işleyen sistemlerin parçası olmak istemeyebilirler. Bu halde çözüm, onları sistemin dışına itmek değildir; tüketicilerin tercih etmeleri halinde sistemin içine dahil olabilecekleri mekanizmalar geliştirilmesidir. Şöyle ki tüketicilerin kişisel verileri üzerinde aktif etkinliğinin veya doğrudan denetiminin bulunması gerekir. Bunun yanında tüketicinin güçsüz konumda olmasının bir yansıması olarak tüketiciler, verileri üzerinde gerçekleştirecekleri eylemlerden önce bilgilendirilmeleridirler. Esasen bütün bu durumları, "teknoloji ile hukukun entegre edilmesi gerekliliği" şeklinde

---

44 Amazon'un tüketicilerin kişisel verilerini kullanmak suretiyle, tamamen ticari kaygılarla gerçekleştirdiği fiyat farklılığı uygulamasına ilişkin detaylı bilgi için bakınız: Steinberg, Big Data, 104

45 Doktrinde bu yeni ekonomiye "gözetim kapitalizmi" de denmektedir. Detaylı bilgi için bakınız: Murat Volkan Dülger, *Kişisel Verilerin Korunması Hukuku*, (İstanbul: Seçkin Yayıncılık, 2020), s. 19-21.

46 Gregorio, Digital Constitutionalism, 216.

47 Gregorio, Digital Constitutionalism, 126; Çekin, Avrupa Birliği, 20.

48 Nagenborg, *Surveillance*, 45.

ifade edebiliriz.[49] Bu noktada tüketiciler açısından teknolojinin, tüketicinin korunması mantığı ile uyumlu hale getirilmesi zorunluluğu doğar.

II. TÜKETİCİ KİŞİSEL VERİLERİNİN TEKNİK ANLAMDA KORUNMASI

A. *Privacy by Design* ve *Privacy by Default*

Kişisel verilere sağlanacak olan korumayı yalnızca normatif alan ile sınırlandırmak mümkün değildir[50]. Kişisel verilerin korunması, bütün veri işleme sürecini içine alan çok daha geniş bir alanda yükümlülükler doğurur. Bu anlamda *"teknik ve organizasyonel"*[51] açıdan ve belirli ilkeler çerçevesinde sistemsel yapılanmaların varlığı, kişisel verilerin korunması için zorunluluktur. Nitekim veri öznesinin tüketici olduğu durumlarda, teknik alan oldukça önem kazanmaktadır. Çünkü kişisel veri işleme faaliyetinin, tüketici boyutunda sahip olması gereken bazı sistemsel gereklilikler vardır. Aşağıda bu konu detaylıca incelenecektir.

Veri güvenliğinin sağlanmasına ilişkin olarak alınacak teknik tedbirler, GDPR madde 25 hükmünde ikili bir ayrıma tabi tutulmuştur. Bu ayrım, "*data protection by design*" (tasarım ile veri koruma) ve "*data protection by default*" (varsayılan olarak veri koruma) şeklinde yapılmıştır. Öngörülen bu tedbirler ile

---

[49] Urs Gasser, Big Data and Global Trade Law, *Futuring Digital Privacy Reimaging the Law/Tech Interplay*, Edit. Mira Burri, (Cambridge University Press, 2021): 195-211.

[50] Mesut Serdar Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku* (İstanbul: Oniki Levha Yayınları, 2020), 12.

[51] Çekin, , *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku,* 12.

teknolojinin, kişisel verilerin korunması ihtiyacına adapte edilerek gelişmesi sağlanır.

"Privacy by design" (PbD), tasarımdan itibaren veri koruma gerekliliğine odaklanılmasını sağlar. Başka bir anlatımla, verinin yaşam döngüsü süresince ve hatta verilerin işlenmesinin veri sahiplerinin hak ve özgürlükleri üzerindeki olası etkisini başlamadan önce gizliliğe ilişkin tedbirlerin alınmasını gerekli kılar.[52] Bu tedbirlerin alınması ile *"gizlilik dostu sistemler"*[53] ortaya çıkar ve tüketici verilerinin güvenliği en başından itibaren sağlanmış olur.

ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı) PbD için, "veri odaklı" (*data oriented strategies*) ve "süreç odaklı" (*process oriented strategies*) olmak üzere sekiz farklı tasarım stratejisi belirlemiştir. Veri odaklı stratejiler, "azaltmak" (*minimise*), "gizlemek" (*hide*), "ayırmak" (*seperate*) ve "birleştirme/gruplandırma" (*aggregate*) dır.[54]

Bunlar arasından en önemlisi toplanan kişisel veri miktarının en azda tutulmasıdır. Çünkü elde edilen veri miktarının en azda tutulması, ortaya çıkabilecek olan risklerinde sınırlandılması sonucunu doğurur. Belirtilen strateji, KVKK madde 4/ç ve GDPR madde 5/c' de kişisel verilerin işlenmesine ilişkin genel ilkelerden sayılmıştır. Dolayısıyla elde edilen kişisel verilerin işlendikleri amaçla bağlantılı ve sınırlı olması sağlanırsa, veri minimizasyonu da sağlanmış olur ve risk en aza indirilir. Veri minimizasyonunun sağlanması için veri işlemeyi

---

52 European Union Agency for Network and Information Security(ENISA), Privacy and Data Protection by Design – from policy to engineering, (2014): 11, Erişim Tarihi Aralık 28, 2022, https://www.enisa.europa.eu/.

