www.kvkk.gov.tr
Kişisel Verileri Koruma Dergisi
Cilt:4 Sayı:1
Geliş:17.05.2022
Kabul:28.06.2022

Bir Uyum Aracı Olarak Veri Koruma Etki Analizinin Türk Hukuku Bakımından Değerlendirilmesi

Öykü Beste, Bayram
Kadir Has Üniversitesi Özel Hukuk Tezli Yüksek Lisans Öğrencisi. ARI Teknokent Proje Geliştirme Planlama A.Ş. İstanbul, Türkiye, oyku.beste@hotmail.com.
ORCID: https://orcid.org/ 0000-0001-5727-7244.

ÖZ
Özellikle yapay zekâ teknolojileri gibi gelişen teknolojiler karşısında gerçek kişiler açısından oluşabilecek risklerin yönetilmesi ve temel hak ve özgürlüklerinin korunabilmesi veri koruma düzenlemeleri ile yakından ilgilidir. Avrupa Birliği veri koruma hukukunda kişisel veri işlemenin doğurduğu risklerin tasarımdan itibaren ele alınarak önlenmesi amacıyla hesap verebilirlik ilkesi ve çeşitli uyum araçları benimsenmiştir. Bunların arasında, risklerin tespit edilmesi ve önlenmesi kapsamında işlevsel olarak değerlendirilen veri koruma etki analizi dikkat çekmektedir. Türk veri koruma hukukunun da gelişen teknolojilere bağlı olarak ortaya çıkabilecek yeni risk ve tehditler dikkate alınarak geliştirilmesi gerekmektedir. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun Genel Veri Koruma Tüzüğü ile uygun hale getirilmesi hedefi kapsamında hesap verebilirlik ilkesinin ve uyum araçlarının Türk hukukunda da düzenlenmesi beklenmektedir. Bu çalışmada Avrupa Birliği veri koruma hukukunda benimsenen veri koruma etki analizi düzenlemesinin amacı, hesap verebilirlik ilkesiyle ilişkisi, kapsamı ve uygulaması incelenmiştir. Sonrasında bu uygulama Türk hukuku bakımından ele alınarak mevzuatımızda düzenlenmesinin hangi açılardan faydalı olabileceği değerlendirilmiştir.
Anahtar Sözcükler: Hesap Verebilirlik, Mahremiyet, Risk, Uyum

Analyzing of Data Protection Impact Assessment As A Compliance Instrument In Terms of Turkish Law

ABSTRACT
Data protection regulations are closely related to the management of risks that may arise in terms of natural persons, especially in the face of developing technologies such as artificial intelligence technologies, and the protection of their fundamental rights and freedoms. Under the European Union data protection law, the principle of accountability and numerous compliance instruments are adopted in order to prevent the risks posed by personal data processing from the design stage. Among these instruments, data protection impact assessment, which is considered specific and functional for determining and preventing risks, draws attention. Turkish data protection law also needs to be developed by considering the new risks and threats that may arise in the future depending on the advancing technologies. It is expected that the principle of accountability and compliance instruments will also be regulated in Turkish law with the updates to be made in the Personal Data Protection Law No. 6698 in line with the General Data Protection Regulation. In this article, the purpose, scope, application of data protection impact assessment and its relationship with the principle of accountability are examined. Following, this practice is analyzed in terms of Turkish law and discussed in which aspects it would be beneficial to be regulated in our legislation.
Keywords: Accountability, Privacy, Risk, Compliance

Atıf Gösterme Bayram, Ö. B., (2022). M Bir Uyum Aracı Olarak Veri Koruma Etki Analizinin Türk Hukuku Bakımından Değerlendirilmesi, *Kişisel Verileri Koruma Dergisi*. *4*(1), 38-53.

GİRİŞ

Kişisel verilerin işlenmesi doğası gereği gerçek kişilerin temel hak ve özgürlükleri açısından çeşitli riskler barındırmaktadır. Teknolojideki gelişmelere bağlı olarak veri sorumlularının kişisel verileri elde etme ve işleme süreçleri karmaşıklaşmıştır. Özellikle yapay zeka, makine öğrenmesi ve nesnelerin interneti gibi büyük miktarda verinin (big data) işlenmesini gerektiren yeni teknolojilerin kullanıldığı hallerde kişisel veriler yapay zeka teknolojilerini beslerken, yapay zeka teknolojileri de çıkarımlar yaparak daha fazla kişisel veri üretmektedir. Bu durum kişisel verilerin korunması açısından birçok soruna sebep olabilecektir (Dülger, 2020). Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ile Sanayi ve Teknoloji Bakanlığı iş birliğinde hazırlanan Ulusal Yapay Zeka Stratejisi (2021-2025) kapsamında (i) yapay zeka uzmanlarını yetiştirmek ve alanda istihdamı artırmak, (ii) araştırma, girişimcilik ve yenilikçiliği desteklemek, (iii) kaliteli veriye ve teknik altyapıya erişim imkanlarını genişletmek, (iv) sosyoekonomik uyumu hızlandıracak düzenlemeleri yapmak, (v) uluslararası iş birliklerini güçlendirmek ve (vi) yapısal ve işgücü dönüşümünü hızlandırmak hedeflenmiştir. Bu hedefler doğrultusunda dikkate alınacak olan temel ilkelerden bir tanesi de mahremiyet olarak belirlenmiştir. Bu çerçevede yapay zeka sistemlerinin kişisel verilerin korunmasına halel getirmeyecek şekilde geliştirilmesi ve çalıştırılması gerektiğine dikkat çekilmiştir. Teknolojik gelişmeler teşvik edilirken gerçek kişilerin hak ve özgürlüklerinin korunabilmesi amacıyla gerekli hukuki alt yapının oluşturulması önem arz etmektedir.

Avrupa veri koruma hukuku düzenlemelerinde, gelişen teknolojilerle bağlantılı olarak özellikle bu tür yeni veri elde etme veya kullanım biçimlerinin sebep olabileceği risklere karşı kişisel verilerin etkin bir şekilde korunabilmesi amacıyla hesap verebilirlik ilkesine ve bunun destekleyicisi olan uyum araçlarına ağırlık verilmiştir. Türk veri koruma hukuku düzenlemelerinin de etkin fayda sağlayabilmesi için veri sorumlularının sorumluluklarının artırıldığı ve veri işlemenin doğurduğu risklerin tasarımdan itibaren dikkate alındığı bir yaklaşım benimsenerek gerekli geliştirmelerin yapılması önerilmektedir. Nitekim önümüzdeki dönemde 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun Genel Veri Koruma Tüzüğü dikkate alınarak geliştirilmesi beklenmektedir.

