İSTANBUL ÜNİVERSİTESİ YAYINEVİ

İstanbul Hukuk Mecmuası, 78 (4), 1859-1897

DOI: 10.26650/mecmua.2020.78.4.0005
http://dergipark.gov.tr/iuhfm
http://mecmua.istanbul.edu.tr/tr/_

İstanbul Hukuk Mecmuası

Başvuru: 06.09.2020
Kabul: 09.01.2021

ARAŞTIRMA MAKALESİ / RESEARCH ARTICLE

Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi

Mehmet Bedii Kaya*

Öz

Siber risklerin değişen niteliği, analitik ve yapay zekâ uygulamalarıyla kişisel verilerin işlenmesinin yaygınlaşması, veri işleme ve saklama ortamlarının çeşitlenmesi, sektörel düzenlemelerin artması, klasik veri koruma yaklaşımlarının yetersiz kalmasına sebep olmuştur. Bu bağlamda, değişen veri koruma ve mahremiyet düzlemlerinde ortaya çıkan yeni riskler ve sorunlar için etkin bir çözüm olarak hesap verebilirlik ilkesi ortaya çıkmıştır.

Hesap verebilirlik ilkesi, salt mevzuata uyumu aşan ve kavramsal derinliği haiz bir paradigma değişikliğidir. Bu ilke, veri sorumlularının, veri koruma düzenlemelerine uyum için uygun ve etkin tedbirleri almasını ve talep halinde de bunu ispat etmelerini gerektirmektedir. Diğer bir deyişle hesap verebilirlik ilkesi, kişisel verilerin korunmasının bir veri sorumlusu nezdinde sürekli gözetilen, etkin şekilde uygulanan ve düzenli olarak denetlenen bir değer olduğunun ispatı sürecidir.

Bu makalenin amacı, veri koruma hukuku bağlamında hesap verebilirlik ilkesini mukayeseli olarak incelemektir. Çalışma, hesap verebilirlik ilkesinin temelini ve kapsamını sorgulamayı, diğer veri koruma ilkeleriyle ilişkisini tespit etmeyi ve ilkenin veri sorumluları ile veri işleyenler üzerindeki normatif etkisini ortaya koymayı hedeflemektedir.

Anahtar Kelimeler
Hesap verebilirlik, Veri koruma, Mahremiyet, Uyum, İspat

The New Paradigm of Data Protection Law: The Principle of Accountability

Abstract

The inadequacy of classical data protection approaches have been uncloaked by the evolving nature of cyber risks, the tremendous increase in personal data processing through analytics and artificial intelligence technologies, the diversification of data processing and storage environments and the proliferation of sectoral regulations. The principle of accountability is proposed as the most efficacious solution to tackle new emerging risks and challenges in the changing landscape of data protection and privacy contexts.

The principle of accountability is a paradigm shift in data protection which has a conceptual breadth and magnitude that goes far beyond mere compliance. It requires data controllers to implement appropriate and effective measures to comply with the principles and obligations set out under data protection regulations and to further demonstrate this compliance on request. This is a process of proving that the protection of personal data is an essential value that is constantly observed, effectively applied, and regularly audited by data controllers.

This article aims to provide a thorough analysis of the principle of accountability in the context of data protection law by adopting a comparative approach. The article aims to scrutinise the scope and underpinnings of the principle, identify its relationship with other data protection principles, and discuss the normative effects of such a principle has on data controllers and data processors.

Keywords
Accountability, Data protection, Privacy, Compliance, Proof

* **Sorumlu Yazar:** Mehmet Bedii Kaya (Dr. Öğr. Üyesi), İstanbul Bilgi Üniversitesi, Hukuk Fakültesi, Bilişim ve Teknoloji Hukuku Ana Bilim Dalı, İstanbul, Türkiye. Eposta: mehmet@mbkaya.com ORCID: 0000-0001-5256-9854

Atıf: Kaya MB, "Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi" (2020) 78(4) İstanbul Hukuk Mecmuası 1859. https://doi.org/10.26650/mecmua.2020.78.4.0005

Extended Summary

The possibilities for the use of personal data have increased tremendously as a result of a data-wide range of analytics tools, the Internet of Things (IoT), artificial intelligence technologies and other similar methods. As highlighted by the Article 29 Working Party, the amount of personal data that exists, is processed and is further transferred continues to grow; the ever-increasing amount of personal information is accompanied by an increase in its value in social, political and economic terms; and breaches of personal information may have significant negative effects for data controllers in public and private sectors.

The proliferation of national, regional, and international regulations for better protection of personal data and privacy have impacted business operations, government administrations and the personal activities of individuals. The inadequacy of classical data protection approaches have been uncloaked by the evolving nature of cyber risks, the tremendous increase of personal data processing through analytics and artificial intelligence technologies, the diversification of data processing and storage environments and the proliferation of sectoral regulations. The principle of accountability is proposed as the most efficacious solution to tackle new emerging risks and challenges in the changing landscape of data protection and privacy contexts.

Accountability is a principle that exists in different national and international regulations, and its importance is increasing over time. For instance, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the pioneer instrument that addresses new and elevated privacy risks, prescribes the principle of accountability alongside other major data protection principles, such as collection limitation, data quality, purpose specification, use limitation, security safeguards, openness and individual participation principles. The OECD identified accountability as a key concept and underlined that a data controller should be held accountable for complying with measures which give effect to these principles.

While Convention 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) did not explicitly include the principle of accountability, it is argued that the modernised Convention 108, also called as Convention 108+, is based on the accountability principle. The modernised Convention imposes broader obligations on those who process data or have data processed on their behalf. Accordingly, accountability becomes an integral part of the protective scheme, with an obligation on controllers to be able to demonstrate compliance with the data protection rules.

The Article 29 Working Party has underlined that there is an increasing need and interest in ensuring that data controllers take effective measures to deliver real data protection. The Article 29 Working Party's discussions on the legal architecture of

accountability-based systems has paid off. The principle of accountability is currently articulated under Article 5(2) of the General Data Protection Regulation ("GDPR"). The GDPR lays down six distinct data protection principles and requires controllers to be responsible for and be able to demonstrate compliance with these principles. This compliance requirement is briefly referred to as 'accountability'.

Turkish Data Protection Law does not mention accountability among its principles, which is not surprising as Turkish Data Protection Law is modelled after Directive 95/46/EC. However, in the long term, accountability is expected to be included among other core data protection principles since the Turkish government, under the latest development plan, announced its intention to reform Data Protection Law in accordance with the GDPR.

The principle of accountability is a paradigm shift in data protection which has a conceptual breadth and magnitude that goes far beyond mere compliance. It requires data controllers to implement appropriate and effective measures to comply with the principles and obligations set out under data protection regulations and to further demonstrate this compliance on request. It is the process of proving that the protection of personal data is an essential value that is constantly observed, effectively applied, and regularly audited by data controllers. The principle of accountability imposes an increased duty of care on data controller and calls the data controller to act prudently according to changing risks. This principle is directly interlinked with other core data protection principles and creates a special liability regime. It could even be said that the principle encapsulates parts from all the data protection principles.

According to the Article 29 Working Party, common accountability measures may include the following non-exhaustive list: establishment of internal procedures; creation of written and binding data protection policies; maintenance of an inventory of data processing operations; appointment of a data protection officer; offering adequate data protection, training and education; implementing procedures to manage access, correction and deletion requests; establishment of an internal complaints handling mechanism; setting up internal procedures for the effective management and reporting of security breaches; performance of privacy impact assessments; and implementation and supervision of verification procedures. It is important to note that a data controller can determine the level of accountability that is desired to be achieved, which depends on the legal and institutional framework to which the controller is subject.

This article aims to provide a thorough analysis of the principle of accountability in the context of data protection law by adopting a comparative approach. The article aims to scrutinise the scope and underpinnings of the principle, identify its relationship with other data protection principles, and further discuss the normative effects of

such a principle has on data controllers and data processors. In the context of this analysis, the article will attempt to shed light on how to demonstrate compliance with requirements set out under data protection laws/regulations in a practical way.

Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi

"*Mevzuata uyumlu ve teknik olarak yapılması mümkün olan her şey, ahlaken sürdürülebilir olmayabilir.*" Giovanni Buttarelli[1]

Giriş

Bilgi ve iletişim teknolojilerinin hayatın her alanında kendisini hissettirdiği dijital dönüşüm, bu teknolojiler karşısında bireyi ve verilerini korumaya yönelik taleplerin artmasına, bu alanda yeni bir regülasyon dalgasının başlamasına sebep olmuştur. Kişisel verilerin en üst düzeyde korunmasına ilişkin dünyanın neredeyse tamamında gözlemlenen katı bir düzenleme eğilimi vardır.

Devletler, vatandaşlarının dijital mahremiyetlerini en üst düzeyde korumak için yasal düzenlemeler yapmakta, mevcut düzenlemelerini mevcut risklere göre güncellenmekte ve bu alanda kurallarını uluslararası antlaşmaların ışığında mümkün olduğunca yeknesaklaştırmaktadır.[2] Yeni kurallar yeni idari yapıların gerekliliğini de ortaya çıkarmış ve kişisel verilerin korunması alanındaki hukuki düzenlemeler daha ziyade bağımsız düzenleyici otoriteler eliyle icra edilmeye başlanmıştır.

Bilgi ve iletişim teknolojilerindeki dönüşüm, mevcut düzenlemelerin gözden geçirilmesinin ve regülasyon dalgasının momentumu olmuştur. Daha fazla verinin daha hızlı şekilde işlenmesine olanak tanıyan teknolojilerin yaygınlaşması ve nispeten makul ücretlerle bunların erişilebilir olması, 3G ile başlayan ve 5G ile farklı bir düzeye taşınan mobil bağlantıların yaygınlaşması, ağa bağlanan cihazların çeşitlenmesi ve her şeyin interneti (*Internet of Everything - IoE*) gibi teknolojilerin sağlıktan eğitime hayatın her alanında kullanılmaya başlanması, yapay zekâ teknolojilerinin yaygınlaşması, kullanılan sistemlerin iç içe geçmesi dönüşümü etkileyen temel teknik gelişmelerdir. Dijital dönüşüm tüm iş süreçlerini otomatikleştirmekte, otomatik olmayan veri işleme süreçlerini istisnai bir hale getirmektedir.

Hizmetlerin serbest dolaşımına ilişkin uluslararası ticaret hukuku kurallarının da etkisiyle dijital hizmet sağlayıcıların çok farklı coğrafyalara uzaktan hizmet sunmaya başlaması ise bu alandaki dönüşümü etkileyen en önemli gelişmelerden birisidir. Öyle ki, bir veri sorumlusu kişisel verinin elde edilmesi, sınıflandırması, anlamlandırılması veya sadece saklanması için farklı ülkelerde bulunan bazen veri işleyen bazen de ortak veri sorumlusu sıfatıyla hareket eden hizmet sağlayıcılarla

---

1 "*Not everything that is legally compliant and technically feasible is morally sustainable.*" Giovanni Buttarelli (1957-2019) (European Data Protection Supervisor), EDPS 'ICDPPC 2018 Debating Ethics: Dignity and Respect in a Data Driven Life (24 Ekim 2018)' https://edps.europa.eu/sites/edp/files/publication/18-10-24_choose_humanity_speech_en_1.pdf [Erişim Tarihi: 01.09.2020].

2 Kişisel verilerin korunması alanındaki düzenlemeler ve bunları uygulayan düzenleyici otoriteler için bkz CNIL 'Data protection around the world' https://www.cnil.fr/en/data-protection-around-the-world [Erişim Tarihi: 01.09.2020].

çalışmak durumunda kalmaktadır. Bu durum, aynı anda birden fazla mevzuatın ve kuralının uygulanmasını kaçınılmaz kılmaktadır.

Kişisel verilerin korunması alanında Avrupa Birliği Genel Veri Koruma Tüzüğü[3] ("*GVK Tüzüğü*") ile 108 sayılı Sözleşme olarak da anılan Avrupa Konseyi'nin Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi[4] bu alandaki reformların temel çerçevesini oluşturmaktadır. 1981 tarihli 108 sayılı Sözleşme de bilgi ve iletişim teknolojilerinin dinamikliği karşısında reform edilmiş ve 108+ numaralı Sözleşme olarak da anılan 223 numaralı Sözleşme[5], modern bir çerçeve çizmeye çalışmıştır.

Alanda ortaya çıkan yeni ihtiyaçlar ve bunlara karşılık üretilen yeni kurallar yeni idari yapıların gerekliliğini de ortaya çıkarmış ve kişisel verilerin korunması alanındaki hukuki düzenlemeler daha ziyade bağımsız düzenleyici otoriteler eliyle icra edilmeye başlanmıştır.

Kişisel veri işleme süreçlerinin hukuka uygun şekilde sürdürülmesinin temin edilmesi ve kişisel verilerin hukuka uygun şekilde işlendiğinin ispat edilmesi uygulamadaki temel sorunlardan biridir. Hatta bazen bir veri sorumlusu başka bir ülkede dolaylı olarak hesap vermek durumunda kalabilmektedir. Sektör-spesifik düzenlemelerin artması, sınır aşan veri akışlarının özel kurallara riayet edilmesini gerekli kılması ve yukarıda izah edilen dijital dönüşümdeki gelişmeler sebebiyle sınır aşan nitelikte olsun veya olmasın standart, hızlı, makul maliyetsiz ve güvenilir ispat araçlarının varlığı ve bu alanda yeknesak kuralların geliştirilmesi hem denetleyici otoriteler için hem de tüm paydaşlar için temel bir ihtiyaçtır.

Nihayetinde veri sorumluları, ilgili kişileri aydınlatmaktan, kişisel verilerin hukuka aykırı işlenmesini ve erişilmesini önlemeye, belirli koşullarda açık rızalarını almaktan kişisel verileri silme, yok etme ve imha etmeye kadar çok geniş yelpaze yükümlülükleri bulunmaktadır. Tüm bu hususlarda hukuka uygun davrandığını ispat külfeti veri sorumlusunun üzerindedir.

Dijital dönüşüm ve iş süreçlerinin karmaşıklaşması sadece veri sorumluları için değil, veri koruma otoriteleri için de ciddi maliyet doğurmakta ve sorun oluşturmaktadır. Yapay zekâ teknolojilerinin kullanıldığı, büyük ölçekli veri işlemenin gerçekleştiği ve içerik dağıtım ağlarıyla verinin parçalarının dünyanın farklı coğrafyalarına yayıldığı işlemeler karşısında, veri koruma otoriteleri ile veri

[3] 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), OJ L 119, 4.5.2016.

[4] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (No. 108), Strasbourg, 28.01.1981.

[5] Council of Europe, Amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 18.05.2018.

sorumluları veya daha genel ifadeyle dijital hizmet sağlayıcılar arasında teknik bilgi asimetrisi oluşmaktadır. Hizmet sağlayıcılara girift teknolojiler ve yöntemleri kullanmayı yasaklamak ölçüsüz bir tedbir olacağı için, otoritelerin teknik bilgi asimetrisini ortadan kaldıracak pratik denetim araçlarına ihtiyacı vardır.

Tüm bu sebeplerle, mevzuata uyum, uyumun ispatı ve otoritelerin paydaşları hızlı ve etkin şekilde denetleyebilmesi için yeni bir yaklaşıma ihtiyaç duyulmaktadır. Bu yaklaşım, hesap verebilirlik yaklaşımıdır. Hesap verebilirlik ilkesi ("*accountability principle*"), kişisel verilerin korunması alanındaki düzenlemelere uyumda temel bir paradigma değişikliğidir. Hesap verebilirlik, öz bir ilkedir. Ancak, bu ilke derinlemesine incelendiği zaman, aslında birden fazla veri koruma ilkesinin bu ilkeden beslendiği ve bu ilkeyi doğrudan veya dolaylı olarak desteklediği görülmektedir.