53 Jaap-Henk Hoepman , "Privacy Design Strategies (The Little Blue Book)", (2022):1, erişim tarihi Aralık 28, 2022, https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf.

54 ENISA, 19.

gerektiren sebeplerin net bir şekilde belirlenmesi gerekir.[55] Bunun için ise şeffaf bir veri işleme süreci oluşturulmalıdır. Sürecin şeffaf ilerlemesi hem veri işleyenlerin kişisel verilerin güvenliğini sağlanmasına ilişkin yükünü azaltır hem de tüketicilerin kişisel verileri üzerindeki denetimini sürdürmesine imkan tanır. Veri minimizasyonun sağlanması esasen bu amaçla programlanmış sistemsel bir sürecin de varlığını gerektirir.[56] Şöyle ki özellikle veri işleme faaliyetinin bir depolama işlemi haline dönüşmemesi adına, kişisel verilerin silinmesi belirli periyotlara bağlanmalıdır.[57] Bu şekilde veri minimizasyonun tasarımsal anlamda bir kural haline getirilmesi mümkündür.

İkinci olarak kişisel veri işleme faaliyetinin farklı açılardan ayrılması ve bu şekilde verilerin birbiriyle ilişkilendirilmesinin zorlaştırılması gerekir.[58] Bu anlamda merkezi bir işleme yerine dağıtılmış bir işleme faaliyeti gerçekleştirilmelidir.[59] Ayrılmanın fiziksel ya da mantıksal olarak sağlanması mümkündür.[60]

Üçüncü olarak kişisel verilerin gizlenmesi gerekir. Gizleme noktasında, "mahremiyet artırıcı teknolojiler" (*Privacy-Enhancing Technologies*)' in kullanılması gerekir. Mahremiyet artırıcı teknolojiler, kişisel verilerin istenmeyen şekilde işlenmesini engellemek için geliştirilen gizliliği artırıcı teknolojilerdir.[61] Bu teknolojilerde, anonimlik (*anonymity*), takma

---

55 Hoepman, Privacy, 6.

56 Zeynep Öğretmen Kotil, *Kişisel Verilerin Korunması Çerçevesinde Yapay Zeka*, (İstanbul: Oniki Levha Yayınevi, 2022), 304.

57 Öğretmen Kotil, *Kişisel Verilerin, 304.*

58 Hoepman, Privacy, 8.

59 ENISA, 20.

60 Hoepman, Privacy, 8.

61 PISA (Privacy Incorporated Software Agent), Handbook of Privacy and Privacy-Enhancing Technologies The case of Intelligent Software Agents, Editors: G.W. van Blarkom, J.J. Borking, J.G.E. Olk, (2003): 52, erişim tarihi

ad kullanma (*pseudonymity*), gözlemlenemezlik (*unobservability*), bağlantısızlık (*unlinkability*), reddedilebilirlik (*deniability*) yöntemleri kullanılır.[62] Mahremiyet artırıcı teknolojilerin kullanılması esasen veri güvenliğinin sağlanmasına yönelik olarak KVKK ve GDPR'de öngörülen bir yükümlülüktür. KVKK madde 12/1 hükmünde, "*Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır."* demek suretiyle veri sorumlusu için teknik yeterliliğin sağlanmasını öngören bir yükümlülük getirmiştir. GDPR ise madde 32'de daha detaylı bir düzenlemeye yer vermiştir ve gereken güvenlik düzeyinin sağlanabilmesi için "*kişisel verilerde takma ad kullanımı ve şifreleme"* nin kullanılabileceğini öngörmüştür. Son olarak verilerin genel başlıklar altında gruplandırılmak suretiyle işlenmesi gerekir.[63] Bu şekilde verinin, tek bir kişi ile ilişkilendirilmesi zorlaştırılmış olur.[64] Başka bir anlatımla verinin soyutluğu sağlanarak veri, öznesinden uzaklaştırılır.[65]

Süreç odaklı stratejiler, "bilgilendirme" (*inform*), "denetim" (*control*), "uygulama" (*enforce*) ve "gösterme/ kanıtlama" (*demonstrate*) dır.[66] Süreç odaklı stratejiler veri odaklı sratejilere oranla daha fazla veri öznesine yönelir. Kişilerin, verilerini

---

Aralık 28, 2022, https://andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf.

62 Detaylı bilgi için bakınız: Alfred Kobsa, Yang Wang, Privacy-Enhancing Technologies, (2008): 7, erişim tarihi Aralık 28, 2022, https://www.ics.uci.edu/~kobsa/papers/2008-Handbook-LiabSec-kobsa.pdf.