Bu çalışmada ilk olarak Avrupa Birliği veri koruma hukukunda kişisel verilerin korunması kapsamında işlevsel bir uygulama olarak değerlendirilen uyum araçlarından biri olan veri koruma etki analizi incelenmiştir. Daha sonra veri koruma etki analizinin amacının ve işlevinin daha iyi anlaşılabilmesi için yüksek risk kavramına ilişkin açıklamalara yer verilmiştir. Son olarak ise veri koruma etki analizinin Türk veri koruma hukuku kapsamındaki ihtiyaçlara uygunluğu değerlendirilmiştir.

AVRUPA VERİ KORUMA HUKUKUNDA VERİ KORUMA ETKİ ANALİZİ

25 Mayıs 2018 tarihinde, 95/46 sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi'nin yerine geçerek yürürlüğe giren Genel Veri Koruma Tüzüğü ("Tüzük") ile Avrupa Birliği'nde ve şartların sağlandığı hallerde Avrupa Birliği'nin sınırları ötesinde veri sorumluları için ortak veri koruma haklarının ve kurallarının belirlenmesi ve veri koruma düzenlemelerinin kişisel verilerin etkin bir şekilde korunmasını zorlaştıran teknolojik gelişmelere uyum sağlaması amaçlanmıştır (European Data Protection Supervisor, 2012). Bu amaç doğrultusunda mevzuata uyum, uyumun ispatı ve veri koruma otoritelerinin denetimlerinin hızlı ve etkin bir şekilde gerçekleştirilmesi hususlarını temin etmek için hesap verebilirlik yaklaşımı benimsenmiştir. (Kaya, 2020). Tüzük'e hakim olan hesap verebilirlik ilkesine göre, veri sorumlusu Tüzük'te düzenlenen ilkelere uygun davranmak ve gerektiğinde de bunlara uygun davrandığını ispat etmek zorundadır (Tüzük m. 5/2). Bir diğer bakış açısıyla, bu ilke veri sorumlusu nezdinde kişisel verilerin korunmasının sürekli gözetilen, etkin şekilde uygulanan ve düzenli olarak denetlenen bir değer olduğunun ispatı sürecidir (Kaya, 2020). Hesap verebilirlik ilkesiyle asıl olarak veri sorumlusunun kişisel verilerin korunmasına ilişkin rolünün ve sorumluluğunun artırılması amaçlanmıştır. Bu doğrultuda çeşitli uyum araçları belirlenerek kişisel verilerin korunmasına ilişkin prensiplerin daha etkili şekilde uygulanmasını sağlayabilecek mekanizmalar düzenlenmiştir (Demetzou, 2019). İşte bu uyum araçlarından biri de ilk defa Tüzük kapsamında bir yükümlülük olarak düzenlenen veri koruma etki analizi gerçekleştirilmesi ve değerlendirme sonucunun gerektirmesi halinde denetim makamına başvurulmasıdır (Tüzük m. 35-36). Bu mekanizmanın gerçek kişilerin temel hak ve özgürlüklerinin korunması amacı doğrultusunda daha spesifik ve işlevsel olduğu düşünülerek ilgili düzenlemenin yapılmasıyla birlikte sicil kayıt yükümlülüğü kaldırılmıştır (Tüzük Gerekçe 89).

Veri sorumlularının Tüzük kapsamındaki temel yükümlülüğü veri işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hak ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak söz konusu veri işleme faaliyetine uygun tedbirleri uygulamaktır (Tüzük m. 24/1). Veri koruma etki analizi gerçekleştirme yükümlülüğü de kişisel verilerin işlenmesinden doğan risklerin gereği gibi yönetilmesine ilişkin hükümlerin bir parçasıdır (Article 29 Data Protection Working Party, 2017). Bu uygulama veri sorumlularının halihazırda var olan veri işleme faaliyetlerinin belirlenmesi ve belgelendirilmesi, gerekli teknik ve idari tedbirlerin sağlanması ve kişisel verilerin işlenmesine ilişkin ilkelere uyum gibi başlıca yükümlülüklerin yüksek risk şartına bağlı olarak gözden geçirilmesini ve uygulanmasını tamamlayan bir çerçeve yükümlülük olarak düzenlenmiştir (Yordanov, 2017; Demetzou, 2019).

Ana hatlarıyla veri koruma etki analizi, bir veri işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçları dikkate alındığında gerçek kişilerin hak ve özgürlükleri açısından yüksek risk yaratma ihtimalinin bulunduğu hallerde, veri sorumlusunun gerçekleştirmekle yükümlü olduğu incelemedir. Bu yükümlülük, hesap verebilirlik ilkesinin ağırlığının artırılması amacıyla kişisel verilerin korunmasına ilişkin zarara sebep olacak olaydan sonra değil önce gerçekleştirilecek şekilde, proaktif bir yapıda tasarlanmıştır (Article 29 Data Protection Working Party, 2017; Demetzou, 2019; Tüzük m. 35:/1, 35/10; Tüzük Gerekçe 90, 93). Başlangıçtan itibaren veri koruması (data protection by default) ve tasarımdan itibaren veri koruması (data protection by design) yaklaşımına da uygun olarak, veri koruma etki analizine, veri işleme faaliyetlerinin tamamı henüz bilinmiyor olsa dahi bunların tasarımında uygulanabilir olduğu ölçüde olabildiğince erken başlanması gerekmektedir (Tüzük Gerekçe 78). Böylece çalışmalar esnasında kişisel verilerin korunması mutlaka dikkate alınacak olup uyumluluğu teşvik eden çözümlerin gelişmesi için uygun ortam oluşacaktır (Article 29 Data Protection Working Party, 2017). Veri koruma etki analizini olabildiğince erken gerçekleştirmenin bir diğer faydası da olası risklerin erken belirlenmesi halinde bunların ele alınmasının daha kolay ve daha ekonomik olmasıdır (Metin, Erkan, Atasu ve Yılmaz, 2019; Lopez,Domingo ve Torrijos, 2021). Veri koruma etki analizi tek sefere mahsus bir yükümlülük değildir (Tüzük m. 35/11). Özellikle dinamik ve sürekli değişime tabi olan veri işleme faaliyetleri kapsamında projenin yaşam döngüsü boyunca süreklilik gösteren bir yükümlülüktür (Article 29 Data Protection Working Party, 2017). Veri işleme faaliyetlerinin ve bunların etkilerinin hızlıca değişebilen niteliği sebebiyle her zaman yeni güvenlik açıklarının ortaya çıkabileceği dikkate alındığında, veri koruma etki analizinin güncellenmesi veri güvenliğinin sağlanabilmesi amacıyla da gerekli görülmektedir (Article 29 Data Protection Working Party, 2017). Bunun yanında, veri sorumlusu, en azından veri işleme faaliyetinin teşkil ettiği risk açısından bir değişiklik meydana gelmesi halinde, işleme faaliyetinin veri koruma etki analizi kapsamında varılan sonuca uygun olarak gerçekleştirilip gerçekleştirilmediğini de değerlendirmelidir (Tüzük m. 35/11).