Bu çalışma kapsamında öncelikle hesap verebilirlik ilkesi etraflıca incelenecek olup ilkenin esas mahiyeti ortaya koyulmaya ve ilke somutlaştırılmaya çalışılacaktır. Çalışma kapsamında, hesap verebilirlik ilkesinin kapsamı, diğer veri koruma ilkeleriyle ilişkisi, getirdiği temel yükümlülükler ve sorumluluklar ile veri sorumlusu ile veri işleyenlere etkileri incelenecektir. Bu inceleme bağlamında veri koruma düzenlemelerine uyum nasıl ispat edilebilir sorusuna yanıt bulunmaya çalışılacaktır. Bu amaçla, farklı nitelikteki veri koruma hukuku ispat araçları ele alınarak, bu araçların veri sorumluları tarafından kullanılabilme şartları ile araçların sunduğu avantajlar ve dezavantajlar incelenecektir.

Hesap verebilirlik kavramının muhtelif disiplinlerde çeşitli anlamları bulunmaktadır.[6] Bu çalışma kapsamında hesap verebilirlik kavramı sadece veri koruma hukuku bağlamındaki anlamı ve kapsamıyla ele alınacaktır. Hesap verebilirlik ilkesi ve uyum ispat araçları konusu Avrupa Birliği hukuku ve Türk hukuku bağlamında ele alınacaktır. Metodolojik açıdan çalışmada mukayeseli hukuk ve doktrinsel inceleme metotları kullanılacaktır. Çalışmanın merkezinde Avrupa Birliği Genel Veri Koruma Tüzüğü ("GVK Tüzüğü") ile Türk hukukundaki en temel yasal çerçeve olan 6698 sayılı Kişisel Verilerin Korunması Kanunu yer alacaktır. Bu alandaki sektör-spesifik düzenlemelere sadece önemli görülen yerlerde atıf yapılacaktır. Çalışmadaki temel amaç, veri koruma hukukunda hesap verebilirliğin ve ispatın nasıl gerçekleştirildiği sorusunun yanıtını bulmaktır. Bu sebeple, çalışmada tam veya yarı-yapısal herhangi bir ampirik çalışma yapılmamıştır. Konu hukuk bağlamında ele alındığı için ispat araçlarına ilişkin herhangi bir ekonomik analiz de gerçekleştirilmemiştir.

[6] Etik, kamu yönetimi ve finans başta olmak üzere kavramın farklı manaları için bkz Paul De Hert, '*Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law*' in Daniel Guagnin and others (eds), *Managing Privacy through Accountability* (Palgrave Macmillan 2012), 195-196; Ayrıca bkz Andrea C Bianculli, Xavier Fernández-i-Marín ve Jacint Jordana (eds), *Accountability and Regulatory Governance* (Palgrave Macmillan 2015); Jernej Letnar Černič, *Corporate Accountability under Socio-Economic Rights* (Routledge 2019).

Çalışmanın ilk bölümünde farklı düzlemlerde hesap verebilirlik ilkesinin nasıl düzenlendiği ve hangi anlamda kullanıldığı incelenecektir. İkinci bölümde, Avrupa Birliği hukuku açısından konu incelenecek ve üçüncü bölümde temel hesap verebilirlik araçları olan veri koruma etki analizi, veri koruma görevlisi ve davranış kuralları ile sertifikasyon konuları incelenecektir. Çalışmanın dördüncü bölümünde konu Türk hukuku bağlamında ele alınarak, Kişisel Verilerin Korunması Kanunu ve bu kanunun uygulayıcısı Kişisel Verileri Koruma Kurumu'nun hesap verebilirlik ilkesine yaklaşımı analiz edilecektir. Son bölümde ise konuya ilişkin genel değerlendirmelere yer verilecektir.

I. Farklı Düzlemlerde Hesap Verebilirlik İlkesi

A. OECD

İktisadi İşbirliği ve Kalkınma Teşkilatı (*Organisation for Economic Co-operation and Development - OECD*) tarafından 23 Eylül 1980 tarihinde kabul edilen Özel Yaşamın Gizliliğinin ve Sınır Aşan Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler, kişisel verilerin korunması alanında öncü bir uluslararası metindir.[7] Bu Rehberde veri toplamanın sınırlı olması (madde 7), veri niteliği (kalitesi) (madde 8), amacın belirliliği (madde 9), kullanımın sınırlanması (madde 10), veri güvenliği ilkesi (madde 11), açıklık (madde 12), kişisel katılım (madde 13) şeklinde ilkelere yer verilmiştir.

Tüm bu ilkeler, bunları yatay düzlemde kesen on dördüncü ilke olarak hesap verebilirlik ilkesi (madde 14) ile anlamlı hale gelmiştir. "Hesap Verebilirlik İlkesi" Rehberde şu şekilde tanımlanmıştır: "*Bir veri sorumlusu, belirtilen ilkelere uyulması için öngörülen önlemlere uymaması halinde sorumluluk taşımalıdır.*"

OECD Rehber İlkeleri, 2013 yılında gözden geçirilmiştir.[8] 2013 yılındaki revizyonun odak noktası ise hesap verebilirlik ilkesi olmuştur. Risk yönetimi ile artırılmış beraber-çalışabilirlik konularına daha fazla yer veren güncel ilkelerde, hesap verebilirlik ilkesinin uygulanmasına ilişkin müstakil bir üçüncü bölüm ayrılmış ve "*mahremiyet yönetim programı*" kavramsallaştırılmıştır. 1980 tarihli ilkeler ile 2013 tarihli ilkelerdeki hesap verebilirlik karşılaştırıldığında, ilkinde sadece veri sorumlusunun sorumluluğundan bahsedilirken ikincisinde veri sorumlusunun düzenleyici otoritelere uyumu gerçekleştirmek için gerekli araçlara sahip olduğunu ispat etmesi gerekmektedir. Gerçekleştirilen revizyon ile sorumluluk, ispat edilebilir uyumla desteklenmiştir.

---

7 OECD, '*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data'* (1980) http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [Erişim Tarihi: 01.09.2020]

8 OECD, '*The OECD Privacy Framework - Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data'* (2013) https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [Erişim Tarihi: 01.09.2020], 11-17.

OECD 2013 Rehber İlkelerine göre, bir veri sorumlusu mahremiyet yönetim programı uygulamaya koymalıdır. OECD, sadece bu programı anmakla yetinmemiş, programın mahiyetini de açıklamıştır. OECD'ye göre mahremiyet yönetim programı, kontrolündeki tüm kişisel verilere ilkelerin uygulanmasını sağlamalı, faaliyetinin yapısı, ölçeği, boyutu ve hassasiyetine göre uygun olarak geliştirilmeli, mahremiyet risk değerlendirmesine dayalı uygun teminatları sağlamalı, yönetişim yapısına entegre edilmeli ve iç denetim mekanizmaları kurmalı, taleplere ve olaylara yanıt verecek planlar içermeli, sürekli gözetleme ve periyodik değerlendirme ışığında güncellenmelidir.

Veri sorumlusu, mahremiyet uyum programını aktif bir şekilde tutmalı ve yetkili mahremiyet otoritesinin talebi durumunda bu programını sunmaya hazır olmalıdır. Mahremiyet yönetim programı, yerel mevzuat, uluslararası yükümlülükler, öz-düzenleyici programlar ve akdi düzenlemeleri de içermektedir.

Veri sorumlusunun bir diğer önemli yükümlülüğü ise, kişisel verileri etkileyen esaslı bir güvenlik ihlali olması durumunda mahremiyet otoriteleri ile ilgili diğer makamları bilgilendirmektir. İhlalin veri süjelerini (ilgili kişileri) de olumuz etkileme ihtimali varsa, veri sorumlusu ayrıca etkilenen veri süjelerini de bilgilendirmelidir.

OECD, hesap verebilirlik ilkesinin öneminin zamanla arttığı ve veri korumada kurumsal sorumluluğu geliştirmek amacıyla kullanılan yeni bir araca dönüştüğü görüşündedir.[9] Veri sorumlusunun, "*kontrolündeki*" tüm kişisel verilere ilişkin hesap verebilirlik mekanizmasını oluşturması gerekmektedir. Bu şekilde, sadece kendi iç faaliyetlerinden değil, kişisel verinin kime aktarıldığından bağımsız olarak tüm faaliyetlerden veri sorumlusu sorumlu tutulmaktadır.[10]

Veri sorumlusunun tüm faaliyetlerinde ve üçüncü kişilerle olan ilişkilerinde bu sorumluluğu gözeterek uygun koruma mekanizmaları geliştirmesi beklenmektedir. OECD'ye göre veri sorumlunun mahremiyet politikaları ve uygulamalarındaki uyumu adresleyen hükümler, bir güvenlik ihlali olması durumunda veri sorumlusuna bildirim yapmaya ilişkin protokoller, çalışanların talim ve eğitimi, alt-yüklenicilere ilişkin yükümlülükler ve denetim yapmaya ilişkin süreçler bu tür koruma mekanizmalarına örnektir.[11]

Peki, mahremiyet yönetim programı nasıl kurgulanmalıdır? OECD, bu programı tasarlarken ve uygularken esnekliğe ihtiyaç olduğunu belirtmektedir.[12] Esneklikten anlaşılması gereken, veri sorumlusunun faaliyette bulunduğu alan, işlediği veri boyutu veya verinin hassasiyetine göre farklı kapsam ve nitelikte bir tedbir alınması gerekliliğidir. Şöyle ki, birden fazla konum ve ülkede faaliyet gösteren büyük bir

[9] OECD (n 8) 23.

[10] OECD (n 8) 23.

[11] OECD (n 8) 23.

[12] OECD (n 8) 24.

veri sorumlusu ile tek bir konumda faaliyette bulunan küçük veya orta ölçekli veri sorumlusundan farklı nitelikte iç denetim mekanizması kurması beklenmektedir.

Farklı muamele gerekliliği verinin ölçeği ve hassasiyeti için de geçerlidir. Dolayısıyla, mahremiyet yönetim programı her veri sorumlusu için özel olmalıdır ve sorumluluk da buna göre belirlenmelidir. Bu doğrultuda OECD, veri sorumlularının hesap verebilirlik ilkesi bağlamında sorumluluğu beklenirken aynı veya eşit statüde olanlara aynı veya eşit muamele yapılması gerektiğini hatırlatmaktadır.

OECD'nin 2013 yılında güncellediği rehber ilkelerindeki diğer bir odak noktası risk temelli yaklaşımdır. OECD, hesap verebilirliği temin için gerekli olan tedbirlerin bireylerin mahremiyetine ilişkin risklerin tanımlanması, analizi ve değerlendirilmesiyle tespit edilmesi gerektiğini, gerektiği durumlarda mahremiyet etki analizi gerçekleştirilmesi gerektiğini, mahremiyet yönetim programının gerekli olduğu durumlarda tasarımda mahremiyet (*privacy by design*) yaklaşımını da desteklediğini belirtmiştir.[13]

Hesap verebilirlik, kurumsal yönetişim ile doğrudan bağlantılı bir konudur. OECD, mahremiyet yönetim programının veri sorumlularının kurumsal yapılarına entegre edilmesini ve uygun iç denetim mekanizmalarıyla desteklenmesini önermektedir.[14] Kurumsal liderliğin desteğinin bu konuda kolaylaştırıcı olduğu vurgusunu yapan OECD, yeterli kaynak ve personelin programın sürdürülebilirliğine doğrudan etki ettiğini belirtmektedir. Keza, veri koruma görevlisinin varlığı da başarının bir diğer etkenidir.

Mahremiyet yönetim programının bir diğer önemli unsuru ise kişisel verilere ilişkin taleplere ve olaylara yanıt verecek planlardır. Özellikle olay müdahale planının varlığı şarttır. Nihayetinde mahremiyet yönetim programları statik değil, dinamik programlardır. Bu programlar, düzenli olarak gözden geçirilmeli ve risk ortamına uygunluklarını temin etmek amacıyla güncellenmelidir.

OECD'ye göre hesap verebilirliğin varlığından bahsedebilmek için henüz herhangi bir veri ihlalinin gerçekleşmediği veya uyumsuzluk iddiasının olmadığı bir aşamada mahremiyet yönetim programının etkinliği ve yeterliliği temin edilmiş olmalıdır.[15] Bu konuda yetkili makamların talepleri durumda, uyum derhal ve pratik şekilde ispat edilebilmelidir.

OECD Rehber İlkeleri, hesap verebilirliğin sorumluluk boyutunu yeterince ortaya koymadığı ve yükümlülüğün muhataplarını müphem bıraktığı gerekçesiyle

13 OECD (n 8) 24.

14 OECD (n 8) 24.

15 OECD (n 8) 25.

eleştirilmektedir.[16] Ayrıca, bağlayıcı olmaması sebebiyle etkili olmadığı da belirtilmektedir.[17] Diğer yandan bu rehber ilkeler, uluslararası birçok düzenlemeye ilham kaynağı olmuş ve bu alandaki temel çerçevenin belirlenmesinde öncü olmuş, hesap verebilirlik ilkesinin daha bilinir olmasına önemli katkılar sunmuştur. 1980 yılında yalnızca bir söylem gibi görünen hesap verebilirlik ilkesi, 2013 yılında mutlak şekilde gözetilmesi gereken müstakil bir ilkeye evrilmiştir.

B. 108 sayılı Avrupa Konseyi Sözleşmesi

108 sayılı Sözleşme olarak da anılan Avrupa Konseyi'nin Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, OECD Rehber İlkelerinin aksine bağlayıcı nitelikte bir uluslararası belgedir. 55 farklı ülke tarafından kabul edilen bu Sözleşme, Avrupa Konseyi üyesi olmayan devletlerin de taraf olmasıyla, bölgesel nitelikten uluslararası niteliğe kavuşmuştur.[18] Sözleşme, birçok devletin kişisel verilerin korunmasına ilişkin mevzuatının hazırlanmasına ve geliştirilmesine katkı sağlamıştır.[19]

108 sayılı Sözleşmede yer alan kişisel verilere ilişkin temel ilkeler şunlardır: verilerin niteliği (madde 5), hassas kişisel verilerin özel olarak korunması (madde 6), veri güvenliğinin sağlanması (madde 7), ilgili kişinin bilgi alma, verilere erişme ve gerektiğinde onları düzeltme hakkı (madde 8). Verilerin niteliği başlıklı 5. madde uyarınca otomatik işleme konu olan kişisel veriler, dürüst şekilde ve hukuka uygun şekilde elde edilir ve işlenir; belirli ve meşru amaçlar için saklanır ve bu amaçlara aykırı şekilde kullanılamaz; kaydedilme amaçlarına uygun ve yerinde olur ve aşırı olamaz; doğru bilgileri yansıtır ve gerektiğinde güncellenir; kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkan veren bir biçimde saklanır.

108 sayılı Sözleşme kişisel verilerin korunması alanında bağlayıcı kurallar getiren öncü bir düzenlemedir. Sözleşme belirli bir teknolojiyi dikte etmeksizin, genel ilkelerle taraf devletlere bu alanda esnek bir çerçeve sağlamıştır. Keza, kişisel verilerin uluslararası serbest akışı için özel bir kural getirerek liberal bir serbest dolaşım rejiminin altyapısını kurmuştur.

---

16 Graham Greenleaf, '*Accountability Without Liability: 'To Whom' and 'With What Consequences'? (Questions for the 2019 OECD Privacy Guidelines Review) UNSW Law Research Paper No. 19-67'* (2019) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3384427 [Erişim Tarihi: 01.09.2020], 4.

17 Paul De Hert ve Vagelis Papakonstantinou, '*The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition*' (2014) 30 Computer Law & Security Review 633, 634.

18 108 sayılı Sözleşmeye taraf olan devletler ve Sözleşmenin yürürlük tarihi için bkz Chart of signatures and ratifications of Treaty 108 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=ligcOAUk [Erişim Tarihi: 01.09.2020]

19 Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014), 92-93.

108 sayılı Sözleşme uyarınca kişisel verilerin akit devletler arasında serbest dolaşımı esastır. Sözleşmenin 12. maddesi uyarınca bir taraf devlet, münhasıran özel yaşamın korunması amacıyla kişisel verilerin diğer bir taraf devlete sınır ötesi akışını yasaklayamaz veya özel izne tabi tutamaz. Bu genel rejimin iki temel istisnası vardır: (1) belirli kişisel veri kategorileri için özel kurallar ve/veya korumalar getirilmiş olması ve aktarımın yapılacağı taraf devlette getirilen bu korumalara "eşdeğer" bir korumanın bulunmaması veya (ii) aktarımın 108 sayılı Sözleşmeye taraf olmayan üçüncü bir devlet aracılığıyla yapılacak olması.

