Dezavantajlı Kişilerin Kullandıkları Akıllı Cihazların GVKT'ye Uyumu

Complying with the GDPR When Vulnerable People Use Smart Devices

Stanislaw PIASECKI(*)
Jiahong CHEN(**)
Çev.: **Mustafa KESKİN**(***)

Öz:

Gün geçtikçe akıllı ev cihazlarının sayısı artmaktadır. Özel olarak kendileri için mi yoksa toplumun geneli için mi tasarlandıklarına bakılmaksızın, akıllı cihazlar (akıllı kapı kilitleri, akıllı alarm sistemleri veya sesli asistanlar gibi) dezavantajlı kişiler tarafından kullanılmaktadır. Bu Makale, çocuklara ve doğası gereği dezavantajlı yetişkinlere odaklanmakta ve Bilgi Komiserliği Ofisi rehber ve raporlarına atıfta bulunarak akıllı cihazlar kullanıldığında Genel Veri Koruma Tüzüğü'ne ("GVKT") nasıl uyulacağını analiz etmektedir. Dezavantajlı kişilerin verilerinin işlenmesiyle ilgili GVKT hükümlerine uymak yalnızca bu kişiler için değil aynı zamanda akıllı cihazlar geliştiren ve dağıtan kuruluşlar için de faydalı olacaktır. Bu makale, her akıllı cihazda tasarım ve varsayılan olarak dezavantajlı kişilerin verilerinin korunmasından yanadır. Aynı zamanda bu çalışmanın amacı, tüm veri koruma ilkeleri genelinde güvenlik açığı hakkında düşünme ihtiyacına dikkat çekmek ve bu bağlamda GVKT'ye nasıl uyulacağına dair çözümler önermektir.

Anahtar Kelimeler:

Çocuklar, Dezavantajlı Kişiler, GVKT, Akıllı Cihazlar, Akıllı Evler.

Abstract:

The number of smart home devices is increasing. They are used by vulnerable people regardless of whether they are designed specifically for them or for the general population (eg, smart door locks, smart alarms, or voice assistants). This article focuses on children and inherently vulnerable adults, and analyses how to comply with the General Data Protection Regulation (GDPR) when the latter use smart products, with a particular focus on the UK through references made to the Information Commissioner's Office guidelines and reports. Complying with the GDPR provisions related to the processing of vulnerable people's data would be beneficial not only for the latter but also for organizations developing and

(*) University of Nottingham, Doktora Öğrencisi,
E-posta: stanislaw.piasecki@nottingham.ac.uk; Orcid Id: https://orcid.org/0000-0001-5748-8631.

(**) University of Sheffield, Öğretim Üyesi,
E-posta: jiahong.chen@sheffield.ac.uk; Orcid Id: https://orcid.org/0000-0002-1970-6762.

(***) Kadir Has Üniversitesi, Özel Hukuk Doktora Öğrencisi,
E-posta: mkeskin@stu.khas.edu.tr; Orcid Id: https://orcid.org/0000-0001-7593-0059.

Bu makale, Mustafa Keskin tarafından İngilizce'den Türkçe'ye çevrilmiştir. İngilizce makale, International Data Privacy Law Cilt: 12, Sayı: 2, Mayıs 2022'de yayınlanmıştır. https://academic.oup.com/idpl/article/12/2/113/6510568, Erişim tarihi: 27.10.2022.

Yayın Kuruluna Ulaştığı Tarih: 27.10.2022 / **Kabul Tarihi:** 15.12.2022.

deploying smart devices. This article argues in favour of protecting vulnerable people's data by design and default in every smart product. The objective of this work is also to draw attention to the need of thinking about vulnerability across all data protection principles and to propose solutions on how to effectively comply with the GDPR in this context.

Keywords:
Children, Vulnerable People, GDPR, Smart Devices, Smart Home Devices.

Arka Plan ve Hedefler

Bu makale, dezavantajlı kişilerin kullandıkları akıllı cihazları üreten ve dağıtan kuruluşların veri koruma düzenlemelerine uyumları konusunu eleştirel bir gözle analiz etmektedir. Doğaları gereği dezavantajlı yetişkinlere ve çocuklara yoğunlaşılacak ve onların verilerinin nasıl daha iyi korunabileceği incelenecektir. Genel Veri Koruma Tüzüğü'ne (General Data Protection Regulation, Bundan sonra "GVTK olarak anılacaktır.) uymak yalnızca dezavantajlı kişiler için değil aynı zamanda akıllı cihazlar geliştiren ve dağıtan kuruluşlar için de faydalı olacaktır. Şirketler, dezavantajlı müşterilerinin haklarını koruyarak cezalardan, iş kesintilerinden kaçınabilir ve müşterilerinin güvenini kazanabilir. Özel olarak, kendileri için mi yoksa toplumun geneli için mi tasarlandıklarına bakılmaksızın, akıllı cihazlar (akıllı kapı kilitleri, akıllı alarm sistemleri veya sesli asistanlar gibi) dezavantajlı kişiler tarafından kullanılmaktadır. GVKT dezavantajlı kişilere ilişkin çeşitli hükümler içermektedir ve kuruluşların bu hükümlere uyması gerekmektedir. Örneğin, kuruluşlara çocukların haklarını korumak için özel önlemleri alma yükümlülüğü getirmektedir (Gerekçe 38)[1]. Bu önlemlerin bazıları tüm kişiler için yararlı olabilirken (örneğin, gizlilik politikasının çocukların anlayabilecekleri dilde kaleme alınması gibi), bazı önlemlerin de dezavantajlı kişilerin özel ihtiyaçlarına uyumlu hale getirilmesi gerekmektedir (örneğin, demanslı kişilere satılacak akıllı cihazlarda olduğu gibi). Bilgi mahremiyeti, çocukların ve dezavantajlı yetişkinlerin haysiyetleri korunan insanlar olarak tanınması için esastır[2]. Birleşmiş Milletler Çocuk Hakları Sözleşmesi gibi uluslararası düzenlemelerin dışında, GVKT de insan haysiyetiyle bilgi mahremiyeti arasında temel bir bağ olduğunu kabul etmekte ve 88'inci madde de bu husus düzenlenmektedir[3]. Akıllı cihazları dezavantajlı kişiler tarafından kullanılan kuruluşlar GVKT uyarınca hangi önlemleri almalıdır? GVKT'nin hangi ilkesine odaklanmalıdırlar?

İşbu makalede, ilk olarak akıllı ev ve dezavantajlı kişiler kısaca tanımlanacaktır. Takip eden bölümlerde, hukuka uygunluk sebebinin seçimi (hukuka uygunluk ilkesi) ve GVKT'nin konuyla ilintili diğer ilkeleri değerlendirilecektir.

Akıllı Ev ve Dezavantajlı Kişilerin Kısa Tanımları

Dezavantajlı Kişiler Tanımı

GVKT uyarınca, ebeveyn onayı mekanizması genellikle çocuk 16 yaşından küçük olduğunda geçerlidir[4]. Kişisel verinin hukuka uygun işlenebilmesi için, çocuğun ebeveynin veya vasisinin bu işlemeye onay vermesi gerekmektedir.[5] ancak üye devletlerin kendi ulusal mevzuatlarında

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation, ('GDPR') [2016] OJ 2016 L 119/1.

[2] BUİTELAAR, CJ, "Child's Best Interest and Informational Self-Determination: What the GDPR can Learn from Children's Rights", International Data Privacy Law, Cilt: 8, Sayı: 4, 2018, s. 293.

[3] Çevirmenin Notu: Çocuk Hakları Sözleşmesi, Birleşmiş Milletler Genel Kurulu tarafından 20 Kasım 1989 tarihinde kabul edilmiştir. Hem AB hem de Türkiye sözleşmeye taraftır.

[4] GVKT madde 8.

[5] TİKKİNEN, Christina/ROHUNEN, Anna/MARKKULA, Jouni, "EU General Data Protection Regulation: Changes and Imp lications for Personal Data Collecting Companies", Computer Law & Security Review, Cilt: 34, Sayı: 1, 2018, s. 134.

bu eşiği 13 yaşına kadar düşürmeleri mümkündür. Çocuklar GVKT'de açıkça belirtilen tek dezavantajlı gruptur (gerekçe 38, gerekçe 58, gerekçe 65, gerekçe 71, gerekçe 75, madde 6.1(F), madde 8, madde 12, madde 40.2(g) ve madde 57.1(b)). Dezavantajlılık teriminin geçtiği tek yer gerekçe 75'tir ve şu şekilde yer almıştır: "gerçek kişilerin hak ve özgürlüklerine yönelik, değişen olasılık ve şiddette risk, fiziksel, maddi veya manevi zarara yol açabilecek kişisel veri işlenmesinden kaynaklanabilir" bilhassa "dezavantajlı gerçek kişilerin, özellikle çocukların kişisel verilerinin işlendiği durumlarda". Bu nedenle GVKT, açık bir şekilde herhangi bir şeyden bahsetmemekle birlikte, diğer dezavantajlı kişi kategorilerini hariç tutmazken, özellikle çocuklara dikkat edilmesine vurgu yapar[6]. Gerekçe 38'e göre, "kişisel verilerin işlenmesiyle ilgili riskler, sonuçlar, güvenceler ve hakları hakkında daha az bilinçli olabileceklerinden" veri sorumluları tarafından çocukların kişisel verileri için özel önlemlerin alınması gerekmektedir[7]. Bu ifade, özel önlemlerin alınması gereken diğer dezavantajlı gruplar için de geçerli olacaktır. Bu yaklaşım Örneğin, 39. gerekçede veri sahibine sağlanan herhangi bir bilginin "çocuklar gibi dezavantajlı kişilerin ihtiyaçlarına göre uyarlanması gerektiğini" belirten 2016/680 sayılı Direktif gibi diğer Avrupa Birliği (AB) veri koruma mevzuatına uygundur[8].

[6] Çevirmenin Notu: Bu makalede, konuya ilişkin olarak AB mevzuatı değerlendirilmektedir. Türkiye'deki kişisel verilerin korunması mevzuatına, dezavantajlı kişilerin verilerinin korunması penceresinden, bu dip not içerisinde bakmak isteriz. 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nda (07.04.2016 tarihli Resmi Gazete'de yayınlanmıştır), GVKT'nün aksine çocuklara özgü bir düzenleme bulunmamaktadır. Keza Kanun'unda dezavantajlı yetişkinleri zikreden bir düzenleme de yer almamaktadır. İkincil düzenlemelere bakıldığında, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'de (10.03.2018 tarihli Resmi Gazete'de yayınlanmıştır) çocuklara veya dezavantajlı yetişkinlere yönelik yapılacak aydınlatmalara ilişkin herhangi bir düzenleme yer almamaktadır. Tebliğ'in G) bendinde "Aydınlatma yükümlülüğü yerine getirilirken, genel nitelikte ve muğlak ifadelere yer verilmemelidir" ve Ğ) bendinde "Aydınlatma yükümlülüğü kapsamında ilgili kişiye yapılacak bildirimin anlaşılır, açık ve sade bir dil kullanılarak gerçekleştirilmesi gerekmektedir." hükümleri vardır; ancak bu hükümlerin doğrudan dezavantajlı kişiler için gerekli özenin gösterilmesi vurgusu yaptığını söylemek güçtür. Kanun ve Tebliğ'de hüküm altına alınan aydınlatma yükümlülüğünün nasıl yerine getirileceği hakkında uygulamada açıklık sağlanması ve iyi uygulama örnekleri oluşturması bakımından Kişisel Verilerin Korunması Kurulu ("Kurul") tarafından "Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi" yayınlanmıştır. Rehberde görme engellilerin aydınlatmaya erişebilmesine vurgu yapılmış, ancak diğer dezavantajlı gruplarından (çocuklar, yaşlılar ve diğer engelli grupları (örneğin, anlama güçlüğü çekenler) söz edilmemiştir. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf, s. 14, (Erişim Tarihi: 31.08.2022). Kurul tarafından çıkartılan Açık Rıza Rehberi'nde de dezavantajlı gruplara yer verilmemiş, tarafların eşit konumda olmadığı veya taraflardan birinin diğeri üzerinde etkili olduğu durumlarda rızanın özgür iradeyle verilip verilmediğinin dikkatle değerlendirilmesi gerekliliğine dikkat çekilmiş ve örnek olarak işçi-işveren ilişkisi verilmiştir. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf, s. 7, (Erişim Tarihi: 31.08.2022). Kişisel Verilerin İşlenme Şartları Rehberi'nde de dezavantajlı kişilere ilişkin herhangi bir düzenleme yer almamaktadır. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/9feefe58-9b0f-49c9-a0c7-2b2eb8c012bb.pdf (Erişim Tarihi: 31.08.2022). Çerez Uygulamaları Hakkında Rehber'de, çocuklara yönelik aydınlatmaya ilişkin açıklamalarda bulunulmuş; dezavantajlı yetişkinlere için herhangi bir açıklamaya yer verilmemiştir. "Ürün ve hizmetin hitap edeceği kitle çocuklar ise aydınlatma yükümlülüğü kapsamında çocukların algı düzeyine uygun bilgilendirici metinler hazırlanmalı, gerekirse resim ve görsel efektlerle desteklenen daha anlaşılır, sade ve açık bir dil kullanılmalıdır. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/fb193dbb-b159-4221-8a7b-3addc083d33f.pdf, s. 39, (Erişim Tarihi: 31.08.2022). Bu cümlede, Kurul'un konuya ilişkin hazırladığı şu broşüre atıfta bulunulmuştur: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/db0b3f30-c636-4fcb-930a-bf8f2e524de8.pdf, (Erişim Tarihi: 31.08.2022). Kişisel Verilerin korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi'nde ise, işleme şartları kapsamında açık rızaya ilişkin bölümde, bankacılık mevzuatının ilgili hükümleri gereği engellilerin engellilik durumlarını bildirmesinden ötürü engellilik verisinin işlenmesi için rızalarını ilettiklerinin kabul edilmesi değerlendirilmiştir. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/12236bad-8de1-4c94-aad6-bb93f53271fb.pdf, s. 31 (Erişim Tarihi: 31.08.2022). Rehber kapsamında, banka müşterisi olması muhtemel diğer dezavantajlı gruplara (özellikle yaşlılara) ilişkin bir içerik bulunmamaktadır.

[7] TİKKİNEN/ROHUNEN/MARKKULA, s. 134.

[8] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the

Birleşik Krallık Bilgi Komiserliği Ofisi (bundan sonra "ICO" olarak anılacaktır) özgürce rıza vermelerinin veya kişisel verilerinin işlenmesine itiraz etmelerinin ya da işlemenin sonuçlarını anlama yetilerinin kısıtlı olduğu durumlar içerisinde olan bireyleri dezavantajlı kişiler olarak tanımlamaktadır.[9] Bu, çok çeşitli durumları kapsayan çok geniş bir dezavantajlılık tanımıdır. Bu, ICO'nun amacının, veri koruması söz konusu olduğunda, her türlü dezavantajlılığı kapsamak olduğunu ortaya koymaktadır. Dezavantajlı yetişkinlere ilişkin olarak, kesin bir liste vermemekle birlikte ICO yaşlıları ve belirli engelleri olan kişileri örnek olarak vermektedir. Bir kişinin otomatik olarak dezavantajlı olarak kategorize edilemediği durumda bile, başka bir kişiyle ilişkilerinde bir güç dengesizliği olması GVKT kapsamında dezavantajlılık olarak değerlendirilebileceği ICO tarafından ifade edilmektedir. Kişisel verilerinin işverenleri tarafından işlenmesine itiraz etmekte zorlandıkları bir güç dengesizliği olduğunda işçilerin dezavantajlı grup olarak tanımlanması bu durumun örneğini oluşturur.[10] ICO kişinin mali durumuyla ilgili konular (kredi notunun oluşturulması vb.) veya hastanın tıbbi bakımı nedeniyle kişisel verilerinin işlenmesi hali gibi farklı durumların da dezavantajlı sayılma hususuna örnek teşkil edeceğini belirtmektedir[11].

AB düzeyinde de Madde 29 Veri Koruma Çalışma Grubu[12] (bundan sonra "Çalışma Grubu" olarak anılacaktır) dezavantajlı ilgili kişilerin, çalışanları, çocukları (bilinçli ve düşünceli olarak rıza verme veya veri işleme faaliyetlerine itiraz etme kapasitelerinin olmadığı kabul edilebileceğinden), özel korumaya ihtiyaç duyan nüfusun dezavantajlı gruplarını (ruh sağlığı sorunları olan kişiler, yaşlılar, hastalar vb.) ve veri sorumlusuyla ilgili kişi arasında güç dengesizliğinin mevcut olduğu herhangi bir durumda olan kişileri kapsadığını ifade etmektedir[13]. Bu oldukça geniş tanım ve sınırlı sayıda olmayan dezavantajlı kişi listesi, ICO'nun rehberiyle benzerlik göstermektedir.

Dezavantajlılık çok çeşitli gerçeklere dayalı durumları ifade etmektedir. Dikkat edilmesi gereken fiziksel ve zihinsel koşullar esnek bir yaklaşım gerektirir. Herkes, bazı özel durumların varlığı halinde dezavantajlı olabilir. Bu durumların gerçekleştiği hallerde, mevzuat ve ilgili aktörler uyumlu ve duyarlı olmalıdır. Bu, mevcut ve ortaya çıkmakta olan dezavantajlı kişi grupları hakkında sürekli genişleyen bir içtihat oluşturan Avrupa İnsan Hakları Mahkemesi'nin (bundan sonra "AİHM" olarak anılacaktır) yaklaşımında yansımasını bulmaktadır. Bu yaklaşım, daha "sağlam bir eşitlik fikri" elde etme misyonuna yardımcı olabilir[14].

Dezavantajlılık, mahremiyet ve veri koruma, araştırmacılar tarafından nadiren araştırılırken, Malgeiri ve Niklas yakın zamanda "dezavantajlı ilgili kişi kavramının rolünü ve potansiyelini" analiz etti[15]. Onlar, dezavantajlılığın evrensel

Purposes of the Prevention, Investigation, Detection, or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA [2016] OJ L119.

9 ICO, "When Do We Need to Do a DPIA?", https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/ (Erişim Tarihi: 06.10.2021).