Veri koruma etki analizinin ne şekilde gerçekleştirileceği Tüzük'te doğrudan düzenlenmemiştir. Gerekli analizin hangi adımlar uygulanarak gerçekleştirileceği ve tercih edilecek yöntem her somut olay kapsamında ilgili veri işleme faaliyetinin özellikleri dikkate alınarak belirlenmelidir (Yordanov, 2017). Veri koruma etki analizi gerçekleştirilirken veri koruma görevlisinin tavsiyeleri ve uygun hallerde, ticari menfaatlerin veya kamu menfaatlerinin korunmasına ya da işleme faaliyetlerinin güvenliğine zarar gelmeyecek şekilde, ilgili kişilerin görüşleri de alınmalıdır (Tüzük m. 35/2, 35/9). Analiz sonuçlarının güvenilirliğinin ve etkinliğinin artırılması için çok disiplinli bir yaklaşım uygulanarak hem hukuk hem de teknik yönünden kapsamlı bir değerlendirme yapılması önemlidir (Bieker, Martin, Friedewald ve Hansen 2018; Sarrat ve Brun, 2018; Metin ve arkadaşları, 2019; Lopez ve arkadaşları 2021). Yapılacak analiz kapsamında somut olaya göre tek bir veri işleme faaliyetinin veya mahiyet, kapsam, bağlam,

amaç ve riskler açısından benzerlik gösteren birden çok veri işleme faaliyetinin değerlendirilmesi mümkündür. (Tüzük m. 35/1). Örneğin, kamu kurumlarının ortak bir uygulama veya işleme platformu kurmayı amaçladığı ya da birden fazla veri sorumlusunun bir endüstri sektöründe veya genelinde yürütülecek genel bir faaliyet kapsamında ortak bir uygulama veya işleme platformu kurmayı amaçladığı durumlarda veri koruma etki analizinin konusunun tek bir veri işleme faaliyetinden daha kapsamlı olması makul ve daha ekonomik olabilecektir (Tüzük Gerekçe 92). Örnekleri çoğaltacak olursak, tek başına veri sorumlusu olan bir demiryolu operatörü, tren istasyonlarının tamamında uygulayacağı güvenlik kamerası kullanımı için tek bir veri koruma etki analizi gerçekleştirebileceği gibi birden fazla belediye tarafından benzer bir kapalı devre kamera sistemi kullanılması halinde de farklı veri sorumluları tarafından gerçekleştirilecek bu veri işleme faaliyetleri kapsamında tek bir veri koruma etki analizi yapılması makul olabilir (Article 29 Data Protection Working Party, 2017).

Veri koruma etki analizi sonucunda yapılan değerlendirmeler bir rapor halinde ortaya konulmalıdır. Oluşturulacak değerlendirme raporunda asgari olarak yer alması gereken hususlar (i) planlanan işleme faaliyetinin ve mümkün olduğu hallerde veri sorumlusunun menfaati de dahil olmak üzere işleme amaçlarının sistematik bir açıklaması, (ii) işleme faaliyetinin ulaşılmak istenen amaçlar doğrultusunda gerekli ve ölçülü olup olmadığının değerlendirmesi, (iii) ilgili kişilerin hak ve özgürlüklerine yönelik risklerin değerlendirmesi ve (iv) bu risklere karşı alınması planlanan tedbirler olarak düzenlenmiştir (Tüzük m. 35/7). Bunların yanında, hukuki, teknik ya da işletmesel sebeplerle başka noktalara değinilmesinde fayda görülüyorsa raporda ayrıca bunlara da yer verilmelidir (Aşıkoğlu, 2018; Çekin, 2020). Farklı veri sorumluları tarafından yürütülen benzer veri işleme faaliyetleri kapsamında tek bir veri koruma etki analizi gerçekleştirilmesi halinde, analiz sonunda oluşturulacak rapor, çalışmanın farklı veri sorumluları tarafından ortak yürütülmüş olmasının gerekçelerine ilişkin açıklamaları da içermelidir (Article 29 Data Protection Working Party, 2017).

Veri koruma etki analizi sonucunda, veri işleme faaliyetinin, veri sorumlusu tarafından uygulanacak gerekli tedbirler olmadığı takdirde ilgili kişilerin hak ve özgürlükleri açısından yüksek risk taşıdığının tespit edilmesi halinde, veri sorumlusunun işleme faaliyetine başlamadan önce veri koruma otoritesine danışması gerekmektedir (Tüzük m. 36/1). Veri koruma otoritesi, söz konusu veri işleme faaliyetinin Tüzük'ü ihlal edeceği ve veri sorumlusunun ilgili riskleri belirlemekte ve azaltmakta yetersiz kaldığı görüşünde olması halinde, veri sorumlusuna ve varsa veri işleyene yazılı tavsiyede bulunmaktadır. Bunun yanında veri koruma otoritesi bu halde Tüzük'ün 58. maddesinde düzenlenen haklarını kullanma yetkisine sahiptir (Tüzük m. 36/2).