108 sayılı Sözleşmenin tamamlayıcısı niteliğinde 181 sayılı Ek Protokol ile de hem veri koruma otoritelerinin kurulması hem de sınır aşan veri akışının "*yeterlilik*" kuralları yeniden düzenlenmiş ve oluşturulan uluslararası veri koruma rejimi perçinlenmiştir.[20] Şöyle ki, 181 Sayılı Ek Protokol uyarınca; 108 sayılı Sözleşmenin tarafları, Sözleşmeye taraf olmayan ve yeterli korumayı sağlamayan bir devletin/kuruluşun yetki alanına tabi olan bir alıcıya aktarım yapılmasına şu durumlarda izin verebilmektedirler: (i) İlgili kişinin belirli bir menfaati veya (özellikle önemli kamu menfaati olmak üzere) üstün gelen meşru menfaatler nedeniyle iç hukukun izin verdiği haller, ya da (ii) İlgili veri aktarımından sorumlu olan veri sorumlusu tarafından sağlanan ve ilgili otorite tarafından iç hukukuna göre uygun bulunan koruma tedbirleri (ki bu koruma tedbirleri aktarıma konu olan sözleşme hükümlerinin bir sonucu olarak ortaya çıkabilir).

Hesap verebilirlik ilkesi 108 sayılı Sözleşmede doğrudan zikredilmiş bir ilke değildir. Sözleşmenin kabul edildiği dönemde henüz hesap verebilirlik ilkesi genel kabul görmüş ve öne çıkmış bir ilke olmadığı için bu durum doğaldır. Yine de kişisel verilerin yurtdışına aktarılmasında 108 sayılı Sözleşmeye taraf olma koşulu ile 181 sayılı Protokol bağlamında yeterli korumayı sağlama kriteri dolaylı bir hesap verebilirlik yöntemi olarak değerlendirilebilir.

C. 108+ sayılı Avrupa Konseyi Sözleşmesi

Kişisel verilerin işlenmesi ve korunması dinamik bir alan olup giriş bölümünde izah edilen teknik değişimler ve sosyo-ekonomik gelişmeler sebebiyle bu alana özgü yeni sorunlar ortaya çıkmıştır. 108 sayılı Sözleşme, getirdiği ilkelerle bu alanda temel koruma seviyesini oluşturmuşsa da teknik gelişmelerin ortaya çıkardığı sorunları karşılamaktan uzak kalmıştır. Bu sebeple, 2010 yılında 108 sayılı

[20] 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Konvansiyonu ve Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol (181 Sayılı Ek Protokol) (Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows), 08.11.2001.

Sözleşme reform çalışmaları başlatılmış ve 108+ sayılı Sözleşme olarak da anılan 223 numaralı Sözleşme ile uluslararası veri koruma hukuku rejiminde ikinci faza geçilmiştir.[21]

Hesap verebilirlik ilkesi, 108+ sayılı Sözleşmede de açıkça yer almamaktadır. 108+ sayılı Sözleşme bu sebeple de eleştirilmektedir.[22] Yine de 108+ sayılı Sözleşme'nin farklı hükümlerinde hesap verebilirlik ilkesinin izlerini bulmak mümkündür. Hesap verebilirlik ilkesi en fazla da 108+ sayılı Sözleşmenin "*İşlemenin şeffaflığı*" başlıklı 8. maddesi ile "*Ek yükümlülükler*" başlıklı 10. maddesinde farklı unsurlarıyla görünür durumdadır. Madde başlığından da anlaşılacağı üzere, bu yükümlülükler diğer temel yükümlülükleri yatay kesen şekilde gözetilmesi ve uygulanması gereken yükümlülüklerdir.

108+ sayılı Sözleşmenin 8. maddesi, 108 sayılı Sözleşmede yer almayan yeni bir ilke getirmiştir: şeffaflık ilkesi. Söz konusu hükme göre, veri sorumlusu, kişisel verilerin adil ve şeffaf işlenmesinin sağlanması için gerekli her türlü ek bilgiler dahil olmak üzere (i) kimliği ve mutat meskeni veya kuruluşu; (ii) hedeflenen işlemenin hukuki sebebi ve amaçları; (iii) işlenen kişisel verilerin kategorileri, (iv) varsa, kişisel verilerin alıcıları veya alıcı kategorileri ve (v) ilgili kişinin haklarını kullanma yolları hakkında ilgili kişilerin bilgilendirilmesini sağlar.

108+ sayılı Sözleşmenin Açıklayıcı Raporunda, şeffaflığın nasıl gerçekleştirilmesi gerektiği izah edilmiştir.[23] Açıklayıcı Rapora göre, sunulan bilgiler kolayca erişilebilir, okunaklı, anlaşılabilir ve ilgili kişilere uyarlanmış olmalıdır (örneğin, gerektiğinde çocukların anlayabileceği bir dilde).[24] Keza, adil şekilde veri işlemeyi sağlamak için gerekli veya faydalı olan, saklama süresi veya veri işlemenin altında yatan nedenler veya başka bir taraf veya taraf olmayan devlette bulunan bir alıcıya veri aktarımı gibi her türlü ilave bilgi de sağlanmalıdır.

Açıklayıcı Rapora göre veri sorumlusu, ilgili kişileri toplu olarak (bir web sitesinde veya genel duyuru suretiyle) veya bireysel olarak bilgilendirmek için uygun, makul ve düşük maliyetli herhangi bir yöntemi kullanabilir ve bilgilendirme, işleme başlarken bunu yapmak mümkün değilse, daha sonraki bir aşamada, örneğin veri sorumlusu herhangi bir yeni nedenden dolayı ilgili kişi ile temasa geçtiğinde yapılabilir.

---

21 1 Ağustos 2020 itibariyle 36 devlet 108+ sayılı Sözleşmeyi imzalamıştır. Bkz Chart of signatures and ratifications of Treaty 223 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures [Erişim Tarihi: 01.09.2020]

22 De Hert ve Papakonstantinou, '*The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition*', 639 ve n 45'te anılan Cécile De Terwangne, Jean-Marc Van Gyseghem ve Yves Poullet, *Rapport sur les lacunes de la Convention no 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (Partie II)*, 2010) http://www.crid.be/pdf/public/6559.pdf [Erişim Tarihi: 01.09.2020] (Serbest Çeviri), 48.

23 Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Açıklayıcı Rapor") https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a [Erişim Tarihi: 01.09.2020] 108+ sayılı Sözleşmenin ve Açıklayıcı Raporun Türkçe çevirisi için bkz https://itlaw.bilgi.edu.tr/media/document/2019/09/avrupa-konseyi-108plus-konvansiyon-tercume.pdf [Erişim Tarihi: 01.09.2020]

24 108+ sayılı Sözleşme: Açıklayıcı Rapor (n 23) para. 68.

108+ sayılı Sözleşmenin 10. maddesinin birinci fıkrası uyarınca, her bir taraf devlet, veri sorumlularının ve uygun olduğu ölçüde veri işleyenlerin 108+ sayılı Sözleşmenin getirdiği yükümlülüklere uymaları için uygun tedbirleri almasını ve kendi kontrollerindeki veri işlemenin Sözleşme hükümlerine uyumlu olduğunu ispat etmesini sağlamakla yükümlü tutulmuştur. Dolayısıyla, istisnalara dayalı işleme halleri saklı kalmak kaydıyla, sadece tedbirlere uyum değil, bu uyumun ispatı da gereklidir. Hesap verebilirlik yaklaşımına göre hem uyumun doğrulanıyor olması hem de ispat edilebilir olması asıldır.

108+ sayılı Sözleşmenin Açıklayıcı Raporunda uygun tedbirler, çalışanların eğitimi, uygun bildirim prosedürlerinin oluşturulması, yetki devri olan durumlarda özel sözleşmesel hükümlerin oluşturulması ve uyumun doğrulanması ve ispatı için dahili süreçlerin oluşturulması şeklinde örneklendirilmiştir.[25] Keza, bir veri işleme istisnasına dayalı olarak faaliyet gerçekleşiyorsa, bu istisnaya dayanıldığının da ispatı gerekmektedir.

Açıklayıcı Raporda, üzerinde durulan bir diğer uygun tedbir ise veri koruma görevlisi atanmasıdır.[26] Uygun yetkiyle donatılan bir veri koruma görevlisinin uyumu doğrulama ve ispatlama sürecini kolaylaştıracağı öngörülmektedir. Veri koruma görevlisi, tüm veri işleme durumları için zorunlu değil, ihtiyari bir yöntem olarak önerilmektedir.

10. maddedeki bir diğer yenilik ise mahremiyet etki analizine ilişkindir. 108+ sayılı Sözleşmenin 10. maddesinin ikinci fıkrası uyarınca, her bir taraf devletin, veri sorumlularının ve uygun olduğu ölçüde veri işleyenlerin, veri işlemeye başlamadan önce hedeflenen veri işlemenin ilgili kişilerin hak ve temel özgürlükleri üzerindeki olası etkilerini değerlendirmesini ve veri işlemeyi bu hak ve temel özgürlüklere müdahale riskinin önlenmesine veya minimize edilmesine yönelik tasarlamasını sağlaması gerekmektedir.

108+ sayılı Sözleşmenin Açıklayıcı Raporunda, mahremiyet etki analizinin aşırı bir formaliteye bağlı olmaksızın gerçekleştirilebileceği ve bu analiz yapılırken ölçülülük ilkesi açısından planlanan işlemenin ele alınması gerektiği belirtilmektedir.[27] Veri sorumlusu bir veri işleyen kullanacaksa, veri sorumlusunun riski değerlendirmesi gerektiğinin altı çizilmektedir.[28] Peki, riski veri sorumlusunun hangi iç ekibi değerlendirecektir? Açıklayıcı Raporda, riskin güvenlik ve tasarım uzmanları dahil BT sistem geliştiricileri tarafından hukukçularla beraber değerlendirilmesi tavsiye edilmektedir.[29] Bu tavsiye, veri koruma hukukunun disiplinler arası niteliğiyle uyumlu nitelikte bir tavsiyedir.

[25] 108+ sayılı Sözleşme: Açıklayıcı Rapor (n 23) para. 85.

[26] 108+ sayılı Sözleşme: Açıklayıcı Rapor (n 23) para. 87.

[27] 108+ sayılı Sözleşme: Açıklayıcı Rapor (n 23) para. 88.

[28] 108+ sayılı Sözleşme: Açıklayıcı Rapor (n 23) para. 88.

[29] 108+ sayılı Sözleşme: Açıklayıcı Rapor (n 23) para. 88.

108+ sayılı Sözleşmeyle hem veri sorumlularının hem de uygun ölçüde veri işleyenlerin, veri işlemenin tüm aşamalarında kişisel verilerin korunması hakkını dikkate alarak teknik ve idari tedbirleri uygulanmakla yükümlü olduklarının altı çizilmiştir. 10. maddenin üçüncü fıkrasındaki bu kural, sürdürülebilir bir veri koruma yaklaşımına işaret etmektedir. Veri sorumluları ve de uygun olduğu ölçüde veri işleyenler hem iç hem de dış organizasyonlarında aynı seviyede ve titizlikle kişisel verilerin korunmasına ilişkin tedbirleri işler kılmakla yükümlüdür.

Teknik ve idari tedbirlerin sürekli işlerliğinin sağlanması genel bir yükümlülük olarak tanımlandığı için, bu süreçlerin gerçekten de var olup olmadığı, etkin şekilde uygulandığı ve üçüncü taraf paydaşlar tarafından da bu standartların takip edildiğinin kontrolü için bir hesap verebilirlik sisteminin kurulmuş olmasına ihtiyaç vardır. Nihayetinde, teknik ve idari tedbirlerin sadece var olması değil, etkin şekilde sürdürülebilirliğinin ispatı da temelde veri sorumlularına yüklenmiş dinamik bir yükümlülüktür. Aslında, dolaylı olarak "tasarımda mahremiyet" (privacy by design) ve "varsayılan değer olarak mahremiyet" (privacy by default) ilkelerine atıf yapılmıştır.

108+ sayılı Sözleşmenin Açıklayıcı Raporunda, bu veri koruma yükümlülüklerinin uygulanmasının sadece veri işlemeye yönelik teknolojilere indirgenmemesi; ilgili iş ve yönetim süreçlerinin de dikkate alınması ve uygulanabilir hukuka uyumu kolaylaştıracak kolay kullanılabilir araçların kullanılmasının gerekliliğinin altını çizmiştir.[30] Ayrıca, ilgili kişilerin verilerine erişmesi ve bu veriyi taşıması (veri taşınabilirliği) de bu bağlamda sayılmıştır. Esasında, kendisiyle ilgili süreçlere ilgili kişinin hızlıca erişebilmesi ve bu veriyi kolayca taşıyabilmesi bir hesap verebilirlik aracı olarak da nitelendirilebilir.

10. maddedeki son "*ek yükümlülük*" ise risk temelli yaklaşımın benimsenmesidir. 108+ sayılı Sözleşmenin 10. maddesinin dördüncü fıkrası uyarınca her bir taraf devlet, ilgili kişinin menfaatleri, hakları ve temel özgürlüklerinden doğan riskleri göz önünde bulundurarak, 108+ sayılı Sözleşmenin sayılan her üç yükümlülüğünün verinin türü ve hacmi, işlemenin türü, kapsamı ve amacı ve veri sorumlusu ile uygun olduğu hallerde veri işleyenin boyutuna göre iç hukukunda uygulanmasını sağlamakla yükümlü kılınmıştır.

Bu yükümlülük, OECD'nin 2013 tarihinde güncellediği rehber ilkelerinden ilham alınmıştır. Bu ilke, tıpkı OECD ilkeleri gibi, kişisel verilerin korunması süreçleri tasarlanırken ve uygulanırken esnek davranılması gerektiğini; veri sorumlusunun faaliyette bulunduğu alan, işlediği veri boyutu veya verinin hassasiyetine göre farklı kapsam ve nitelikte bir tedbir alınması gerektiğini öngörmektedir. Farklı muamele gerekliliği verinin ölçeği ve hassasiyeti için de geçerlidir. Diğer bir deyişle, uyum her

[30] 108+ sayılı Sözleşme: Açıklayıcı Rapor (n 23) para. 89.

veri sorumlusu için özel olmalıdır ve sorumluluk da buna göre belirlenmelidir. 108 sayılı Sözleşmenin Açıklayıcı Raporunda da farklı statülere ve durumlara göre farklı nitelikte bir süreç işletilmesi gerektiği belirtilmektedir.[31]

108+ sayılı Sözleşmede hesap verebilirlik lafzında olmasa da özünde yer bulmuştur ve Sözleşme hesap verebilirlik yaklaşımı üzerine inşa edilmiştir.[32] Sözleşme bu amaçla şeffaflık ilkesini getirmiş, uyumun doğrulanması ve uyumun ispatını müstakil yükümlülükler olarak tanımlamış, tasarımda mahremiyet yaklaşımını ortaya koymuş, mahremiyet etki analizini tanımlamış ve uyum sürecinin özel bir süreç olarak kurgulanması ve uygulanması gerektiğini vurgulamıştır. Bu doğrultuda hesap verebilirlik, başta veri sorumlusu ve niteliğine uygun düştükçe veri işleyenin hem iç organizasyon hem de dış organizasyonunda bir değer olarak yer bulması gerekmektedir.