10 Art 29 Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679" (WP 248, 4 Ekim2017).

11 ICO, "Veri koruma etki değerlendirmesine ne zaman ihtiyaç duyarız?", N. 8.

12 Art 29 Working Party, 25 Mayıs 2018 tarihine (GDPR'nin uygulamaya girişi) kadar mahremiyetin ve kişisel verilerin korunmasına ilişkin konularla ilgilenen bağımsız Avrupa çalışma grubudur. Çalışma Grubu ile ilgili arşive buradan ulaşılabilir: https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en (Erişim Tarihi: 31.08.2022).

13 Art 29 Working Party, "Guidelines on Data Protection Impact Assessment (DPIA)", N. 9.

14 ARNARDÓTTİR, Oddný Mjöll, "Vulnerability under Article 14 of the European Convention on Human Rights", Oslo Law Review, Cilt: 1, Sayı: 3, 2017, s. 150; PERONİ, Lourdes/ TİMMER, Alexandra, "Vulnerable Groups: The Promise of an Emerging Concept in European Human Rights Convention Law", International Journal of Constitutional Law, Cilt: 11, Sayı: 4, 2013, s. 1056.

15 MALGİERİ, Gianclaudio/NİKLAS, Jędrzej, "Vulnerable Data Subjects", Computer Law & Security Review, 37, 2020, s. 105415.

(tüm kişiler dezavantajlıdır) veya özel (bazı kişiler diğer kişilerden daha dezavantajlıdır) olarak iki farklı yaklaşımla ele alınabileceğini belirtmektedirler. Gerçekten de araştırmacılar daha önce her ikisinin de lehinde tartışmışlardır. Fineman dezavantajlılık insanlığın evrensel bir unsuru olduğunu ve herkes tarafından paylaşıldığını ileri sürerken, Cooper ise bunun doğru olması halinde, evrensel bir yaklaşımın, polis nazarında her zaman şüpheli olmaya devam eden siyahi genç erkeklerin kimliğe dayalı belirli deneyimlerinin göz ardı edileceğinin altını çizmektedir[16]. Malgieri ve Niklas dezavantajlılığı veri koruma çerçevesi içine yerleştirmenin sorunlu bir yaklaşım olduğunu düşünmektedirler. Çünkü tüm ilgili kişiler evrensel olarak dezavantajlı olarak kabul edilirse, aralarındaki önemli farkların göz ardı edilebileceğini, böylece de bazı kişilerin zaten dezavantajlı olan durumlarının daha da kötüleşebileceğini, daha spesifik veri koruma kurallarının mevcutta da karmaşık olan yasal ortamın daha da parçalanmasına neden olabileceğini ileri sürmektedirler[17]. Bu bilmeceye bir çözüm olarak Luna'nın katmanlı dezavantajlılık teorisini öneriyorlar[18]. Luna, tüm insanların dezavantajlı olduğunu, ancak bazı kişilerin diğerlerinden daha fazla dezavantajlılık katmanına sahip olduğunu savunarak evrensel ve özel ayrımının üstesinden gelir. Bu katmanlı yaklaşım, GVKT'nin risk temelli yaklaşımını yansıtıyor gibi görünüyor; ikincisi, herkesin dezavantajlı olabileceğini, ancak çeşitli düzeylerde ve farklı bağlamlarda olabileceğini öne sürüyor. Aynı zamanda Calo'nun "hiç kimse her zaman ve her bağlamda tamamen dezavantajlı değildir" ve "hepimiz dereceler ve koşullara göre dezavantajlıyız" durumunu yansıtıyor[19]. Calo, hukukun dezavantajlılığı genellikle bir kişi veya grubun statüsü ya da bireyler veya kuruluşlar arasındaki bir ilişki olarak kabul etmesine rağmen, Hukuki araştırmaların, bu kavramın en iyi, bazı bireylerde ve bağlamlarda, ancak bazen tüm insanlarda daha sık ve yoğun bir şekilde var olan bir durum olan 'kişilik katmanı' olarak algılandığını giderek daha fazla kabul etmekte olduğunu ileri sürmektedir[20]. Bu tartışma, bu makalenin veri koruma alanında yapmaya çalıştığı katkıya nasıl dönüşüyor?

Bu çalışma, dezavantajlılık katmanlarının herhangi bir kişide ortaya çıkabileceğini ve katmanlı yaklaşımın, herkesi, hatta en ince dezavantajlılık durumlarını bile dikkate alma avantajına sahip olduğunu ve aynı zamanda kesişen ve kümülatif bir yaklaşımı teşvik ettiğini kabul etmektedir. Bununla birlikte, bazı durumlarda dezavantajlı bireylerin kategorilere ayrılmasının, veri korumalarının daha yüksek düzeyde sağlanmasına yardımcı olabileceğini de savunmaktadır. Bu makale, "bağlamsal" dezavantajlılığa değil, doğası gereği dezavantajlı olarak kabul edilen, yani engelli yetişkinler gibi dezavantajlılık katmanları sürekli ve kesin olarak mevcut olan çocuklar ve yetişkinlere odaklanmaktadır. Çocukların 'veriye dayalı mimarinin karmaşıklığını anlama kapasitesi sınırlıdır, daha az deneyime sahiptir, riskler ve haklar konusunda daha az farkındalığa sahiptir ve kolayca manipüle edilebilir' (bu, GVKT'nin hükümlerine yansıtılmıştır), engelli yetişkinlerin doğasında bulunan dezavantajlılık, AİHM içtihatlarında kendisine yer bulmuştur[21]. İnsanların dezavantajlı olarak kabul edilebileceği (örneğin, işverenler ve çalışanlar arasındaki yukarıda

[16] FINEMAN, Martha Albertson, "The Vulnerable Subject: Anchoring Equality in the Human Condition", Yale Journal of Law and Feminism, Cilt: 20, Sayı: 1, 2008, s. 1; COOPER, Frank Rudy, "Always Already Suspect: Revising Vulnerability Theory", North Carolina Law Review, Cilt: 93, Sayı: 5, 2015, s. 1379.

[17] MALGİERİ/NİKLAS, N. 13, s. 5.

[18] LUNA, Florencia, "Elucidating the Concept of Vulnerability: Layers Not Labels", International Journal of Feminist Approaches to Bioethics, Cilt: 2, Sayı: 1, 2009, s. 121.

[19] CALO, Ryan, "Privacy, Vulnerability, and Affordance", DePaul Law Review, Cilt: 66, Sayı: 2, 2017, s. 593.

[20] CALO, s. 593.

[21] TİMMER, Alexandra, "Vulnerability: Reflections on a New Ethical Foundation for Law and Politics", A Quiet Revolution: Vulnerability in the European Court of Human Rights, Ed. Martha Albertson Fineman ve Anna Grear (Ashgate, Farnham 2013); TİMMER, Alexandra, "Strengthening the Equality Analysis of the European Court of Human Rights: The Potential of the Concepts of Stereotyping and Vulnerability" (Doctor of Law, Universiteit Gent 2014); MALGİERİ/NİKLAS, N. 13.

bahsedilen güç dengesizliği durumları) birçok dezavantajlılık katmanı veya diğer durumlar vardır, ancak bunların gerçekte olup olmayacağına karar vermek, vaka bazında bir analiz gerektirir. Bu ince dezavantajlılık durumları bu çalışmanın kapsamına girmez. Böyle bir odak seçimi, uç örneklerden gelen daha az dikkat dağıtıcı ile en acil pratik zorlukları vurgulama avantajına sahiptir. Tabii ki bu, ikincisinin herhangi bir şekilde daha az önemli olduğu anlamına gelmez, ancak bu çalışmanın amacı, argümanlarımızı göstermek için doğası gereği dezavantajlı bireylerden örnekler kullanarak GVKT ve akıllı ev bağlamındaki dezavantajlılığı daha geniş bir şekilde yansıtmaktır.

GVKT'nin yalnızca bir grup dezavantajlı kişiden (çocuklardan) açıkça bahsetmesinden kaynaklanabilecek bir sorun, kuruluşların diğer dezavantajlı grupları görmezden gelirken sadece çocuklara odaklanma ihtimalidir. Dezavantajlı yetişkinler kesinlikle Avrupa veri koruma yasaları tarafından korunmaktadır, ancak dezavantajlılık, akıllı ürünler üzerinde çalışanlar için veri koruma önlemlerini etkin bir şekilde ayarlamak için çok fazla soyut bir kavram olarak görülebilir. Bazı kuruluşlar, GVKT'de dezavantajlı yetişkinlere ilişkin somut düzenleme eksikliğini, dezavantajlı yetişkinleri korumak için çocuklardaki kadar çok kaynak ayırmaya gerek olmadığının bir göstergesi olarak görebilir. Bu nedenle, Avrupa ve ulusal veri koruma yetkililerinin GVKT'nin nasıl uygulanacağına ilişkin rehberleri özellikle önemlidir. Ancak, İngiltere'nin ICO'su tarafından Yaşa Uygun Tasarım uygulama kurallarının benimsenmesi, hem veri koruma yetkililerinin hem de veri sorumlularının çocukların durumuna odaklanacağının bir başka göstergesidir[22]. Bir veri sorumlusu, ürününün çocuklar tarafından kullanılmayacağını düşünürse (daha sonra tartışacağımız gibi, her zaman olabileceğini varsaymak daha iyidir), veri sorumlusunun benimsemesi gereken özel veri koruma önlemlerini görmezden gelebileceği veya bu önlemler hakkında bilgi sahibi olmayabileceğinden, bu dezavantajlı yetişkinlerin veri korumasını zayıflatabilir. Bu soruna bir çözüm, Komisyonun uygulama tasarrufları yoluyla bir davranış kurallarının (code of conduct) "Birlik içinde genel geçerliliğe" sahip olduğuna karar verebileceğini belirten GVKT'nin 40. maddesi olabilir. Dezavantajlı yetişkinleri tartışan bir davranış kuralları yazılırsa, Komisyon tüm Üye Devletlerde uygulanmasını teşvik edebilir.

Akıllı Evler ile İlgili Önemli Veri Koruma Sorunları

Akıllı evler nedir ve neden bu özel ortama odaklanmalıyız? Akıllı ev, "konfor, sağlık, güvenlik, asayiş, enerji ve tasarrufu için konut yönetimine zekayı dahil eden, her yerde bulunan bilgi işlemin çağdaş bir uygulaması" olarak tanımlanabilir[23]. Gerçekten akıllı bir ev, "çevreyle ilgili tüm bilgilerin toplu olarak depolandığı ve analiz edildiği, kalıpların çıkartıldığı ve kullanıcının müdahalesi olmadan kararların alındığı" bir evdir[24]. Herhangi bir cihaz akıllı hale gelebilir ve insanların evlerinde kullanılabilir. Akıllı evle ilgili ürünlerin bazı kategorileri şunlardır: akıllı güvenlik cihazları (akıllı kilitler, güvenlik kameraları, duman dedektörleri gibi), ev otomasyonu ve akıllı alarm sistemi, eğlence cihazları (akıllı televizyonlar, hoparlörler gibi), akıllı ev asistanları (Alexa, Siri, Cortana, Google Home gibi), akıllı elektronik aletler (bulaşık makineleri, buzdolapları, su ısıtıcıları, ampuller gibi)... Bu cihazlara, genellikle nesnelerin interneti ürünleri (internet of things) de denir. Elektrik ve Elektronik Mühendisleri Enstitüsü, nesnelerin internetinin ne olduğuna ilişkin bir tanım ortaya koymaya çalışmıştır[25]. Tanımlayabilmek için, standardizasyon kuruluşları, akademisyenler, ve diğer

[22] Information Commissioner's Office, "Age Appropriate Design: A Code of Practice for Online Services" (2 September 2021) https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/, (Erişim Tarihi: 4.10.2021).

[23] MOCRİİ, Dragos/ CHEN, Yuxiang/ MUSİLEK, Petr, "IoT-Based Smart Homes: A Review of System Architecture, Software, Communications, Privacy and Security", 1-2 Internet of Things, 2018, s. 81.

[24] MOCRİİ/CHEN/MUSİLEK, s. 81.

[25] IEEE, "Towards a Definition of the Internet of Things (IoT)" (27 May 2015), 74 https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf, (Erişim Tarihi: 06.10.2021).

birçok kaynak tarafından sağlanan tanımların en son haritasını çıkartmışlardır. Bu çalışmanın sonunda, Enstitü, nesnelerin internetini şu şekilde açıklamıştır: "Nesnelerin interneti, benzersiz bir şekilde tanımlanabilen nesneleri internete bağlayan bir ağ olarak tanımlanabilir. Nesneler, algılama/hareket etme ve potansiyel programlanabilirlik yeteneklerine sahiptir. Benzersiz tanımlama ve algılamanın kullanılmasıyla, nesne hakkında bilgi toplanabilir ve nesnenin durumu her yerden, her zaman, herhangi bir şey tarafından değiştirilebilir.[26] Bu çalışmada, akıllı cihazlar ve nesnelerin interneti ürünleri birbirinin yerine kullanılacaktır.

Akıllı cihazların her yerde bulunması bir gerçeklik haline gelmekte ve küresel ölçekte sayılarının artması uzun vadede kesin görülmektedir. 2018 raporuna göre, 2025 yılına kadar 21,5 milyar nesnelerin interneti cihazı hayatımızda olacak ve %25'ten fazla siber saldırı gerçekleştirilecek (2018'deki 7 milyar cihaza kıyasla)[27]. Akıllı cihazlar, giderek artan miktarda veriyi internet üzerinden aktarmaktadır. Bu cihazlar, genellikle kişisel verileri toplarlar ve analiz için bunları buluta aktarırlar. Analiz sonuçları, hizmeti daha etkili hale getirmek için cihaza geri entegre edilir. Örneğin, kuruluşlar, akıllı hoparlörler aracılığıyla toplanan verileri analiz ederek ses kalıpları ve insanların tercihleri hakkında bilgi edinebilirler[28]. Zayıf güvenlik önlemleri (varsayılan parolaların değiştirilmemesi gibi) ve mevcut veri madenciliğine, bulut veri tabanlarında depolamaya ve bununla ilişkili çeşitli veri gizliliği tehditlerine yol açan bulut mimarileri nedeniyle nesnelerin interneti ürünleriyle ilgili veri hack'lerinin sayıca artması muhtemeldir[29]. Son veri ihlallerinin skalası, bunun gerçekleşmesinin muhtemel olduğunu göstermektedir[30].

Tüketiciler, akıllı ürünleri kullandıklarında ve güvenli bir akıllı ev ortamı oluşturmak için teknik kapasiteye sahip olmadıklarında, verilerinin taşıdığı risklerin nadiren farkına varırlar[31]. Cihaz yönetimi ve ağ yönetimi ile ilgili sık sık sorunlar yaşarlar. Sonuç olarak, akıllı cihazlara, bunları geliştiren ve dağıtan kişilerin yanı sıra politika yapıcılar tarafından da özel ilgi gösterilmelidir. İnsanların cihazlarını ve ağlarını etkin bir şekilde yönetebilmeleri (ve dolayısıyla verilerini koruyabilmeleri) ancak onların kullanımı için bu cihazlar kolaylaştırıldığında mümkün olabilecektir[32].

Akıllı ev ürünleriyle ilgili tehditler yeni bir sorun değil, bazıları uzun zamandır iyi bilinmektedir. Daha 2014 yılında, Çalışma Grubu akıllı cihazlardan kaynaklanan kişisel veri güvenliğine yönelik çeşitli tehditlerin varlığını kabul etmiştir[33]. Bu tehditler, üçüncü kişiler tarafından izlenen ve kişisel verilerinin nasıl kullanıldığı üzerinde gerçek bir kontrole sahip olmayan tüketicilerle bağlantılıdır. Diğer riskler, insanların verilerini işleme amacını, profil oluşturma teknikleri ve kullanıcıların davranış kalıpları hakkında bilgi edinmeyle ilgilidir. Evlerinde nesnelerin interneti cihazları olan kişiler için anonim kalmak giderek daha zor hale gelmiştir[34]. İnsanlar,

[26] IEEE, "Towards a Definition of the Internet of Things (IoT)" (27 May 2015) 74 <https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15 (Erişim Tarihi: 06.10.2021).

[27] LUETH, Knud Lasse "State of the IoT 2018: Number of IoT Devices now at 7B - Market Accelerating'" (IoT Analytics, 8 August 2018) <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/> (Erişim Tarihi: 6.10.2021).

[28] URQUHART, Lachlan/SCHNÄDELBACH, Holger/JÄGER, Nils, "Adaptive Architecture Regulating Human Building Interaction", International Review of Law, Computers & Technology, 33(1), 2019, s. 3.

[29] PİASECKİ, Stanislaw/URQUHART, Lachlan/MCAULEY, Derek, "Defence Against the Dark Artefacts: Smart Home Cybercrimes and Cybersecurity Standards", Computer Law & Security Review, 42, 2021, s. 105542.

[30] GARTNER, "Leading the IoT: Gartner Insights on How to Lead in a Connected World", 13, 2017, https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf, (Erişim Tarihi: 6.10.2021).

[31] HEUVEL, Karlijn van den, "Securing the Smart Home", Masters thesis, University of Amsterdam, 2018.

[32] ADAMS, Anne/ SASSE, Martina Angela, "Users are Not the Enemy" Communications of the ACM, Cilt: 42, Sayı: 12, 1999, s. 40.

[33] Art 29 Working Party, "Opinion 8/2014 on the Recent Developments on the Internet of Things" (WP 223, 16 September 2004).

[34] Art 29 Working Party, "Opinion 8/2014 on the Recent Developments on the Internet of Things" (WP 223, 16 September 2004).

kimlik hırsızlığı, siber taciz ve ayrımcılığın kurbanı olabilir ve verilerin sızdırılması ve ele geçirilmesi nedeniyle itibar kaybı yaşayabilirler. Ayrıca, siber suçlular yeni tehditler icat etmeyi sürdürürler ve genellikle güvenlik engellerini aşmada başarılı olurlar. Dezavantajlı kişilerin bu tür veri güvenliği risklerine karşı kendilerini savunma kapasiteleri daha düşük olabilir. GVKT, veri koruma mekanizmalarını dezavantajlı kişilerin ihtiyaçlarına göre uyarlama ihtiyacı olduğunu kabul eder (örneğin GVKT'nin 38 ve 75 gerekçeleri).