VERİ KORUMA ETKİ ANALİZİ İLE YÜKSEK RİSK KAVRAMININ İLİŞKİSİ

Veri koruma etki analizi, Tüzük'e hakim risk temelli yaklaşıma da uygun olarak, her veri işleme faaliyeti için değil, yalnızca gerçek kişilerin hak ve özgürlükleri açısından yüksek risk teşkil eden işleme faaliyetleri için bir yükümlülük olarak düzenlenmiştir (Article 29 Data Protection Working Party, 2017). Söz konusu hak ve özgürlükler yalnızca veri koruma ve mahremiyet hakkıyla sınırlı değildir. Aynı zamanda ifade özgürlüğü, düşünce özgürlüğü, hareket özgürlüğü, ayrımcılık yasağı, özgürlük, vicdan ve din hakkı gibi diğer temel hakları da kapsamaktadır (Article 29 Data Protection Working Party, 2017). Veri sorumlusu öncelikle işleme faaliyetinin sebep olabileceği riskleri tespit etmeli, daha sonra bu riskleri değerlendirmeli ve bunların yüksek risk olduğunun tespit edilmesi halinde bunları kabul edilebilir bir düzeye indirmek amacıyla gerekli tedbirleri almalıdır (Demetzou, 2019).

Kişisel verilerin işlenmesi niteliği gereği her zaman risk içermektedir ancak tüm veri işleme faaliyetleri aynı etkide risk teşkil etmediğinden veri sorumlularının her veri işleme faaliyeti için aynı tedbirleri uygulaması gerektiği düşünülemez (Demetzou, 2019). Dolayısıyla, kişisel verilerin korunmasına etkin fayda sağlayacak bir veri koruma etki analizi gerçekleştirilebilmesi için öncelikle kişisel verilerin korunması kapsamında neyin risk teşkil ettiğine ve söz konusu riskin olasılığının ve ciddiyetinin nasıl değerlendirileceğine ilişkin nesnel ve ortak bir anlayışa sahip olunması gerekmektedir (Demetzou, 2019).

Avrupa Birliği mevzuatı risk kavramını tanımlarken örneklendirme yöntemini tercih etmiştir. Tüzük'ün gerekçesine göre kişisel verilerin korunması kapsamındaki olası riskler ayrımcılık, kimlik hırsızlığı veya dolandırıcılık, maddi zarar, itibarın zedelenmesi, mesleki gizlilik kapsamında korunan kişisel verilerin gizliliğinin yitirilmesi, psödönimizasyonun yetkisiz olarak geri alınması ve diğer önemli sosyal ve ekonomik dezavantajlar olarak örneklendirilmiştir (Tüzük Gerekçe 75). Bunun yanında, Tüzük'ün 35. maddesi de, bunlarla sınırlı olmamak üzere, veri işlemenin gerçek kişilerin hak ve özgürlükleri açısından yüksek risk doğurmasının muhtemel olduğu faaliyetleri (i) gerçek kişiler üzerinde, profil çıkarma dahil otomatik bireysel kararlar alma amacıyla sistematik ve kapsamlı olarak işleme yapılması ve söz konusu kararların gerçek kişileri ilgilendiren hukuki sonuçlar doğurması veya kayda değer şekilde etkilemesi, (ii) özel nitelikli kişisel verilerin veya ceza mahkumiyeti ve suçlara ilişkin kişisel verilerin geniş kapsamlı işlenmesi ve (iii) kamuya açık alanların büyük ölçekte ve sistematik bir şekilde izlenmesi olarak örneklendirmiştir (Tüzük m. 35/3). Gerçek kişilerin hak ve özgürlükleri açısından yüksek risk doğurma olasılığı bulunan veri işleme faaliyetleri bunlarla sınırlı değildir (Article 29 Data Protection Working Party, 2017).

Article 29 Data Protection Working Party ve European Data Protection Supervisor, hangi veri işleme faaliyetlerinin veri koruma etki analizi gerçekleştirilmesini gerektireceği konusunda yol gösterici olması amacıyla kapsamlı çalışmalar gerçekleştirmiştir ve Tüzük'ün gerekçesini de göz önünde bulundurarak gerekli değerlendirmenin yapılabilmesi için dikkate alınması önerilen dokuz kritere dikkat çekmiştir (Article 29 Data Protection Working Party, 2017; European Data Protection Supervisor, 2018). Bu çalışmalarda açıklanan kriterler ve bunlara göre bir veri işleme faaliyetinin veri koruma etki analizi gerektirip gerektirmediğine ilişkin örneklerin bir kısmı aşağıdaki tabloda gösterilmektedir.

Tablo 1
Risk Değerlendirmesinde Dikkate Alınması Önerilen Dokuz Kriter ve Bunlara İlişkin Örnekler

	Yüksek Riskin Varlığı Değerlendirilirken Dikkate Alınacak Kriter	**İlgili Kriteri Sağlayan Veri İşleme Faaliyetine Örnekler**	**İlgili Kriteri Sağlamayan Veri İşleme Faaliyetine Örnekler**
1.	Özellikle ilgili kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketleri ile ilgili yönlerden profil çıkarma ve tahminde bulunma da dahil olmak üzere, değerlendirme veya puanlama	Bir finans kurumunun müşterilerini bir kredi referans veri tabanında veya kara para aklama ve terörle mücadele finansmanı (AML/CTF) veya dolandırıcılık veri tabanında taraması	Standart değerlendirme görüşmeleri yapılması, personelin eğitim planları geliştirmesine yardımcı olmak amacıyla 360° değerlendirmeler yapılması
		Bir biyoteknoloji şirketinin kişilerin hastalık/sağlık risklerini değerlendirmek ve tahmin etmek için doğrudan tüketicilere genetik testler sunması	
		Bir şirketin internet sitesindeki kullanıma veya gezinmeye dayanarak davranışsal pazarlama profilleri oluşturması	
		Bir bankanın olası dolandırıcılık işlemlerini tespit etmek için yürürlükteki yasalara uygun olarak işlemleri incelemesi	
2.	İlgili kişi hakkında hukuki sonuçlar veya benzer şekilde	Bireylere karşı dışlanmaya veya ayrımcılığa yol açacak işlemeler	Bir haber sitesinin makaleleri kullanıcının geçmiş