Ç. Avrupa İnsan Hakları Sözleşmesi ve AİHM

Avrupa İnsan Hakları Sözleşmesi'nde ("AİHS") açıkça hesap verebilirlik ilkesi, yer almamaktadır. Sözleşmenin düzenlediği alan ve kabul edildiği dönem dikkate alındığında bu durum makuldür. Keza, Sözleşmede kişisel verilerin korunması açıkça düzenlenmemektedir. Bu konudaki temel çerçeve AİHS'nin 'Özel hayata ve aile hayatına saygı hakkı' başlıklı 8. maddesinin uygulanmasının yorumlanmasıyla, AİHM'nin içtihatlarıyla çizilmiştir.[33] Bu içtihatlardan 2008 yılında verilmiş *I v Finlandiya*[34] kararı, kişisel verilerin bilişim sistemlerinin kullanılması suretiyle işlenmesi ve de hesap verebilirlik bağlamında önemli çıktıları olan öncü bir karardır.[35]

I v Finlandiya davasında başvurucu, bir devlet hastanesinde çalışan bir hemşiredir ve aynı hastanede yapılan testlerde HIV virüsü taşıdığı tespit edilmiştir. Başvurucu, söz konusu hastalığından diğer çalışma arkadaşlarının bilgisi olduğunu ve bunun da hastanedeki hasta kayıtlarına hastane çalışanları ve hekimlerin herhangi bir kısıtlama olmaksızın doğrudan erişebilmesinden kaynaklandığını iddia etmiştir. Süreç içerisinde başvurucuya başka takma adla özel bir veri girişi yapılmış olsa da başvurucu, hastane bilişim sistemlerine herhangi bir güvenlik tedbiri alınmadığından bahisle, AİHS'nin 8. maddesinde güvence altına alınan özel yaşamına saygı hakkının ihlal edildiğini iddia etmiştir. Davanın esasını inceleyen AİHM, başvurucuyu haklı bulmuş ve 8. maddenin ihlal edildiğine hükmetmiştir.

---

31 108+ sayılı Sözleşme: Açıklayıcı Rapor (n 23) para. 90.

32 Council of Europe, The modernised Convention 108: novelties in a nutshell, s.3-4, https://rm.coe.int/16808accf8 [Erişim Tarihi: 01.09.2020]

33 AİHM'nin kişisel veriler bağlamın da verdiği içtihatların güncel bir derlemesi için bkz European Court of Human Rights: Factsheet - Personal data protection https://www.echr.coe.int/documents/fs_data_eng.pdf [Erişim Tarihi: 01.09.2020]

34 *I. v Finlandiya* App no 20511/03 (ECHR, 17 July 2008) http://hudoc.echr.coe.int/eng?i=001-87510 [Erişim Tarihi: 01.09.2020]

35 Bu çalışmanın kapsamı ve metodolojik sınırları sebebiyle AİHM'nin tüm içtihatlarını derinlemesine ele almak mümkün değildir. Bu konuda kapsamlı bir inceleme için bkz De Hert (n 6) 212 vd.; Ayrıca bkz Sabire Sanem Yılmaz, *Tıp Alanında Kişisel Verilerin Açıklanması Suçu* (Seçkin 2014), 59-62.

Uyuşmazlığın çıktığı dönemde Finlandiya'da veri koruma kanunu vardır ve uygulanmaktadır.[36] Söz konusu düzenleme uyarınca veri sorumluları gerekli güvenlik tedbirlerini almak ve sadece yetkili personelin erişimini sağlamakla yükümlü tutulmuştur. Ancak, AİHM Finlandiya'nın kişisel verileri korumasına yönelik yükümlülüğünü hatırlatmış, sağlık verilerinin (özellikle de hassas nitelikteki hastalıklara ilişkin) hassas ve tam koruma sistemlerinin kurulması gerektiğini belirtmiş, somut olayda bu güvenlik tedbirlerinin gereği gibi uygulanmadığı ve bu sebeple de kişisel verilerin yetkisiz kişilerce erişilmesine sebebiyet verildiği için başvurucunun mahremiyet hakkının ihlal edildiğine hükmetmiştir.

Başvurucunun iddiası, aslında bilişim sistemlerinin kötüye kullanımını önleyecek proaktif bir kontrol mekanizmasının yokluğu olarak özetlenebilir. AİHM, Finlandiya veri koruma kanunu katı şekilde uygulanmış olsaydı, ihlalin ortaya çıkmayacağı görüşündedir.[37] Sorun, bilişim teknolojilerindeki bir eksikliğin mahremiyet ihlaline yol açmasından ziyade, veri sorumlusu tarafından mahremiyet farkındalığının olmamasıdır.[38] *I v Finlandiya* kararı, şirketler ve kurumlar tarafından kişisel verilerin korunması kanunlarında yer alan güvenlik tedbirlerini almanın salt ahlaki veya basit bir hukuki yükümlülük olarak değil, pozitif bir insan hakları yükümlülüğü olarak nitelendirilmesi gerektiğinin altını çizmiştir.[39] Öyle ki, *I v Finlandiya* kararı veri koruma düzenlemelerinin pozitif insan hakları yükümlülükleri bağlamında değerlendirilmesi için bir kontrol noktası olarak nitelendirilmektedir.[40]

I v Finlandiya kararında başvurucunun çalışma arkadaşlarının başvurucunun sağlık dosyasına eriştiği tam olarak ispat edilmemiştir.[41] AİHM, başvurucunun bu konudaki iddialarını güvenilir bulsa da konuya ilkesel temelde yaklaşmıştır. Diğer bir ifadeyle, somut bir ihlalden ziyade sağlık verilerinin erişilmesine yönelik risk temelli bir değerlendirme yapmıştır. Karar, kişisel verilerin korunması düzenlemelerinin gerekliliklerinin yerine getirmenin salt uyum sağlamakla sınırlı olmadığı şeklinde de yorumlanmaktadır.[42]

AİHM'nin bu metodolojisi, bilişim sistemlerinin kişisel veri işlemek için kullanıldığı (özellikle de sağlık gibi hassas veriler için) durumlarda güvenliği ve mahremiyeti sağlamak için temel bir hesap verebilirlik yükümlülüğünün AİHS'nin 8. maddesinin bünyesinde yer aldığını göstermektedir. Bu konuda devletlerin pozitif

[36] *I. / Finlandiya*, para. 39.

[37] *I. / Finlandiya*, para. 40.

[38] De Hert (n 6) 189.

[39] De Hert (n 6) 214.

[40] De Hert (n 6) 214; Pozitif yükümlülük, kişisel verilerin korunmasına saygı gösterirken devletin aktif olarak da bu durumun önünde engel teşkil eden düzenlemeler ile ilgili gerekli değişiklikleri yapmak ve bu hakların fiilen uygulanmasını sağlayan her tür tedbiri almak olarak tanımlanmaktadır. Bu konuda bkz Yılmaz (n 35) 58.

[41] *I. / Finlandiya*, para. 43.

[42] De Hert (n 6) 219.

yükümlülüğü olduğu için, veri sorumluların buna uygun şekilde hareket etmeleri yalnızca kurumsal sosyal sorumluluğun değil, AİHS'nin 8. maddesinin açık bir gereğidir.

D. Uluslararası Standartlar Organizasyonu

Uluslararası Standardizasyon Kurumu (*International Organization for Standardization - ISO*) tarafından ve Uluslararası Elektroteknik Komisyonu'nun (IEC) işbirliği ile hazırlanan "Bilgi Teknolojileri - Güvenlik Teknikleri - Gizlilik Çerçevesi" ISO/IEC 29100 Standardı" ("ISO 29100"), bilgi ve iletişim teknolojileri sistemlerinde kişisel verilerin korunmasına ilişkin organizasyonel, teknik ve prosedürel standartlar getirmektedir.[43] ISO 29100 ile kişisel verilerin korunmasında ortak bir anlayış geliştirilmesi ve kişisel verilerin işlenmesi temelinde mevcut güvenlik standartlarının iyileştirilmesi hedeflenmiştir.[44]

Hesap verebilirlik, ilk mahremiyet standardı olan ISO 29100'de açıkça yer almaktadır. Standart, kişisel bilgilerin işlenmesinin bir özen yükümlülüğü ve bu bilgilerin korunmasına yönelik somut ve pratik tedbirler alınmasını gerektirdiğini belirterek, hesap verebilirlik ilkesinin gerekliliklerinin yerine getirilmesi için dokuz farklı eylem sıralamıştır.[45] Söz konusu eylemler şunlardır:[46]

(1) Mahremiyetle ilgili tüm politikaların, prosedürlerin, uygulamaların belgelenmesi ve yayınlanması,

(2) Organizasyonda belirli bir kişiye (uygun olduğu ölçüde organizasyon dışında başkalarına da devredilebilir) mahremiyetle ilgili politikaların, prosedürlerin ve uygulamaların icra edilmesi görevinin verilmesi,

(3) Kişisel bilgiyi üçüncü kişilere aktarırken sözleşmeler veya zorunlu iç politikalar gibi diğer yöntemler aracılığıyla alıcı üçüncü kişinin aynı ölçüde mahremiyet korumasını sağlayacağını temin etme (uygulanabilir mevzuat uluslararası veri transferlerine ilişkin ilave yükümlülükler içerebilir),

(4) Kişisel bilgiye erişecek veri sorumlusunun çalışanlarına uygun eğitimin verilmesi,

(5) Etkin bir iç şikâyet yönetim ve tazmin prosedürü oluşturulması,

[43] ISO, '*ISO/IEC 29100:2011 - Information technology - Security techniques - Privacy framework*' https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en [Erişim Tarihi: 01.09.2020]

[44] Leyla Keser Berber, '*Çapraz Etkileşim: Mahremiyete İlişkin Mevzuat ve Mahremiyet Standartları Arasındaki İlişki*' in Leyla Keser Berber and Ali Cem Bilgili (eds), *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku* (On İki Levha Yayıncılık 2020), 2.

[45] ISO (n 43) 18.

[46] ISO 29100, tazminat prosedürlerini hesap verebilirliğin oluşturulmasının önemli bir parçası olarak nitelendirmektedir. Standarda göre tazminat ilgili yöneticinin kişisel bilginin kötüye kullanımı durumunda sorumluyu mesul tutması için önemli bir araç sağlamaktadır. Bkz ISO (n 43) 18.

(6) Esaslı zarara yol açabilecek mahremiyet ihlalleri ve çözüm için alınan tedbirler hakkında ilgilileri bilgilendirme (meğer ki yasaklanmış olsun, örneğin soruşturma süreçlerinde),

(7) Bazı hukuki rejimlerde zorunlu olduğu üzere ve ilgili riskin seviyesine bağlı olarak ilgili tüm mahremiyet paydaşlarına (örneğin, veri koruma otoriteleri) mahremiyet ihlallerine ilişkin bildirim yapma,

(8) Şikâyet eden kişisel veri ilgililerinin uygun ve etkin yaptırımlara sahip olmasına ve/veya mahremiyet ihlali ortaya çıkmışsa düzeltme, silme eski hale iade gibi tazmin yollarına erişmesine izin verme,

(9) Gerçek kişinin mahremiyetini ihlal olmadan önceki döneme getirmek zor veya imkansızsa bu tür durumlara yönelik tazminat prosedürlerini geliştirme.

ISO ve IEC tarafından hazırlanan bir başka standart ise, 2019 yılında yayınlanan ISO/IEC 27701 "Güvenlik teknikleri - Gizlilik bilgi yönetimi için ISO/IEC 27001 ve ISO/IEC 27002'ye ek - Gereklilikler ve rehber" standardıdır ("ISO 27701").[47] Bu standart, kişisel verilerin işlenmesi süreçlerinin nasıl yürütüldüğünün -ISO 27701'e uygunluk sonucunda- belgelenmesi ve bu şekilde iş ortakları ile sözleşmelerin kolaylaştırılmasıdır.[48] ISO 27701, hesap verebilirlik ilkesine yer vermekte ve bu amaçla kullanılabilecek hesap verebilirlik araçları için ISO 29100'e atıf yapmaktadır. Bu çapraz-atıflar sayesinde standartlar arasında bütüncül ve tutarlı bir sistematik kurulmuştur.

E. Muhtelif Düzlemlerde Hesap Verebilirlik

Hesap verebilirlik ilkesi, bu bölümde değinilen rehberler ve düzenlemeler dışında, farklı metinlerde de yer bulmaktadır. Örneğin, dünyanın farklı yerlerinden gelen elliyi aşkın veri koruma otoritesinin 2009 yılında kabul ettiği "Madrid Kararı" hesap verebilirliği müstakil bir ilke olarak saymıştır.[49] Kararın 11. maddesinde sorumlu kişi ("*responsible person*") olarak ifade edilen aktörün, tüm veri koruma ilkelerini sağlamak için gerekli tedbirleri alması ve hem veri süjeleri hem de düzenleyici otoritelerin hakları ve yetkilerini kullanması durumunda uyumu ispat için gerekli iç mekanizmaları kurması gerekmektedir.

Asya-Pasifik Ekonomik İşbirliği Forumu (APEC) da 2005 yılında kabul ettiği APEC Mahremiyet Çerçevesi kapsamında hesap verebilirlik ilkesine açıkça yer

---

47 ISO, '*ISO/IEC 27701:2019(en) Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines*' https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en [Erişim Tarihi: 01.09.2020]

48 Keser Berber (n 44) 2.

49 Bkz Madrid Resolution on International Standards for the Protection of Privacy http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf [Erişim Tarihi: 01.09.2020]

vermiştir.[50] APEC Cross-Border Privacy Rules (CBPR) kurallarıyla, sınır aşan veri akışlarında "*Accountability Agent*" olarak adlandırılan hesap verebilirlik temsilcisi atanmasını zorunlu kılınmıştır.[51] Bu şekilde, sınır aşan veri akışlarında bölgesel düzenlemelere uyum pratik bir şekilde temin edilmektedir.

Tüm bunların yanında, Birleşmiş Milletler İş Hayatı ve İnsan Hakları Rehber İlkeleri'nden Koruma, Saygı Gösterme ve Telafi Edici Çözüm Üretme Çerçevesinin Uygulanması"[52] da hesap verebilirlik yaklaşımını yaygınlaştıran bir enstrüman olarak anılmaktadır.[53] Bu belge bağlayıcı olmasa da muhtelif yargı kararlarında iyi uygulama örneği olarak anıldığı içini hesap verebilirlik uygulamasına dolaylı bir etkisi vardır.

II. Avrupa Birliği Veri Koruma Hukukunda Hesap Verebilirlik İlkesi

A. Madde 29 Çalışma Grubu'nun Hesap Verebilirlik Raporu

Hesap verebilirlik ilkesi, bir sonraki bölümde detaylıca inceleneceği üzere GVK Tüzüğü'nde açıkça zikredilen bir kişisel verilerin korunması ilkesidir. Bu ilke Madde 29 Çalışma Grubu'nun (*Article 29 Data Protection Working Party*) öncülüğü sonucu GVK Tüzüğü'nde yer almıştır. Madde 29 Çalışma Grubu'nun 'Mahremiyetin Geleceği'[54] başlıklı 1 Aralık 2009 tarihli raporu ve sonrasında tamamen hesap verebilirlik konusuna adanmış 13 Temmuz 2010 tarihinde yayınlamış olduğu hesap verebilirlik görüşü hesap verebilirlik ilkesinin GVK Tüzüğü'nde yer almasının temelini atmıştır.[55]

Madde 29 Çalışma Grubu, veri korumanın teoriden uygulamaya geçmesi gerektiğini vurgulayarak, hesap verebilirlik temelli mekanizmaların etkin veri korumanın sağlanması için veri sorumlularına pratik araçlar/imkanlar sağladığını belirtmiştir. AB'nin 95/46 sayılı Direktifinde reform yapılarak, yeni düzenlemede hesap verebilirlik ilkesinin yer alması gerektiğini önermiş ve bunun veri sorumlusunun rolünü güçlendirerek, sorumluluğunu artıracağını ifade etmiştir.[56]

Madde 29 Çalışma Grubuna göre, kişisel veriler alanında hesap verebilirliği gerekli kılan üç temel gelişme vardır: (1) Veri tufanı etkisi olarak nitelendirilecek

[50] APEC, '*APEC Privacy Framework*' https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework [Erişim Tarihi: 01.09.2020]

[51] APEC, '*APEC Cross-Border Privacy Rules (CBPR) System*' http://cbprs.org/ [Erişim Tarihi: 01.09.2020]

[52] Birleşmiş Milletler, '*Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework'* (2011) https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf [Erişim Tarihi: 01.09.2020]

[53] De Hert (n 6) 197.