Yeni teknolojiler, dezavantajlı bireylere çeşitli şekillerde yardımcı olmak için uzun süredir kullanılmaktadır. Farklı sağlık koşullarına sahip olan veya sadece yaşlılığa bağlı semptomlar yaşayan insanlar, teknolojik gelişmelerin bir sonucu olarak daha özerk bir şekilde yaşayabilmektedir. Bu, ortam destekli yaşam (ambient assisted living) başlığı altında bilgisayar alanında uzun süredir devam eden bir araştırma dizisinin konusu olmuştur. Akıllı cihazların kullanımı bu alandaki en son gelişmedir. Bu ürünlerin dezavantajlı kişilerin verilerini nasıl işlediğini tespit etmek çok önemlidir. Dezavantajlılık, veri işleme sırasında (örneğin, aydınlatmaya dayalı izin verme açısından bazı kişiler için daha fazla risk olabilir) veya işlemenin bir sonucu olarak (veri işleme, ayrımcılığa veya örneğin psikolojik zararlara yol açabilir) sonuçlar doğurabilir[35]. akıllı cihazların bazıları, belirli kişi kategorilerini hedeflemektedir[36]. Çocuklar örneğinde, etkileşimli bebekler veya robotlar gibi mağazaların raflarında internete bağlı oyuncaklar ortaya çıkmaktadır[37]. Ebeveynler ayrıca çocuklarının uyku düzenini, konumunu ve tıbbi verilerini takip eden akıllı bebek telsizleri veya akıllı saatler gibi ürünleri satın almaktadır[38]. Demanslı kişiler söz konusu olduğunda, günlük yaşam faaliyetlerinde onları desteklemek için geliştirilmiş birçok sağlık cihazı veya izleme cihazı bulunmaktadır[39]. Nüfusun belirli kısımlarını hedefleyen nesnelerin interneti ürünleri, tüketicilerin belirli dezavantajlılık katmanlarına dayalı olarak [ve kuruluşların bu bağlamda yürütmesi gereken veri koruma etki değerlendirmeleri (bundan sonra "VKED" olarak anılacaktır) açısından]veri sorumlularından daha odaklı bir yaklaşım sergilemesini gerektirir. Çünkü bu yaklaşım, önlemlerin veri işleme aşamasında dezavantajlı kişilerin ihtiyaçlarına daha iyi uyarlanmasını sağlamaya yardımcı olabilir. Sesli asistanlar gibi yaygın olarak kullanılan cihazların, herkesin dezavantajlılık katmanları farklı olduğu için herkese uyum sağlaması daha zordur. Bu, bu makalenin ilerleyen kısımlarında incelenecek olan daha genel veri koruma önlemleri [tasarım yoluyla ve varsayılan olarak veri koruma ilkesinin uygulanması] yoluyla veri işlemenin olası olumsuz etkilerinin önlenmesiyle kısmen ele alınabilir.

Nesnelerin interneti dünyasının hızla genişlemesinin ve zamanla artan sayıda insanın akıllı evlerde yaşayacağı gerçeğinin bir sonucu olarak, en dezavantajlı olanların kişisel verilerinin en iyi şekilde nasıl korunacağını tartışmak çok önemlidir. Çoğu nesnelerin interneti ürününün şu anda tasarlanma şekli nedeniyle, sayıları arttıkça güvenlik sorunlarının sayısı da maalesef büyük olasılıkla artacaktır. Veri koruma hükümlerini, dezavantajlı kullanıcıları olası ihlallere karşı koruyacak ve verilerinin nasıl işleneceğine karar vermeleri için onlara yardımcı olacak şekilde uygulamak elzemdir. Çocukların çevrimiçi etkinlikleriyle ilgili özel veri koruma önlemleri ve Birleşmiş Milletler Çocuk Haklarına Dair Sözleş-

[35] MALGİERİ/NİKLAS, N. 13.

[36] ARNOLD, Brent/SİVASOTHY, Kavi, "He Sees You when You're Sleeping, He Knows When You're Awake: Smart Toys and Regulating the IoT in Canada", Gowling WLG, 17 December 2018, https://gowlingwlg.com/en/insights-resources/articles/2018/smart-toys-and-regulating-the-iot-in-canada/ (Erişim Tarihi: 06.10.2021).

[37] COLLINGWOOD, Lisa, "Villain or Guardian? 'The Smart Toy is Watching You Now...'", Information & Communications Technology Law, Cilt: 30, Sayı: 1, 2021, s. 75.

[38] MİLKAİTE, Ingrida/LİEVENS, Eva, "Child-Friendly Transparency of Data Processing in the EU: From Legal Requirements to Platform Policies", Journal of Children and Media, Cilt: 14, Sayı: 1, 2019, s. 5.

[39] GIBSON, Grant, "Smart Technologies in Dementia Care - Future Opportunities and Challenges", 21 March 2019, https://dementia.stir.ac.uk/blogs/dementia-centred/2019-03-21/smart-technologies-dementia-care-future-opportunities-and (Erişim Tarihi: 06.10.2021).

me'nin 16. Maddesinde yer alan temel haklarını mahremiyete dönüştürmek için yapılan çağrılar, önceki AB mevzuatına kıyasla dezavantajlılığa ilişkin yeni GVKT hükümleriyle sonuçlanmıştır.[40] Bu, kuruluşların veri koruma politikalarını çocukların ve diğer dezavantajlı kişilerin ihtiyaçlarına göre uyarlamaları gerektiği anlamına gelmektedir. Kuruluşlar için veri koruma düzenlemelerine uymak, yalnızca parasal yaptırımlardan kaçınmak değil, aynı zamanda müşterilerin güvenini kazanmak için stratejik bir hamle olabilir.

Tedbirleri Dezavantajlı Kişilerin İhtiyaçlarına Göre Uyarlayarak Seçilen Yasal Dayanağın Gerekliliklerini Karşılamak

Veri koruma sorunlarından kaçınmanın en etkili yolu kişisel verilerin işlenmesinden kaçınmaktır. Ancak bazı durumlarda dezavantajlı kişilerin verilerinin işlenmesi gerekecektir.[41] Hukuki dayanak seçimi, veri sorumlusunun sıradan veya özel nitelikteki kişisel verileri işleyip işlemediğine göre farklılık gösterecektir. Bu makale, akıllı bir ürün kullanan dezavantajlı kişi bağlamında her bir yasal dayanağın nasıl uygulanacağını kısaca açıklamaktadır. Rıza mekanizması, dezavantajlı kişiler akıllı cihaz kullandığında, dezavantajlı kişilerin ihtiyaçlarına göre uyarlanmalıdır. Alternatif hukuki dayanaklarla ilgili olarak, sözleşmenin ifası, meşru menfaat gibi hukuki dayanaklar aynı durumda nasıl uygulanır?

Varsayılan Olarak Rıza Bağlamında Dezavantajlı Kişiler İçin Özel Önlemlerin Benimsenmesi

İnsanların neyi kabul ettiklerini anlamalarını ve seçimlerinin potansiyel sonuçlarının bilincinde olmalarını sağlamada rızanın etkililiği hakkında sahip olunan görüş ne olursa olsun, bu yasal zeminin şartlarını yerine getirmek, en azından günümüzde web üzerindeki rıza yönetimi platformlarının kasıtlı olarak manipülatif uygulamalarını azaltacaktır. Bu manipülatif uygulamalar web sitelerinde kullanılıyorsa, kesinlikle nesnelerin interneti sektöründe ve dezavantajlı kişiler tarafından evlerinde kullanılan milyarlarca akıllı üründe de uygulanmaktadır[42].

GVKT uyarınca, bir rızanın geçerli olabilmesi için rızanın özgürce verilmesi, bilgilendirmeye dayalı olması, spesifik ve açık olması gerekmektedir[43]. Bu bağlamda işbu makale, çocuklar ve dezavantajlı yetişkinler için özel veri koruma önlemlerini alınmasının önemini vurgulamaktadır[44]. Örneğin Birleşik Krallık veri koruma otorite-

[40] MACENAİTE, Milda, "From Universal Towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation", New Media & Society, Cilt: 19, Sayı: 5, 2017, s. 765; Convention on the Rights of the Child, N. 3.

[41] ŽLİOBAİTĖ, Indrė/CUSTERS, Bart, "Using Sensitive Personal Data May be Necessary for Avoiding Discrimination in Data-Driven Decision Models", Artificial Intelligence and Law, Cilt: 24, Sayı: 2, 2016, s. 183.

[42] Rızanın gerçekten tercih edilen uyum seçeneği olmasının bir başka önemli nedeninin de sektöre özel diğer mevzuat tarafından da gerekli olabileceği belirtilmelidir. Örneğin, eGizlilik Yönergesi'nin 5(3) maddesi (bazen halk arasında "çerez yasası" olarak bilinir), "terminal ekipmanı" tanımına girme olasılığı yüksek olduğundan akıllı cihazlar için potansiyel olarak geçerli olabilir. (Elektronik iletişim sektöründe kişisel verilerin işlenmesi ve mahremiyetin korunmasına ilişkin 12 Temmuz 2002 tarihli Avrupa Parlamentosu ve Konseyinin 2002/58/EC sayılı Direktifi (Gizlilik ve elektronik haberleşmeye ilişkin Direktif), [2017] OJ L 201 /37) Bu maddeye göre, 'bilginin saklanmasına veya halihazırda depolanmış bilgilere erişim sağlanmasına' yalnızca üç durumda izin verilmektedir: (i) rızanın verilmesi; (ii) yalnızca iletişim iletimi içindir; veya (iii) kullanıcı tarafından talep edilen bir hizmetin sağlanması için kesinlikle gerekli olması. eGizlilik Yönergesi şu anda yasal bir revizyondan geçiyor ve Komisyon, yeni madde 8(1)'de web izleyici ölçümü için dördüncü bir izin veren koşul eklemeyi önerdi. (Avrupa Komisyonu, 'Avrupa Parlamentosu ve Konseyinin özel hayata saygı ve elektronik iletişimde kişisel verilerin korunmasına ilişkin Yönetmelik 2002/58/EC sayılı Direktifi yürürlükten kaldırmasına ilişkin Öneri (Gizlilik ve elektronik iletişim hakkında Yönetmelik), 2017 /0003' (COD), Brüksel, COM (2017) 10 final). Bununla birlikte, eGizlilik çerçevesi kapsamındaki meşrulaştırma gerekçelerinin listesinin GVKT kapsamındakilerden farklı olduğu ve farklı olmaya devam edeceği açıktır ve iki yasal çerçevenin örtüşmesinin akıllı ev teknolojileri alanında nasıl sonuçlanacağını belirlemek için daha fazla araştırmaya ihtiyaç vardır.

[43] GVKT 4; Gerekçe 32.

[44] GVKT 4; Gerekçe 32; Gerekçe 38. Özel veri koruma önlemleri, bir yasal vasinin, bilinçli veri işleme kararları verme kapasitesine sahip olmadığı durumlar-

si, gizlilik bildirimlerinin açık, sade ve yaşa uygun bir dille kaleme alınmasını önermiştir[45]. Bu makale, herkes tarafından kullanılan akıllı cihazlar (örneğin, sesli asistanlar) için, dezavantajlı kişileri destekleyen önlemlerin (ICO tarafından Yaşına Uygun Tasarım uygulama kurallarında önerilenler gibi) tüm ilgili kişiler için otomatik olarak benimsenmesi gerektiğini ileri sürmektedir. İlk olarak, bu, yukarıda sözü edilen dezavantajlı kişilerle ilgili hükümlere veri koruma uyumunu kolaylaştıracaktır. İkinci olarak, çoğu insan teknik ve karmaşık dili anlayamadığı için, basit terimler ve açık kavramlar kullanmak, tüm gizlilik politikaları için standart bir uygulama olmalıdır.

Hassas veriler açısından, açık rıza adı verilen olağan rızaya karşılık gelen bir yasal dayanak vardır. Kuruluşun hassas verileri akıllı cihazlar üzerinden işlemeye karar vermesi halinde, iki aşamalı doğrulama süreci (örneğin ilgili kişinin işlenecek veriler "kabul ediyorum" ifadesini içeren bir e-posta göndermesini ve ayrıca seçimini onaylaması için bir doğrulama bağlantısını tıklamasını istemek) veya ilgili kişiden dijital imza alınması (daha önce bahsedilen tüm olağan rıza şartlarına ek olarak) gerekecektir[46]. Nesnelerin interneti sektörünün mevcut durumunda, dezavantajlı kişiler tarafından kullanılan birçok akıllı ürün (sesli asistanlar, akıllı TV'ler, akıllı sağlık cihazları vb.) hassas verileri toplar (veya toplayabilir) ve bu ek açık rıza gereklilikleri büyük olasılıkla birçok durumda geçerli olacaktır. Örneğin, Amazon 2019 yılında kendilerinin veya yasal vasilerinin rızası olmadan çocukları kaydettiği iddiasıyla dava edildi. Şikayette, Amazon'un kayıtlı olmayan kullanıcıların rızasını almak bir yana Alexa etkileşimlerinin kalıcı ses kayıtlarını oluşturduğu konusunda hiçbir noktada uyarıda bulunmadığı belirtilmiştir[47]. Bu olaylar sırasında, Alexa'nın gizlilik bildirimi yalnızca önceki ses isteklerinin işleyişi iyileştirmek için analiz edildiğini belirtmekte, ancak insanların bu kayıtları dinlediğini açıkça belirtmemektedir. Bu tür ses kayıtları dezavantajlı kişilerin hassas verilerini içerebilir ve şikayet AB sınırları içerisinde yapılmış olsaydı Amazon'un faaliyetlerinin büyük olasılıkla GVKT hükümlerini ihlal ettiği değerlendirilirdi. Bu vakada Amazon, cihazlarını kullanan çocukların ihtiyaçlarına göre uyarlanmış iki aşamalı bir onay doğrulama sürecinin uygulanmasını sağlamalıydı. Rıza gereksinimlerinin karşılandığından emin olmak için güçlü yaptırım mekanizmaları gereklidir.

da, savunmasız bir yetişkin adına hareket etmesine ne ölçüde izin verildiğini de ilgilendirmelidir. Bu soru, potansiyel sağlık sorunlarını belirlemek için sosyal bakım hastalarının davranışlarını ve elektrik kullanımını (sensörler ve AI teknolojisi aracılığıyla) evlerinde izleyen Lilli gibi sistemlerin geliştirilmesiyle daha sık sorulacak. [Bkz. Chris Baraniuk, "Sensors and AI to Monitor Dorset Social Care Patients", BBC, 2021, https://www.bbc.com/news/technology-58317106 (Erişim Tarihi: 05.10.2021)]. Önceki noktaya benzer şekilde, Avustralya hükümeti tarafından sağlık verilerini ve biyometrik verileri (duygusal tetikleyici yapay zeka ve makine öğrenimi yoluyla) izlemek için oluşturulan sanal asistan 'Nadia' örneğinde, Devletin meşru çıkarlarını nasıl uzlaştırmalıyız? Mahremiyet ve veri koruma haklarıyla engelli kişilerin devlet hizmetlerine erişimini iyileştirmek mi? Bu senaryoda, yasal vasiler savunmasız bir birey adına onay verebilmeli mi? [Bkz. ADAMS, Rachel/NÓRA, Loideain/CLIFFORD, Damian: "Gender as Emotive AI and the Case of "Nadia" Regulatory and Ethical Implications", 2021, 9, ssrn: 3858431 http://dx.doi.org/10.2139/ssrn.3858431 (Erişim Tarihi: 08.09.2021)]. Son olarak Claire Bessant, "paylaşma" (çevrimiçi çocukların bilgilerinin paylaşılması) konusunu tartışıyor ve Birleşik Krallık'ta, bir ebeveynin çocuklarının verilerinin nasıl kullanılacağına karar verme hakkının, çocuğun veri koruma hakkının yerini ne zaman alacağının kesin olmadığının altını çiziyor. (Bkz. BESSANT, Claire, "Sharenting: Balance the Balancing the Conflicting of Annes and Children", Cilt: 23, Sayı: 1, 2018, İletişim Yasası 7). Bunların tümü, toplumun yanıt bulması gereken açık sorulardır. Bir yasal vasi, korunması gereken kişi adına her zaman iyi niyetli veya bilinçli kararlar verme kapasitesine sahip olmayabileceğinden, savunmasız bir kişinin verilerine sınırsız erişime sahip olmamalıdır. Kanun hükümlerinin tek başına başarılı bir çözüm olması pek olası değildir ve bunları etkili kılmak için veri koruma yönetimi alanındaki teknolojik gelişmelerle birleştirilmelidir (kişisel bilgi yönetim sistemleri ve diğer gizlilik artırıcı teknolojiler gibi). Bu konu daha fazla akademik çalışma gerektirir.

[45] ICO, "Age Appropriate Design", N. 20.

[46] EDPB, "Guidelines 05/2020 on Consent under Regulation 2016/679", 4 May 2020, 21 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf (Erişim Tarihi: 06.10.2021).

[47] KELİON, Leo, "Amazon Sued over Alexa Child Recordings in US" BBC, 2019, https://www.bbc.com/news/technology-48623914 (Erişim Tarihi: 06.10.2021).