63 ENISA, 19.

64 ENISA, 20.

65 Hoepman, Privacy, 10.

66 ENISA, 20-22.

paylaşmadan önce de süreç odaklı stratejilerin işletilmesi gerekir. Bu anlamda bilgilendirme işleminin doğru zamanda yapılması önem teşkil eder. Veri öznesi olarak tüketicilerin henüz kişisel verileri işlenmeye başlamadan önce bilgilendirilmesi gerekir. Aksi halde bilgilendirilme ile hedeflenen fayda sağlanamaz. Bilgilendirmenin ayrıca yeterli düzeyde olması gerekir. İçerik itibariyle yeterli olmayan bir bilgilendirme, tüketicinin korunması amacıyla çelişir. Buna göre tüketicilerin hangi kişisel verilerinin işlendiği başta olmak üzere, bu verilerin neden işlendiği ve hangi süre ile işleneceği gibi hususların bilgilendirmede bulunması gerekir.[67] Tüketicilerin güçsüz konumunun bir parçası olan bilgisizlik dikkate alındığında, bilgilendirmenin mutlaka orta zekada bir tüketicinin anlayabileceği düzeyde, teknik terimler içermeyen, *"en az on iki punto büyüklüğünde, anlaşılabilir bir dilde, açık, sade ve okunabilir"* olması gerekliliği vurgulanmalıdır. Bu kapsamda yapılacak bir bilgilendirme sonucunda tüketici, kişisel verilerini paylaşıp paylaşmama noktasında bir kanaate varabilecektir. Tüketicinin, tam bir kanaate varma imkanı sunulmadan rıza göstermesi, veri işlemenin temel şartı olan "açık rıza"nın oluşumunu sağlamaz ve bu rızaya dayanarak yapılan veri işleme faaliyeti hukuka aykırılık teşkil eder.

Tüketici, kişisel verilerinin işlenmesine rıza gösterdikten sonra işlenen verileri üzerinde denetime sahip olmalıdır. Bunun için öncelikle tüketicilere kişisel verilerini inceleyebilme ve güncelleme imkanı sunulmalıdır.[68] Sonrasında ise tüketicilere bilgilerinin silinmesini isteyebilmesi ve verilerinin işlenmesine gösterdiği rızayı çekebilmesi için açık bir yol gösterilmelidir.[69]

---

67 Hoepman, Privacy, 14.

68 Hoepman, Privacy, 16.

69 Hoepman, Privacy, 16.

Tüketicilerin, kişisel verilerine ilişkin olarak gerçekleştirdikleri bütün tercihlerin, onlar adına daha anlamlı bir hale gelebilmesi için bu tecihlerin tek bir noktadan incelebilir olması önemlidir.[70] Bu anlamda tüketicilerin kullanımına sunulan bir "gizlilik panosu" nun oluşturulması gerekir.[71] Tüketiciler bu pano üzerinden kişisel verilerine ilişkin bütün işlemleri gerçekleştirebilmelidirler.

Tüketicilerin verileri üzerinde denetime sahip olması, veri işleme sürecinde veri sorumlusu ile arasında olan "güç dengesizliği"nin giderilmesine de hizmet eder.[72] Veri sorumlularının teknik anlamda gizliliği sağlaması tek başına yeterli değildir. Organizasyonel boyutta da gizlilik dostu bir ortam yaratılmalıdır ve bir gizlilik politikası oluşturulmalıdır. Bu şartlar sağlandıktan sonra şartların sağlandığı veri denetçileri tarafından ortaya konulması yani gösterilmelidir.[73]

"*Privacy by default*", veri güvenliğini sağlayan tercihlerin en başta veri sorumlusu tarafından kabul edilerek yerine getirilmesi gerekliliğidir. Buna göre gizlilik için gerekli olan ayarlamaların ve tercihlerin, tüketici tarafından ilk kullanımda değiştirilmesine gerek olmaksızın gizliliğin sağlanması adına gerekli olan en iyi şekilde bulundurulması varsayılan olarak gizliliği ortaya çıkarır.[74]

GDPR madde 25/2 düzenlemesinde varsayılan olarak sağlanan gizlilik şu şekilde belirtilmiştir:

---

70 Öğretmen Kotil, 308.

71 Öğretmen Kotil, 308.

72 Yıldırım Keser, "Tüketicinin Kişisel Verisinin İşlenmesinde Açık Rıza", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, no:3, (2020): 1181 – 1215.

73 Hoepman, Privacy, 20-22

74 Daniela Jezova, "Principle of Privacy by Design and Privacy by Default", *Regional Law Revie*w, (Şubat, 2021), Erişim Tarihi Ocak 28, 2022, SSRN: https://ssrn.com/abstract=3755514.

"Kontrolör, olağan durumda, yalnızca her spesifik işleme amacı için gereken kişisel verilerin işlenmesini sağlamaya yönelik uygun teknik ve düzenlemeye ilişkin tedbirler uygular. Söz konusu yükümlülük toplanan kişisel veri miktarı, bunların işlenme derecesi, saklama süresi ve bunlara erişilebilirliğe uygulanır. Özellikle, söz konusu tedbirler, olağan durumda, bireyin müdahalesi olmaksızın kişisel verilerin belirsiz sayıda gerçek kişinin erişimine açılmamasını sağlar."

Görüldüğü üzere varsayılan olarak gizliliğin sağlanması şu dört kriterin varlığını gerektirir: "minimum miktarda kişisel veri", "kişisel verilerin işlenmesinin kapsamının asgari düzeyde tutulması", "kişisel verilerin minimum süre için saklanması", "kişisel verilerin minimum erişilebilirliği".[75] Bu şekilde veri sahiplerinin etkileşiminin en aza indirilmesi sağlanır ve veri güvenliğine ilişkin riskler sınırlandırılmış olur. Ancak veri sahiplerine varsayılan ayarları değiştirilebilme imkanı da sağlanmalıdır.[76]

Tüketiciler açısından değerlendirilidiğinde gizliliğin, tüketicinin aktif tercih ve ayarlamalarına bırakılmadan sağlanmış olması tüketicinin korunması mantığı ile de uyumludur. Gizliliğin varsayılan olarak kabulü, teknoloji karşısında tüketicinin bilinçsizliğine ilişkin bir koruma olarak değerlendirilebilir.

---

75 ENISA, Recommendations on shaping technology according to GDPR provisions, Exploring the notion of data protection by default, (2018): 17, erişim tarihi Aralık 29, 2022, https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2.