[54] Madde 29 Çalışma Grubu, '*The Future of Privacy'* (1 Aralık 2009) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf [Erişim Tarihi: 01.09.2020]

[55] Madde 29 Çalışma Grubu, '*Opinion 3/2010 on the principle of accountability'* (13 Temmiz 2010) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf [Erişim Tarihi: 01.09.2020]

[56] Madde 29 Çalışma Grubu (n 55) 3.

şekilde, var olan kişisel verilerin işlenmesini ve transferinin hızlıca artması; (2) Sürekli artan kişisel bilgilerin sosyal, politik ve ekonomik bağlamda değerinin artması; (3) Kişisel bilgilerin ihlallerinin artmasının hem kamuda hem özel sektördeki veri sorumluları için önemli olumsuz etkilerinin olması.[57] Bu gelişmeleri ve sorunları tanımladıktan sonra Çalışma Grubu, hesap verebilirliğin nasıl bir mimaride geliştirilmesi gerektiğini ortaya koymaya çalışmıştır. Çalışma Grubunun yerinde bir şekilde vurguladığı üzere, hesap verebilirliğe ilişkin kurallar temel kişisel verilerin korunması ilkelerini değiştirmemekte veya etkilememekte; sadece bu ilkeleri daha işler kılmaktadır.[58]

Çalışma Grubu, hesap verebilirliğin 'hukuki mimarisini' ikiye ayırmaktadır: (1) tüm veri sorumluları için geçerli olacak zorunlu temel hukuki yükümlülükler (2) minimum hukuki gerekliliklerin üstüne ve ötesine geçen gönüllü hesap verebilirlik sistemleri.[59] Zorunlu temel hukuki yükümlülükler ise uygulama tedbirleri/prosedürleri ve ilgili delillerin muhafazasını içermektedir.

Peki, hesap verebilirlik tam olarak nedir? Çalışma Grubuna göre hesap verebilirlik, sorumlulukların ne şekilde yerine getirildiğini göstermek ve bunu doğrulamaktır.[60] Bu bağlamda Çalışma Grubu, sorumluluk ile hesap verebilirliğin aynı madalyonun iki yüzü ve iyi yönetişimin temel unsurları olduğunu belirtmiştir.

Çalışma Grubu, hesap verebilirliğin farklı dillerdeki anlamı ve hukuki sistemlerdeki yaklaşımların çeşitliliği sebebiyle bu kavramın tam olarak tercüme edilemeyeceğini belirterek, kavramın sadece veri koruma alanı bağlamında ve belirlediği kapsamdaki tanımının esas alınması gerektiğini hatırlatmıştır.[61] Çalışma Grubu, hesap verebilirlik ilkesinin, diğer ilkeleri ve veri sorumlusunun alacağı tedbirleri somutlaştıracağı görüşündedir.[62] Her türlü veri işleme sürecine ve türüne bu ilke uygulanacağı için kişisel verilere daha etkin bir koruma sağlanacaktır. Çalışma Grubu, bu ilkenin sanılanın aksine veri sorumlularına ilave bir yükümlülük getirmediği, mevcut ilkelerin *de facto* şekilde etkinliğini artırdığı görüşündedir.[63]

Bir veri sorumlusunun hesap verebilirlik mekanizmalarını kurması, hukuki sorumluluğunu tamamen ortadan kaldırır mı? Bu soruyu ele alan Çalışma Grubu, bir veri sorumlusunun tüm tedbirleri yerine getirmesine rağmen, hatalı bir muhakeme neticesinde yanlış bir uygulama geliştirebileceğini belirtmiştir. Çalışma Grubuna göre, veri koruma otoriteleri bir ihlal sebebiyle yaptırım uygularken tedbirlerin

57 Madde 29 Çalışma Grubu (n 55) 4-5.

58 Madde 29 Çalışma Grubu (n 55) 5.

59 Madde 29 Çalışma Grubu (n 55) 6.

60 Madde 29 Çalışma Grubu (n 55) 7.

61 Madde 29 Çalışma Grubu (n 55) 8.

62 Madde 29 Çalışma Grubu (n 55) 9.

63 Madde 29 Çalışma Grubu (n 55) 10.

uygulanması ve doğrulanması, diğer bir deyişle hesap verebilirlik mekanizmalarının varlığı ve yaptırımın miktarını belirlerken bir ölçüt olarak kullanılabilir.[64]

Çalışma Grubu, mahremiyet etki analizi ve veri koruma sorumlusu atanmasını hesap verebilirlik ilkesinin tamamlayıcısı olarak saymıştır. Aynı doğrultuda, bağlayıcı topluluk kuralları (*binding corporate rules*), hesap verebilirliği veri sorumlusunun iç ve dış tüm organizasyonunda temin ettiği için önemli bir araç olarak belirtilmiştir. Keza, spesifik politikaların varlığı da (veri işlemenin farklı safhalarına ve paydaşlarına ilişkin) veri sorumluluğununun önemli bir bileşenidir.

Çalışma Grubu, daha da somutlaştırarak, veri sorumlularına yol göstermek adına Madrid Kararlarında yer aldığı gibi tahdidi olmayan şekilde bazı hesap verebilirlik araçlarını listelemiştir.[65] Önemli hesap verebilirlik araçlarını listeledikten sonra Çalışma Grubu, bu mekanizmaların veri işlemenin oluşturduğu risk ile işlenen kişisel verinin niteliği (örneğin, hassas nitelikli veri işleme durumu) dikkate alınarak uygulanması gerektiğini vurgulama gereği duymuştur.[66] Şeffaflık ise bu sürecin başarısını gösteren ana etken olarak sayılmıştır.

Hesap verebilirliğin, tüm bu araçlara rağmen hukuki belirlilik taşımadığı ve keyfi uygulamalara yol açabileceği ileri sürülebilir. Özellikle de esneklik ve de ölçeklenebilirliğin belirsizliği artırdığı iddia edilebilir. Çalışma Grubu, bu iddiayı yok saymamıştır. Çalışma Grubu, temel düzenlemede hesap verebilirliğin detaylı olarak yer almasının metodolojik açıdan uygun olmadığını belirtmiş ve burada başta kendi görüş ve çalışmaları olmak üzere, bu alanda ulusal rehberlerin gerekliliğine işaret etmiştir.[67] Nihayetinde uygulanacak tedbirin etkinliği ve bunun ölçümlenmesi de her somut durumda farklılaşacaktır.[68]

Çalışma Grubu'nun hesap verebilirlik ilkesine ilişkin ele aldığı bir diğer husus ise bu ilke karşısında veri koruma otoritelerinin durumudur. Hesap verebilirlik ilkesi, veri koruma otoritelerinin elini güçlendirir mi, zayıflatır mı? Çalışma Grubu, hesap verebilirlik ilkesinin veri koruma otoritelerin yetkisini daraltmayacağı ve denetimlerini daha etkin hale getireceği görüşündedir.[69] Nihayetinde veri sorumlusu uyumu yerine getirmek ve delillerini doğrulanabilir şekilde ortaya koymakla yükümlü olduğu için veri koruma otoritelerinin denetimi de kolaylaşacaktır. Bu şekilde, veri koruma otoriteleri kaynaklarını daha seçici ve stratejik olarak kullanabilecektir.

Çalışma Grubu'na göre veri koruma otoritelerin fonksiyonu daha *ex ante* bir

64 Madde 29 Çalışma Grubu (n 55) 11.

65 Madde 29 Çalışma Grubu (n 55) 12.

66 Madde 29 Çalışma Grubu (n 55) 12.

67 Madde 29 Çalışma Grubu (n 55) 14-15.

68 Madde 29 Çalışma Grubu (n 55) 14-15.

69 Madde 29 Çalışma Grubu (n 55) 16.

fonksiyondan ziyade *ex post* niteliktedir. Hesap verebilirlik de iyi bir veri koruma yönetişimi bağlamında belirli çıktıları hedeflediği için, veri işleme başladıktan sonra, yani *ex-post* niteliktedir.[70] Tabii *ex-post* aşamada yaptırımların da etkin şekilde kullanılması gerekmektedir. Şöyle ki, kendi bağlayıcı politikalarına uymayan bir veri sorumlusu aslında hesap verebilirlik ilkesini ihlal etmiş olacaktır. Çalışma Grubu, hem bu durumlarda yaptırım uygulanmasını hem de veri koruma otoritelerinin detaylı talimatlar vermesini önerdiği sistemin başarıya ulaşmasının koşulları olarak görmektedir.[71]

Peki, veri sorumluları uyumlu olduklarını ispat etmek için hangi araçları kullanacaklardır? Çalışma Grubu, sertifikasyon uygulamalarını hesap verebilirlik için önemli ispat araçları olarak saymakta ve bu alanın özel olarak düzenlenmesi gerektiğini hatırlatmaktadır.[72] Aynı çağrı, bağlayıcı topluluk kuralları bakımından da yapılmıştır.

Çalışma Grubu, özetle, sunmuş olduğu görüşte yer alan tüm tedbirlerin hem kamu hem de özel sektördeki tüm veri sorumluları tarafından uygulanması gerektiğini, bu tedbirlerin ölçeklendirilmesi gerektiğini ve tüm tedbirlerin veri işleme ile verinin niteliğinin oluşturduğu riskle uyumlu olması gerektiğini belirterek, hesap verebilirliği tüm bu gereklilikleri yansıtan yeni bir veri koruma ilkesi olarak önermiştir.

B. Avrupa Birliği Genel Veri Koruma Tüzüğü

Madde 29 Çalışma Grubu'nun hesap verebilirlik ilkesine ilişkin önerisi, GVK Tüzüğü'nde karşılığını bulmuştur. Hesap verebilirlik ilkesi, Avrupa Birliği'nde kişisel verilerin korunması konusunun direktif ("*directive*") ile düzenleme yönteminden tüzük ("*regulation*") ile düzenleme yöntemine geçilmiş olmasıyla yatay düzeyde doğrudan uygulanan yeni veri koruma hukuku düzeninin üzerine kurulduğu ilkedir. Bu bağlamda, hesap verebilirlik ilkesi bu değişikliğin merkez üssünde durmaktadır.

Hesap verebilirlik, GVK Tüzüğü'nün ana metninde sadece bir yerde, parantez içinde ve resitallerde sadece bir yerde yer bulan bir ilkedir. Resitali de dahil sadece iki kez anılan bu ilke, GVK Tüzüğü'nün en önemli yeniliğidir.[73] Zira, kişisel verilerin korunması alanında hukuka aykırılıkla mücadele veri sorumlusunun cephesine taşınmıştır. Avrupa Birliği hukukunda kişisel verilerin korunması alanındaki bu temel paradigma değişikliğiyle, devlet tarafından denetlenme unsuru arka plana geçerek, sorumluluk veri sorumlusu ve/veya veri işleyene yüklenmektedir.[74]

---

70 Madde 29 Çalışma Grubu (n 55) 17.

71 Madde 29 Çalışma Grubu (n 55) 17.

72 Madde 29 Çalışma Grubu (n 55) 17.

73 Christopher Docksey, '*Article 24 - Responsibility of the controller*' in Christopher Kuner, Lee A Bygrave ve Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020), 557.

74 Mesut Serdar Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu* (On İki Levha 2018), 12.

Hesap verebilirlik ilkesi, kişisel verileri işlenen ilgili kişilerin haklarının en üst düzeyde korunmasını temin eden bir ilkedir. Bu ilke sayesinde, kişisel verilerin işlenmesi sürecinde bir sorumluluk ekosistemi oluşturulmaktadır. GVK Tüzüğü'nün 5. maddesinin ilk fıkrasında altı ilke (hukukilik, dürüstlük ve şeffaflık ilkesi, amaçla sınırlılık ilkesi, veri minimizasyonu ilkesi, doğruluk ilkesi, saklama süresinin sınırlandırılması ilkesi, bütünlük ve gizlilik ilkesi) sayılırken, maddenin ikinci fıkrasında tüm bu altı ilkeye çapraz-atıf yapılarak hesap verebilirlik ilkesine yer verilmiştir.[75] 5. maddenin ikinci fıkrasını hatırlatmak gerekirse: "*Veri sorumlusu, 1. fıkraya uygun davranmaktan sorumludur ve buna uygun davrandığını gösterebilmelidir.*"

GVK Tüzüğü'nün 24. maddesi veri sorumlusunun temel yükümlülüklerini tanımlamaktadır. Söz konusu hükme göre veri sorumlusu, işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak işleme faaliyetinin GVK Tüzüğü uyarınca gerçekleştirilmesini sağlamak ve bu şekilde gerçekleştirildiğini gösterebilmek için uygun teknik ve idari tedbirler uygulamakla yükümlüdür. Keza, veri sorumlusu bu tedbirleri gözden geçirmek ve gerektiğinde, güncellemekle yükümlüdür. 24. maddenin ikinci fıkrasında, uygun veri koruma politikalarının uygulanmasına vurgu yapılırken, üçüncü fıkrasında onaylı davranış kuralları ve sertifikasyon mekanizmalarının veri sorumlusunun yükümlülüklerine uygunluğun gösterilmesine ilişkin araç olarak kullanılmasına izin verilmiştir.

GVK Tüzüğü'nün 24. maddesinin en temel çıktıları, risk temelli yaklaşımla uyum gerçekleştirmek, uyumun ispatı için uygun teknik ve idari tedbirleri uygulamak ve gerektiği hallerde bunları güncellemektir. Diğer bir deyişle, dinamik, yaşayan bir uyum yaklaşımı benimsenmiştir. Keza, GVK Tüzüğü'nün 30. maddesi uyarınca her veri sorumlusunun kendi mesuliyeti altındaki işleme faaliyetlerinin kaydını tutması zorunludur. Tıpkı GVK Tüzüğü'nün 5. maddesinin ikinci fıkrası gibi 24. maddesinde de "gösterebilmek" (*to be able to demonstrate*) kelimesi kullanılmıştır. İlk durumda ilkelere uyumun ispatı, ikinci durumda ise işlemenin GVK Tüzüğü'ne nasıl uyumlu gerçekleştirildiğinin ispatı konudur.

Avrupa Birliği hukukundaki en temel tartışma hesap verebilirlik ilkesinin müstakil bir ilke olup olmadığıdır. Diğer bir ifadeyle, hesap verebilirlik sadece diğer ilkelere uyulmasını temin eden bir ilke midir, yoksa başlı başına gözetilmesi gereken bir ilke midir? Nihayetinde, müstakil bir ilke olup olmaması aykırılık durumunda uygulanacak yaptırımı da belirleyecektir. Şöyle ki, eğer müstakil bir ilke olarak kabul

[75] Tüm ilkeler ve gereklilikleri hakkında özet bir tablo için bkz EDPS, '*Guidelines on the protection of personal data in IT governance and IT management of EU institutions*' https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf [Erişim Tarihi: 01.09.2020]

edilirse, diğer ilkelere riayet edilse bile salt bu ilkenin gereğinin yerine getirilmemesi bir hukuka aykırılık hali oluşturacaktır. Eğer müstakil bir ilke olarak kabul edilmezse, ancak başka bir ilkenin ihlali durumunda esas ölçü norm değil, destek ölçü norm gibi bir muameleye tabi tutulacaktır.