Dünya genelinde rıza yararlı bir mekanizma olarak görülmez ve çok sayıda yazar tarafından, özellikle dezavantajlı kişilerin verilerinin toplanması hususunda eleştirilir. Bazı araştırmacılar, rızanın bir kontrol yanılsaması sağladığını[48] ve bunun genellikle güç dengesizliğinin olduğu bağlamlarda verildiğini, bu yüzden özgür iradeye dayalı olarak verilmediğini ileri sürmektedir.[49] bazı makalelerde, güç dengesizlikleri oluşturan ve kişilerin kendi kişisel verileri üzerindeki etkisini ve kontrolünü azaltan ağ ortamlarının doğasının altı çizilmektedir[50]. Çocuklar gibi dezavantajlı kişiler kararları ve veri yönetimi seçenekleri iletişim alanlarının işlevlerine ve tasarımına bağlı olduğundan, kişisel verilerini çevrimiçi ortamlarda tam anlamıyla kontrol edemezler[51]. Bu durum akıllı cihazlar için de geçerlidir. İletişim alanları kuruluşlar tarafından tasarlanır, bu nedenle eğer kuruluş hayır kurumu veya benzeri bir yapı değilse (veya finansal bir teşvik yoksa), iletişim alanlarını kendi ticari çıkarlarına uygun tasarlayacaktır. Rıza isteyen akıllı cihazlar, kullanıcıların aşina olmadıkları, anlaşılması güç gizlilik politikalarını sunarlar. Çocuklara yönelik gizlilik politikaları özellikle kafa karıştırıcı, anlaşılması zor, genellikle uzun ve karmaşıktır[52]. Eğer yaptırımlar ve bunların sonucunda GVKT'ye etkin bir şekilde uyum ivme kazanırsa, akıllı cihazlar geliştiren kuruluşlar davranışlarını değiştirmeye zorlanabilirler. Bunun gerçekleşmesi için, hali hazırda yeterli bütçeye sahip olmayan veri koruma otoritelerine kaynak ayrılmalıdır[53]. Tasarımcılar için ilginç bir fikir, GVKT ihlallerinin ve yaptırımlarının hızlı bir şekilde keşfedilmesine olanak tanıyan otomatik araçlar tasarlayarak düzenleyicileri (yalnızca ilgili kişileri veya platformları değil) desteklemesidir[54]. Bu fikir, mevcut rıza yönetim platformlarının çoğuyla ilişkili karanlık kalıplar bağlamında sunulmuştur. Bu tür otomatik araçlar potansiyel olarak nesnelerin interneti ürünleri için de tasarlanabilir.

Yukarıda da sözü edildiği gibi, gizlilik bildirimleri net bir şekilde yazılmış olsa bile, kişilerin nadiren bu bildirimleri okuduğu yaygın olarak bilinmektedir. Bu nedenle rıza verdikten sonra verilerin bir nesnelerin interneti ürünü tarafından nasıl işlendiğini açıklayan ve ilgili kişinin ayarları kolayca değiştirmesine izin veren pop-uplar gibi kullanıcılara ilgili bilgileri (tabii ki açık ve net bir şekilde) sağlayan diğer mekanizmalarla birleştirilmelidir.

Bir Sözleşmeye Dayalı Olarak Dezavantajlı kişilerin Verilerini İşlemeden Önce Ortalama Bir İlgili Kişinin Bakış Açısını Değerlendirmek

İlgili kişinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce ilgili kişinin talebiyle adımlar atılması için, işleme faaliyetinin gerekli olması halinde veri işlemenin hukuka uygunluk dayanağı sağlanmış olacaktır (GVKT madde 6.1 (b)). İlgili kişi bu yasal dayanağın veri sorumlusu tarafından kullanacağını makul bir şekilde beklemelidir. Veri sorumlusu, veri işleme amacının karşılıklı olarak gerçekten anlaşıldığından emin olmak için "ortalama bir ilgili kişinin bakış açısını" dikkatli bir şekilde değerlendirmelidir[55].

TP Vision tarafından Philips akıllı TV'ler aracılığıyla görsel ve işitsel kişisel verilerin işlen-

[48] BRANDİMARTE, Laura/ACQUİSTİ, Alessandro/LOEWENSTEİN, George, "Misplaced Confidences", Social Psychological and Personality Science, 4(3), 2013, s. 340.

[49] MACENAİTE, Milda/KOSTA, Eleni, "Consent for Processing Children's Personal Data in the EU: Following in US footsteps?", Information & Communications Technology Law, Cilt: 26, Sayı: 2, 2017, s. 146.

[50] HİLDEBRANDT, Mireille, "Profiling and the Rule of Law", Identity in the Information Society, Cilt: 1, Sayı: 1, 2008, s. 55; MACENAİTE/KOSTA, s. 48.

[51] MARWICK, Alice/BOYD, Danah, "Networked Privacy: How Teenagers Negotiate Context in Social Media", New Media & Society, Cilt: 16, Sayı: 7, 2014, s. 1051; MACENAİTE/KOSTA, s. 48.

[52] MİCHETİ, Anca/BURKELL, Jacquelyn/STEEVES, Valerie, "Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand", Bulletin of Science, Technology & Society, 30(2), 2010 s. 130.

[53] VEALE, Michael/BINNS, Reuben /AUSLOOS, Jef, "When Data Protection by Design and Data Subject Rights Clash", International Data Privacy Law, Cilt: 8, Sayı: 2, 2018, s. 105.

[54] NOUWENS, s. 40.

[55] NOUWENS, s. 40.

mesine ilişkin bir soruşturmada, Hollanda Veri Koruma Otoritesi, işleme faaliyetine dahil olan belirli gerçek kişi ile ilgili olarak, işleme faaliyeti için meşru bir sebebin var olması gerektiğini beyan etmiştir[56]. Akıllı TV satın almak, esasen işitsel veya görsel verilerle pek ilgisi olmayan bir satış sözleşmesidir. Ancak akıllı TV'ler genellikle bu verileri toplamaktadır. Bu hususta, verilerin işlenmesi için hukuka uygunluk sebebi olarak sözleşme ifası için gerekli olma dayanağının seçilmiş olması, doğru bir seçim olmayacaktır. Birde ilgili kişi dezavantajlı ise, bu hukuka uygunluk sebebine dayanma ihtimalini daha da azaltacaktır. Sıradan bir insandan, hatta bir çocuktan ya da dezavantajlı bir yetişkinden, televizyonu açıp uzun hüküm ve koşulların sonunda "kabul ediyorum"a tıklayarak sesli ve görsel verilerini işleyecek bir sözleşme imzaladığını bilmesini beklemek mümkün değildir. Veri sorumlusunun, veri işlemenin amacını gerçekten anladığından emin olmak için kullanıcının bakış açısını değerlendirmesi gerekir.

Engelli yetişkinler ve çocuklar söz konusu olduğunda, örneğin tıbbi teşhis veya sağlık hizmetlerinin sunulması amacıyla gerekli olabilecek (hassas veri kategorisine giren) sağlık verilerini toplayan ürünler bulunmaktadır. Bu durumda, Madde 9.2 (h) uygulanabilir ve bir sözleşmenin ifasıyla ilgili ve bununla birlikte kullanılabilecek özel bir kategori yasal dayanağı sağlayabilir. Gerçekten de, bir sağlık uzmanıyla yapılan sözleşme, dezavantajlı bir kişinin akıllı ev ürünü aracılığıyla toplanan hassas verilerinin yasal olarak işlenmesine izin verebilir[57].

Veri Sorumlusunun Meşru Menfaatiyle Dezavantajlı Kişinin Meşru Menfaatini Dengelemek

Meşru menfaatler, özellikle ticaret ve yeni teknolojiler alanlarında, kişisel verileri işlemek için hukuka uygunluk sebebi olarak sık sık kullanılmaktadır[58]. Örneğin Google, Nest akıllı ev cihazlarıyla ilgili olarak, "kullanıcılarımızın ihtiyaçlarını karşılamak için hizmetlerimizi sağlamak, sürdürmek ve geliştirmek gibi meşru menfaatleri sürdürmek için bireylerin bilgileri işlenebilmektedir" şeklinde açıklamada bulunmaktadır[59]. GVKT'nin madde 6.1 (f) hükmü uyarınca, başta ilgili kişinin çocuk olduğu durumlar olmak üzere, ilgili kişinin kişisel verilerin korunmasını gerektiren menfaatleri veya temel hak ve özgürlüklerinin bir veri sorumlusu veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır bastığı haller dışında, söz konusu menfaatler doğrultusunda işleme faaliyetinin gerekli olması halinde veri işleme hukuka uygun olacaktır. Hüküm incelendiğinde, çocukların kişisel verilerinin işlenmesine ilişkin dengeleme uygulamasının daha kat olması gerektiğini vurgulamaktadır[60]. Zorlayıcı bir menfaat ortaya çıkarsa, çocuğun haklarına yönelik risklerin mümkün olduğunca azaltılması gerekir[61]. Eğer bir veri sorumlusu tarafından hukuka uygunluk sebebi olarak meşru menfaate dayanılıyorsa, engelli yetişkinler de uygun koruma önlemlerinden yararlanmalıdır. WP29, meşru menfaatlerin dengelenmesi testi sırasında, ilgili kişinin statüsünün önemli olduğunu ve ilgili kişinin, örneğin akıl hastası, öğrenci, hasta gibi özel korumaya ihtiyaç duyan dezavantajlı bir kişi olup olmadığının veya ilişkide güç dengesizliğine

[56] European Audiovisual Observatory, "Smart TV and Data Protection", 60, 2018, https://rm.coe.int/iris-special-2015-smart-tv-and-data-protection/1680945617 (Erişim Tarihi: 06.10.2021).

[57] GVKT madde 9.2 (h).

[58] FERRETTİ, Federico, "Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?", Common Market Law Review, Cilt: 51, Sayı: 3, 2014, s. 843.

[59] Google, "Technologies" 2021, https://policies.google.com/technologies/partner-sites?hl=en-US (Erişim Tarihi: 06.10.2021).

[60] MİLKAİTE, Ingrida and others, "The General Data Protection Regulation and Children's Rights: Questions and Answers for Legislators, DPAs, Industry, Education, Stakeholders and Civil Society. Roundtable Report", 12, 2017, https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf (Erişim Tarihi: 06.10.2021).

[61] Centre for Information Policy Leadership, "GDPR Implementation in Respect of Children's Data and Consent", 6, 2018, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf (Erişim Tarihi: 06.10.2021).

yol açacak bir durumun olup olmadığının değerlendirilmesinin önlemli olduğunu vurgulamaktadır[62]. Meşru menfaatler, ancak bir kuruluş birinin kişisel verilerini bu kişinin makul olarak bekleyeceği ve mahremiyet üzerinde yalnızca minimum bir etkiye sahip olacak şekilde kullanmayı planlıyorsa veya işleme için ikna edici bir neden varsa uygun bir yasal dayanak olabilir.[63]

Akıllı TV satıcısının amaçlarından biri, reklamlar için bir platform ve ilgili izleyici davranışının analizini sağlamaktır.[64] Ancak, bu tür bir veri işleme, ana hizmetin sağlanması için gerekli değildir. ICO, bunu 'çekirdek olmayan' işleme olarak nitelendirmektedir.[65] Bu senaryoda, bir çocuğun verilerinin reklam amaçlı olarak işlenmesini makul bir şekilde beklemesi olası değildir. Ayrıca, burada dezavantajlı kişilerin temel hak ve özgürlüklerini koruma ihtiyacını geçersiz kılacak hiçbir zorlayıcı menfaat görülmemektedir. Bu bağlamda, hizmet sağlayıcı muhtemelen meşru menfaatler yerine rıza alarak ilerlemeli ve ilgili kişilere, teknik olarak mümkün olduğunda (bunları varsayılan olarak açmak yerine) hizmetin farklı ek unsurlarını açma seçeneği sunmalıdır. Bir görüşe göre, bir veri sorumlusu tarafından meşru menfaatin yasal dayanak olarak kullanılması, yalnızca rıza istemekle karşılaştırıldığında genellikle daha derin muhakeme, strateji oluşturma ve hukuka uygun uygulamaya dikkat etmeyi gerektirecektir.[66]

Hukuka uygunluk sebebi olarak meşru menfaatin, menfaatlerin dengelenmesini ve risk değerlendirmesini gerektirdiğini göz önünde bulundurarak, Veri kontrolörlerinden uygun hafifletici önlemler alma ve hesap verme zorunluluğu ile birlikte, Bireysel bazda riski analiz etmek ve belirli durumlarda belirli risklerin ele alınmasına izin vermek için sağlam bir çerçeve olabilir (bu mantığa uygun olarak, tedbirlerin engelli çocukların ve yetişkinlerin çıkarlarına göre uyarlanmasına yardımcı olacaktır).[67] Sonuç olarak, meşru menfaatler olumlu olarak görülmeli ve ilgili durumlarda kişisel verilerin işlenmesi için yasal bir hukuki zemin olarak tavsiye edilmelidir. Ancak, 9. Madde kapsamında buna karşılık gelen bir muafiyet olmadığı ve dolayısıyla hassas veriler söz konusu olduğunda meşru menfaatlerin uygun bir yasal dayanak olmayacağına dikkat edilmelidir.

Yukarıda belirtilen görüş, kuruluşların derinlemesine dengeleme testlerini yapmak için gerçekten zaman ve çaba harcadıklarını varsaymaktadır. Geçmişte, meşru çıkarların uygulamada nadiren gözden geçirildiğine dair raporlar vardır[68]. Diğer yazarlar, dengeleme uygulamasının zor olduğuna ve bunun sadece veri sorumluları tarafından yapılmaması gerektiğine dikkat çekmektedir[69]. Test, önemli düzeyde hukuki uzmanlık gerektirir ve veri sorumlularını "açık bir çıkar çatışması" durumuna sokar[70]. Meşru bir menfaatin var olup olmadığını belirleyen veri sorumlusu ile veri sorumlusunun kararını kabul etmesi gereken ilgili kişi arasında içsel bir güç dengesizliği vardır. Şirketlerin, örneğin genel olarak yasak olan çocukların profillerini oluşturmaları durumunda, dengesiz "meşru menfaatlere" dayalı dezavantajlı kişilerin verilerini işlemesi engellenmelidir.

Akıllı cihazların artan yaygınlığı göz önüne alındığında, çocuklar ve engelli yetişkinler bunları daha sık kullanacaklardır. Küçük kuruluşlar, dengeleme testini uygulamada hukuki bilgi yetersizliği ve avukat tutacak bütçe eksikliği nedeniyle zorluk yaşayacaklardır. Büyük şirketlerin ise dengeleme testi yapmamak için hiçbir mazeretleri yoktur ve özellikle ürünleri ek koruma

[62] Art 29 Working Party, "Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC", (WP 217, 9 April 2014).

[63] Information Commisioner's Office, "Legitimate Interests" https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/ (Erişim Tarihi: 06.10.2021).

[64] European Audiovisual Observatory, "Smart TV and Data Protection", s. 55.

[65] ICO, "Age Appropriate Design", N. 20.

[66] Centre for Information Policy Leadership, s. 60.

[67] Centre for Information Policy Leadership, s. 60.

[68] Bits of Freedom, "A Loophole in Data Processing", 2012, https://www.bitsoffreedom.nl/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf (Erişim Tarihi: 06.10.2021).

[69] FERRETTİ, s. 57.

[70] FERRETTİ, s. 57.

önlemlerine ihtiyaç duyan dezavantajlı kişiler tarafından kullanıldığında, testi yapmazlarsa sorumlu tutulmaları gerekir.

Nadiren Kullanılan Hayati Menfaat Yasal Dayanağı

GVKT'nin 6.1 (d) hükmünde, ilgili kişi veya başka bir gerçek kişinin hayati menfaatlerinin korunması amacı ile işleme faaliyetinin gerekli olması halinde kuruluşların verileri işleyebileceği düzenlenmektedir. Vakaların çoğunda, sağlık verileriyle ilgili olarak hayati çıkarların korunması gereken bir durum büyük olasılıkla ortaya çıkacaktır. Sağlık verileri, özel veri kategorilerinden biridir ve bu nedenle, 6. Maddedeki koşula ek olarak GVKT'nin 9. Maddesi kapsamında bir işleme koşulunu sağlamayı gerektirir[71]. Sağlık verilerinin işlenmesine ilişkin özel koşullardan biri de kişinin hayati menfaatlerinin korunmasıdır[72]. Ancak bu koşulun uygulanabilmesi için ilgili kişinin rıza veremeyecek durumda olması gerekir. Bu nedenle, birçok durumda açık rıza daha uygun yasal dayanak olacaktır[73]. Akıllı cihazların dezavantajlı yetişkinler veya çocuklar tarafından kullanılması bağlamında hayati menfaat yasal dayanağının geçerli olabileceği durumlar var mı? Hollandalı araştırmacılar, gece nöbetlerinin yüzde 85'ini ve en şiddetli nöbetlerin yüzde 96'sını tespit edebilen yüksek teknoloji ürünü bir akıllı bileklik olan "Nightwatch"ı ürettiler.[74] Araştırmacılar, cihazı 28 zihinsel engelli katılımcıyla test etti ve Nightwatch, bakıcıları gece meydana gelen şiddetli nöbetler hakkında bilgilendirmede başarılı olduğu ortaya çıktı. Bu, epilepsiden etkilenenler için hayati bir ürün olabilir, çünkü ani beklenmedik ölüm, bu durumla yaşayanlar için başlıca ölüm nedenidir ve zihinsel engelli yetişkinler için ölme riski daha da yüksektir[75]. Dezavantajlı ilgili kişi rıza gösteremeyecek durumdaysa ancak Nightwatch akıllı bilekliği takıyorsa, kişisel verilerinin onu zamanında bulmak ve ciddi bir epileptik nöbet sırasında ona yardımcı olmak için işlenmesi, hayati menfaatlerin korunması gerekliliğini karşılamalıdır. Bu gibi nadir durumlarda, bu yasal zemin geçerli olacaktır.

Dezavantajlı Kişiler Akıllı Cihazları Kullandığında GVKT İlkelerinin Uygulanması

Hukuka uygunluk ilkesi, işlemenin meşru bir zemine dayalı olarak gerçekleşmesini gerektirir ve çeşitli yasal dayanaklar yukarıda zaten analiz edilmiştir. Bu makale şimdi, bu çalışma bağlamında en alakalı olarak gördüğü diğer ilkeleri kısaca tartışacaktır, yani şeffaflık, adillik, veri minimizasyonu, tasarım ve varsayılan olarak veri koruma ve bütünlük ve gizlilik. Tüm GVKT ilkelerinin uygulanmasına katkıda bulundukları için veri koruma etki değerlendirmeleri de incelenecektir.

Şeffaflık İlkesi ve Bilgi Edinme Hakkı

Verilerimizin cihazlara kaydedildiği ve bu sistemin işleyişinin kullanıcılar için gizemli kaldığı 'kara kutu toplumundan kaçınmak için şeffaf bilgi ve iletişim hakkı gereklidir.[76] Veriler, bu süreç hakkında şeffaf bilgi ve iletişim olmadan toplanıyorsa, dezavantajlı kişiler, veri koruma haklarını etkin bir şekilde kullanamayacaklardır. Şeffaflık ilkesi, kişisel verilerin "ilgili kişi ile ilgili olarak hukuka uygun, adil ve şeffaf bir şekilde işlenmesi" gerektiğini belirten GVKT'nin 5.1 (a) Maddesinde yer almaktadır[77].