	önemli ölçüde etkisi olan sonuçlar üreten otomatik kararlar alma	"Eğer ele alınan vaka sayısı açısından ekibin en düşük %10'luk kısmındaysanız, değerlendirmenizde tartışmasız bir şekilde "yetersiz" notu alırsınız" gibi otomatik sonuçlar üreten personel değerlendirmeleri	ziyaretlerine göre bir sırayla göstermesi
3.	Ağlar aracılığıyla toplanan veriler veya kamuya açık bir alanın sistematik olarak izlenmesi de dahil olmak üzere, ilgili kişileri gözlemlemek, denetlemek veya kontrol etmek amacıyla kullanılan sistematik izleme	Gizli şekilde kapalı devre kamera sistemi kullanılması	Garaj girişinde kamusal alanı görüntülemeyen görünür kapalı devre kamera sistemi kullanılması
		Kamuya açık alanlarda yüz tanıma yazılımı içerenler gibi akıllı kapalı devre kamera sistemi kullanılması	
		SSL şifrelemesini kıran veri kaybı önleme araçlarının kullanılması	
4.	Özel nitelikli kişisel veriler ve ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili kişisel veriler de dahil olmak üzere hassas veya son derece kişisel nitelikteki verilerin işlenmesi	Bir hastanenin hastaların genetik verilerini ve sağlık verilerini işlemesi	Yüz tanıma veya diğer hassas verileri ortaya çıkarma amacıyla kullanılmadığı sürece fotoğrafların işlenmesi
		Bir özel soruşturmacının araştırdığı kişilere ait veya bir devlet eğitim kurumunun öğrencilere ait ceza mahkumiyetleri ya da suçlara ilişkin detayları tutması	
		İşe alım öncesinde tıbbi muayene ve sabıka kaydı kontrolü gerçekleştirilmesi	
		1:n biyometrik tanımlamanın herhangi bir kullanımı	
5.	Büyük ölçekte veri işleme[1]	Hastalıkların izlenmesi amacıyla ülke genelindeki veya Avrupa	Dahili telefon rehberi kullanılması

1 Tüzük'te büyük ölçekte veri işlemenin bir tanımı bulunmamaktadır. Article 29 Data Protection Working Party, büyük ölçekte veri işlemenin söz konusu olup olmadığı değerlendirilirken (i) belirli bir sayı veya ilgili nüfusun belirli bir oranı olarak ilgili kişilerin sayısının, (ii) veri hacminin ve/veya işlenen farklı veri ögelerinin aralığının,

		genelindeki veri tabanlarının kullanılması	
		Pazarlama ve farklı amaçlarla kullanılmak için çok büyük "yaşam tarzı veri tabanları" oluşturulması	
		Bakanlıklar veya yerel ya da bölgesel kurumlar gibi kamu kontrolörleri arasında büyük ölçekli veri alışverişi yapılması	
6.	Farklı amaçlarla ve/veya farklı veri sorumluları tarafından gerçekleştirilen iki veya daha fazla veri işleme faaliyeti sonucunda oluşan veri setleri de dahil olmak üzere, veri setlerinin eşleştirilmesi veya birleştirilmesi	Erişim kontrol kayıtlarının gizli şekilde çapraz kontrol edilmesi	Kurum değişikliği sonrasında kişisel dosyanın aktarılması
		Bir işverenin devamsızlığı tespit etmek amacıyla erişim kontrol kayıtlarını, bilgisayar kayıtlarını ve esnek zaman bildirimlerini gizli şekilde çapraz kontrol etmesi	
7.	Çocuklar, çalışanlar ve akıl sağlığı yerinde olmayanlar, sığınmacılar, hastalar, yaşlılar gibi nüfusun özel korumaya ihtiyaç duyan hassas kesimleri de dahil olmak üzere, ilgili kişinin ve veri sorumlusunun konumu değerlendirildiğinde dengesizlik tespit edilen her türlü durumdaki korunmasız ilgili kişilerin verilerinin işlenmesi	Korunmasız ilgili kişilerin kişisel verilerinin işlenmesi	Çalışanlar standart prosedürlere ilgili olarak işverenlerine karşı doğrudan korunmasız olarak değerlendirilemez
		Çalışanların faaliyetlerinin uzaktan izlenmesini sağlayan video gözetim ve konum belirleme sistemlerinin kullanılması	
8.	Yenilikçi teknoloji kullanımı veya yeni teknolojik ya da	Gelişmiş fiziksel erişim kontrolü sağlanması amacıyla parmak izi ve	

(iii) veri işleme faaliyetinin süresinin veya kalıcılığının ve (v) işleme faaliyetinin coğrafi kapsamının dikkate alınmasını önermektedir (Article 29 Data Protection Working Party, 2017).

	organizasyonel çözümler uygulanması	yüz tanıma kullanımının birleştirilmesi	Parmak izlerini kullanarak 1:1 biyometrik erişim kontrolü
		Biyometrik verileri işlenmesi ve mobil cihaz takibi gibi çalışanların zamanını ve katılımını izlemeyi amaçlayan yeni teknolojilerin kullanılması	
		"Nesnelerin İnterneti" uygulamaları kullanılarak elde edilen verilerin, bu verilerin kullanılmasının bireylerin günlük yaşamlarının ve mahremiyetlerinin üzerinde önemli bir etkisi olması halinde işlenmesi	
		Makine öğrenimi	
		Bağlantılı arabalar teknolojisi	
9.	İşlemenin kendi başına ilgili kişilerin bir hakkı kullanmasını veya bir hizmet ya da sözleşmeyi kullanmasını engellemesi	Bir bankanın müşterilerine kredi verip vermeyeceğine karar vermek için müşterilerini bir kredi referans veri tabanında taraması	İlgili kişi bir hizmete dahil edildikten sonra gurbetçilik veya bakmakla yükümlü olunan çocuk ödenekleri gibi haklarının belirlenmesi
		Dışlama veri tabanlarının kullanılması	