Bir görüşe göre, AB hukukunda hesap verebilirlik, müstakil şekilde yaptırıma bağlanan bir ilke değildir.[76] Bu ilke, diğer ilkelere uyumu temin eden bir ilkedir ve iki temel unsuru vardır: uyumu temin etmek için alınan iç tedbirleri ve haricen bu uyumun nasıl gerçekleştirildiğini gösterebilmek. Başka bir görüşe göre ise, hesap verebilirlik, diğer ilkelerden müstakil olarak yaptırıma neden olabilecek bir ilkedir.[77]

GVK Tüzüğü, nispeten yeni bir düzenleme olsa da Avrupa Birliği Adalet Divanı ("*ABAD*") önünde ihtilaflara konu olmaya başlamıştır. GVK Tüzüğü ile getirilen hesap verebilirlik ilkesinin de niteliği tartışılmaya başlanmıştır. ABAD Hukuk Sözcüsü Szpunar, C-61/19 referanslı davada rızanın alınmasına ilişkin sunmuş olduğu görüşte GVK Tüzüğü'nün 7. maddesinin birinci fıkrasında yer alan rızaya ilişkin veri sorumlusunun yükümlülüğünü hesap verebilirlik ilkesinin bir uzantısı olarak nitelendirmiştir. Söz konusu hükme göre işleme faaliyetinin rızaya dayandığı hallerde, veri sorumlusu veri süjesinin kişisel verilerinin işlenmesine rıza göstermiş olduğunu ispatlamakla yükümlüdür. Hukuk Sözcüsü Szpunar'a göre hesap verebilirliği düzenleyen GVK Tüzüğü'nün 5. maddesinin ikinci fıkrası veri sorumlusunun sadece ilgili kişinin kendisine rıza verdiğini değil rızaya ilişkin tüm koşulların da gereğince yerine getirildiğini ispat etmesini gerektirmektedir.[78]

Esasında AB veri koruma hukuku, bir bütündür. Farklı düzenlemeler ve araçlar, birbirini tamamlamaktadır.[79] Hesap verebilirlik ilkesi, bu bütünü birbirine bağlayan ve anlamlı kılan özel bir ilkedir. Öyle ki, hesap verebilirlik diğer ilkelerle sıkı ve karşılıklı bir ilişki içerisindedir. Örneğin, şeffaflık ilkesi, hesap verebilirlik ilkesini destekler. Hesap verebilirlik ise şeffaflığın seviyesini ve içeriğini belirler. Hesap verebilirlik ilkesinin uygulamadaki karşılığı, veri sorumlularının yükümlülüklerine uyumu sağlamak için veriyi nasıl ele aldıklarına dair daha şeffaf ve proaktif olmaları gerektiği şeklinde yorumlanmaktadır.[80] Bu bağlamda hesap verebilirlik ilkesinin en somut çıktısı sistematik işlem kaydı tutmaktır. GVK Tüzüğü ile kurulan sistemin

[76] Gehan Gunasekara, '*Paddling in unison or just paddling? International trends in reforming information privacy law*' (2013) 22 International Journal of Law and Information Technology 141, 22.

[77] Docksey (n 73) 566-567.

[78] ABAD, Opinion of Advocate General Szpunar: Case C-61/19 Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), 4 Mart 2020, para. 49.

[79] Örneğin, AB kurumlarının tüm veri işleme süreçlerinde hesap verebilirlik yaklaşımını sağlaması için Avrupa Veri Koruma Süpervizörü müstakil rehberler yayınlamıştır. Bkz EDPS, '*Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies*', https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en [Erişim Tarihi: 01.09.2020]

[80] Privacy International, '*A Guide for Policy Engagement on Data Protection - The Keys to Data Protection*' (2018) https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf [Erişim Tarihi: 01.09.2020], 46.

kayıt tutma yükümlülüğünü ve bu kayıtlarda ne gibi spesifik bilgilerin bulunması gerektiğini daha da somutlaştırdığı belirtilmektedir.[81]

Nihayetinde veri işlemenin hukuki sebebin ve amacın sınırları çerçevesinde kalıp kalmadığını temin etmek için sürekli bir denetim ve doğrulama yapılması kaçınılmazdır. Öyle ki hem yazılım hem donanım seviyesinde güvenliğin sağlanması, algoritmik uyumu temin etmek ve hesap verebilirliği sağlamak amacıyla kaynak kodlarının gözden geçirilmesi, tasarımda mahremiyet yaklaşımının benimsenmesi hesap verebilirliğin sürdürülebilir kılınmasının en temel araçlarıdır.[82] Hesap verebilirlik, güvenlik ihlali bildirimi yapıp yapmamanın da kararının verilmesi için en temel yol gösterici ilkedir.[83]

Hesap verebilirlik, müstakil şekilde yaptırıma konu olan bir ilke olarak kabul edilmelidir. Bunun gerekçesi ise, hesap verebilirlik yaklaşımının bir ihlalin çıkmasını önlemesi veya zararın etkisini minimize etmesidir. Bu şekilde kişisel verilerin veri sorumlusunun tüm iş süreçlerinde en üst düzeyde korunması mümkün olacaktır. Hesap verebilirlik müstakil bir ilke olarak kabul edilmezse, sorumluluk olmayan bir hesap verebilirlik durumu ortaya çıkacaktır ki bu durumda ilkenin normatif hiçbir değeri kalmayacaktır. Ayrıca, kişisel verilerin işlenmesi ve korunmasında risk temelli yaklaşım artık bir zorunluluk haline geldiği için, bu yaklaşımı veri sorumlusu nezdinde egemen kılacak temel ilke olan hesap verebilirliğin somut bir karşılığının olması gerekir.

III. Temel Hesap Verebilirlik Araçları

Hesap verebilirlik ilkesinin bir sonucu olarak, kişisel verilerin korunması alanında ispatlanabilir bir uyum sürecinin gerçekleşmesi gerekmektedir. Hesap verebilirlik, özdenetim mekanizmalarını artırdığı için burada uyumun veri sorumlusunun tanımlı bir iç süreci olarak var olması gerekmektedir. Kişisel verilerin korunması alanındaki düzenlemelerin sayısı ve kapsamı gün geçtikçe artmakta ve karmaşık hale gelmektedir. Hacimce büyüyen bu mevzuat bütünü karşısında veri sorumlularının ve veri işleyenlerin pratik araçlara ihtiyacı vardır.

Madde 29 Çalışma Grubu'nun da işaret ettiği üzere, hesap verebilirlik ilkesi ve beraberinde hayata geçirilecek uyum ispat araçları veri koruma otoritelerinin de denetim işlerini kolaylaştıran niteliktedir. Bu tür araçlar, süreçleri daha standardize hale getirdikleri için veri sorumluları ve otoriteler arasındaki bilgi asimetrisinden kaynaklanan sorunları da azaltmaktadır. Bu durum çok yerinde bir şekilde "*daha az denetim ve daha çok sorumluluk*" olarak özetlenmektedir.[84]

[81] Paul B Lambert, *Understanding the New European Data Protection Rules* (CRC Press - Taylor & Francis 2018), 162-163.

[82] Ronald, Leenes/Rosamunde, Van Brakel/Serge, Gutwirth/Paul De Hert (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer 2017).

[83] Lambert (n 81) 306.

[84] Çekin (n 74) 113.

AB veri koruma hukukunda hesap verebilirlik ilkesinin yerine getirilmesi sırasında kullanılabilecek doğrudan ve dolaylı muhtelif hesap verebilirlik araçları bulunmaktadır. Veri koruma görevlisi atamak, veri koruma etki analizi gerçekleştirmek, davranış kuralları ve sertifikasyon kullanmak, doğrudan hesap verebilirlik araçları olarak sayılabilir. Bunlar dışında tasarımda mahremiyetin sağlanması da bir hesap verebilirlik gereğidir, kişisel verileri güvenli ülkeler içerisinde işlemek, bağlayıcı topluluk kurallarına sahip olmak[85], ilgili kişilerin haklarını etkin kullanmasını sağlamak veya veri taşınabilirliğini pratik şekilde gerçekleştirmek de aynı şekilde uygun araçlardır. Bu çalışmanın amacı da dikkate alındığında, bu bölümde doğrudan hesap verebilirlik araçları genel hatlarıyla ele alınacaktır.

A. Veri Koruma Etki Analizi

Veri koruma etki analizi, GVK Tüzüğü'nün yeniliklerindendir. GVK Tüzüğü'nün 'veri koruma etki analizi' başlıklı 35. maddesi uyarınca veri sorumlusu, özellikle yeni teknolojiler kullanıldığında ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçları dikkate alındığında bir işleme türünün gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, işleme faaliyetinden önce, öngörülen işleme faaliyetlerinin kişisel verilerin korunmasına olan etkisine ilişkin bir değerlendirme yapmakla yükümlü tutulmuştur.[86] Tek bir değerlendirmede benzeri yüksek riskler taşıyan bir dizi benzer işleme faaliyetinin ele alınması mümkündür.

Veri koruma etki analizi, veri sorumlusunun önemli hukuki neticeleri olan bir iç operasyonudur. Veri etki analizi veya farklı ifadeyle "*mahremiyet etki analizi*", kişisel veri işlemeyi içeren bir projenin, politikanın, programın, hizmetin, ürünün veya başka bir girişimin mahremiyet üzerindeki etkilerinin değerlendirildiği ve diğer paydaşlarla da danışarak, olumsuz etkileri önlemek veya asgariye indirmek için gerekli telafi edici eylemlerin alındığı bir süreçtir.[87] Veri koruma etki analizi, bu bağlamda bir erken uyarı mekanizmasına benzetilmektedir.[88] Bir nevi, testi kırılmadan testinin kırılma simülasyonunu hazırlamayı, ortaya çıkacak durumu gözetmeyi gerektirmektedir.

Veri koruma etki analizi, dinamik bir süreçtir ve her bir veri işleme sürecinde bu analizin gerekli olup olmadığı (pozitif veya negatif kapsamın) sorgulanması

85 Madde 29 Çalışma Grubu (n 55) 7.

86 GVK Tüzüğü'nün 35. maddesi uyarınca veri sorumlusu, atanmışsa veri koruma görevlisine de başvurarak, (1) gerçek kişilerle ilgili kişisel özellikler hususunda profil çıkarma da dahil olmak üzere otomatik işlemeye dayalı olan ve gerçek kişi ile ilgili hukuki sonuçlar doğuran veya gerçek kişiyi kayda değer şekilde etkileyen kararların dayandığı sistematik ve kapsamlı bir değerlendirme yapıldığı; veya (2) özel nitelikli kişisel verilerin veya mahkumiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin büyük çaplı olarak işlendiği; veya (3) kamunun erişebileceği bir alanın büyük çaplı olarak sistematik bir şekilde izlendiği durumlarda veri koruma etki analizi gerçekleştirmesi beklenmektedir. Keza, hangi durumlarda bu tür bir analiz yapılacağına (pozitif) ve hangi durumlarda yapılmayacağına dair (negatif) dair bir belirleme yapmaya ilişkin listelerin belirlenmesi de pekâlâ mümkündür.

87 David Wright ve Paul De Hert (eds), *Privacy Impact Assessment* (Springer 2012), 5.

88 Çekin (n 74) 116.

zorunludur. Bu süreç, işleme prosedürünün sistematik şekilde tanımı ve işlenme amaçlarının belirtilmesi, işleme prosedürünün sistematik şekilde tanımı ve işlenme amaçlarının belirtilmesi, ilgili kişilerin hak ve hürriyetleri açısından risk değerlendirmesi, söz konusu risklere karşı alınan önlemleri içermelidir. Eğer ki, bir sorun tespit edilirse, işleme süreci başlatılmadan önce bunun düzeltilmesi ve bu şekilde verisi işlemeye konu ilgili kişilerin korunması mümkün olmaktadır. Veri sorumlusu, olumlu veya olumsuz neden bu karara varıldığını, bu karar alındıktan sonra nasıl bir süreç işletildiğini tüm detaylarıyla raporlamak ve bu sürecin eksiksiz işletildiğini ispat etmekle yükümlüdür. Bu yönleriyle, veri koruma etki analizi en temel hesap verebilirlik aracıdır.

B. Veri Koruma Görevlisi

GVK Tüzüğü'nün bir diğer yeniliği ise veri koruma görevlisidir. Kişisel verilerin korunması mevzuatına uyum teknik, hukuki ve de yönetimsel hususların aynı anda gözetilmesini ve karar alma süreçlerine dahil edilmesini gerektirmektedir. Bu süreç, oldukça özellikli bir hal almıştır. Öyle ki, bu alandaki ulusal ve uluslararası mevzuat hızla gelişmekte, veri koruma otoritelerinin kararları ve mahkeme içtihatlarıyla alan dinamik şekilde kapsam ve şekil değiştirmektedir. Bu tablo karşısında veri sorumlusu bünyesinde, hesap verebilirliğin de bir uzantısı olarak bu süreci koordine edecek bir aktörün varlığının ihtiyacı kaçınılmaz hale gelmektedir.[89]

GVK Tüzüğü, veri koruma görevlisi olarak tanımladığı bir aktörün, atanması, konumu ve görevlerini etraflıca düzenlemiştir. GVK Tüzüğü öncesinde de veri sorumluları bünyesinde benzer bir aktör veya yapılar gözlemlenmekteydi. GVK Tüzüğü, bu aktörün hukuki çerçevesini belirlemek suretiyle kurumsallaşmasını sağlamıştır.

GVK Tüzüğü'nün 37. maddesi uyarınca (hangi tür kişisel veri işlediğinden bağımsız olarak) tüm kamu kurum ve kuruluşlarında veri koruma görevlisi atamak zorunludur. Bunun dışında veri sorumlusu ve veri işleyenin esas faaliyeti şekil kapsam ve amaç açısından kişilerin kapsamlı ve sürekli şekilde gözetlenmesi ise veya veri sorumlusu ve veri işleyenin esas faaliyeti kapsamlı şekilde özel nitelikteki verilerin işlenmesi ise veri koruma görevlisi atanması zorunludur.

Veri koruma görevlisi, kişisel verilerin işlenmesi sürecindeki tüm paydaşların (veri koruma otoriteleri, veri süjeleri (ilgili kişiler), veri sorumluları, veri işleyenler gibi) arasında iletişimi ve koordinasyonu sağlayan bir aracı konumundadır. [90] Muhataplık sorununu önemli ölçüde ortadan kaldıran bir fonksiyonu vardır. Veri koruma

[89] Bu konuda bkz Madde 29 Çalışma Grubu, '*Guidelines on Data Protection Officers ('DPOs')'* (13 Aralık 2016) http://ec.europa.eu/newsroom/document.cfm?doc_id=44100 [Erişim Tarihi: 01.09.2020], 4.

[90] Madde 29 Çalışma Grubu (n 89) 4.

görevlisi doğrudan veri sorumlusu veya işleyenin en üst yönetimine rapor verme yetkisini haizdir. Veri koruma görevlisi atanması sadece veri sorumlusunun değil, veri işleyenin de yükümlülüğüdür.[91]

GVK Tüzüğü'nün 38. maddesi, veri koruma görevlisinin konumunu da tam olarak ortaya koymaktadır. Veri sorumlusu ve veri işleyen, veri koruma görevlisinin kişisel verilerin korunmasına ilişkin tüm konulara uygun bir şekilde ve zamanında müdahil olmasını sağlamakla; kişisel veriler ile işleme faaliyetlerine erişilmesi ve uzmanlık bilgisinin aynı seviyede tutulması için gereken kaynakları sağlamakla yükümlüdür.

Veri koruma görevlisi, GVK Tüzüğü ile özel olarak tanımlanmış bir aktör olduğu için veri sorumlusu ve veri işleyen, veri koruma görevlisine bu görevlerinin yerine getirilmesi ile ilgili olarak talimat veremez, görevlerinin yerine getirilmesi nedeniyle veri sorumlusu ya da veri işleyen tarafından işten çıkarılamaz veya cezalandırılamaz. Diğer bir ifadeyle yeri koruma görevlisi, bir nevi veri koruma otoritesinin veri sorumlusu bünyesindeki iç ajanıdır.[92]

Veri koruma görevlisi, veri sorumlusu ve veri işleyen bünyesinde düzenli işleme kayıtlarının tutulması, tüm iş süreçlerinde ve karar alma süreçlerinde yasal yükümlülüklerin gözetilmesini temin ettiği için temel bir hesap verebilirlik aracı niteliğindedir.[93] Keza, hesap verebilirliğin en önemli gerekliliği olan veri koruma süreçlerinin sürdürülebilirliğini de temin etmektedir.

C. Davranış Kuralları ve Sertifikasyon

Davranış kuralları ve sertifikasyon mekanizmaları, gönüllülük esasına göre kullanılan enstrümanlardır. Davranış kuralları, bir işletmenin veri işleme süreçlerinin büyük bir çoğunluğunu esas alan ve belirli sektörlerde gerçekleştirilen veri işleme faaliyetlerinin hukuka uygun şekilde gerçekleştirilmesini amaçlayan kurallar iken, sertifikalar daha çok, belirli veri işleme süreçlerinin hukuka uygunluğunu belgelemek amacıyla kullanılan araçlardır.[94] Çok yalın bir tanımlamayla davranış kuralları belirli bir sektör veya teknolojiye ilişkin GVK Tüzüğü kapsamındaki yükümlülükleri adreslerken, sertifikasyonlar GVK Tüzüğü kapsamındaki onaylı faaliyetler için uyumu ispatlamak için kullanılmaktadır.[95] Süreçleri ve işlemeleri belgeleme fonksiyonu sebebiyle davranış kuralları ve sertifikasyon, hesap verebilirliğin en temel araçlarındandır.