76 ENISA, Recommendations on shaping technology according to GDPR provisions, s. 10.

B. *Opt-in* ve *Opt-out* Sistemler

Kişisel verilerin işlenmesine ilişkin farklı sistemler mevcuttur. Veri öznelerinin veri işleme faaliyetine nasıl dahil olacağına odaklanan "*opt-in*" (katılma) ve "*opt-out*" (kapatma) sistemler, veri güvenliğinin sağlanması ve kişisel verilerin işlenmesi şartları bakımından incelenmelidir. Opt-in sistem, veri öznelerinin aktif eylemleri ile veri işleme faaliyetine rıza gösterdikleri sistemlerdir. Opt-out sistem ise, rıza verildiğinin varsayıldığı ve varsayılan rızanın geri alınabilmesi için "devre dışı bırakma mekanizmaları" nın bulunduğu sistemdir. Başka bir anlatımla tüketici, varsayılan rızayı geri almadığı sürece kişisel verilerinin işlenmesine rıza gösterdiği kabul edilerek, aktif rıza şartı sağlanmaksızın kişisel veriler işlenmeye başlanır.[77] Buna göre iki sistem arasındaki teknik fark, tüketicilerin eylemsizliğine bağlanmış sonuçlar ile ortaya çıkar. Opt-in sistemde tüketicinin eylemsiz kalması kişisel verilerin paylaşılmaması sonucunu doğururken, opt-out sistemde tüketicinin eylemsizliği kişisel verilerinin paylaşılmasına yönelik bir rıza olarak yorumlanacaktır.[78]

Opt-out sistem, Amazon Türkiye tarafından bir dönem kullanılmış bir sistemdir. Kişisel Verileri Koruma Kurulu'nun kararına[79] da yansıdığı üzere, web sitesine giren kullanıcıların "Amazon Hesabınızı Oluşturun" sekmesine tıkladığında gizlilik bildirimini kabul ettiği varsayılmaktaydı ve kullanıcıların karşısına "Sipariş verdiğinizde Amazon.com.tr'nin Gizlilik

---

77 Thomas Dreier, "Opt in'' and ''opt out'' mechanisms in the internet era – towards a common theory", *Computer and Security Review*, no: 2, (2010): 145.

78 Sarah Hodges, "Examining the Gramm–Leach–Bliley Act's opt-out method for protecting consumer data privacy rights on the Internet", *Information and Communications Technology Law*, no:1, (2013): 60-85.

79 Kişisel Verileri Koruma Kurulu, 27/02/2020 Tarihli ve 2020/173 sayılı Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili karar, erişim tarihi Aralık 29, 2022, https://www.kvkk.gov.tr/Icerik/6739/2020-173.

Bildirimini, Kullanım ve Satış Koşullarını ve Çerez Bildirimini kabul etmiş olursunuz." bildirimi çıkmaktaydı.

Görüldüğü üzere opt-in sistemde gizlilik varsayılan olarak kabul edilirken opt- out sistem, özellikle veri minimizayonu hedefine aykırı bir uygulamada işlemektedir. Şöyle ki opt-out sistem içerisinde özellikle elektronik ticaret uygulamaları kapsamında tüketicilerin her hareketi veri işleme faaliyetinin konusu haline gelebilir. Tüketiciler, ürün çeşitliliği ve elektronik ticaret sitelerinin fazlalığına bağlı olarak çoğu zaman fiyat araştırması yaparak nihai kararlarını vermektedirler. Fiyat araştırması yaparken de birçok farklı web sitesini ziyaret ederler. Opt-out sistemde tüketicilerin herhangi bir üyelik oluşturmadan veya herhangi bir sözleşme kurma niyeti olmadan bir web sitesini ziyaret etmesi kişisel verilerinin işlenmesi için yeterli olacaktır. Bu durum tüketicilerin dijital ortama çok daha fazla kişisel veri aktarmasına neden olur. Nitekim KVKK kapsamında opt-out sistemine dayanılarak kişisel veri işlenmesi hukuka aykırılık oluşturur. Çünkü kişisel veri faaliyetinin yegane şartı olan açık rızanın sağlanabilmesi için kapsamı belirlenmiş bir veri işleme faaliyetine ilişin olarak tüketicinin, veri işlemeye başlamadan önce bilgilendirilmesi ve bilgilendirilmeye dayalı olarak tüketicinin aktif rıza göstermesi gerekir. Ancak özellikle tarayıcıların çerez ayarları opt-out sisteme dahildir ve varsayılan ayarlar "tüm çerezleri kabul et" şeklindedir.[80]

Doktrinde opt-in sistemin opt-out sisteme göre daha fazla gizlilik sağlamadığını ve bunun yanında ekonomik olarak daha maliyetli olduğu, rekabeti azalttığı ve tüketicilere ulaşmayı zorlaştırdığını savunan görüşler de mevcuttur.[81] Fakat tüketiciyi koruma bakış açısı ile değerlendirildiğinde tüketici

---

[80] Jezova, Principle, 135.

[81] Detaylı bilgi için Bkz. Cate, Fred H., Staten Michael E., "Protecting Privacy in the New Millennium: The Fallacy Of "Opt-In"", erişim tarihi Aralık 29, 2022, http://home.uchicago.edu/~mferzige/fallacyofoptin.pdf.

mahremiyetinin, şirketlerin ekonomik çıkarlarından önce gelmesi zorunluluğunun opt-in sistemin uygulama alanı bulmasını zorunlu kıldığı söylenebilir.