Bir veri işleme faaliyetine ilişkin olarak veri koruma etki analizi gerçekleştirilmesi gerekip gerekmediği incelenirken yukarıda belirtilen dokuz kriter kapsamında bir değerlendirme yapılması ve söz konusu veri işleme faaliyetinin iki veya daha fazla kriteri barındırması halinde veri koruma etki analizi gerçekleştirilmesi gerektiği belirtilmektedir (Article 29 Data Protection Working Party, 2017; European Data Protection Supervisor, 2018). Bir veri işleme faaliyeti ne kadar fazla kriteri barındırıyorsa ilgili kişilerin hakları ve özgürlükleri için yüksek bir risk oluşturma ve bu nedenle de veri koruma etki analizi gerektirme olasılığı o kadar yüksek olacaktır (Article 29 Data Protection Working Party, 2017). Ancak her halde, Article 29 Data Protection Working Party ve European Data Protection Supervisor tarafından belirtilen bu kriterlerin dikkate alınması, ilgili veri işleme faaliyetinin değerlendirilmesi için tek başına yeterli görülmemelidir. Veri sorumlusu gerekli değerlendirmeyi yaparken bu kriterlerin incelenmesine ek olarak, veri koruma konusundaki uzmanlardan destek alınması gibi çeşitli yöntemlerle daha kapsamlı bir değerlendirme yapılması gerekip gerekmediğini de göz önünde tutmalıdır (Sarrat ve Brun, 2018). Nitekim, veri sorumlusu tek bir kriterin varlığını veri koruma etki analizi gerçekleştirilmesi için yeterli görme veya gerekçeleriyle ortaya koyarak, belirtilen kriterlerden iki veya daha fazlasını içermesine rağmen söz konusu veri işleme faaliyetinin yüksek riskin oluşmasına sebebiyet vermeyeceğine kanaat getirme imkanına sahiptir (Article 29 Data Protection Working Party, 2017; European Data Protection Supervisor, 2018).

VERİ KORUMA ETKİ ANALİZİNİN TÜRK HUKUKU BAKIMINDAN DEĞERLENDİRİLMESİ

Türk hukukunda kişisel verilerin korunmasına ilişkin düzenlemeler esas olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu ile yapılmıştır. Kanunun 4. Maddesi uyarınca kişisel verilerin işlenmesi sırasında uyulması gereken genel veri koruma ilkeleri (i) hukuka ve dürüstlük kurallarına uygun olma, (ii) doğru ve gerektiğinde güncel olma, (iii) belirli, açık ve meşru amaçlar için işlenme, (iv) işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve (v) ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme olarak belirlenmiştir. Hesap verebilirlik ilkesi ve veri koruma etki analizi gibi hesap verebilirlik ilkesinin destekleyicisi olan uyum araçları Kişisel Verilerin Korunması Kanunu'nda düzenlenmemiştir.

Öte yandan, Kişisel Verileri Koruma Kurumu ("Kurum") uygulamalarını sürdürürken misyon ve vizyonu kapsamındaki temel ilke ve değerleri arasında benimsediği şeffaflık ve hesap verebilirlik ilkesini de dikkate almaktadır. Kurum'un 2019/78 numaralı kararında doğrudan hesap verebilirlik ilkesine atıf yapılmaktadır. Yapay zeka alanında faaliyet gösteren geliştiriciler, üreticiler, servis sağlayıcılar ve karar alıcılar için öneriler içeren Yapay Zeka Alanında Kişisel Verilerin Korunmasına

Dair Tavsiyeler kapsamında kişisel veri işleme temelli yapay zeka çalışmalarında, kişisel verilerin korunması açısından yüksek risk öngörülüyorsa, mahremiyet etki değerlendirmesi uygulanması ve veri işleme faaliyetinin hukuka uygunluğuna bu çerçevede karar verilmesi tavsiye edilmiştir. Bunların yanında, Kurum, bağlayıcı şirket kuralları kapsamında yapılacak başvurularda kullanılmak üzere hazırladığı Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman'da "Hesap Verebilirlik ve Diğer Esaslar/Araçlar" başlığı altında, veri sorumlusunun uyumluluğunun artırılması ve gerektiğinde gerçek kişilerin hak ve özgürlükleri bakımından yüksek risk oluşturması muhtemel olan veri işleme faaliyetleri için risk analizi yapılması gerektiğini ve yapılan risk analizine göre, veri sorumlusu tarafından riski hafifletmek için gerekli tedbirlerin alınmamış olması ve veri işlemenin yüksek risk doğuracağının ortaya çıkması durumunda, veri işleme faaliyetinden önce Kurum'a danışılması gerektiğini belirtmektedir. Kurum'un uygulamalarına bakıldığında hesap verebilirlik ilkesinin ve ilgili uyum araçlarının Avrupa Birliği veri koruma hukukuyla paralel şekilde yorumlandığı anlaşılmaktadır (Kaya, 2020); bu durum uygulamada Kişisel Verilerin Korunması Kanunu ve Tüzük arasındaki uyumluluğun artırılması yönünden olumlu değerlendirilebilecektir. Ancak her ne kadar Kurum, uygulama ve tavsiyelerinde Kişisel Verilerin Korunması Kanunu'nun ruhundan yola çıkarak hesap verebilirlik ilkesine ve hatta spesifik olarak veri koruma etki analinize benzer yapılara yer verse de bu ilke ve yükümlülüklerin yasal olarak tanımlanması önem arz ermektedir. Zira açıklandığı üzere hesap verebilirlik ilkesi ve bu kapsamdaki yükümlülüklerden birisi olarak düzenlenen veri koruma etki analizi kişisel verilerin korunmasına ilişkin önemli sonuçlar doğurmaktadır. Hukuki güvenlik ve belirlilik ilkesi ve kişisel veri koruma hukuku yaklaşımının değiştirilmesi gerekliliği göz önüne alındığında, etkin bir fayda sağlanması ancak bu hususların kanunun lafzında yer alarak benimsenmesiyle mümkün olacaktır.

Hesap verebilirlik ilkesinin ve bununla ilişkili düzenlemelerin Kişisel Verilerin Korunması Kanunu'nda var olmamasının sebebi, 95/46 sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi'nin esas alınmış olması olarak görülmektedir (Kaya, 2020). Türkiye Cumhuriyeti Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı tarafından düzenlenen On Birinci Kalkınma Planı (2019-2023) kapsamında Kişisel Verilerin Korunması Kanunu'nun Tüzük dikkate alınarak güncellenmesi hedeflenmektedir. Bu doğrultuda gerçekleştirilecek değişiklikler kapsamında hesap verebilirlik ilkesinin ve uyum araçlarının da Türk hukukunda düzenlenmesi beklenmektedir (Kaya, 2020).