---

91 Madde 29 Çalışma Grubu (n 89) 9.

92 Veri koruma görevlisi, nitelikleri ve sorumlulukları sebebiyle sıklıkla iş güvenliği uzmanına benzetilmektedir.

93 Bkz Madde 29 Çalışma Grubu (n 89) 4; Aynı görüş için bkz Paul B Lambert, *The Data Protection Officer - Profession, Rules, and Role* (CRC Press - Taylor & Francis 2017), 94-95.

94 Çekin (n 74) 233.

95 Paul Voigt/Axel Von dem Bussche, *The EU General Data Protection Regulation (GDPR) A Practical Guide* (Springer 2017), 5.

Davranış kuralları ve sertifikasyon, klasik devlet regülasyonunun aksine, düzenleme kısmını diğer paydaşlara bıraktığı için regüle edilmiş öz-düzenleme kategorisinde "*regulated self-regulation*" (*co-regulation, enforced self-regulation, enforced voluntary regulation, audited regulation* vb.) enstrümanlardır.[96] Keza, bu enstrümanların oluşturduğu sistem beraber düzenleme "*işbirlikçi yönetişim*" olarak da anılmaktadır.[97]

GVK Tüzüğü'nün 40. maddesinde düzenlenen davranış kuralları, meslek kuruluşları gibi ilgili paydaşların kendi üyeleri için hazırladıkları ve tüm üyelerinin aynı şekilde tabi olduğu kurallar bütünüdür. İlgili paydaş tarafından hazırlanan davranış kuralı, yetkisine tabi olunan veri koruma otoritesinin onayına sunulmak zorundadır.

Davranış kuralları, veri koruma otoritelerinin yetkisini tamamen ortadan kaldırmamaktadır. Keza, bu kuralların varlığı diğer hukuki yükümlülüklere halel getirmemektedir. Bu mekanizmanın en önemli pratik çıktısı, davranış kuralları içerisinde hareket edildiği ispat edilirse, o işleme için hukuka uygunluk karinesinden faydalanılmasıdır.

Sertifikalar ise GVK Tüzüğü'nün 42 ve 43. maddelerinde düzenlenmiştir. Sertifikalar salt GVK Tüzüğü'ne özel bir araç değildir; Avrupa Birliği hukukunda farklı konularda düzenlenen ve uygulanagelen bir enstrümandır. Düzenleme olarak, doğrudan veri koruma otoritesi sertifikasyon sürecini düzenleyip yönetebileceği gibi, bu alanda başka otoriteleri de akredite edip, süreci sadece denetlemekle yetinebilir. Hangi yöntem tercih edilirse edilsin sertifikasyonun hesap verebilirliği göstermek, işlemenin güvenliğini ispatlamak ve tercih edilecek veri işleyeni tercihi kolaylaştırmak gibi bir rolü olduğu belirtilmektedir.[98]

Sertifikasyon olarak kullanılacak özel mühürler (seals) veya damgalar (marks) kullanıldığı durumlarda, kapsamlı bir belgeleme ve standardize hale gelmiş işlem kayıtları tutulması zorunlu olduğu için, sertifikasyonların en çok hesap verebilirlik ilkesine hizmet ettiği söylenebilir. Uyum ispat araçları, denetim araçlarının işletilmesini de standardize hale getirdiği için veri koruma otoritelerinin denetimini kolaylaştırmaktadır.

IV. Türk Veri Koruma Hukukunda Hesap Verebilirlik İlkesi

Türk Hukukunda kişisel verilerin korunması alanındaki temel düzenleme 6698 sayılı Kişisel Verilerin Korunması Kanunu'dur.[99] Kanun'un 4. maddesinde beş temel

[96] Çekin (n 74) 232.

[97] Serge Gutwirth, Ronald Leenes ve Paul De Hert (eds), *Data Protection on the Move - Current Developments in ICT and Privacy/Data Protection* (Springer 2016), 145.

[98] Rowena Rodrigues ve Vagelis Papakonstantinou (eds), *Privacy and Data Protection Seals* (T.M.C. Asser Press 2018), 26-27.

[99] RG 07.04.2016/29677.

genel veri koruma ilkesi yer almaktadır: (1) Hukuka ve dürüstlük kurallarına uygun olma (2) doğru ve gerektiğinde güncel olma (3) belirli, açık ve meşru amaçlar için işlenme; (4) işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma (5) ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

Hesap verebilirlik, Kişisel Verilerin Korunması Kanunu'nda açıkça zikredilen bir ilke değildir. Esasında, Kanun her ne kadar GVK Tüzüğü ile aynı dönemde kabul edilmiş olsa da esas olarak 95/46 sayılı AB Direktifi esas alınarak hazırlanmıştır. Dolayısıyla, hesap verebilirlik ve şeffaflık ilkeleri kanunda yer bulmamıştır. Öte yandan 2019-2023 yıllarını kapsayan 11. Kalkınma Planında Kişisel Verilerin Korunması Kanunu'nun GVK Tüzüğü dikkate alınarak güncellenmesi politik hedefi vardır. Dolayısıyla, uzun vadede bu reform çalışmaları neticesinde hesap verebilirlik ilkesinin de Türk hukukunda yer alması beklenmektedir.

KVK Kanun'unda temel hesap verebilirlik araçları olan veri koruma etki analizi ve veri koruma görevlisi yükümlülükleri de düzenlenmemiştir. Keza, davranış kuralları, sertifikasyon ve bağlayıcı topluluk kurallarına da doğrudan bir atıf yoktur. Lakin, KVK Kanunu'na uyuma ilişkin KVK Kurumu'nun genel düzenleyici yetkileri kapsamında bu konuda bir düzenlemeye gidilmesi pekâlâ mümkündür. Nitekim 10 Nisan 2020 tarihinde bu araçlardan bağlayıcı şirket kurallarına ilişkin atipik bir düzenleme yapılmıştır.[100]

A. Kişisel Verileri Koruma Kurumu'nun Yaklaşımı

Kişisel Verileri Koruma Kurumu, hesap verebilirlik ilkesine özel bir önem atfetmektedir. Öyle ki, Kurum'un Misyon ve Vizyon bağlamında temel ilke ve değerleri arasında şeffaflık ve hesap verilebilirlik ilkesini özel olarak sayılmaktadır.[101] Bu değer, Kurum'un faaliyetlerini mevzuata uygun şekilde yürüterek kararlarını kurallar ve düzenlemeler doğrultusunda açık ve anlaşılır bir şekilde alacağı, ilgili taraflarla paylaşacağı ve gerektiğinde yaptığı işlemler hakkında ilgililere açıklama yapacağı şeklinde açıklanmıştır.[102] Burada hesap verebilirlik kavramı genel anlamıyla kullanılmıştır ve veri işleme süreçlerinden ziyade Kurum'un genel olarak hesap verebilir olduğu ifade edilmiştir. 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'ndaki hesap verebilirlik ilkesini yansıtmaktadır.

Öte yandan, bir veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle KVK

[100] KVK Kurumu, '*Bağlayıcı Şirket Kuralları Hakkında Duyuru*', https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU [Erişim Tarihi: 01.09.2020]

[101] KVK Kurumu, '*Misyon - Vizyon*' https://www.kvkk.gov.tr/Icerik/2074/Misyon---Vizyon [Erişim Tarihi: 01.09.2020]

[102] KVK Kurumu, '2018 Yılı Faaliyet Raporu' https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/cef9699a-579d-4fbd-ab45-cade6f2bba3b.pdf [Erişim Tarihi: 01.09.2020], 18.

Kurulu'na yapmış olduğu başvuruya verilen yanıtta, meşru menfaat belirlenirken söz konusu yararın çok sayıda kişiyi etkilemesi, yalnızca kâr elde edilmesi ya da ekonomik yararın sağlanması amacına yönelik olmaması, iş süreçlerini ya da bir işleyişi kolaylaştırması) gibi şeffaf ve hesap verilebilir nitelikleri haiz kriterlerin esas alınması gerektiği belirtilerek, açıkça hesap verebilirliğe atıf yapılmıştır.[103] Bu karardaki hesap verebilirlik, genel değil özel anlamında kullanılmıştır. Bu açıdan önemli niteliktedir.

KVK Kurumu'nun hesap verebilirliğe açıkça değindiği bir diğer bağlam ise bağlayıcı şirket kurallarıdır ("BŞK"). KVK Kurumu, BŞK için yapılan başvurularda "Hesap Verebilirlik ve Diğer Esaslar/Araçlar" başlığı altında grup üyelerinin, BŞK için nasıl uyum sağlayacağı ve bundan nasıl sorumlu tutulacağını ve grup üyeleri tarafından, her bir veri sorumlusu adına BŞK kapsamında gerçekleştirilecek işleme faaliyetlerinin kaydının nasıl tutulacağının açıklamasını talep etmektedir.[104] Ayrıca, BŞK bakımından hesap verebilirliğin sağlanması amacı ile söz konusu kişisel veri işleme envanterinin hazırlanması gerekmektedir.

KVK Kurumu, hesap verebilirlik ve araçlarını da açıklamaktadır.[105] Kurum, BŞK için başvuracak her bir veri sorumlusunun, BŞK'ye uyumu göstermekle yükümlü ve sorumlu olduğunu belirttikten sonra, uyumun sağlanabilmesi için BŞK üyelerinin, tüm kategorilerdeki veri işleme faaliyetlerinin elektronik yöntemler de dâhil olmak üzere yazılı şekilde kaydını tutması ve talep halinde KVK Kurum'una sunması gerektiğini hatırlatmaktadır. Kurum ayrıca, uyumluluğun artırılması ve gerektiğinde, gerçek kişilerin hak ve özgürlükleri bakımından yüksek risk oluşturması muhtemel olan veri işleme faaliyetleri için risk analizi yapılması gerektiğinin altını çizmektedir.

Kurum, 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 KVK Kurumu'na danışılması gerektiğini belirtmiş, ayrıca veri koruma ilkelerini uygulamak ve uygulamada BŞK'ler tarafından belirlenen gereksinimlere uyumu kolaylaştırmak için uygun teknik ve idari tedbirlerin alınması gerektiğini vurgulamıştır.

BŞK ile ilgili KVK Kurumu düzenlemesinde KVK Kurumu'nun hesap verebilirliği GVKT bağlamındaki anlamıyla yorumladığı görülmektedir. Tüm veri işleme faaliyetlerinin düzgün tanımlanmasını sağlamak için tüm prosedürlerin haritasını

[103] KVK Kurulu, Karar Tarihi: 25.03.2019, Karar No: 2019/78, https://www.kvkk.gov.tr/Icerik/5434/2019-78 [Erişim Tarihi: 01.09.2020]

[104] KVK Kurumu, '*Bağlayıcı Şirket Kuralları, Veri Sorumluları İçin Bağlayıcı Şirket Kuralları Başvuru Formu*' https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/0aa5e8ce-8e4e-403c-a444-7212f581ad23.docx [Erişim Tarihi: 01.09.2020]

[105] KVK Kurumu, '*Bağlayıcı Şirket Kuralları, Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman*', https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/62fb06e5-d623-404d-b3a1-c492891a3bbb.docx [Erişim Tarihi: 01.09.2020]

çıkarma ve tüm veri işleme faaliyetlerinin bir envanterini tutma, detaylı işlem kaydı tutulması, gereken durumlarda veri etki analizinin gerçekleştirilmesi ve Kurum'a ön istişare için başvurulması ve riskin gerektirdiği uygun tedbirlerin alınması da AB hukukuyla paralel şekilde temel hesap verebilirlik araçları olarak anılmıştır.

B. Hesap Verebilirlik Açısından VERBİS

KVK Kurumu'nun hesap verebilirliğe özel olarak değindiği bir diğer bağlam ise veri sorumluları sicili, VERBİS'tir. VERBİS neden kamuya açık tutulmaktadır sorusunun yanıtı olarak Kurum, hesap verebilirliği gerekçe göstermiştir. Kişisel verisi işlenen gerçek kişilerce verileri üzerinde kontrolün sağlanabilmesi, kişisel verilerini işlediği gerçek kişilere her zaman hesap verebilir olması ve şeffaflık ilkeleri gereği VERBİS'e girilen bilgilerin görüntülenebilmesi ve varsa ihlalin tespiti için Kişisel Verilerin Korunması Kanunu'nun, kamuya açıklık ilkesini benimsediği belirtilmiştir.[106] Bu konudaki benzer kararlarda da Veri sorumlularına, Kişisel Verilerin Korunması Kanunuyla VERBİS'e kayıt ve bildirim yükümlülüğü getirilmiş olmasının amacı; kişisel verilerin korunması alanında toplumun tüm kesimlerinde kültür ve farkındalık oluşması ve veri sorumlularının kişisel verisini işlediği kişilere hesap verebilmesi olarak izah edilmiştir.

VERBİS, statik bir sicil değildir. Veri Sorumluları Sicili Hakkında Yönetmeliğin 13. maddesi uyarınca veri sorumluları, VERBİS'te kayıtlı bilgilerde bir değişiklik olması halinde meydana gelen değişiklikleri, değişikliğin meydana geldiği tarihten itibaren yedi gün içerisinde VERBİS üzerinden KVK Kurumu'na bildirmekle yükümlüdür. Bu yükümlülüğün tanımlanması suretiyle, VERBİS'in veri sorumlusunun veri işleme faaliyetinin en son halini yansıtması amaçlanmaktadır.

Peki, VERBİS gerçekten de hesap verebilirliği sağlamaya uygun bir araç mıdır? Veri sorumluları, VERBİS'e kişisel verilerin hangi amaçla işleneceği, veri konusu kişi grubu ve grupları, kişisel verilerin aktarılabileceği alıcı veya alıcı grupları, yabancı ülkelere aktarımı öngörülen kişisel veriler, alınan teknik ve idari tedbirler ile kişisel verilerin mevzuatta öngörülen veya işlendikleri amaç için gerekli olan azami muhafaza edilme süresini kaydetmek zorundadır.

Sicil, detaylı bir envanter olarak değil, temel kategorik bir envanter olarak kurgulanmıştır. Örneğin, işleme amaçları her bir veri için spesifik değil, veri grupları için genel (çoğu zaman da birbirine benzer) niteliktedir. Bu haliyle VERBİS, hesap verebilirliğin sağlanması için bir başlangıç noktası oluştursa da tam manasıyla fonksiyonel bir hesap verebilirlik aracı değildir. Asıl hesap verebilirliği sağlayan araç, doğru, güncel ve kapsamlı tutulduğu durumlarda ana kişisel veri işleme envanteridir.

[106] KVK Kurumu, '*Sorularla Verbis*' https://verbis.kvkk.gov.tr/UploadedFiles/SORULARLA_VERB%C4%B0S.pdf [Erişim Tarihi: 01.09.2020], 15.

Hesap verebilirlik anlayışı gerçek manada uygulandığı durumda zaten VERBİS gibi bir sicilin varlığına da ihtiyaç kalmayacaktır.

C. Politikalar ve Hesap Verebilirlik

Önceki bölümlerde izah edildiği üzere, en önemli hesap verebilirlik bileşeni veri sorumlusunun veri işleme süreçlerini bağladığı politikalardır. KVK Kanunu ve ikincil düzenlemeleri uyarınca veri sorumlularının hazırlaması zorunlu olan iki temel politika vardır: (1) kişisel veri saklama ve imha politikası (2) özel nitelikli kişisel verilere ilişkin politika. Bunlarda ilki Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 5. maddesi uyarınca veri sorumluları siciline kayıt olmakla yükümlü olan veri sorumlularına getirilirken, ikincisi 31 Ocak 2018 Tarihli ve 2018/10 Sayılı KVK Kurulu kararı ile özel nitelikli kişisel veri işleyen tüm veri sorumlularına getirilmiştir. Veri sorumlularının belirli politikaları hazırlaması, uygulaması ve de şeffaf olarak yayınlaması hesap verebilirliğin sağlanması açısından önemli bir gelişmedir.