C. *Opt-in* Sistemin Uygulanması

Opt-in sistem, tüketicinin okuma insiyatifine ve becerisine dayanır.[82] Bu nedenle opt-in sistemin uygulanması başlı başına tüketici mahremiyetinin korunmasını sağlamaz; opt-in sistem içindeki mekanizmaların bazı standartları sağlaması da gerekir. Bu standartlar oluşturulurken geçerli bir rızanın şartları ve tüketicilerin genel davranış eğilimleri gözetilmelidir.

Kişisel verilerin işlenmesine yönelik gösterilecek olan rızayı geçerli kılan şartlar, GDPR madde 4/11 hükmünde belirtilmiştir. Buna göre rızanın tüketicinin özgür iradesine dayanması, rızanın sınırlarının çizilmiş olması ve rızanın bilgilendirmeye dayanması açık bir rızayı ortaya çıkarır.

Geçerli bir rıza için gereken ilk şart "amaç sınırlaması" (*purpose limitation*) nın bulunmasıdır. Amaç sınırlaması, gizlilik politikalarında şeffaflığın ve öngörülebilirliğin sağlanması noktasında önemli bir kriterdir. Bu kriterin yerine getirilebilmesi için veri işleme eyleminin spesifik hale getirilmesi ve bu eylemin amacının, meşru bir temele dayandırılmak suretiyle, açıklanması gerekir.[83] Çünkü veri işleme faaliyetinin çok geniş ve muğlak bir kapsamda gerçekleştirilmesi, veri sahiplerini bilinçlendirme noktasında yetersiz kalacağından onlara gereken korumayı sağlamaz.

Opt-in sistem, belirtilen şartlar sağlanacak şekilde yapılandırılmalıdır. Amaç sınırlaması gözetilerek gerçekleştirilecek olan yapılandırma daha çok tüketici rıza

---

[82] Hodges, Examining, 76.

[83] Article 29 Working Party Guidelines on consent under Regulation 2016/679, (2018): 5,erişim tarihi Ocak 1, 2023, https://ec.europa.eu/newsroom/article29/items/623051.

göstermeden önce yapılacak bilgilendirmenin içeriğine yönelik olacaktır. Bu doğrultuda bilgilendirme metninde şu hususların yer alması gerekir:

- Veri sorumlusunun kimliği,

- Açık rıza gerektiren işleme operasyonlarının her birinin amacı,

- Hangi (tür) verilerin toplanacağı ve kullanılacağı,

- Gösterilen rızanın geri alabilme hakkının varlığı,

- Kişisel verilerin, tamamen veya kısmen otomatik yollarla ya da veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yöntemlerden hangisiyle elde edildiği,

- Veri aktarımlarının olası riskleri,[84]

- Veri sahibinin KVKK kapsamında sahip olduğu haklar,[85]

- Kişisel verilerin aktarılma amacı ve aktarılacak alıcı grupları

Dolayısıyla tüketici, rızasının ne anlama geldiği, gösterdiği rıza sonucunda hangi verilerinin işleneceği ve verilerinin hangi amaçlar için kullanılacağı hususlarında bilgilendirilmelidir. Belirtilenin aksine sürecin esas amacı belirtilmeden alınan genel rıza (*blanket consent*), geçerli bir rıza olarak kabul edilmez. Buna ek olarak, ileride ortaya çıkabilecek muhtemel durumlar sebebiyle kişisel verilerin işlenebileceği kanaatini oluşturan ifadelerden kaçınılmalıdır. Çünkü bu tür bir veri işleme faaliyetinin öngörülebilir olması mümkün olmadığı gibi önceden belirlenmiş bir amaç bulunmadan verilerin

---

84 Article 29 Working Party Guidelines on consent under Regulation 2016/679, 13.

85 Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in madde 4/1 hükmünde ilgili kişinin Kanun'un 11. maddesinde sayılan haklarının da bilgilendirme metninde yer alacağı belirtilmiştir.

depolanması söz konusu olacağından geçerli bir rızanın oluşması söz konusu olmaz. Bu şekilde bir bilgilendirme opt-in sistemlerin tüketiciler açısından en büyük avantajıdır. Tüketiciler bu şekilde hem kişisel verileri üzerinde denetime sahip olurlar hem de veri işleme faaliyetinin meşru amaçlar için gerçekleştirildiğinden emin olabilirler.[86]

İçerik veri sahibine iletilirken ortalama bir insanın anlayacağı kadar açık ve sade bir dil kullanılmalıdır. Teknik terimlerin yoğunlukta olduğu bir aydınlatma metni tüketicilerin hem metni okumadan kaçınmasına neden olur hem de metni anlayarak belirli bir kanaate varmalarına engel olur. Özellikle çerez kullanıma ilişkin yapılacak olan bilgilendirmelerde ne tür çerezlerin kullanıldığı ve bu çerezlerin fonksiyonlarına ilişkin tüketicinin aydınlatılması gerekir. Çünkü ortalama bir tüketicinin çerez teknolojisi, çerez türlerini ve çerez kullanımının olası sonuçlarından haberdar olması beklenemez.