Avrupa Birliği veri koruma hukukunda düzenlenen uyum araçlarının temel faydası, gelişen teknolojiler kapsamında kişisel verilerin işlenmesinin doğurduğu riskler karşısında gerçek kişilerin temel hak ve özgürlüklerinin daha güçlü şekilde korunmasının temin edilmesidir. Teknolojik gelişmelerin

durmaksızın gelişmeye devam ettiği göz önüne alındığında ilgili mevzuatların gelecekte ortaya çıkabilecek yeni risk ve tehditler dikkate alınarak geliştirilmesi kişisel verilerin etkin bir şekilde korunmaya devam edilebilmesi için gereklidir (Aşıkoğlu, 2018; Çimen Bulut, 2020). Şüphesiz bu gereklilik Türk veri koruma hukuku için de geçerlidir.

Türkiye'de kişisel verilerin korunması kapsamında uygulamadaki sorunların başında kişisel veri işleme süreçlerinin hukuka uygun şekilde sürdürülmesinin sağlanması ve kişisel verilerin hukuka uygun şekilde işlendiğinin ispat edilmesi gelmektedir (Kaya, 2020). Veri koruma ilkelerinin ve veri koruma hukukundan doğan yükümlülüklerin veri işleme faaliyeti içeren sistemlerin kuruluş anında değerlendirilmesi bu faaliyetlerin sonradan uyumlu hale getirilmesi sorununu önlemektedir (Aşıkoğlu, 2018). Henüz zarar meydana gelmeden müdahale etmeye elverişli bulunmayan mevcut yapı, büyük miktarda verinin (big data) işlenmesini öngören yeni teknolojiler kapsamında gereken uyumu sağlayamayacaktır (Çekin, 2016). Uygulamadaki sorunların önüne geçilebilmesi ve kişisel verilerin etkin şekilde korunabilmesi için veri işlemenin doğurduğu riskleri tasarımdan itibaren dikkate alan proaktif yapıda bir mekanizma düzenlenmesi önerilmektedir (Çekin, 2016).

Veri koruma etki analizi, veri sorumlularının ilgili işleme faaliyetine başlamadan önce kendi kendini denetlemesini sağladığından gerçek kişiler nezdinde meydana gelebilecek risklerin bertaraf edilmesinde etkin fayda sağlayan bir uyum aracı olarak değerlendirilmektedir (Metin ve arkadaşları, 2019; Kartöz, 2020) Veri koruma etki analizinin Türk hukukunda düzenlenmesi mevzuatımızın geliştirilmesi için önemli bir adım olacaktır. Veri koruma hukuku düzenlemelerinin kişisel verilerin korunmasına etkin fayda sağlayacak bir şekilde uygulamaya geçirilmesinin sağlanabilmesi için yaptırıma dayalı bir hukuk mekanizmasındansa veri sorumlularının veri koruma kültürünü benimsemesini ve iç süreçlerini buna göre geliştirmesini teşvik eden bir yaklaşım tercih edilmelidir (Aşıkoğlu, 2018; Ni Loideain ve Adams, 2020). Bu kapsamda veri koruma etki analizinin Türk veri koruma hukukuna sürdürülebilir bir şekilde kazandırılması için, veri sorumlularının, veri işleme faaliyetlerinin gerçek kişilerin temel hak ve özgürlükleri açısından meydana getirebileceği riskler ve bunların önlenmesi için gerekli çalışmaların yapılmasının önemi konusunda bilinçlendirilmesi gerekecektir. Etkin fayda sağlayacak bir veri koruma etki analizi gerçekleştirilebilmesi için risklerin nasıl tespit edileceği ve değerlendirileceği, analiz gerçekleştirmenin yöntemi belirlenirken nelere dikkat edileceği, analiz sonucunda oluşturulacak raporda hangi hususlara yer verilmesi gerektiği ve bu raporun hangi durumlarda yayınlanması gerektiği gibi konularda yol gösterici düzenlemeler yapılması yerinde olacaktır. Bu kapsamda veri koruma otoritelerinin rehberlikleri, yönlendirmeleri ve denetim yetkileri önem arz etmektedir (Ni Loideain ve Adams, 2020). Veri koruma etki analizi uygulamasının veri sorumluları tarafından benimsenebilmesi ve iç süreçlerinin buna göre şekillendirilebilmesi için veri koruma otoritelerine danışılmasının ve

uzmanlardan destek alınmasının teşvik edilmesi faydalı olacaktır (Kartöz, 2020) Veri koruma etki analizi yapılmasının yalnızca ilgili işleme faaliyetinin gerçek kişilerin hak ve özgürlükleri açısından yüksek risk teşkil etmesi olasılığı kapsamında yükümlülük olarak düzenlenmesi halinde dahi, veri sorumlularının yükümlü olmasalar bile veri koruma etki analizi gerçekleştirmelerinin teşvik edilmesinde fayda vardır. Zira bu uygulama veri sorumlusunun ilgili veri koruma mevzuatına ne ölçüde uyumlu olduğunu da ortaya koyan bir süreçtir (Yordanov, 2017; Metin ve arkadaşları, 2019).

Türk veri koruma hukuku düzenlemelerinin uygulamada etkili bir şekilde benimsenmesinin sağlanması için ayrım gözetmeyen genel bildirim yükümlülükleri yerine veri işleme faaliyetlerinin doğurabileceği risklerin önlenmesine odaklanan etkili prosedürler kullanılmalıdır (Kartöz, 2020) Öte yandan Avrupa Birliği veri koruma hukukunda sicil yükümlülüğü kaldırılmışken Türk hukukunda bunun tersine bir düzenlemenin uygulanmasının Avrupa Birliği mevzuatına uyumluluk açısından sorunlara sebep olabileceği de göz önüne alınmalıdır (Çekin, 2020).

SONUÇ

Gerçek kişilerin temel hak ve özgürlüklerinin, kişisel verilerin elde edilmesi ve kullanılmasına ilişkin yöntemler kapsamında her geçen gün farklılaşan kişisel veri işleme süreçleri içeren gelişen teknolojiler karşısında korunabilmesi veri koruma hukuku düzenlemeleri ile yakından ilgilidir. Bu doğrultuda kişisel veri işlemenin doğurduğu risklere karşı etkin koruma sağlanabilmesi için veri koruma düzenlemelerinin işlevsel mekanizmalara ve uyumluluğu teşvik edici bir yaklaşıma sahip olması gerekmektedir. Bu amaç çerçevesinde Avrupa Birliği veri koruma hukukunda hesap verebilirlik ilkesi ve bu ilkeyi destekleyen uyum araçları benimsenmiştir.