Ç. Veri Sorumlusunun Yükümlülükleri Bağlamında Hesap Verebilirlik

Hesap verebilirliğin unsurlarının araştırılabileceği bir diğer nokta ise veri sorumlusunun yükümlülükleridir. KVK Kanunu'nun 12. maddesi uyarınca veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. GVK Tüzüğü'nün 24. maddesinden farklı olarak hesap verebilirliğin en temel bileşeni olan işlemenin düzenlemeye uygun şekilde gerçekleştirildiğini gösterebilmek yükümlülüğü KVK Kanunu'nda yer almamaktadır.

Risk temelli yaklaşım zaten alınan idari ve teknik tedbirlerin değişen risk ortamına göre uyarlanmasını zorunlu kılmaktadır. Kabahatler Kanunu'nun 17. maddesinin ikinci fıkrası uyarınca idari para cezasının miktarı belirlenirken işlenen kabahatin haksızlık içeriği ile failin kusuru ve ekonomik durumunun birlikte göz önünde bulundurulması gerekmektedir. Dolayısıyla failin kusurunun tespitinde risk temelli yaklaşıma uygun hareket edip etmediği önemli bir kriter olacaktır. Eğer fail, yani veri sorumlusu hesap verebilirlik ilkesine uygun şekilde riskleri tespit etmiş, gerekli teknik ve idari tedbirleri almış, gerektiğinde güncellemiş ve tüm bu iş süreçlerine ilişkin bağlayıcı bir kurumsal politika geliştirmişse, bunu ispat etmek suretiyle sorumluluğunu bertaraf etmesi mümkün olacaktır.

Sonuç

Hesap verebilirlik ilkesi, veri koruma hukuku alanındaki farklı ulusal ve uluslararası düzenlemelerde kendisine yer bulmuş ve gün geçtikçe de önemi artan bir ilkedir. Öz, fakat hukuki sonuçları itibariyle çok boyutlu bir ilkedir. Kişisel verileri işlenen ilgili kişilerin haklarının en üst düzeyde korunmasını temin eden bir ilke olan hesap verebilirlik, veri sorumlusuna artırılmış bir özen yükümlülüğü getirmekte, veri sorumlusunu riske göre basiretli şekilde davranmaya davet etmektedir. Bu ilke, tüm diğer veri koruma ilkeleriyle doğrudan bağlantılı olup, kişisel verilerin işlenmesi sürecinde bir sorumluluk ekosistemi oluşturmaktadır.

OECD, hesap verebilirliği mahremiyet yönetim programı ile somutlaştırmıştır. Hesap verebilirlik ilkesi 108 sayılı Sözleşmede yer almazken, 108+ sayılı Sözleşmede hesap verebilirlik lafzında olmasa da özünde yer bulmuştur ve Sözleşme hesap verebilirlik yaklaşımı üzerine inşa edilmiştir. AİHM içtihatları incelendiği zaman veri güvenliği ve mahremiyeti sağlamak için temel bir hesap verebilirlik yükümlülüğünün AİHS'nin 8. maddesinin bünyesinde yer aldığı görülmektedir.

Hesap verebilirlik, ISO tarafından hazırlanan alanındaki ilk mahremiyet standardı olan ISO 29100:2011'de açıkça yer almakta; somut eylemlerle bu ilke desteklenmekte ve veri sorumluları için standart bir iş akışı sunulmaktadır. Tüm bunların yanında, hesap verebilirlik, Avrupa Birliği veri koruma hukukunun merkez üssünde yer almaktadır. Aslında ilkeyi dünyada bu kadar bilinir kılan GVK Tüzüğü olmuştur.

Hesap verebilirlik, veri sorumlusunun sadece kendi duvarları içerisinde değil hem veriyi alırken hem de veriyi aktarırken, tüm paydaşlarıyla işlerinde sürekli olarak gözetmesi gereken bir ilkedir.[107] Hesap verebilirlik, mevzuata salt uyumu aşan bir ilkedir. Hesap verebilirliğin uyumdan farklı olmasının temelinde, veri işleme ve koruma süreçlerinin dinamikliği ve sürekliliği yer almaktadır.

Uyum "kör güven" (*blind trust*), hesap verebilirlik ise "doğrulanmış güven" (*proven trust*) olarak nitelendirilmektedir.[108] Gerçek manada uyum tek seferlik bir işlem değil, kurumsal yönetişimde sürekli var olan bir iş sürecidir. Bu bağlamda hesap verebilirlik ilkesi, kişisel verilerin korunmasının bir veri sorumlusu nezdinde devamlı gözetilen, etkin şekilde uygulanan ve sürekli olarak denetlenen bir değer olduğunun ispatı sürecidir. İlkenin özü, sorumluluğun nasıl yerine getirildiğini göstermek ve bunu doğrulamaktır.

Hesap verebilirlik, kanundan, sözleşmeden, sektörel veya genel bir davranış kuralına bağlılıktan veya kurumsal sosyal sorumluluktan kaynaklanabilir ve her

[107] Damien Geradin/Dimitrios Katsifis/Theano Karanikioti, '*GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech - ILEC Discussion Paper No. 2020-012'* (2020) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3598130 [Erişim Tarihi: 01.09.2020], 12.

[108] De Hert (n 6) 199.

kurum, şirket, yapı, veri işleme süreci, veri türüne göre farklı bir görünümü ve kapsamı vardır. Aslında veri sorumlusu hangi hususlardan dolayı hesap vereceğini tespit ederse, nasıl bir tedbir alacağını veya nasıl bir uyum gerçekleştirmesi gerektiğini de belirlemiş olacaktır. Sorumluluğunun bilincinde olmayan ve bunu test etmemiş bir veri sorumlusu için uyum bir formaliteden öteye geçmeyecektir.

Hesap verebilirlik ilkesinin ilk önemli çıktısı, veri işleme süreçlerinin tüm aşamalarına ilişkin detaylı kayıt tutma yükümlülüğüdür. Bu kayıt tutma yükümlülüğü, kişisel veri envanterini aşan, nitelikli bir kayıt tutma yükümlülüğüdür. Benzetme yapılırsa kaptanın seyir defteri gibi "hesap verebilirlik seyir defteri" tutulmasıdır. Hesap verebilirlik, veri sorumlusunun uyum sürecini ispat edilebilir şekilde yürütmesini gerektirmektedir.

Hesap verebilirlik ilkesinin ikinci önemli çıktısı uyumun sürekliliğini sağlamak için gerekli kurumsal yapıları kurma yükümlülüğüdür. Daha da somutlaştırmak gerekirse, işlemenin tüm aşamalarının veri koruma ilkelerine uyumlu olduğunu temin için bu konuda bağlayıcı bir politika olmalı, bu politika eksiksiz şekilde uygulanmalı ve denetlenmelidir. Uyum var olmalı, buna yönelik farkındalık tüm çalışanlarda yer almalıdır. Diğer bir deyişle, politika, insanlar ve süreçler arasında etkin ve dinamik bir bağlantı var olmalıdır. Bu yapı statik değil, dinamik olmalı ve değişen risklere göre de uyarlanmalıdır.

Uyarlama, uygulanacak uyum sürecinin de esnekliğini gerektirmektedir. OECD tarafından da vurgulandığı üzere, esneklikten anlaşılması gereken, veri sorumlusunun faaliyette bulunduğu alan, işlediği veri boyutu veya verinin hassasiyetine göre farklı kapsam ve nitelikte bir tedbir alması gerekliliğidir. Şöyle ki, birden fazla konum ve ülkede faaliyet gösteren büyük bir veri sorumlusu ile tek bir konumda faaliyette bulunan küçük veya orta ölçekli veri sorumlusu farklı nitelikte iç denetim mekanizması kurması beklenmektedir. Aynı farklı muamele gerekliliği verinin ölçeği ve hassasiyeti için de geçerlidir. Dolayısıyla, mahremiyet yönetim programı her veri sorumlusu için özeldir ve sorumluluk da buna göre belirlenmelidir.

Hesap verebilirlik ilkesinin üçüncü önemli çıktısı ise denetimdir. Hesap verebilirliğin varlığından bahsedebilmek için herhangi bir veri ihlali gerçekleşmediği veya uyumsuzluk iddiası olmadığı bir aşamada uyum sürecinin etkinliği ve yeterliliği temin edilmiş olmalıdır.[109] Bir nevi, testi kırılmadan testinin kırılma simülasyonunu hazırlamayı ve ortaya çıkacak durumu gözetmeyi gerektirmektedir.

Bir veri sorumlusunun hesap verebilirlik ilkesini yerine getirdiğinin muhtelif karineleri vardır. Hesap verebilirliğin en temel göstergesi, uyum sürecine ilişkin veri sorumlusu bünyesinde iç kontrol ve denetim mekanizmalarının varlığıdır. Mahremiyet yönetimi için ayrılan kaynaklar ve yapılan harcamalar bile bir veri sorumlusunun kişisel verilere ilişkin hesap verebilirlik yaklaşımına karinesidir. Keza, veri korumadan

[109] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law* (European Union Agency for Fundamental Rights and Council of Europe, 2018), 137.

sorumlu kişinin varlığı ve veri sorumlusunun operasyonel büyüklüğüne göre sayısı veya bir ihlalin iç disiplin kurallarına göre yaptırımla neticelenip neticelenmemiş olması da hesap verebilirliğe ilişkin önemli göstergelerdir. Nihayetinde, hesap verebilirlik veri sorumlusu için doğrudan ve dolaylı maliyetler çıkarmaktadır.[110]

Özetle, iç prosedürler, bağlayıcı politikalar, detaylı veri envanteri, veri koruma görevlisi, eğitim ve talimatlar, yeterli kaynaklar, etkin ilgili kişi başvuru yöntemleri, dahili şikâyet yönetim mekanizması, güvenlik ihlal yönetim sistemleri, mahremiyet etki analizi, iç ve dış denetim, davranış kuralları ve sertifikasyon temel hesap verebilirlik araçlarıdır. Bunlar veri sorumlularının ispat yükümlülüğünü yerine getirmek için başvurulabilecekleri pratik araçlardır.

Hesap verebilirlik sanılanın aksine veri sorumlusunun yenilikçi teknolojileri kullanmada takdir marjını artırmaktadır. Veri sorumlusu analitik araçlardan yapay zekâ teknolojilerine kadar dilediği teknolojiyi kullanabilir yeter ki hesap verebilirlik anlayışıyla hareket etmiş olsun. Bu yaklaşımla hareket ettiğini ispat ettiği durumda veri koruma otoritesi nezdinde sorumluluğu özel olarak değerlendirilecektir.

Hesap verebilirlik ilkesi, veri koruma otoritelerin yetkisini daraltan bir ilke değil, bilakis denetimlerini daha etkin hale getiren, destekleyici bir ilkedir. İlkenin bilgi asimetrisini azaltan bir özelliği vardır ve *ex-post* denetimi kolaylaştırmakta, veri koruma otoritelerinin daha seçici ve stratejik davranmalarını, işlemleri önceliklendirmelerini ve tasarruf yapmalarını sağlamaktadır. İdarenin en az maliyetle en etkin denetimi yapmasını sağlayan bu durum, çok yerinde bir şekilde daha az denetim ve daha çok sorumluluk olarak özetlenmektedir.

Hesap verebilirlik ilkesi, Türk veri koruma hukukunda açık normatif dayanağı olan bir ilke değildir. Kanunun lafzında değil ruhunda yer almaktadır. Yine de bu ilkenin kişisel verilerin korunmasına ilişkin önemli etkileri sebebiyle yasal düzeyde tanımlanması ve şeffaflık ilkesiyle de desteklenmesi gerekmektedir. Zira, şeffaflık olmadan uygulanan tedbirlerin etkinliğinin gerçek manada doğrulanması mümkün değildir. Bu iki ilkenin müstakil ilkeler olarak kabul edilmesiyle, veri koruma hukukunda temel yaklaşım değişecek ve yeni bir sorumluluk ekosistemi oluşacaktır. Veri sorumlusuna, iç ve dış tüm iş süreçlerinde artırılmış bir özen yükümlülüğü getirileceği için kişisel verilerin daha etkin bir biçimde korunması mümkün olacaktır.

Hakem Değerlendirmesi: Dış bağımsız.
Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.
Finansal Destek: Yazar bu çalışma için finansal destek almadığını beyan etmiştir.

Peer-review: Externally peer-reviewed.
Conflict of Interest: The author has no conflict of interest to declare.
Grant Support: The author declared that this study has received no financial support.

[110] Geradin/Katsifis/Karanikioti (n 107) 12.

Bibliyografya/Bibliography

Bianculli A C, Xavier F ve Jacint J (eds), *Accountability and Regulatory Governance* (Palgrave Macmillan 2015).

Birleşmiş Milletler, '*Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*' (2011) https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

Çekin MS, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu* (On İki Levha 2018).

Černič JL, *Corporate Accountability under Socio-Economic Rights* (Routledge 2019).

De Hert P, '*Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law*' in Guagnin D and others (eds), *Managing Privacy through Accountability* (Palgrave Macmillan 2012).

De Hert P ve Vagelis P, '*The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition*' (2014) 30 Computer Law & Security Review 633.

De Terwangne C, Jean-Marc VG ve Yves P, *Rapport sur les lacunes de la Convention no 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (Partie II)* (2010) http://www.crid.be/pdf/public/6559.pdf

Docksey C, '*Article 24 – Responsibility of the controller*' in Kuner C, Bygrave LA and Docksey C (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

European Union Agency for Fundamental Rights ve Council of Europe, *Handbook on European data protection law* (European Union Agency for Fundamental Rights and Council of Europe, 2018).

Fuster GG, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).

Geradin D, Dimitrios K ve Theano K, *GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech - ILEC Discussion Paper No. 2020-012*, 2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3598130>

Greenleaf G, '*Accountability Without Liability: 'To Whom' and 'With What Consequences'? (Questions for the 2019 OECD Privacy Guidelines Review) UNSW Law Research Paper No. 19-67'* (2019) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3384427

Gunasekara G, '*Paddling in unison or just paddling? International trends in reforming information privacy law*' (2013) 22 International Journal of Law and Information Technology 141.

Gutwirth S, Ronald L ve De Hert P (eds), *Data Protection on the Move - Current Developments in ICT and Privacy/Data Protection* (Springer 2016).

Keser Berber L, '*Çapraz Etkileşim: Mahremiyete İlişkin Mevzuat ve Mahremiyet Standartları Arasındaki İlişki*' in Keser Berber, Leyla and Bilgili, Ali Cem (eds), *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku* (On İki Levha Yayıncılık 2020).

Lambert P, *The Data Protection Officer - Profession, Rules, and Role* (CRC Press - Taylor & Francis 2017).

Lambert P, *Understanding the New European Data Protection Rules* (CRC Press - Taylor & Francis 2018).

Leenes R, Van Brakel R, Gutwirth S ve De Hert P (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer 2017).

Madde 29 Çalışma Grubu, 'Guidelines on Data Protection Officers ('DPOs')' (13 Aralık 2016) http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

Madde 29 Çalışma Grubu, '*Opinion 3/2010 on the principle of accountability*' (13 Temmiz 2010) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf

Madde 29 Çalışma Grubu, '*The Future of Privacy*' (1 Aralık 2009) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf

OECD, '*The OECD Privacy Framework*' (2013) https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Privacy International, '*A Guide for Policy Engagement on Data Protection - The Keys to Data Protection*' (2018) https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf

Rodrigues R ve Papakonstantinou V (eds), *Privacy and Data Protection Seals* (T.M.C. Asser Press 2018).

United Nations,'*Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*' (2011) https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

Voigt P ve Von dem Bussche A, *The EU General Data Protection Regulation (GDPR) A Practical Guide* (Springer 2017).

Wright D ve De Hert P (eds), *Privacy Impact Assessment* (Springer 2012).

Yılmaz SS, *Tıp Alanında Kişisel Verilerin Açıklanması Suçu* (Seçkin 2014).