---

[71] FERRETTİ, s. 57. Information Commisioner's Office, "Vital Interests", 2019, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/, (Erişim Tarihi: 06.10.2021).

[72] GVKT madde 9 (2) (c).

[73] Information Commisioner's Office, "Vital Interests", s. 70.

[74] ARENDS, Johan and others, "Multimodal Nocturnal Seizure Detection in a Residential Care Setting: A Long-Term Prospective Trial", Neurology e2010, 91, 2018.

[75] Eindhoven University of Technology, "New Epilepsy Warning Device Could Save Thousands of Lives", 2018, https://www.tue.nl/en/news/news-overview/24-10-2018-new-epilepsy-warning-device-could-save-thousands-of-lives/#top (Erişim Tarihi: 06.10.2021).

[76] PASQUALE, Frank, The Black Box Society: The Secret Algorithms that Control Money and Information, Cambridge, 2016.

[77] GVKT madde 12 (1).

GDPR maddeleri ve gerekçeleri, şeffaflık ilkesinin anlamı ve etkisi konusunda bilgilendiricidir. 12. Maddeye göre, bilgilendirme, kısa, şeffaf, kolay erişilebilir ve anlaşılır olmalı ve özellikle çocuklara bilgi verilirken dil açık ve sade olmalıdır[78]. GVKT'nin 58. Gerekçesinde, çocuğa ait verinin işlendiği durumda bilgilendirme, çocuğun kolayca anlayabileceği kadar açık ve sade bir dilde olmalıdır. Anlaşılabilirlik şartı yakın zamanda daha da genişletilerek genel dezavantajlı gruplar da kapsama dahil edilmiştir[79]. Bu makale, her bir şeffaflık koşulunu analiz ederek ayrıntılara girmeyecektir. Bununla birlikte, akıllı ürünler bağlamında dezavantajlı kişiler için özel şeffaflık önlemlerinin varlığına ihtiyaç duyulduğunu (ve gerekli olduğunu) göstermek için şimdi birkaç konu tartışılacaktır.

Kolayca erişme gereksinimi, ilgili kişinin bilgi aramak zorunda kalmaması ve bu bilgiyi nerede bulacağını hızlıca anlayabilmesi anlamına gelmektedir. Akıllı cihazların, yinelenen kullanıcı arayüzü eksikliği gibi üstesinden gelinmesi gereken kendine özgü sorunları vardır.[80] Kullanıcıyı, gizlilik bildiriminin bulunabileceği ve gizlilik ayarlarının değiştirilebileceği bir web sitesine veya uygulamaya bakması için yalnız bırakmak, kişisel verilerinin nasıl işleneceğini seçebilmekten, yaşlılar gibi dezavantajlı kişileri alıkoyabilir[81]. Basılı bir talimat kılavuzu ve gizlilik bildirimi ve ayarlarına başvurulabilecek bir web sayfası adresinin URL'sini paylaşmak bir çözüm örneği olabilir. Özellikle görme engelli kişilere veya yazılı bilgileri anlamada veya bunlara erişimde sorun yaşayabilecek dezavantajlı kişilere ekransız akıllı cihazların ses özellikleri aracılığıyla sözlü olarak bilgi vermeleri de bu tür özelliklere sahip olmaları durumunda önemli bir yöntem olabilir[82].

Avrupa Birliği Adalet Divanı, Avrupa Veri Koruma Kurulu (EDPB) ve çeşitli yazarlar, ilgili kişinin haklarının kullanımını zorlaştırdığı için açık ve sade dil kullanılmamasının önemli bir sorun olduğunu savunuyorlar[83]. Bu Kullanıcıların profil oluşturmasının yaygın olduğu günümüzün veriye dayalı nesnelerin interneti dünyasında özellikle önem arz etmektedir[84]. Öte yandan, bazı yazarlar ise, veri işleme faaliyetlerini açık ve sade bir dille açıklamanın karmaşıklığının altını çizer ve bunun çoğu zaman kişisel verilere ilişkin durumu yeterince yansıtmayan basit açıklamalarla sonuçlanabileceğini belirtir[85]. Bazı araştırmacılar, iletişimin basitleştirilmesinin bilginin kalitesini sınırlayabileceğini düşünmektedir[86]. Ancak diğer görüşteki yazarlar için, bilginin bir çocuğa yönelik olması, bu bildirimin kapsamının daraltıldığı anlamına gelmez[87]. Bu makalenin yazarları, kullanıcılar verilere odaklanırken okumak isterse, şirketlerin daha karmaşık gizlilik politikasına bir bağlantı sağlayabileceğini düşünmektedir. 'Yetişkinler için' karmaşık gizlilik politikaları yerine anlaşılması kolay bildirimler herkes için çok daha faydalı olacaktır. Dezavantajlı birçok

[78] Art 29 Working Party, "Guidelines on Transparency under Regulation 2016/679", (WP 260, 11 April 2018).

[79] EDPB, "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default" (13 November 2019), 14, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf (Erişim Tarihi: 06.10.2021).

[80] InfoWorld, "IoT Silliness: 'Headless' Devices without a UI", 2015, https://www.infoworld.com/article/2867356/beware-this-iot-fallacy-the-headless-device.html (Erişim Tarihi: 06.10.2021).

[81] InfoWorld, "IoT Silliness: 'Headless' Devices without a UI", 2015, https://www.infoworld.com/article/2867356/beware-this-iot-fallacy-the-headless-device.html (Erişim Tarihi: 06.10.2021).

[82] Art 29 Working Party, "Guidelines on Transparency under Regulation 2016/679", s. 77.

[83] SMARANDA Bara and Others v Casa Națională de Asigurări de Sănătate and Others, Case C-201/14, [2015] (ECLI:EU:C:2015:638); EDPB, 'Guidelines 05/2020 on Consent under Regulation 2016/679' s. 45; Art 29 Working Party, "Guidelines on Transparency under Regulation 2016/679", s. 77.

[84] LOİDEAİN, Nóra, "A Port in the Data-Sharing Storm: The GDPR and the Internet of Things", Journal of Cyber Policy, 4(2), 2019, s. 178.

[85] CUSTERS, Bart/others, "A Comparison of Data Protection Legislation and Policies Across the EU", Computer Law & Security Review, Cilt: 34, Sayı: 2, 2018, s. 234.

[86] WACHTER, Sandra "The GDPR and the Internet of Things: A Three-Step Transparency Model" Innovation and Technology, Cilt: 10, Sayı: 2, 2018, Law, s. 266.

[87] VOLOSEVİCİ, Dana, "Child Protection under GDPR", A Journal of Social and Legal Studies, Cilt: 6, Sayı: 2, 2019, s. 17.

yetişkin, gizlilik politikalarının karmaşık ve anlaşılmaz olduğundan şikayet eder. Sade ve açık bir dil kendileri için daha anlaşılır olacaktır.

Her durumda, şeffaflık tek başına dezavantajlı kullanıcıların verilerini korumak için yeterli değildir. Kullanıcıları eğitmek ve bilinçli seçimler yapmalarını desteklemek için önemli bir unsur olsa da, bir ilgili kişi bilgilendirildiği için bu kişinin rasyonel seçimler yapacağını ve haklarını kullanabileceğini beklemek mümkün değildir[88]. Şeffaflık, adalet ve veri minimizasyonu gibi diğer veri koruma ilkeleriyle birlikte çalışmalıdır.

Dezavantajlı Kişilerin Verilerinin Akıllı Cihazlar Tarafından Adil Bir Şekilde İşlenmesi

Adillik ilkesi, dezavantajlı kişilerin GVKT sağladığı korumadan ve haklardan diğer vatandaşlarla aynı şekilde yararlanmasını sağlaması gerektiği için mantıksal olarak çok önemlidir. Tıpkı şeffaflık gibi, bu ilke de GVKT'nin 5.1 (a) Maddesinde yer almaktadır. Bazı yazarlara göre 'adillik, öznel, bağlama bağlı ve oldukça politize bir kavramdır' ve 'algoritmik karar verme bağlamında veya başka bir bağlamda neyin adil olduğuna dair küresel bir fikir birliğinin ortaya çıkması olası değildir'[89]. Diğerlerine göre, 'adalet, kapsamlı bir şekilde açıklanması zor olan geniş bir kriterdir; aynı zamanda bağlama da bağlıdır[90]. Bütün bunlar doğru olsa da, bu çalışma bağlamında veri sorumluları tarafından adilliğin nasıl uygulanması gerektiği üzerinde düşünmek önemlidir. Sübjektif yorumlar ne GVKT uyumluluğuna ne de dezavantajlı kişilerin haklarını korumaya yardımcı olmayacağı için kuruluşların yönlendirilmesi gerekir. GVKT'de adillik ilkesinin önemi, veri sorumlusu ile ilgili kişi arasındaki artan güç dengesizliğinin kanıtıdır[91]. Bu güç dengesizliği, çocuklar veya dezavantajlı yetişkinler teknoloji kullandığında daha da artar.

İlk olarak, adillik ve şeffaflık arasında açık bir bağlantı vardır. GVKT'de adillik tanımlanmamasına rağmen, akademisyenler, Çalışma Grubu ve Avrupa Veri Koruma Kurumu tarafından adillik ilkesi tanımlanmıştır. Onlar bu ilkenin farkındalıkla ilgili olduğunu düşünmektedirler[92]. Adil olma ilkesi uyarınca, kişisel verilerin yalnızca ilgili kişi bu işleme faaliyetinden haberdar edildiğinde toplanması gerekmektedir[93]. ICO, Yaşına Uygun Tasarım Raporu'nda, bir kuruluşun sunduğu hizmet ve nasıl işlediği konusunda 'net, açık ve dürüst' değilse, 'çocuğun kişisel verilerinin toplanması ve sürekli kullanımının adil olması muhtemel değildir'[94]. Örneğin, bir sağlıkla ilgili akıllı ürün, kalp atışı verilerini izler ancak aynı zamanda cihazın arayüzü veya başka yollarla ilgili kişiyi bu konuda uygun şekilde bilgilendirmeden kandaki oksijen seviyelerini de toplar[95]. Bunlar birbirine bağlıyken adalet ve şeffaflık aynı anlama gelmez. Adillik, şeffaflığın yorumlanmasında bir araçtır. Akıllı bir cihaz, genel nüfusa şeffaf bir şekilde bilgi sağlıyorsa, ancak bu ürünü kullanan zihinsel engelli azınlığa bilgilendirmede bulunmuyorsa, bu, 'adil şeffaflık' olarak kabul edilemez. Daha da derinlemesine belirtmek gerekirse, bu makale, adil şeffaflığın, kuruluşların herhangi bir akıllı üründe varsayılan olarak dezavantajlı kişiler için özel veri koruma önlemleri benimsemesini gerektirmesi olarak görülmesi gerektiğini savunuyor (örneğin, yüksek gizlilik ayarları, kabul mekanizmaları veya çocuk dostu dil gibi).

Dezavantajlı kişiler için varsayılan olarak özel veri koruma önlemlerinin benimsenmesi lehindeki argüman bağlamında, belirtilmesi gereken

[88] MOEREL, Lokke/PRİNS, Corien, "Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things", 2016, ssrn: 2784123 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123 (Erişim Tarihi: 08.10.2021).

[89] ABİTEBOUL, Serge/Stoyanovich, Julia, "Transparency, Fairness, Data Protection, Neutrality", Journal of Data and Information Quality, Cilt: 11, Sayı: 3, 2019 s. 1.

[90] BUİTELAAR, s. 2.

[91] BUTTERWORTH, Michael, "The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework", Computer Law & Security Review, Cilt: 34, Sayı: 2, 2018 s. 257.

[92] WACHTER, s. 85.

[93] WACHTER, s. 85.

[94] ICO, "Age Appropriate Design", N. 20.

[95] Art 29 Working Party, "Opinion 8/2014 on the Recent Developments on the Internet of Things", s. 31.

bir başka önemli konu daha vardır. Aniden bozulan sağlık veya diğer koşullar nedeniyle herkes herhangi bir noktada dezavantajlı hale gelebilir. Akıllı bir cihazın dezavantajlı müşterileri hedef almaması, bu kişilerin zaman içinde dezavantajlı hale gelmeyecekleri anlamına gelmez. Bu nedenle, her zaman akıllı bir cihazın dezavantajlı kişiler tarafından kullanılabileceğini varsaymak, yalnızca şu anda dezavantajlı olan akıllı ürün tüketicilerini değil, gelecekte dezavantajlı hale gelecek olanları da koruyacaktır. Bu aynı zamanda adillik ilkesine daha etkin bir şekilde uyulmasını da sağlayacaktır.

İkinci olarak, adillik, ilgili kişilerin verilerinin dengeleme çalışmaları yoluyla veri sorumluları tarafından yanlış kullanılmasını önlemek için çok önemli bir kapalı amacı vardır (bu, GVKT'nin pratikte nasıl çalıştığının önemli bir unsurudur). Bir dengeleme uygulamasının genellikle veri sorumluları tarafından gerçekleştirilmesi için GVKT tarafından zımnen gereklilik vardır[96]. Adil dengeleme, vaka bazında yapılmalı ve değerlendirilmelidir. Bu makalenin konusuna ilişkin rehberler çok azdır. Bazı öneriler, ICO'nun Yaşa Uygun Tasarım Raporu'nda bulunabilir[97]. Dezavantajlı kişilerin verileri akıllı bir ürün tarafından işleniyorsa, veri sorumlularının, veri işlemenin adil olmasını sağlamak için kendileri ve ilgili kişi arasındaki artan güç dengesizliğini dikkate almaları gerekecektir. Örneğin, çocukların kişisel verilerini üçüncü bir tarafla paylaşan bir akıllı cihazın, veri işlemenin adil olması için 'çocuğun yüksek yararını göz önünde bulundurarak bunu yapmak için zorlayıcı bir nedenle' gerekçelendirilmesi gerekir[98]. Adil işleme bağlama bağlıdır ve nesnelerin interneti sektöründe daha fazla adil dengeleme örneği veri sorumluları için kesinlikle yararlı olacaktır.

Adillik ilkesinin anlamı ile ilgili açıklamalara hala ihtiyaç duyulduğu için, veri etiği girişimlerini ifade etmek için onu daha bütünsel olarak tanımlama ve onu katı yasal sınırlamaların ötesine geçirme fırsatı vardır[99]. AB Temel Haklar Ajansı'na göre, GVKT kapsamında adillik, verilerin etik bir şekilde işlenmesini gerektiren ve ilgili kişiye şeffaf bir şekilde bilgi sağlama gerekliliğini getiren bir kavramdır[100]. Avrupa Veri Koruma Denetçisi, adillik ilkesinin bu bağlamda nasıl algılanması gerektiğinin tartışılmasının öneminin altını çizerek, etik ve veri koruma konusunda acil bir düşünme çağrısında bulunmuştur[101].

Dezavantajlı Kişilerin Veri İhlal tehditlerine Maruziyetini En Aza İndirme

Genel savunmasızlıklarının bir sonucu olarak ve hukuka uygunluk ve adillik ilkelerine uygun olarak, akıllı ürünleriyle çocukları hedefleyen kuruluşlar, 'veri minimizasyonu ve amaç sınırlaması ilkelerine daha da sıkı uymalıdır'[102]. GVKT Madde 5.1 (c) kişisel verilerin işlenmesinin 'yeterli, ilgili ve işlendikleri amaçlarla bağlı olarak gerekli olanlarla sınırlı' olması gerektiğini belirtir. Kişisel veriler, yalnızca işleme amacının başka yollarla makul şekilde yerine getirilememesi durumunda işlenmelidir[103]. ENISA, veri minimizasyonunun yalnızca bir formdaki veri alanlarını azaltmak anlamına gelmediğini, aynı zamanda 'yalnızca nicel değil, nitel bir yaklaşımı izleyerek' veri toplama ve veri işleme faaliyetlerini en aza indirmenin diğer herhangi bir yolunu ifade ettiğini gözlemlemiştir[104]. Bu ilke, nesnelerin interneti ürünleri tarafından toplanan, de-

[96] CLIFFORD, Damian /AUSLOOS, Jef, "Data Protection and the Role of Fairness", Yearbook of European Law, 37, 2018, s. 130.

[97] ICO, "Age Appropriate Design", s. 20.

[98] ICO, "Age Appropriate Design", s. 20.

[99] CLIFFORD/AUSLOOS, s. 95.

[100] FRA, "Handbook on European Data Protection Law", 2018, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf> (Erişim Tarihi: 6.10.2021).

[101] EDPS, "Opinion 4/2015 Towards a New Digital Ethics", 2015, https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf, (Erişim Tarihi, 6.10.2021).

[102] Art 29 Working Party, "Opinion 02/2013 on Apps on Smart Devices", (WP 202, 2013).

[103] Art 29 Working Party, "Opinion 02/2013 on Apps on Smart Devices", (WP 202, 2013).

[104] ENISA, "Recommendations on Shaping Technology According to GDPR Provisions - Exploring the Notion of Data Protection by Default", 2018, https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2, (Erişim Tarihi: 6.10.2021).

polanan ve genellikle bulutta analiz edilen büyük miktarda bilgiyle ilişkili "veri maksimalizmi" ile taban tabana zıttır[105]. 2013 yılında, Çalışma Grubu, bu uygulamaların işlevselliği ile gerçek bir ilişki olmaksızın, akıllı telefonlardaki birçok uygulama tarafından aşırı veri toplamanın, veri minimizasyonu ilkesinin endişe verici şekilde göz ardı edildiğinin göstergesi olduğuna dikkat çekti[106]. GVKT'nin sonucu olarak, veri sorumlularının, kapsayıcı hesap verebilirlik ilkesi doğrultusunda ilgili veri minimizasyonuna yönelik en iyi uygulamalara ve gereksinimlere uyduklarını kanıtlamaya artık hazır olmaları gerekmektedir[107].