Bilgilendirmenin hangi durumlarda yapılacağı Kişisel Verileri Koruma Kurumu tarafından 2018 yılında yayınlanan "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ" ile detaylı bir şekilde açıklanmıştır. Tebliğ'in "Usul ve Esaslar" başlıklı madde 5 hükmüne göre kural, kişisel veri işlendiği her durumda aydınlatma yükümlülüğünün yerine getirilmesidir. Veri işleme faaliyetinin belirli bir amaç çerçevesinde gerçekleştirilmesine paralel olarak Tebliğ'de kişisel veri işleme amacı değiştiğinde, veri işleme faaliyetinden önce bu amaç için aydınlatma yükümlülüğü ayrıca yerine getirilmesi gerektiği belirtilmiştir. . Bu anlamda bilgilendirme bir kerelik bir işlem değildir ve özellikle amaç ile bağlatısı gözetilerek birden çok defa gerçekleştirilmesi gerekebilir.

Sadece içeriğe odaklanan bir yapılandırma veri sahiplerini korumak için yeterli olmayacaktır. Biçimsel bazı nitelikler ile

---

[86] Hodges, Examining, 76.

içeriğin desteklenmesi gerekir. Bu doğrultuda ICO (Information Commissioner's Office), web sitelerinin elektronik ortamda gerçekleştirecekleri bilgilendirmelerin en verimli şekilde işlevini gerçekleştirebilmesi için üç kriter belirlemiştir. Bu kriterler, biçime (*formatting*), konuma (*positioning*) ve ifadeye (*wording*) ilişkindir.[87] Buna göre web sitesinde yer alan bilgilendirmenin (özellikle çerez kullanılıyorsa çerez kullanıldığına ilişkin bilgilendirmenin) boyutu veya yazı tipi web sitesinin içeriğinde kullanılan boyut ve tipten farklı olmalıdır. Ek olarak web sitesindeki konumu veri sahiplerinin dikkatini çekecek bir şekilde konumlandırılmalıdır ve onay mekanizmasının tüketiciler gözünde görünürlüğü artırılmalıdır.[88] Ayrıca Tebliğ'de aydınlatma yükümlülüğü ile rıza gösterme işlemlerinin ayrı ayrı gerçekleştirilmesi gerektiği belirtilmiştir. Kanaatimizce bu düzenleme ile veri sahiplerinin aşırı bilgi yığını ile muhatap olmalarının önüne geçilmek istenmiştir.

Tüketicilere, rıza göstermeye ya da göstermemeye yönelik bulunduğu tercihi değiştirme imkanı da sunulmalıdır ve rızalarını nasıl geri çekecekleri konusunda bilgilendirilmelidirler[89]. Elektronik ortamda gösterilen rızanın geri çekilmesi, rıza göstermek için gerekli olan işlemden zor bir prosedüre tabi olmamalıdır.[90] Başka bir anlatımla tüketicinin

---

87 Information Commissioner's Office, How do we comply with the cookie rules?, (2019), erişim tarihi Ocak 1, 2023, https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/.

88 Hodges, Examining, 74.

89 Article 29 Data Protection Working Party, Working Document 02/2013 providing guidance on obtaining consent for cookies, 2, erişim tarihi Ocak 1, 2023, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf.

90 Article 29 Working Party Guidelines on consent under Regulation 2016/679, 21.

rızasını geri çekmesi için gerçekleştireceği işlemler web sitesi içerisinde kolayca ulaşılabilir olmalıdır.

Tüketicinin rızayı özgür iradesi ile göstermesi gerekir. Özgür irade verilen bir rızadan bahsedebilmek için tüketicinin rıza göstermeyi bir zorunluluk olarak görmemesi veya rıza göstermemesinin olumsuz sonuçlar doğuracağını düşünmemesi gerekir.[91] Web sitelerinin, tüketiciler üzerinde bu yönde etkisi olan uygulamalardan kaçınması gerekir. Ancak uygulamada genellikle, rıza gösterilmesinin web sitesinin içeriğine ulaşılabilmesi için tüketiciye bir şart olarak dayatıldığı görülür. Bu halde tüketici web sitesinin hizmetlerinden faydalanmak adına çoğu zaman aydınlatma metinlerini okumadan rıza gösterme yoluna gider. Tüketicinin içeriğe ulaşma isteği ile ya da başka bir anlatımla hizmetten yoksun kalma baskısı ile gösterdiği bir rızanın özgür iradeye dayandığının kabulü mümkün değildir. Dolayısıyla opt-in sistemlerde web sitesinden yararlanma kişisel verilerin işlenmesi şartına bağlanmamalıdır.

Yukarıda belirtilenlerden yola çıkarak çağımızda tüketicilerin kişisel verilerinin korunabilmesinin bazı sistemsel gerekliliklerin bulunmasını gerekli kıldığı sonucuna varırız. Başka bir anlatımla teknoloji, hukuk ve ticari hayat arasındaki üçgende tüketicilerin, "algoritmik gözetim"[92] öznesi olarak yer aldığı kabul edilerek veri sorumlularının web sitelerini tüketici odaklı olacak şekilde oluşturmaları gerekir.[93] Esasen ancak bu şekilde tüketicinin korunması amacı ile kişisel verilerin korunması amacı uyum içinde hareket edebilir. Teknolojinin

---

91 Article 29 Working Party Guidelines on consent under Regulation 2016/679, 5.

92 Mariavittoria Catanzariti "Algorithmic Law: Law Production by Data or Data Production by Law?", Constitutional Challenges in the Algoritmic Society, Edit. Hans-W. Micklitz, Oreste Pollicino, Amnon Reichman, Andrea Simoncini, Giovanni Sartor, Giovanni De Gregorio, (Cambridge University Press, 2021): 78-92.