Türk hukukunda Kişisel Verilerin Korunması Kanunu'nun özellikle büyük verinin (big data) işlenmesini gerektiren yapay zeka sistemleri gibi yeni teknolojiler karşısında etkin fayda sağlayabilmesi için bazı yönlerden geliştirilmesi gerekmektedir. Nitekim Türkiye Cumhuriyeti Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı tarafından düzenlenen On Birinci Kalkınma Planı (2019-2023) kapsamındaki hedeflerden biri de Kişisel Verilerin Korunması Kanunu'nun Tüzük dikkate alınarak güncellenmesidir.

Bu çalışmada Avrupa birliği veri koruma hukukunda veri sorumlularının iç süreçlerine etki ederek sorumluluklarının artırılması konusunda etkin fayda sağladığı değerlendirilen bir uyum aracı olan veri koruma etki analizi incelenerek Türk hukuku bakımından değerlendirilmiştir. Veri koruma etki analizinin Türk hukukunda da benimsenmesinin uygulamadaki sorunların çözümü için fayda sağlayacağı düşünülmektedir. Ancak Avrupa Birliği hukukunda düzenlenen uyum araçlarının hesap verebilirlik ilkesiyle birlikte bir bütün teşkil ettiği unutulmamalıdır. Türk veri koruma hukukunda da

teknolojik gelişmelere bağlı olarak gelecekte ortaya çıkabilecek yeni risklerin önlenmesine odaklanan proaktif bir yapı benimsenmelidir. Bu yapının etkin fayda sağlayabilmesi için veri sorumlularının, veri işleme faaliyetlerinin gerçek kişilerin temel hak ve özgürlükleri açısından doğurabileceği risklerin bilincinde olması ve iç süreçlerini bunların önlenmesini amaçlayarak geliştirmesi gerekmektedir. Bu doğrultuda, veri koruma kültürünün benimsenmesinin sağlanması için gerçekleştirilecek mevzuat çalışmalarının kapsamı ve bunların veri sorumluları tarafından anlaşılmasının sağlanması amacıyla Kişisel Verileri Koruma Kurumu'nun rehberliği büyük önem arz etmektedir.

KAYNAKLAR

Article 29 Data Protection Working Party. (2017). 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. https://ec.europa.eu/newsroom/article29/items/611236/en

Aşıkoğlu, Ş. İ. (2018). Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri. İstanbul: On İki Levha Yayıncılık.

Bieker, F., Martin, N., Friedewald, M. ve Hansen, M. (2018). Data Protection Impact Assessment: A Hands-On Tour of the GDPR's Most Practical Tool. Privacy and Identity Management. The Smart Revolution. 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Ispra, Italy, September 4-8, 2017, Revised Selected Papers. ed. Marit Hansen - Eleni Kosta - Igor Nai Fovino - Simone Fischer Hübner. Springer, Cham. 207-220. DOI: https://doi.org/10.1007/978-3-319-92925-5_13.

Çekin, M. (2016). 6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi. İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 74 (2), 629-644.

Çekin, M. S. (2020). Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku. İstanbul: On İki Levha Yayıncılık.

Çimen Bulut, İ. (2020). Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları. Anadolu Üniversitesi Sosyal Bilimler Dergisi 20 (2), 127-142. DOI: https://doi.org/10.18037/ausbd.758041.

Demetzou, K. (2019). Data Protection Impact Assessment: A tool for accountability and the unclarified concept of "high risk" in the General Data Protection Regulation. Computer Law & Security Review 35 (6). DOI: https://doi.org/10.1016/j.clsr.2019.105342.

Dülger, M. V. (2020). Kişisel Verilerin Korunması Hukuku. İstanbul: Hukuk Akademisi.

European Data Protection Supervisor. (2012). Opinion of the European Data Protection Supervisor on the Data Protection Reform Package. https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf

European Data Protection Supervisor. (2018). Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments. https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_1_en_0.pdf

Kartöz, M. O. (2020). Şeffaflık ve Hesap Verilebilirlik Açısından Kişisel Verilerin Korunması ve Yapay Zeka. (Yüksek Lisans Tezi). İstanbul Üniversitesi, İstanbul.

Kaya, M. B. (2020). Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi. İstanbul Hukuk Mecmuası 78(4), 1859-1897. DOI: https://doi.org/10.26650/mecmua.2020.78.4.0005

Lopez, C. T., Domingo, I. A. ve Torrijos, J. V. (2021). Approaching the Data Protection Impact Assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals. A

special reference to Identity Management systems. ARES 2021: The 16th International Conference on Availability, Reliability and Security. Association for Computing Machinery. DOI: https://doi.org/10.1145/3465481.3469207

Metin, B., Erkan, S., Atasu, İ. ve Yılmaz, E. (2019). Privacy Impact Assessment as a Tool for GDPR Compliance Preparation. Kişisel Verileri Koruma Dergisi, 1(2): 75-86. https://dergipark.org.tr/tr/pub/kvkd/issue/50609/646782.

Ni Loideain, N. ve Adams, R. (2020). From Alexa to Siri and the GDPR: The gendering of Virtual Personal Assistants and the role of Data Protection Impact Assessments. Computer Law & Security Review 36. DOI: https://doi.org/10.1016/j.clsr.2019.105366

Sarrat, J. ve Brun, R. (2018). DPIA: How to Carry Out One of the Key Principles of Accountability. Privacy Technologies and Policy: 6th Annual Privacy Forum, APF 2018, Barcelona, Spain, June 13-14, 2018, Revised Selected Papers. ed. Manel Medina-Andreas Mitrakas-Kai Rannenberg-Erich Schweighofer-Nikolaos Tsouroulas. Springer, Cham. 172-182. DOI: https://doi.org/10.1007/978-3-030-02547-2_10

Yordanov, A. (2017). Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation. European Data Protection Law Review 3 (4), 486-495. DOI: https://doi.org/10.21552/edpl/2017/4/10