Dezavantajlı kişiler tarafından kullanılan akıllı cihazlar özelinde akla gelen bir sorun, bilgi toplumu hizmetleri (ISS) sağlayan kuruluşların, kişisel verilerini işlemeden önce yasal olarak yetkili bir temsilciden onay almaları gerekip gerekmediğini öğrenmek için ilgili kişinin yaşını belirlemek için kişisel verileri kaydetmesi ve toplamasıdır. Veri sorumlularının bu bağlamda da veri minimizasyonu ilkesine uymaları gerektiğini unutmamaları gerekmektedir[108]. Bunu yapmak için, yalnızca belirli kullanıcıların yaşı hakkında onları bilgilendirmek için kesinlikle gerekli olan kişisel veri miktarını toplamaları gerekecektir. Bu veriler yalnızca yaşa uygun ayarlar ve önlemler sağlamak amacıyla kullanılmalıdır ve reklamcılık gibi başka bir amaç için kullanılmamalıdır (meğerki bunun için izin alınmış olsun veya başka bir yasal dayanak buna izin vermiş olsun). The Center for Information Policy Leadership, bir veri sorumlusunun müşterinin yaşını doğrulayabileceği üç yolu ortaya koymuştur. Evrensel yaş değerlendirmesinin, ilgili kişilerin yaşını doğrularken çok müdahaleci olacağını, hizmetler çocukları hedeflediklerini açıkça belirttiğinde kapsayıcı olmayacağını belirtmiştir. Sonuç olarak, the Center for Information Policy Leadership, teklifin kasıtlı olarak çocuklara çekici gelip gelmediğini; çocukların geçmişte bilgi toplumu hizmetlerine veya benzer hizmetlere ilgi gösterip göstermediğini; ve ISS'ye kayıt işleminin, kullanıcıların dijital rıza yaşının üzerinde olduğu varsayımını yansıtıp yansıtmadığını değerlendirerek bir risk analizi gerçekleştirmeyi ileri sürmüştür[109]. Veri koruma açısından bakıldığında, bu makale bu yaklaşımı iki nedenden dolayı uygun görmemektedir. İlk olarak, çocuklar kendileri tarafından kullanılmak üzere tasarlanmayan hizmetlere ilgi duyabilir ve bunun doğrulanması zor olabilir. İkincisi, kuruluşların, özellikle halihazırda GVKT'ye uyması beklenen küçük kuruluşların başka bir risk analizi yapmasını beklemek gerçekçi görünmemektedir. Sonuç olarak, bu çalışma, bu tür teknolojilerin kullanımını teşvik etmek ve bunların nasıl uygulanacağına dair kılavuzlar geliştirmek için mevcut en iyi mahremiyeti koruyan teknolojileri kullanan yaş doğrulama mekanizmaları aracılığıyla veri toplamanın en aza indirilmesinden yanadır.

Elbette yaş doğrulama, dezavantajlı kişiler akıllı ürünler kullandığında veri minimizasyonu bağlamında düşünülmesi gereken tek konu değildir. Bir başka örnek, bir çocuk veya dezavantajlı bir yetişkin adına rıza vermek için yasal olarak yetkili temsilciyi belirleme ihtiyacı olabilir. En son teknolojiler bu konuda da yardımcı olabilir. Veri koruma uyumluluğunu kolaylaştırmak için yasal kurallarla nasıl etkileşime girebilecekleri bu makalenin kapsamında değildir ancak bu, gelecekteki disiplinler arası çalışmaların konusu olabilir.

Akıllı Ürünlerin Geliştirilmesi ve Devreye Alınması Süreçlerinde Dezavantajlı Kişilerin Verilerinin Korunmasını Düşünmek

GVKT'nin 25. Maddesi, kişisel veri işlemenin GVKT hükümleriyle uyumlu olduğundan emin olmak ve tüketicilerin veri koruma haklarının korunmasını sağlamak için tasarlanmış teknik ve organizasyonel önlemleri kullanma konusunda veri sorumlularına nitelikli bir sorumluluk getirir. Bu görev aynı zamanda veri koruma ilkelerinin

[105] Wachter, s. 85.

[106] Art 29 Working Party, "Opinion 02/2013 on Apps on Smart Devices", s. 101.

[107] Information Commissioner's Office, "Principle (c): Data Minimisation", https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/, (Erişim Tarihi: 6.10.2021).

[108] ICO, "Age Appropriate Design", N. 20.

[109] Centre for Information Policy Leadership, N. 60.

varsayılan olarak uygulanması ve kişisel verilere kimlerin erişebileceğine ilişkin varsayılan sınırlamalarla da ilgilidir[110]. Tasarım ve varsayılan olarak veri koruma yaklaşımı, akıllı cihazları kullanan dezavantajlı kişiler açısından nasıl uygulanır?

Nesnelerin İnterneti Ürünlerini Tasarlarken Mevcut PET Gizlilik Paradigmasına Odaklanma

Yetersiz bütçeye sahip veri koruma otoriteleri tarafından mevzuatın uygulanmasındaki zorluklara yanıt olarak, genellikle tasarım yoluyla gizliliğin uygulanması bağlamında, kişisel verilerin daha sorumlu ve etkili bir şekilde işlenmesine izin vermek için mahremiyet arttırıcı teknolojiler ("privacy enhancing technologies", bundan sonra "PET" olarak anılacaktır) adı altında bir dizi teknik yaklaşım ortaya çıkmıştır[111]. Bazı yazarlar, PET'lerin, tasarım yoluyla veri korumanın sağlaması gereken tüm GVKT ilkelerinin ve haklarının korunmasını sağlamak yerine, bilgi ifşasının önlenmesine odaklanmasını eleştirmektedir[112]. PET'lerin odağının, kontrol olarak mahremiyet (GVKT'nün yaklaşımı) yerine gizlilik olarak mahremiyet olduğunu belirtmektedirler. Bu kapsamda, Siri sesli asistanı hakkında yakın zamanda yapılan bir araştırma, Apple'ın yaklaşımını eleştirmektedir. Apple'ın kararları, bazılarının "gizlilik ve veri güvenliğini büyük ölçüde ele alan oldukça dar bir mahremiyet tanımı" olarak tanımladığı şeye odaklanan veri yönetimine ve yazılıma gizliliğin dahil edilmesine bir örnektir[113]. Bir şirketin, ilgili kişilerin normalde kullanabilmesi gereken diğer GVKT haklarına kıyasla veri gizliliğine neden öncelik verdiğini açıkça belirtmesi kesinlikle önemlidir. İlgili kişinin hak ve özgürlüklerinin korunması gerekir[114]. Ancak bunu vurguladıktan sonra söyleyebiliriz ki, bazı durumlarda, örneğin veri koruma etki değerlendirmesi yoluyla şeffaf bir şekilde açıklandığı takdirde ilgili kişinin hakların sınırlandırılması yeterli bir çözüm olabilir. Dezavantajlı bir kişinin ihtiyaçları perspektifinden ve GVKT'nin çocuklarla ilgili özel koruma önlemlerinin alınmasının gerekliliğine[115] ve dezavantajlı kişilerin verileri işlenirken artan risklerin üstesinden gelinmesine ilişkin hükümleri dikkate alındığında[116] Apple'ın diğer ilgili kişilerin haklarını kullanma olasılığı üzerinde gizlilikte ısrar etme yaklaşımı doğru olabilir. Tabii ki hem gizlilik hem de diğer hakların kullanımı tatmin edici düzeyde sağlanabiliyorsa, bu yapılmalıdır. Her durumda, bu yönde çaba gösterilmelidir. Kişisel verilerini etkili bir şekilde yönetebilen ve koruyabilen kişiler varsa, çocuklar veya bazı engelli yetişkinler için erişim haklarını kullanabilmenin faydaları, (bu hakkın kullanılması daha yüksek veri ihlali risklerinin oluşmasına neden olacaksa) muhtemelen daha yüksek veri gizliliğinin faydalarından daha fazla olmayacaktır.

Dezavantajlı Kişilerin Verilerini Varsayılan Olarak Koruma

Belirli nesnelerin interneti cihazlarının sunduğu gizlilik düzeyini değerlendirirken, standart ayarlar, kullanıcıların, ürünün veri koruma uyumlu kullanımı için ilgili yapılandırmayı uygulamalarının ne kadar kolay olduğunu belirledikleri için önemlidir[117]. Kişisel verilerinin daha geniş bir şekilde kullanılmasına izin vermek isteyip istemediğine karar vermek ilgili kişiye bırakılmalıdır[118]. Dezavantajlı kişiler, kişisel verileriyle

[110] EDPB, "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default", s. 78; BYGRAVE, "Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements", Oslo Law Review, Cilt: 4, Sayı: 2, 2017, s. 105.

[111] DIAZ, Claudia/TENE, Omer/GUERSES, Seda "Hero or Villain, "The Data Controller in Privacy Law and Technologie", Ohio State Law Journal, 74, 2013, s. 923.

[112] VEALE/BINNS/AUSLOOS, s. 52.

[113] SCHARTUM, "Dag Wiese, "Making Privacy by Design Operative", International Journal of Law and Information Technology, Cilt: 24, Sayı: 2, 2016, s. 151.

[114] GVKT madde 35.

[115] GVKT Madde 35; gerekçe 38.

[116] Gerekçe 38; gerekçe 75.

[117] HANSEN, Marit, "Data Protection by Default in Identity-Related Applications", (IDMAN 2013: Policies and Research in Identity Management, London, April 2013) <https://link.springer.com/chapter/10.1007%2F978-3-642-37282-7_2> (Erişim Tarihi: 6.10.2021).

[118] EDPS, "European Data Protection Supervisor: Opinion of the European Data Protection Supervisor on the Data Protection Reform Package", 2012, https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf (Erişim Tarihi: 6.10.2021).

ilişkili haklarını kullanamayabilir veya kişisel verileri üzerinde kontrollerini sağlayamayabilir. Bu, GVKT'nin 58. Gerekçesinde de vurgulanmıştır. Buna göre, çocukların korunmasının gerekçesi, çocukların anlama kapasitelerinin azlığına dayanır (Belirtilmelidir ki, açıklamalar belirsiz AB hukuku hükümlerinin yorumlanmasına yardımcı olabilir, ancak yasal olarak bağlayıcı değildir).[119] Çocukların kişisel verilerinin işlendiği dijital ortamı anlamaları açısından gelişimlerinde önemli boşluklar bulunmaktadır[120]. Örneğin, 16-17 yaşar arasındaki kişiler söz konusu olduğunda, ICO, varsayılan yüksek gizlilik ayarını değiştirmeye çalışırlarsa bilgilerine ne olacağını ve ilgili risklerini açıklayan yazılı, video veya sesli materyallerin sağlanmasını ve herhangi bir endişeleri olup olmadığını veya kendilerine iletilen şeyi anlamadıklarını bir yetişkinle kontrol edilmesini önermektedir[121]. ICO'nun raporu, bu varsayılan ayarların ne kadar önemli olduğunu gösterir. Veri işlemenin mümkün olduğunca her bireyin seçimine bırakılması çok önemlidir. Ne yazık ki, şu anda gerçek bu değil ve birçok nesnelerin interneti cihazı, ilgili kişiye bu faaliyetler hakkında bilgilendirmeden bile kişisel verileri üçüncü taraflara aktarmaya devam etmektedir.[122]

Bu makale, sıradan vatandaşlar ve çocuklar veya dezavantajlı yetişkinler arasında ayrım yapmak yerine, her zaman ve herkes için açık tercih mekanizmalarının benimsenmesi lehinde görüş ileri sürmektedir. Yaşına Uygun Tasarım raporunda, ICO, kuruluşların varsayılan olarak "yüksek gizliliği" benimsemelerini, "çocuğun yüksek çıkarlarını göz önünde bulundurarak farklı bir varsayılan ayar için zorlayıcı bir neden gösteremezseniz" varsayılan olarak konum belirleme ve profil oluşturmayı kapatmalarını ifade etmektedir[123]. Bazı yazarlar ayrıca, bir hizmeti kullanan reşit olmayanlar söz konusu olduğunda, 'varsayılan ayarların özellikle katı olması gerektiğini' belirtmişlerdir[124]. Bu, birkaç nedenden dolayı sorunludur. Birincisi, kuruluşlar akıllı ürünlerinin genel nüfusa yönelik olması nedeniyle, varsayılan ayarlarının yalnızca çocukların kullandığı ürünler kadar koruyucu olması gerekmediğini iddia edebilir. Herkes için varsayılan olarak 'yüksek gizlilik' varsayılan ayarlarının benimsenmesi, yalnızca tüm vatandaşların verilerini daha güvenli hale getirmekle kalmaz, aynı zamanda bir ürünün çocuklar (veya dezavantajlı yetişkinler) tarafından kullanılıp kullanılmadığı belirsiz olduğunda, varsayılan gizlilik ayarlarının kullandıklarında veya daha sonra kullanmaya karar verdiklerinde onları yine de koruyacağından emin olur. İkinci olarak, ICO, GVKT hükümlerinden ve ruhundan sapmayı neyin haklı çıkarabileceğine dair örnekler vermeden, yüksek gizlilik ayarından farklı bir varsayılan ayarın zorlayıcı nedenlerinden bahseder. Bu makale, böyle bir istisna yapılmamasını savunmaktadır. Aksi kanıtlanana kadar, yüksek bir gizlilik varsayılan ayarının uygulanmaması gereken bir durumu öngörmek zordur. Üçüncüsü ve ilk iki hususla ilgili olarak, ICO, birçok çocuğun 'sunulan varsayılan ayarları kabul edeceğini ve gizlilik ayarlarını asla değiştirmeyeceğini'[125] ifade eder. Bizce bu, çoğu durumda dezavantajlı yetişkin için de söz konusudur. Bu nedenle, tüm dezavantajlı bireylerin korunmasını sağlamak için her ilgili kişi için varsayılan olarak yüksek gizlilik ayarlarının uygulanması son derece önemlidir. Ayrıca, bireylerin, verilerinin belirli bir amaç için işlenmesini istemeleri durumunda gizlilik ayarlarını değiştirmelerini sağlamak, onları nesnelerin interneti dünyasında kişisel veri işleme konusunda da eğitecektir (çünkü aktif adımlar atmaları ve seçimlerini düşünmeleri gerekecek), böylece şeffaflık ilkesi gibi diğer GVKT hükümlerine uyumluluğa katkıda bulunur.

[119] MALGİERİ/NİKLAS, N. 13.

[120] LİEVENS, Eva/ HOF, Simone van der: "The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data under the GDPR", Communications Law, Cilt: 23, Sayı: 1, 2018, s. 33.

[121] ICO, "Age Appropriate Design", N. 20.

[122] JİNGJİNG, Ren and others, "Information Exposure from Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach" (IMC '19: Proceedings of the Internet Measurement Conference, Amsterdam, Ekim 2019) https://dl.acm.org/doi/10.1145/3355369.3355577, (Erişim Tarihi: 6.10.2021).

[123] ICO, "Age Appropriate Design", N. 20.

[124] HANSE, s. 117.

[125] ICO, "Age Appropriate Design", N. 20.

Dezavantajlı Kişilerin Verilerinin İşlenmesinde Yüksek Risk ve VKED

VKED'nin amacı, bir veri işleme faaliyeti gerçekleşmeden önce, veri işleme faaliyetiyle ilgili riskleri değerlendirmek, belirlemek ve en aza indirmektir. GVKT madde 35.1 uyarınca, VKED, belirli bir işleme planı veya projesinin bireylerin hak ve özgürlükleri için yüksek bir risk barındırması muhtemel olduğunda gereklidir. GVKT madde 35.3, VKED'nin gerekli olduğu 3 durum belirtmektedir: ("önemli etkileri olan sistematik ve kapsamlı profil oluşturma", "hassas verilerin büyük ölçekli kullanımı", "kamu izleme") ve ICO, 10 örnek daha listeleyen Madde 35.4'e uygun bir belge yayınlamıştır[126]. İkincisi arasındaki bazı faaliyetler otomatik olarak bir VKED gerektirirken, diğerlerinin Avrupa kılavuzlarındaki kriterlerden biri ile birlikte gerçekleşmesi gerekir (Çalışma Grubu 9 kriter daha listelemiştir). Yenilikçi teknolojiler tarafından toplanan veriler temelinde işleme faaliyetleri, Çalışma Grubu tarafından listelenenlerden biriyle birleştirilmesi gereken ICO'nun kriterlerinden biridir. Bu nedenle, bu makale bağlamında ilk soru, akıllı cihazların yenilikçi teknolojiler olarak kabul edilip edilemeyeceğidir. Gerekçe 91'de, yenilikçi teknolojilerden küresel olarak teknolojik alandaki gelişmeler olarak bahsedilmektedir. ICO, akıllı teknolojiler (giyilebilir cihazlar dahil) bu tanıma gireceğini belirtmektedir[127]. Sonuç olarak, ICO'nun kriterleri kapsamında nesnelerin interneti cihazları yenilikçi teknoloji ürünleridir. İkinci soru, bunun Çalışma Grubu'nun yüksek riskle sonuçlanması muhtemel durum örneklerinden biriyle birleştirilip birleştirilemeyeceğidir. Çalışma Grubu için, dezavantajlı kişilerin verilerinin işlenmesi, onlarla ilgili yüksek bir risk olabileceğinin bir göstergesidir. Dezavantajlı kişilerin (çocuklar veya dezavantajlı yetişkinler gibi) verilerinin işlenmesine kolayca rıza gösteremeyecekleri veya itiraz edemeyebilecekleri anlamında, ilgili kişiler ile veri sorumluları arasında bir güç dengesizliği bulunduğundan, dezavantajlı kişilerin verileri işlendiğinde doğal olarak yüksek bir risk vardır[128]. Sonuç olarak, dezavantajlı kişiler tarafından kullanılan akıllı cihazlar (ICO'nun yenilikçi teknoloji kriterleri) (Çalışma Grubu'nun dezavantajlı kişilerin verilerinin işlenmesi kriterleri uyarınca) yüksek risklerle sonuçlanabilecek bir durumu temsil eder ve bu nedenle her zaman bir VKED yapılması gerekecektir.