93 Catanzariti, Algorithmic, 82.

tüketicilere adapte edilmesi de sistemsel gerekliliklerin sağlanması ile mümkündür. Dolayısıyla sadece normatif alanda yapılan düzenlemeler ile dijital ortamda tüketicilerin korunması tam olarak sağlanamaz.

SONUÇ

Dijital ortamda kişisel verilerin korunması, normatif düzenlemelerin yanında bazı teknik uygulamaların da varlığını gerektirir. Teknik uygulamaların varlığı, teknoloji ile tüketicinin korunması amacının adapte edilmesi sonucunu doğurur. Bu doğrultuda bir web sitesinin tasarımdan itibaren (*privacy by design*) veri korumaya odaklı bir şekilde oluşturulması ve veri güvemliğinin varsayılan olarak kabul etmesi gerekir. Başka bir anlatımla veri güvenliği veri sahibinin insiyatifinde bir durum değildir ve onun tercihine bırakılmamalıdır. Bu durum opt-in sistemin uygulanmasını gerekli kılar. Ancak opt-in sisteminde bazı hususlar dikkate alınarak yapılandırılması ve tüketici dostu bir biçimde oluşturulması gerekir. Yapılandırma, içerik bakımından olacağı kadar biçimsel olarak da gerçekleştirilmelidir. Fakat herhalde veri işleme faaliyetine egemen olan ilke "veri minimizasyonu" olmalıdır.

Elde edilen verinin sınırlandırılması, veri güvenliğine ilişkin endişelerin azalmasına neden olacağı gibi veri sorumlularının veri güvenliğinin sağlanması yükümlülüğünü de hafifletecektir. Çünkü elde edilen veri sayısının artmasıyla doğru orantılı şekilde riskler de artmaktadır. Veri minimizasyonunun sağlanması, işleme sürecinin bu kurala adapte edilmesini ve periyodik olarak silme işleminin gerçekleştirilmesini gerekir. Zira tasarımın veri koruma çerçevesinde oluşturulması, kanaatimizce en başta veri işlemenin istisna olduğu sistemlerin ortaya çıkmasına bağlıdır.

Tüketici odaklı düşünüldüğünde özellikle kaçınılması gereken uygulama veri işleme sürecinde genel rızanın alınmasıdır. Bu durum KVKK'ya uygun olmadığı gibi

tüketicilerin korunması mantığı ile de bağdaşmaz. Çünkü tüketicilerin, gösterdikleri rızanın anlamı yanında kapsamını da tam olarak algılayabilmeleri gerekir. Bu nedenle tüketiciler için, kişisel verileri üzerinde gerçekleştirdikleri bütün işlemleri aynı anda ve bütün olarak görebilecekleri sistemler oluşturulmalıdır.

KAYNAKÇA

Acquisti, Alessandro. "The Economics of Personal Data and the Economics of Privacy", The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines, Erişim Tarihi Aralık 21, 2022, https://www.oecd.org/sti/ieconomy/46968784.pdf.

Aksoy,Hüseyin Can ve Halıcıoğlu, Mesut. "AB ve Türk Hukuklarında Çerezler: Kişisel Verilerin Korunması Açısından Karşılaştırmalı Bir Değerlendirme", Kişisel Verileri Koruma Dergisi, no:1,(2021): 61-88.

Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data, Erişim Tarihi Aralık 21, 2022, 12251/03/EN (clinicalstudydatarequest.com.

Article 29 Data Proteciton Working Party. Opinion 04/2012 on Cookie Consent Exemption, (2012), Erişim Tarihi Aralık 23, 2022, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

Article 29 Working Party. Guidelines on consent under Regulation 2016/679, (2018), Erişim Tarihi Ocak 1, 2023, https://ec.europa.eu/newsroom/article29/items/623051.

Ateş, Emre Cihan ve Bostancı, Erkan ve Güzel, Mehmet Serdar. "Big Data, Data Mining, Machine Learning, and Deep Learning Concepts in Crime Data", Ceza Hukuku ve Kriminoloji Dergisi, no: 2, (2021): 293-319.

Banterle, Francesco. "The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database sui generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis", Personal Data in Competition, Consumer Protection and Intellectual Property Law, Ed. Mor Bakhoum · Beatriz Conde Gallego Mark-Oliver Mackenrodt Gintarė Surblytė-Namavičienė, (Berlin,

part of Springer Nature, 2018): 411-443. DOI: https://doi.org/10.1007/978-3-662-57646-5

Catanzariti, Mariavittoria. "Algorithmic Law: Law Production by Data or Data Production by Law?", Constitutional Challenges in the Algoritmic Society, Edit. Hans-W. Micklitz, Oreste Pollicino, Amnon Reichman, Andrea Simoncini, Giovanni Sartor, Giovanni De Gregorio, (Cambridge University Press, 2021): 78-92. DOI: https://doi.org/10.1017/9781108914857.006

Cate Fred H. Ve Staten, Michael E.. "Protecting Privacy in the New Millennium: The Fallacy Of "Opt-In"", Erişim Tarihi: Ocak 29, 2022, http://home.uchicago.edu/~mferzige/fallacyofoptin.pdf.

Chirita, Anca D.. "The Rise of Big Data and the Loss of Privacy", Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?, Ed. Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt, Gintarė Surblytė-Namavičienė, (Germany, part of Springer Nature, 2018): 153-189. DOI: 10.1007/978-3-662-57646-5_7

CMA. The Commercial Use of Consumer Data, (2015), Erişim Tarihi Aralık 21, 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf.