Veri Koruma Direktifi zamanında VKED zorunlu değildi. VKED'leri belirli durumlarda gerçekleştirme yükümlülüğü GVKT tarafından getirilmiştir. Zorunlu etki değerlendirmeleri, salt kural koyucu yasal düzenlemeler değil, daha çok yasal gerekliliklerin yanı sıra kuruluşların (ilgili paydaşların katılımıyla) kendilerinin geliştirmesi ve uygulaması gereken politikaların bir karışımıdır[129]. Bir yazar, 'ortak düzenleyici' terimini şu şekilde tanımlamıştır: VKED'lerin ne olduğunu tanımlamada yetersiz ve kesinlikten yoksundur[130]. Bunun yerine, Christine Parker tarafından geliştirilen 'meta-düzenleme' kavramını kullanmayı önerir[131]. Bu kavram, hükümetlerin şirketleri kendi öz-düzenleme girişimlerinden sorumlu kılma çabalarını tanımlar. Diğer düzenleme türlerine kıyasla meta-düzenlemenin yararı, kuruluşların kendi kendini yönetme kapasitesinden faydalanması, ancak düzenleyicinin beklentilerini karşılayıp karşılamadıklarını doğrulamak için mekanizmalar içermesidir. Bununla birlikte, VKED'lerin meta-düzenleme yaklaşımının etkinliği, veri koruma yetkililerinin kuruluşların risk azaltma planlarını inceleme yeteneğine de bağlı olacaktır. GVKT, onlara bunu yapma yetkisi verir. Madde 36.1 uyarınca '35. Madde kapsamında bir VKED'nin işlemenin yüksek bir riskle sonuçlanacağını belirt-

[126] ICO, "When Do We Need to Do a DPIA?", N. 8.

[127] ICO, "When Do We Need to Do a DPIA?", N. 8.

[128] Art 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA), s. 9.

[129] BINNS, Reuben, "Data Protection Impact Assessments: a Meta-Regulatory Approach", International Data Privacy Law, Cilt: 7, Sayı: 1, 2017, s. 22.

[130] BINNS, s. 22.

[131] PARKER, Christine, "Meta-regulation: Legal Accountability for Corporate Social Responsibility", The New Corporate Accountability: Corporate Social Responsibility and the Law, Cilt: 29, Doreen McBarnet, Ed.: Aurora Voiculescu and Tom Campbell CUP, Cambridge, 2007.

tiği durumlarda, veri sorumlusu işlemeden önce denetim makamına danışacaktır'.' Çocukların veya savunmasız yetişkinlerin verileri işlenirken VKED'lerin nasıl değerlendirileceği gibi konularda düzenleyici kurumların ve veri koruma yetkililerinin uzmanlığının oluşturulması, uyumluluğun ve veri korumanın artırılmasına yönelik önemli bir adım olabilir. Son olarak, paydaş katılımı başarılı meta-düzenlemenin önemli bir parçasıdır. GVKT bunu yansıtmaktadır. Madde 35.9'a göre, 'uygun hallerde, veri sorumlusu, ticari veya kamu menfaatlerinin korunmasına veya işleme faaliyetlerinin güvenliğine halel getirmeksizin, amaçlanan işleme hakkında ilgili kişilerin veya temsilcilerinin görüşlerini alacaktır[132]. Özellikle 'uygun olduğunda' ifadesi nedeniyle bunun ne kadar etkili olduğunu zaman gösterecektir[133]. Bu temel GVKT hükmünün zayıflığı hukuk literatüründe eleştirilmiştir[134]. Sonuç olarak, neyin 'uygun olduğunda' ifadesiyle neyin kastedildiğini tam olarak ortaya konulması için bir rehber çıkartılması, kuruluşların belirli bir durumda kime danışılması gerektiğine ilişkin kararları üzerinde önemli bir etkiye sahip olabilir. Örneğin, özellikle demanslı insanlar için tasarlanmış bir akıllı cihaz söz konusu olduğunda, VKED sürecinde bu dezavantajlı durumdaki bireyler grubuna veya bakıcılarına danışmak uygun görünmektedir.

Halihazırda, VKED'lerde bir hak için risk kavramının nasıl anlaşılacağı konusunda ne teoride ne de pratikte bir fikir birliği yoktur[135]. Bu çalışmada, Alessandro Mantelero tarafından önerilen, teknoloji yerine farklı uygulama alanlarına (suç önleme veya sağlık gibi) ve çeşitli hak, değer ve özgürlük gruplarına odaklanan 'hak temelli ve değer odaklı model' benimsenmekte ve bunu destekleyecek argümanlar sunulmaktadır[136]. Bir nesnelerin interneti cihazı, başka bir akıllı üründen tamamen farklı bir veri toplama yöntemine sahip olabilir (örneğin, biri görsel verileri toplayıp üçüncü bir ülkedeki bulut sunucularında depolarken, bir diğeri yalnızca ses verilerini toplayıp cihazda yerel olarak depolayabilir). Bu nedenle, belirli bir teknoloji, vatandaşların haklarını ve değerlerini korumak için alınacak en uygun önlemlerin seçimini etkilediğinden, elbette, kullanılan teknolojinin türü etki değerlendirme sürecinde hala önem taşımaktadır. Ancak asıl önemli olan, veri sorumlusu tarafından bireylerin haklarının ve değerlerinin farklı bağlamlarda nasıl korunduğudur[137]. Bir çocuk (veya dezavantajlı bir yetişkin) bir nesnelerin interneti cihazını kullandığında ya da büyük veri analitiğine tabi olduğunda, VKED'de dikkate alınması gereken kullanılan teknolojinin türü değil, bu teknolojiyi kullananın çocuk olması ve onun hak ve değerlerinin söz konusu olmasıdır. VKED'ler ayrıca akıllı cihazın hangi sektörde kullanıldığını ayırt etmelidir. Bir çocuk evde eğlence amaçlı bir nesnelerin interneti ürününü veya sağlıkla ilgili nedenlerle hastanede akıllı bir cihaz kullanıyorsa, bunlar çok farklı ayarlardır ve dolayısıyla etkilenen haklar ve değerler de farklılık gösterecektir. Örneğin, bir sağlık hizmeti ortamında, seçim özgürlüğü veya zarar vermeme ilkesi çok önemli olabilirken, akıllı bir şehirde eşit muamele veya sivil katılım hakim değerler olabilir[138]. Farklı koşullar, etki değerlendirmeleri için bir referans noktası olarak dikkate alınması gereken farklı değerlerle ilişkilendirilir. GVKT, bireylerin hak ve özgürlüklerinin ve toplumsal sorunların korunmasının önemini vurgulasa da, halihazırda geliştirilen DPIA modelleri toplumsal yansımaları göz ardı etmeye devam etmektedir[139]. Mevcut uygulamaları değiştirmeye yönelik teşvikler, ulusal

[132] PARKER, Christine, "Meta-regulation: Legal Accountability for Corporate Social Responsibility", The New Corporate Accountability: Corporate Social Responsibility and the Law, Cilt: 29, Doreen McBarnet, Ed.: Aurora Voiculescu and Tom Campbell CUP, Cambridge, 2007.

[133] BINNS, s. 129.

[134] VEALE/BINNS/AUSLOOS, s. 52.

[135] DİJK, Niels Van/GELLERT, Raphaël/ROMMETVEİT, Kjetil, "A Risk to a Right? Beyond Data Protection Risk Assessments", Computer Law & Security Review, Cilt: 32, Sayı: 2, 2016, s. 286.

[136] MANTELERO, Alessandro, "AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment", Computer Law & Security Review, Cilt: 34, Sayı: 4, 2018, s. 754.

[137] MANTELERO, s. 754.

[138] MANTELERO, s. 754.

[139] MANTELERO, s. 754.

ve AB düzeyinde yaptırım eylemleri veya ek rehberler yoluyla verilebilir.

Dezavantajlı Kişilerin Verilerinin Bütünlüğünü ve Gizliliğini Koruyabilen Akıllı Cihazlar

Ses kayıtları ve resimleri (ilgili kişiler tarafından özel kabul edilen) kamuya açık hale getiren veya üçüncü kişiler tarafından zahmetsizce erişilebilir hale getiren, çocuklar için tasarlanmış akıllı cihazlardan, siber suçluların onları bozmasına veya zarar vermesine izin veren hacklenmiş akıllı ısıtma sistemlerine ve güvenliği ihlal edilmiş akıllı kilitler sonucunda meydana gelen hırsızlıklara kadar, akıllı evlerde yaşayan dezavantajlı kişilerin karşı karşıya kalacağı bir çok güvenlik sorunu vardır[140]. Örneğin, 2015 yılında, Mattel şirketi, çocukları dinleme ve onlarla konuşma kapasitesine sahip bir nesnelerin interneti ürünü olan Hello Barbie bebeği üretti. Bu oyuncak, çocukların seslerini kaydeden ve veri analizi için üçüncü taraflara aktaran bir mikrofon ile donatılmıştır. Bebek, cihazın dosyalarına (ses kayıtları dahil) erişim sağlayan ve bebeğin mikrofonunu kullanabilen bir araştırmacı tarafından kolayca hacklendi[141]. Benzer şekilde Cayla adlı başka bir bebek de Alman makamları tarafından akıllı ev üyelerini gözetlemek ve topladığı verileri ABD'ye göndermekle suçlandı[142]. Son olarak, 5 milyondan fazla müşteri hesabı ve çocuk profilinin bilgilerini tehlikeye atan dijital bebek telsizleri üreten bir şirket olan Vtech'in hacklenmesi veya dijital bebek telsizlerine erişen ve onlar aracılığıyla bebeklerle konuşan birçok bilgisayar korsanı hikayesi bu durumun diğer örnekleridir[143]. Bu cihazlar, dezavantajlı kullanıcılar ve tüketicilerin kişisel verilerinin güvenliğini baltalayarak GVKT uyumluluğu sorunlarına yol açtığından tehlike arz etmektedir.

'Bütünlük ve gizlilik' ilkesinin hüküm altına alınmasıyla birlikte GVKT'nin 5. maddesi veri güvenliğinin sağlanması eylemini basit bir gereklilikten ana veri koruma ilkelerinden biri haline getirmiştir[144]. Verilerin güvenliğinin sağlanması, yasal veri işleme için bir ön koşul olduğundan, GVKT'nin 4.12 maddesinde, kişisel veri ihlali' "iletilen, saklanan veya bir başka şekilde işlenen kişisel verilerin kazara veya hukuka aykırı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlali" olarak tanımlanmıştır. Verileri silme, ifşa etme veya verilere erişme gibi işleme faaliyetleri bu şekilde hukuka aykırı değildir[145]. Veri sorumlusunun ilgili güvenlik önlemlerini aldığı ve ihmalkar olmadığı tespit edilirse, veri ihlali tesadüfi olarak kabul edilecektir[146]. Bununla birlikte, uygun veri koruma önlemleri uygulanmaz ve bunun sonucunda bir veri ihlali meydana gelirse, bu, bütünlük ve gizlilik ilkesinin açık bir ihlali olur ve herhangi bir hukuka uygunluk sebebinin kullanımını imkansız hale getirir. Bu durum vaka bazında değerlendirilir[147]. Son birkaç yılda, bilgisayar korsanlarının, bilgileri olmadan ilgili kişileri gözetlemek veya hassas kişisel bilgiler vererek onları kandırmak için Amazon Alexa ve Google Home akıllı asistanlarını kullanabildikleri kanıtlandı[148]. Bu, Amazon ve Google'ın her saldı-

[140] DCMS, "Secure by Design: Improving the Cyber Security of Consumer Internet of Things Report", (2018), https://www.gov.uk/government/publications/secure-by-design-report, (Erişim Tarihi: 6.10.2021).

[141] GIBBS, Samuel, "Hackers can Hijack Wi-Fi Hello Barbie to Spy on your Children", The Guardian (2015) https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children, (Erişim Tarihi: 6.10.2021).

[142] Forbrukerradet (Norwegian Consumer Council), "#Toyfail an Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys" (2016) <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf> erişim 6 Ekim 2021; Bouvet on behalf of the Norwegian Consumer Council, "Investigation of Privacy and Security Issues with Smart Toys" (2016) https://fil.forbrukerradet.no/wp-content/uploads/2016/12/2016-11-technical-analysis-of-the-dolls-bouvet.pdf (Erişim Tarihi: 6.10.2021).

[143] LUPTON, Deborah/WILLIAMSON, Ben, "The Datafied Child: The Dataveillance of Children and Implications for their Rights", New Media & Society, Cilt: 19, Sayı: 5, 2017, s. 780.

[144] Nİ LOİDEAİN, s. 83.

[145] CLIFFORD/AUSLOOS, s. 95.

[146] Nİ LOİDEAİN, s. 83.

[147] Nİ LOİDEAİN, s. 83.

[148] ZDNet, "Alexa and Google Home Devices Leveraged to Phish and Eavesdrop on Users, Again", (2019) <ht-

rıdan sonra karşı önlemler almasına rağmen birkaç kez oldu. Dezavantajlı kişilerin bir nesnelerin interneti cihazının olağandışı bir şekilde davrandığını anlaması ve bir veri güvenliği tehdidini tespit etmesi beklenemez. Bu cihazlar, güvenlik önlemlerinin yeterince güçlü olmasını sağlamalıdır. Bir veri ihlali teorik olarak her zaman gerçekleşebilirken, tekrar tekrar gerçekleşmesi endişe verici bir işarettir. Bu durumda yetkililer veri ihlalini tesadüfi olarak değerlendirir mi? Google ve Amazon tarafından benimsenen karşı önlemlerin nispeten kısa süreler içinde düzenli olarak etkisiz olduğu kanıtlanırsa, yanıt muhtemelen olumsuz bir yanıt olmalıdır (özellikle, bu şirketlerin tasarrufundaki kaynaklar göz önüne alındığında).

Bu makalede ayrıca GVKT'nin bütünlük ve gizlilik ilkesine uyum ve dezavantajlı müşterilerin korunması için standartların önemine dikkat çekilmek istenmektedir. Sertifikasyon mekanizmaları, standartlara örnek olarak verilebilir. Sertifikasyonun amacı, bir grup standarda uygunluğu kanıtlamaktır. Kişilerin, ürünlerin ve/veya süreçlerin belirli bir dizi gereksinime uygunluğunu değerlendirmeye hizmet eden 'uygunluk değerlendirmesi' olarak tanımlanabilir[149]. Etiketleme şemaları son zamanlarda endüstri, sertifikasyon kuruluşları ve hükümet tarafından ortaya atılmıştır[150]. Örneğin, Birleşik Krallık hükümeti yakın zamanda tüketiciler için nesnelerin interneti ürün güvenliği için bir etiketleme planı önerdi[151]. Akıllı ürün alıcıları, bir cihaz böyle bir program aracılığıyla sertifikalandırılırsa, herhangi bir güvenlik ve güvenlik riskiyle meşgul olmaları gerekmediğini düşünebilir. Aslında, 'standartlar ve sertifikalar, son kullanıcı ve vatandaş için güvenilirlik ve güvence ile eşanlamlı olabilir'[152]. Standartların yazılma şeklinin nesnelerin interneti sektörü için çok önemli olmasının nedeni budur. Etkili standartlara ihtiyaç vardır ve bunların dayandığı varsayımların doğru olması gerekir. Aksi takdirde, tüketiciler sertifikasyona körü körüne güvenebilir ve kendi güvenlik ve emniyetlerini tehlikeye atabilir. Doğru standartlar GVKT uyumluluğuna yardımcı olabilir, dezavantajlı kişilerin haklarını güçlendirebilir ve bu kişilerin daha güvenli seçimler yapmasına yardımcı olabilir. Özellikle, dezavantajlı kişilere veya yasal olarak yetkili temsilcilerine kuruluşun uygun güvenlik önlemlerini (veya en azından bazılarını) uyguladığını iletmenin basit ve etkili bir yolu olabilirler. Tüketiciler büyük olasılıkla güvenli olduğu resmi olarak onaylanmış ürünleri tercih edeceğinden, ilgili standartların uygulanması rekabet avantajına dönüşebilir.

Sonuç

Bu analizin amacı, bir çocuk veya dezavantajlı bir yetişkin akıllı bir ürün kullandığında ilgili hukuka uygunluğunun ve bu kişilerin hukuki gereksinimleri üzerinde düşünmektir. Ardından, dezavantajlı kişilerin kişisel verilerini toplayan nesnelerin interneti cihazlarına nasıl uygulandıklarını daha iyi anlamak için diğer ilgili GVKT ilkeleri eleştirel bir şekilde tartışılmıştır.

Bu çalışma, kuruluşların dikkatini veri minimizasyonu, güvenlik, verilerin korunmasında tasarım ve varsayılana ve VKED'lere odaklayarak sorunların önlenmesi ve kişisel veri işlemenin

tps://www.zdnet.com/article/alexa-and-google-home-devices-leveraged-to-phish-and-eavesdrop-on-users-again/>, (Erişim Tarihi: 6.10.2021).

[149] ENISA, "Security Certification Practice in the EU", 2013, https://www.enisa.europa.eu/publications/security-certification-practice-in-the-eu-information-security-management-systems-a-case-study, (Erişim Tarihi: 6.10.2021).

[150] JOHNSON, Shane D and others, "The Impact of IoT Security Labelling on Consumer Product Choice and Willingness to Pay" PLoS One 1, Cilt: 15, Sayı: 1, 2020.

[151] DCMS, "Consultation on the Government's Regulatory Proposals regarding Consumer Internet of Things (IoT) Security", 2020, https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/consultation-on-the-governments-regulatory-proposals-regarding-consumer-internet-of-things-iot-security, (Erişim Tarihi: 6.10.2021).

[152] KAMARA, Irene/SVEİNSDOTTİR Thordis/ WURSTER, Simone, "Raising Trust in Security Products and Systems through Standardisation and Certification: The Crisp Approach", (2015 ITU Kaleidoscope: Trust in the Information Society (K-2015), Barcelona, December 2015), https://ieeexplore.ieee.org/document/7383632, (Erişim Tarihi: 6.10.2021).

azaltılmasından yanadır. Tabii ki, kişisel verilerin işlenmesinden kaçınılamayan durumlarda ve ilgili kişilerin verilerinin işlenmesine yönelik isteklerini açıkça dile getirdikleri durumlarda ilgili hukuki zeminin uygun şekilde uygulanması hayati önem taşımaktadır. Ayrıca, hiçbir güvenlik önlemi mükemmel değildir ve veri ihlali riskleri her zaman olacaktır. Veri sorumlularının işleme başlamadan önce tüm GVKT gereksinimlerini karşıladıklarından ve ilgili kişilerin bilinçli kararlar verdiğinden emin olmaları gerekir. Hukuka uygunluk sebebinin seçimi bağlama bağlı olacaktır ve duruma göre tercih edilmelidir. Hukuka uygunluk sebebinin seçimi ne olursa olsun, veri sorumlusunun dezavantajlı bireylerle ilgili özel veri koruma önlemleri alması ve temel hak ve özgürlüklerini korumak için eylemlerini bu kişilerin ihtiyaçlarına göre uyarlaması gerekmektedir. Bu makale, bu tür önlemlerin her akıllı üründe varsayılan olarak benimsenmesi gerektiğini savunmaktadır. Herhangi bir akıllı cihaz, dezavantajlı bir kişi tarafından kullanılabilir ve herkes zamanla dezavantajlı hale gelebilir. Ayrıca, şeffaflığı ve genel olarak veri korumasını artıracağı için diğer vatandaşlar da bu önlemlerden faydalanacaktır. Hukuka uygunluğa ek olarak, aynı GVKT hükmünde iki başka ilkeden bahsedilmektedir: şeffaflık ve adillik. Bunlar, dezavantajlı insanların haklarının etkin bir şekilde korunmasını sağlamak için gerekli olan kapsayıcı ilkelerdir. Adillik ilkesi henüz tam olarak tanımlanmamıştır, bu da bazı bilim insanları ve Avrupa Veri Koruma Denetçisi tarafından önerildiği gibi veri etiği girişimlerini kapsayan bir tanım geliştirme fırsatı verir.

Bir veri sorumlusu dezavantajlı kişilerin verilerini toplamaya karar verdiğinde, sorunların çıkabileceği nokta tam da burasıdır. Örnek olarak rıza alındığı durumda, rızanın şartlarını yerine getirmek ve dezavantajlı kişilerin kişisel verilerini korumak için özel önlemler almak çok çaba gerektirir ve ne kadar çok veri toplanırsa, o kadar fazla sorun ortaya çıkabilir. İkinci olarak, rıza bazı araştırmacılar tarafından verilerin nasıl işlendiği üzerinde gerçek bir kontrol sağlamadığı ve bir güç dengesizliği durumunda alındığı için eleştirilmiştir, bu argüman dezavantajlı kişiler söz konusu olduğunda daha da ön plana çıkmaktadır. Bu güç dengesizliği diğer hukuka uygunluk sebepleri için de geçerlidir; örneğin, bir kuruluş meşru menfaat sebebine dayandığında ve kendi menfaatlerini ilgili kişinin menfaatlerinin üstünde tuttuğu durumda. Çocukların ve dezavantajlı yetişkinlerin temel hak ve özgürlüklerini korumanın yanı sıra veri sorumluları açısından uyumu kolaylaştırmak için bu makale, yukarıda belirtilen GVKT mekanizmalarının, yani veri minimizasyonu, verilerin korunması için tasarım ve varsayılan, VKED'DPIA'ların ve bütünlük ve gizlilik ilkesinin önemini vurgulamaktadır. Bu ilkeler, sorunları önleme ve dezavantajlı bireylerin korunmasını artırma imkanına sahip oldukları için teşvik edilmeli, uygulanmalı ve geliştirilmelidir (gizliliği koruyan yeni teknolojilerin dezavantajlı kişiler bağlamında bu ilkelerle hukuki uyumu nasıl destekleyebileceğine ilişkin daha fazla çalışmaya ihtiyaç vardır). Ancak bu mümkün olan en iyi şekilde yapıldıktan sonra, bir kuruluş dezavantajlı kişilerin kişisel verilerinin işlenmesi hala gerekliyse hangi hukuka uygunluk sebebinin kullanılacağını değerlendirmelidir.

Kaynakça

ABİTEBOUL, Serge/STOYANOVİCH, Julia: "Transparency, Fairness, Data Protection, Neutrality", Journal of Data and Information Quality, Cilt: 11, Sayı: 3, 2019.

ADAMS, Anne/SASSE, Martina Angela: "Users are Not the Enemy Communications of the ACM, Cilt: 42, Sayı: 12, 1999.

ARENDS, Johan and others: "Multimodal Nocturnal Seizure Detection in a Residential Care Setting: A Long-Term Prospective Trial", Neurology e2010, 91, 2018.

ARNARDÓTTİR, Oddny Mjöll: "Vulnerability under Article 14 of the European Convention on Human Rights", Oslo Law Review, Cilt: 1, Sayı: 3, 2017.

ARNOLD, Brent/ SİVASOTHY, Kavi: "He Sees You when You're Sleeping, He Knows When You're Awake: Smart Toys and Regulating the IoT in Canada", (Gowling WLG, 17 December 2018), https://gowlingwlg.com/en/insights-resources/articles/2018/smart-toys-and-regulating-the-iot-in-canada/, (Erişim Tarihi: 6.10.2021.)

Art 29 Working Party: "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (WP 248, 4 Ekim2017).

Art 29 Working Party: "Opinion 8/2014 on the Recent Developments on the Internet of Things" (WP 223, 16 September 2004).

Art 29 Working Party: "Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC" (WP 217, 9 Nisan 2014).

BINNS, Reuben: "Data Protection Impact Assessments: a Meta-Regulatory Approach" International Data Privacy Law, Cilt: 7, Sayı: 1, 2017.

Bits of Freedom: 'A Loophole in Data Processing' (2012) <https://www.bitsoffreedom.nl/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf> (Erişim tarihi: 6.10.2021).

BRANDİMARTE, Laura/ACQUİSTİ, Alessandro/LOEWENSTEİN, George: "Misplaced Confidences", Social Psychological and Personality Science, Cilt: 4, Sayı: 3, 2013.

BUİTELAAR, CJ: "Child's Best Interest and Informational Self-Determination: What the GDPR can Learn from Children's Rights", International Data Privacy Law, Cilt: 8, Sayı: 4, 2018.

BUTTERWORTH, Michael: "The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework" Computer Law & Security Review, Cilt: 34, Sayı: 2, 2018.

CALO, Ryan: "Privacy, Vulnerability, and Affordance", DePaul Law Review, Cilt: 66, Sayı: 2, 2017, s. 593.

Centre for Information Policy Leadership: "GDPR Implementation in Respect of Children's Data and Consent", 2018, s. 6 <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf> erişim 6 Ekim 2021.

CLIFFORD, Damian /AUSLOOS, Jef: "Data Protection and the Role of Fairness", Yearbook of European Law, 37, 2018.

COLLINGWOOD, Lisa: "Villain or Guardian? "The Smart Toy is Watching You Now ...", Information & Communications Technology Law, Cilt: 30, Sayı: 1, 2021.

COOPER, Frank Rudy: "Always Already Suspect: Revising Vulnerability Theory", North Carolina Law Review, Cilt: 93, Sayı: 5, 2015.

CUSTERS, Bart and others: "A Comparison of Data Protection Legislation and Policies Across the EU", Computer Law & Security Review, Cilt: 34, Sayı: 2, 2018.

DİAZ, Claudia/TENE, Omer/GUERSES, Seda: "Hero or Villain: The Data Controller in Privacy Law and Technologies", Ohio State Law Journal, 74, 2013.

DİJK, Niels VAN/GELLERT Raphael/ROMMETVEİT, Kjetil: "A Risk to a Right? Beyond Data Protection Risk Assessments", Computer Law & Security Review, Cilt: 32, Sayı: 2, 2016.

EDPS: "European Data Protection Supervisor: Opinion of the European Data Protection Supervisor on the Data Protection Reform Package" (2012) <https://edps.europa.eu/sites/edp/files/publication/12-0307_edps_reform_package_en.pdf> (Erişim Tarihi: 6.10.2021).

EDPB: "Guidelines 05/2020 on Consent under Regulation 2016/679" (4 May 2020) 21 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf, (Erişim Tarihi: 6.10.2021).

EDPB: "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default" (13 November 2019) 14 https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf, (Erişim Tarihi: 6.10.2021).

EDPS: "Opinion 4/2015 Towards a New Digital Ethics", 2015, https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf, (Erişim Tarihi: 6.10.2021).

Eindhoven University of Technology: "New Epilepsy Warning Device Could Save Thousands of Lives", 2018, https://www.tue.nl/en/news/news-overview/24-10-2018-new-epilepsy-warning-device-could-save-thousands-of-lives/#top, (Erişim Tarihi: 6.10.2021).

ENISA: "Recommendations on Shaping Technology According to GDPR Provisions - Exploring the Notion of Data Protection by Default", 2018, https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2, (Erişim Tarihi: 6.10.2021).

ENISA: "Security Certification Practice in the EU", 2013, https://www.enisa.europa.eu/publications/security-certification-practice-in-the-eu-information-security-management-systems-a-case-study, (Erişim Tarihi: 6.10.2021).

European Audiovisual Observatory: 'Smart TV and Data Protection' 60, 2018. https://rm.coe.int/iris-special-2015-smart-tv-and-data-protection/1680945617, (Erişim Tarihi: 6.10.2021).

FERRETTİ, Federico: "Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?", Common Market Law Review, Cilt: 51, Sayı: 3, 2014.

FINEMAN, Martha Albertson: "The Vulnerable Subject: Anchoring Equality in the Human Condition", Yale Journal of Law and Feminism, Cilt: 20, Sayı: 1, 2008.

FRA: "Handbook on European Data Protection Law", 2018, https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf, (Erişim Tarihi: 6.10.2021).

GARTNER: "Leading the IoT: Gartner Insights on How to Lead in a Connected World" 13, 2017, https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf, (Erişim Tarihi: 6.10.2021).

GIBSON, Grant: 'Smart Technologies in Dementia Care - Future Opportunities and Challenges' (21 March 2019), https://dementia.stir.ac.uk/blogs/dementia-centred/2019-03-21/smart-technologies-dementia-care-future-opportunities-and, (Erişim Tarihi: 6.10.2021.

GIBBS, Samuel: "Hackers can Hijack Wi-Fi Hello Barbie to Spy on your Children", The Guardian, 2015, https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children, (Erişim Tarihi: 6.10.2021).

HANSEN, Marit: "Data Protection by Default in Identity-Related Applications" (IDMAN 2013: Policies and Research in Identity Management, London, April 2013) https://link.springer.com/chapter/10.1007%2F978-3-642-37282-7_2, (Erişim Tarihi: 6.10.2021).

HEUVEL, Karlijn van den: Securing the Smart Home, Masters Thesis, University of Amsterdam, 2018.

HİLDEBRANDT, Mireille: "Profiling and the Rule of Law", Identity in the Information Society, Cilt: 1, Sayı: 1, 2008.

InfoWorld: "IoT Silliness: "Headless" Devices without a UI", 2015, https://www.infoworld.com/article/2867356/beware-this-iot-fallacy-the-headless-device.html, (Erişim Tarihi: 6.10.2021).

Information Commissioner's Office: "Age Appropriate Design: A Code of Practice for Online Services" (2 September 2021), https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/, (Erişim Tarihi: 4.10.2021).

Information Commissioner's Office: "When Do We Need to Do a DPIA?" https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/, (Erişim Tarihi: 6.10.2021).

Information Commissioner's Office: "Principle (c): Data Minimisation" <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/> (Erişim Tarihi: 6.10.2021).

Information Commisioner's Office: "Legitimate Interests" https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/, (Erişim Tarihi: 6.10.2021).

Information Commisioner's Office: "Vital Interests", 2019, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/, (Erişim Tarihi: 6.10.2021).

IEEE: "Towards a Definition of the Internet of Things (IoT)" (27 May 2015) 74 https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf, (Erişim Tarihi: 6.10.2021).

JİNGJİNG, REN and others: "Information Exposure from Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach" (IMC '19: Proceedings of the Internet Measurement Conference, Amsterdam, Ekim 2019) <https://dl.acm.org/doi/10.1145/3355369.3355577> (Erişim Tarihi: 6.10.2021).

KAMARA, Irene/SVEİNSDOTTİR, Thordis/ WURSTER, Simone: "Raising Trust in Security Products and Systems through Standardisation and Certification: The Crisp Approach" (2015 ITU Kaleidoscope: Trust in the Information Society (K-2015), Barcelona, December 2015) <https://ieeexplore.ieee.org/document/7383632> (Erişim Tarihi: 6.10.2021).

KELION, Leo: "Amazon Sued over Alexa Child Recordings in US", BBC, 2019, <https://www.bbc.com/news/technology-48623914> (Erişim Tarihi: 6.10.2021).

LİEVENS, Eva/ HOF, Simone van der: "The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data under the GDPR", Communications Law, 23(1), 2018.

LOİDEAİN, Nora: "A Port in the Data-Sharing Storm: The GDPR and the Internet of Things", Journal of Cyber Policy, Cilt: 4, Sayı: 2, 2019.

LUETH, Knud Lasse: "State of the IoT 2018: Number of IoT Devices now at 7B - Market Accelerating" (IoT Analytics, 8 August 2018) <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/> (Erişim Tarihi: 6.10.2021).

LUNA, Florrencia: "Elucidating the Concept of Vulnerability: Layers Not Labels", International Journal of Feminist Approaches to Bioethics, Cilt: 2, Sayı: 1, 2009.

LUPTON, Deborah/WILLIAMSON, Ben: "The Datafied Child: The Dataveillance of Children and Implications for their Rights", New Media & Society, Cilt: 19, Sayı: 5, 2017.

MACENAİTE, Milda: "From Universal Towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation", New Media & Society, Cilt: 19, Sayı: 5, 2017.

MACENAİTE, Milda/ KOSTA, Eleni: "Consent for Processing Children's Personal Data in the EU: Following in US footsteps?", Information & Communications Technology Law, 26(2), 2017.

MALGİERİ, Gianclaudio/NİKLAS, Jedrzej: "Vulnerable Data Subjects", Computer Law & Security Review, 37, 2020.

MANTELERO, Alessandro: "AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment", Computer Law & Security Review, Cilt: 34, Sayı: 4, 2018.

MARWICK, Alice/ BOYD, Danah: "Networked Privacy: How Teenagers Negotiate Context in Social Media", New Media & Society, Cilt: 16, Sayı: 7, 2014.

MİCHETİ, Anca/ BURKELL, Jacquelyn/ STEEVES, Valerie: "Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand", Bulletin of Science, Technology & Society, Cilt: 30, Sayı: 2, 2010.

MİLKAİTE, Ingrida/ LİEVENS, Eva: "Child-Friendly Transparency of Data Processing in the EU: From Legal Requirements to Platform Policies", Journal of Children and Media, Cilt: 14, Sayı: 1, 2019.

MİLKAİTE, Ingrida and others: The General Data Protection Regulation and Children's Rights: Questions and Answers for Legislators, DPAs, Industry, Education, Stakeholders and Civil Society. Roundtable Report, 2017, <https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf> (Erişim Tarihi: 6.10.2021).

MOCRİİ, Dragos/ CHEN, Yuxiang/ MUSİLEK, Petr: "IoT-Based Smart Homes: A Review of System Architecture, Software, Communications, Privacy and Security" Internet of Things, 1-2, 2018.

MOEREL, Lokke/PRİNS, Corien: "Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things" (2016), ssrn: 2784123 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123> (Erişim Tarihi: 8.9.2021.

PARKER, Christine: "Meta-regulation: Legal Accountability for Corporate Social Responsibility", The New Corporate Accountability: Corporate Social Responsibility and the Law, Cilt: 29, Ed.: Doreen McBarnet, Aurora Voiculescu and Tom Campbell, CUP, Cambridge 2007.

PASQUALE, Frank: The Black Box Society: The Secret Algorithms that Control Money and Information, Harvard University Press, Cambridge 2016.

PERONİ, Lourdes/ TİMMER, Alexandra: "Vulnerable Groups: The Promise of an Emerging Concept in European Human Rights Convention Law", International Journal of Constitutional Law, Cilt: 11, Sayı: 4, 2013.

PİASECKİ, Stanislaw/ URQUHART, Lachlan/ MCAULEY, Derek: "Defence Against the Dark Artefacts: Smart Home Cybercrimes and Cybersecurity Standards", Computer Law & Security Review 105542, 42, 2021.

SCHARTUM, Dag Wiese: "Making Privacy by Design Operative", International Journal of Law and Information Technology, Cilt: 24, Sayı: 2, 2016.

TİMMER, Alexandra: "Vulnerability: Reflections on a New Ethical Foundation for Law and Politics", A Quiet Revolution: Vulnerability in the European Court of Human Rights, Ed.: Martha Albertson Fineman ve Anna Grear, Ashgate, Farnham, 2013.

TİMMER, Alexandra: Strengthening the Equality Analysis of the European Court of Human Rights: The Potential of the Concepts of Stereotyping and Vulnerability, Universiteit Gent 2014.

URQUHART, Lachlan/ SCHNÄDELBACH, Holger/ JÄGER, Nils: "Adaptive Architecture Regulating Human Building Interaction", International Review of Law, Computers & Technology, Cilt: 33, Sayı: 1, 2019.

TİKKİNEN, Christina/ROHUNEN, Anna/ MARKKULA, Jouni: "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies" Computer Law & Security Review, Cilt: 34, Sayı: 1, 2018.

WACHTER, Sandra: "The GDPR and the Internet of Things: A Three-Step Transparency Model", Law, Innovation and Technology, Cilt: 10, Sayı: 2, 2018.

VEALE, Micheal/ BİNNS, Reuben / AUSLOOS, Jef: "When Data Protection by Design and Data Subject Rights Clash" International Data Privacy Law, Cilt: 8, Sayı: 2, 2018, s. 105.

VOLOSEVİCİ, Dana: "Child Protection under GDPR", A Journal of Social and Legal Studies, Cilt: 6, Sayı: 2, 2019.

ŽLİOBAİTĖ, Indre/CUSTERS, Bart: "Using Sensitive Personal Data May be Necessary for Avoiding Discrimination in Data-Driven Decision Models", Artificial Intelligence and Law, Cilt: 24, Sayı: 2, 2016.