Çekin, Mesut Serdar. Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku. İstanbul: Oniki Levha Yayınları, 2020.

Dreier, Thomas. "Opt in'' and ''opt out'' mechanisms in the internet era – towards a common theory", Computer and Security Review, no: 2, (2010):144-150.

Dülger, Murat Volkan. Kişisel Verilerin Korunması Hukuku. İstanbul: Seçkin Yayınevi, 2020.

ENISA. Recommendations on shaping technology according to GDPR provisions, Exploring the notion of data protection by default, (2018), Aralık 29, 2022, https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2.

ENISA. Privacy and Data Protection by Design – from policy to engineering, (2014), Erişim Tarihi Aralık 28, 2022, https://www.enisa.europa.eu/.

Forgó, Nikolaus ve Hänold, Stefanie ve Schütze, Benjamin . "The Principle of Purpose Limitation and Big Data", New Technology, Big Data and the Law, Ed: Marcelo Corrales, Mark Fenwick, Nikolaus Forgó, (Singapore, part of Springer Natur, 2017): 17-42. DOI 10.1007/978-981-10-5038-1

Gasser, Urs. Big Data and Global Trade Law, Futuring Digital Privacy Reimaging the Law/Tech Interplay, Edit. Mira Burri, (Cambridge University Press, 2021): 195-211. DOI:https://proxy.hacibayram.edu.tr:2079/10.1017/9781108919234

Gregorio, Giovanni De, Digital Constitutionalism in Europe, (Cambridge University Press, 2022), DOI: https://doi.org/10.1017/9781009071215.

Hodges, Sarah. "Examining the Gramm–Leach–Bliley Act's opt-out method for protecting consumer data privacy rights on the Internet", Information and Communications Technology Law, no:1, (2013): 60-85.

Hoepman, Jaap-Henk."Privacy Design Strategies (The Little Blue Book)", (2022), Erişim Tarihi Ocak 28, 2022, https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf.

Information Commissioner's Office (ICO). How do we comply with the cookie rules?, (2019), Erişim Tarihi 1 Ocak, 2023, https://ico.org.uk/for-organisations/guide-to-pecr/guidance-

on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/.

Jezova, Daniela. "Principle of Privacy by Design and Privacy by Default", Regional Law Review, (Şubat, 2021), Erişim Tarihi Ocak 28, 2022, SSRN: https://ssrn.com/abstract=3755514.

Kemp, Katharine. "Concealed data practices and competition law: why privacy matters", European Competition Journal", (2020): 628-672. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3432769.

Keser, Yıldırım. "Tüketicinin Kişisel Verisinin İşlenmesinde Açık Rıza", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, no:3, (2020): 1181 – 1215.

King, Nancy J. ve Forder, Jay. "Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data", Computer Law & Security Review, no:5, (2016): 696-714.

Kişisel Verileri Koruma Kurumu. Çerez Uygulamaları Hakkında Rehber, (2022), Erişim Tarihi Aralık 23, 2022, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/fb193dbb-b159-4221-8a7b-3addc083d33f.pdf.

Kişisel Verileri Koruma Kurulu, 27/02/2020 Tarihli ve 2020/173 sayılı Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili karar, Erişim Tarihi Aralık 29, 2022, https://www.kvkk.gov.tr/Icerik/6739/2020-173.

Kobsa, Alfred ve Wang, Yang, Privacy-Enhancing Technologies. (2008), Erişim Tarihi Aralık 28, 2022, https://www.ics.uci.edu/~kobsa/papers/2008-Handbook-LiabSec-kobsa.pdf.

Lavin, Marilyn. "Cookies: What do consumers know and what can they learn?", Journal of Targeting, Measurement and Analysis for Marketing, (2006): 279-288.

Nagenborg, Michael. "Surveillance and persuasion", Ethics and Information Technology, (2014): 43-49.

OECD. Consumer Data Rights and Competition - Background note, (2020), Erişim Tarihi Aralık 21, 2022, https://www.oecd.org/competition/consumer-data-rights-and-competition.htm.

OECD. Consumer Protection in E-commerce, OECD Recommendation, (2016), Erişim Tarihi Aralık 22, 2022, https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf.

Ooijen, Iris van ve Vrabec, Helena U.. "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective", Journal of Consumer Policy, (2018): 91-107.

Öğretmen Kotil, Zeynep. Kişisel Verilerin Korunması Çerçevesinde Yapay Zeka. İstanbul: Oniki Levha Yayınevi, 2022.

PISA (Privacy Incorporated Software Agent). Handbook of Privacy and Privacy-Enhancing Technologies The case of Intelligent Software Agents, Editors: G.W. van Blarkom, J.J. Borking, J.G.E. Olk, (2003), Erişim Tarihi Aralık 28, 2022, https://andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf.

Steinberg, Etye. "Big Data and Personalized Pricing", Business Ethics Quaterly, no: 1, (2019): 97-117.

Zevkliler, Aydın ve Özel, Çağlar. Tüketicinin Korunması Hukuku. Ankara: Seçkin Yayınevi, 2016.

Hakem Değerlendirmesi: Çift kör hakem.

Finansal Destek: Yazar bu çalışma için finansal destek alıp almadığını belirtmemiştir.

Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.

Etik Kurul Onayı: Yazar etik kurul onayının gerekmediğini belirtmiştir.

Peer Review: Double peer-reviewed.

Financial Support: The author has not declared whether this work has received any financial support.

Conflict of Interest: The author has no conflict of interest to declare.

Ethics Committee Approval: The author stated that ethics committee approval is not required.